مجلة جامعة البعث

سلسلة العلوم الأساسية

مجلة علمية محكمة دورية

المجلد 42 . العدد 12

1442 هـ - 2021 م

الأستاذ الدكتور عبد الباسط الخطيب

رئيس جامعة البعث

المدير المسؤول عن المجلة

أ. د. ناصر سعد الدين	**رئيس هيئة التحرير**
أ. د. درغام سلوم	**رئيس التحرير**

مديرة مكتب مجلة جامعة البعث

بشرى مصطفى

د. محمد هلال	**عضو هيئة التحرير**
د. فهد شريباتي	**عضو هيئة التحرير**
د. معن سلامة	**عضو هيئة التحرير**
د. جمال العلي	**عضو هيئة التحرير**
د. عباد كاسوحة	**عضو هيئة التحرير**
د. محمود عامر	**عضو هيئة التحرير**
د. أحمد الحسن	**عضو هيئة التحرير**
د. سونيا عطية	**عضو هيئة التحرير**
د. ريم ديب	**عضو هيئة التحرير**
د. حسن مشرقي	**عضو هيئة التحرير**
د. هيثم حسن	**عضو هيئة التحرير**
د. نزار عبشي	**عضو هيئة التحرير**

تهدف المجلة إلى نشر البحوث العلمية الأصيلة، ويمكن للراغبين في طلبها الاتصال بالعنوان التالي:

رئيس تحرير مجلة جامعة البعث

سورية . حمص . جامعة البعث . الإدارة المركزية . ص . ب (77)

. هاتف / فاكس : 2138071 31 963 ++

. موقع الإنترنت : www.albaath-univ.edu.sy

. البريد الالكتروني : magazine@ albaath-univ.edu.sy

ISSN: 1022-467X

شروط النشر في مجلة جامعة البعث

الأوراق المطلوبة:

- 2 نسخة ورقية من البحث بدون اسم الباحث / الكلية / الجامعة) + CD / word من البحث منسق حسب شروط المجلة.
- طابع بحث علمي + طابع نقابة معلمين.
- **اذا كان الباحث طالب دراسات عليا:**

يجب إرفاق قرار تسجيل الدكتوراه / ماجستير + كتاب من الدكتور المشرف بموافقته على النشر في المجلة.

- **اذا كان الباحث عضو هيئة تدريسية:**

يجب إرفاق قرار المجلس المختص بإنجاز البحث أو قرار قسم بالموافقة على اعتماده حسب الحال.

- **اذا كان الباحث عضو هيئة تدريسية من خارج جامعة البعث :**

يجب إحضار كتاب من عمادة كليته تثبت أنه عضو بالهيئة التدريسية و على رأس عمله حتى تاريخه.

- **اذا كان الباحث عضواً في الهيئة الفنية :**

يجب إرفاق كتاب يحدد فيه مكان و زمان إجراء البحث ، وما يثبت صفته وأنه على رأس عمله.

- **يتم ترتيب البحث على النحو الآتي بالنسبة لكليات (العلوم الطبية والهندسية والأساسية والتطبيقية):**

عنوان البحث . . ملخص عربي و إنكليزي (كلمات مفتاحية في نهاية الملخصين).

1- مقدمة

2- هدف البحث

3- مواد وطرق البحث

4- النتائج ومناقشتها .

5- الاستنتاجات والتوصيات .

6- المراجع.

- **يتم ترتيب البحث على النحو الآتي بالنسبة لكليات (الآداب – الاقتصاد– التربية – الحقوق – السياحة – التربية الموسيقية وجميع العلوم الإنسانية):**
- عنوان البحث . . ملخص عربي و إنكليزي (كلمات مفتاحية في نهاية الملخصين).

1. مقدمة.
2. مشكلة البحث وأهميته والجديد فيه.
3. أهداف البحث و أسئلته.
4. فرضيات البحث و حدوده.
5. مصطلحات البحث و تعريفاته الإجرائية.
6. الإطار النظري و الدراسات السابقة.
7. منهج البحث و إجراءاته.
8. عرض البحث و المناقشة والتحليل
9. نتائج البحث.
10. مقترحات البحث إن وجدت.
11. قائمة المصادر والمراجع.

7- يجب اعتماد الإعدادات الآتية أثناء طباعة البحث على الكمبيوتر:

أ- قياس الورق 17.5×25 B5.

ب- هوامش الصفحة: أعلى 2.54- أسفل 2.54 – يمين 2.5- يسار 2.5 سم

ت- رأس الصفحة 1.6 / تذييل الصفحة 1.8

ث- نوع الخط وقياسه: العنوان . Monotype Koufi قياس 20

. كتابة النص Simplified Arabic قياس 13 عادي . العناوين الفرعية Simplified Arabic قياس 13 عريض.

ج . يجب مراعاة أن يكون قياس الصور والجداول المدرجة في البحث لا يتعدى 12سم.

8- في حال عدم إجراء البحث وفقاً لما ورد أعلاه من إشارات فإن البحث سيهمل ولا يرد البحث إلى صاحبه.

9- تقديم أي بحث للنشر في المجلة يدل ضمناً على عدم نشره في أي مكان آخر، وفي حال قبول البحث للنشر في مجلة جامعة البعث يجب عدم نشره في أي مجلة أخرى.

10- الناشر غير مسؤول عن محتوى ما ينشر من مادة الموضوعات التي تنشر في المجلة

11- تكتب المراجع ضمن النص على الشكل التالي: [1] ثم رقم الصفحة ويفضل استخدام التهميش الإلكتروني المعمول به في نظام وورد WORD حيث يشير الرقم إلى رقم المرجع الوارد في قائمة المراجع.

تكتب جميع المراجع باللغة الانكليزية (الأحرف الرومانية) وفق التالي:

آ . إذا كان المرجع أجنبياً:

الكنية بالأحرف الكبيرة . الحرف الأول من الاسم تتبعه فاصلة . سنة النشر . وتتبعها معترضة (–) عنوان الكتاب ويوضع تحته خط وتتبعه نقطة . دار النشر وتتبعها فاصلة . الطبعة (ثانية . ثالثة) . بلد النشر وتتبعها فاصلة . عدد صفحات الكتاب وتتبعها نقطة.

وفيما يلي مثال على ذلك:

–MAVRODEANUS, R1986– **Flame Spectroscopy**. Willy, New York, 373p.

ب . إذا كان المرجع بحثاً منشوراً في مجلة باللغة الأجنبية:

. بعد الكنية والاسم وسنة النشر يضاف عنوان البحث وتتبعه فاصلة، اسم المجلد ويوضع تحته خط وتتبعه فاصلة . المجلد والعدد (كتابة مختزلة) وبعدها فاصلة . أرقام الصفحات الخاصة بالبحث ضمن المجلة.

مثال على ذلك:

BUSSE,E 1980 Organic Brain Diseases **Clinical Psychiatry News** , Vol. 4. 20 – 60

ج. إذا كان المرجع أو البحث منشوراً باللغة العربية فيجب تحويله إلى اللغة الإنكليزية و التقيد

بالبنود (أ و ب) ويكتب في نهاية المراجع العربية: (المراجع In Arabic)

رسوم النشر في مجلة جامعة البعث:

1. دفع رسم نشر (20000) ل.س عشرون ألف ليرة سورية عن كل بحث لكل باحث يريد نشره في مجلة جامعة البعث.
2. دفع رسم نشر (50000) ل.س خمسون الف ليرة سورية عن كل بحث للباحثين من الجامعة الخاصة والافتراضية .
3. دفع رسم نشر (200) مئتا دولار أمريكي فقط للباحثين من خارج القطر العربي السوري .
4. دفع مبلغ (3000) ل.س ثلاثة آلاف ليرة سورية رسم موافقة على النشر من كافة الباحثين.

المحتوى

استراتيجية الغذاء عند النوع *Evadne spinifera* صف Branchiopoda رتبة cladocera على الأعماق المختلفة في المياه الشاطئية لمدينة بانياس

د. كمال الحنون*

وسيم ميا**

ملخص:

تقدم الدراسة فكرة واضحة عن استراتيجية التغذية للنوع *Evadne spinifera*، رتبة متفرعات القرون Cladocera وذلك من خلال دراسة بنية الفقيم ومحتوى المعي عنده لتحديد الغذاء المستخدم من قبله في الطبقات المائية المختلفة في مناطق الدراسة تحت تأثير العوامل البيئية. تمت الدراسة على 87عينة جمعت بشكل عمودي مستمر ومتدرج مترافقة مع أخذ القياسات الهيدروفيزيائية و الهيدروكيميائية في ثلاث مناطق تختلف عن بعضها البعض بخصائصها البيئية وذلك في الفترة الممتدة ما بين أذار وكانون الأول للعام 2020. بلغ عدد أفراد النوع المذكور أعلاه والتي جرت دراستها 63 فرداً منها 43 من الإناث و20 فرداً من الذكور، وقد تبين أن عدد أنواع و أجناس العوالق النباتية التي تغذى عليها النوع المذكور أعلاه 8 ثمانية أنواع و6 أجناس منها (4) أربعة أنواع و(3) ثلاثة أجناس من المشطورات Bacillariophyceae و(4)أنواع و(2) جنسين من السوطيات Dinophyceae و(1) جنس واحد من Cryptophyceae، كما تغذى النوع *E.spinifera* على (1) نوع واحد و(1) جنس واحد من الهدبيات Ciliata.

الكلمات المفتاحية:

استراتيجية التغذية، الفقيم، العوامل البيئية، القياسات الهيدروفيزيائية والهيدروكيميائية.

---

* أستاذ- قسم علم الحياة الحيوانية – كلية العلوم- جامعة تشرين- اللاذقية – سورية.

** طالب دراسات عليا (دكتوراه)- قسم علم الحياة الحيوانية- كلية العلوم – جامعة تشرين- اللاذقية- سورية.

Feeding Strategy of *Evadne Spinifera*(Branchiopoda-cladocera) at different depths in the coastal waters of Baniyas City

*Dr. Kamal Al-Hanoun
** Wassim Mayya

ABSTRACT:

This paper Introduces a clear idea about Feeding Strategy of *Evadne Spinifera* (Cladocera) by studying the structure of the Mandible and the gut content of this previous species to determine the food used by it in the different water layers in the study areas under the influence of environmental factors. 87 samples have been collected vertically with taking hydrophysical and hydrochemical measurements in three areas that differ from each other by their environmental characteristics, in the period between March and December of the year 2020. The number of members of (*E.spinifera*) that were studied reached (63) individuals, of which (43) are female and (20) are male. The number of species and genera of phytoplankton on which the aforementioned species feed is 8 species and 6 genera, (4) species and (3) three genera of Bacillariophyceae, (4) species and (2) two genera of Dinophyceae and (1) One genus of Cryptophyceae, and E. spinifera feeding on (1) species and (1) genus of Ciliata.

Keywords: Feeding Strategy**,** Mandible, Environmental Factors**,** Hydrophysical and Hydrochemical measurements.

* Professor, Department of Zoology, Faculty of Sciences, Tishreen University, Lattakia, Syria.

** Postgraduate Student, Department of Zoology, Faculty of Sciences, Tishreen University, Lattakia, Syria.

1- مقدمة:

تشكل العوالق الحيوانية القشرية Crustacean Zooplankton الغذاء الأساسي للعديد من المستهلكات ذات الأهمية الإقتصادية في النظام البيئي البحري وتضم العوالق الحيوانية بصورة عامة ممثلين عن كل صفوف المملكة الحيوانية تقريباً[3].

تعتبر متفرعات القرون البحرية Marine cladocera أحد المجموعات الهامة التي تساهم مع جماعات العوالق الحيوانية القشرية الأخرى في النظم البيئية البحرية وخاصة في الشهور الأكثر دفئاً، حيث تظهر متفرعات القرون بغزارة بالرغم من أن المعلومات المتوفرة عن أنواعها البحرية قليلة مقارنة مع أنواعها المنتشرة في المياه العذبة والتي جرت عليها الكثير من الدراسات المكثفة.

أنجز الباحثان Nival and Ravera في العام 1979 دراسة مورفولوجية تركزت على اللواحق الفموية لمتفرعات القرون البحرية عند النوع *Evadne spinifera* ، وذلك لتوضيح المتطلبات الغذائية للنوع السابق، حيث ركزت الدراسة على بنية الفقيم والأرجل الصدرية المجهزة بأشعار قوية وأشواك قصيرة وهذا ما ساهم بدور كبير في استراتيجية التغذية الاصطفائية عند النوع المذكور[17].

قام الباحث Kim وأخرون في العام 1989 بدراسة العادات الغذائية عند متفرعات القرون البحرية في بحر اليابان مبيناً الدور الذي تلعبه في شبكات الغذاء البحرية وخاصةً في الفصول الدافئة[10].

تابع الباحث Turner وأخرون في العام 1998 دراسة البيئة الغذائية للعوالق الحيوانية من خلال تغذي مجذافيات الأرجل ومتفرعات القرون البحرية على العوالق النباتيةPhytoplankton والطحالب الخضراء المزرقة في ميناء كينغيستون في جامايكا،

وقد بينت الدراسة بأن التكيف الرئيس في استراتيجية التغذية عند متفرعات القرون البحرية يتجلى بأن فقدان الطاقة على عملية التصفية(الترشيح) يعوّض من خلال زيادة شدة التغذية[18].

أوضح الباحثان Marrazzo and Valentin في العام 2001 التوزع الزماني والمكاني والطيف الغذائي للنوعين *Evadne tergestina،Penilia avirostris* في الخليج الاستوائي في البرازيل، حيث بينت دراستهما قدرة متفرعات القرون البحرية على تحقيق التوازن الهام بين معدل ابتلاع الفريسة وزمن بقائها في أمعائها وبين معدلات النمو لديها مما ساهم في إعطاء متفرعات القرون كفاءة نمو عالية[13] .

درس الباحث Broglio وأخرون في العام 2004 تأثير الاصطفاء الغذائي للفرائس الذي تقوم به العوالق الحيوانية القشرية على الجراثيم في المناطق الساحلية القليلة التغذية في غرب المتوسط[4] .

أجرى الباحث Liu وآخرون في الأعوام (2010–2014) دراسات حول التغذية الاصطفائية للعوالق الحيوانية في المياه الساحلية شبه الاستوائية وتوضيح عملية الترشيح التي تقوم بها متفرعات القرون البحرية من خلال تصفية وعزل العوالق النباتية من المياه البحرية باستخدام الحركات المعقدة للأرجل الصدرية، حيث جرت تلك الدراسات تحديداً خلال فترة ازهرار العوالق النباتية أو ما تسمى ظاهرة Bloom (النمو الطحلبي الكثيف)[11–12].

أشار الباحثان Al–Hanoun and Zaeni في الأعوام (2017–2020) إلى أن القشريات متفرعات القرون تنتمي إلى الكائنات المسالمة التي تملك جهازاً ترشيحياً خاصاً، بحيث تتغذى على الدقائق الصغيرة مثل الطحالب المجهرية والتي تحصل عليها عن طريق تصفية المياه، كما أشار الباحثان إلى أن من أهم التكيفات في استراتيجية

التغذية عند متفرعات القرون تتجلى في تعويضها الطاقة المصروفة على عملية الترشيح من خلال زيادة شدة التغذية لديها[2-3].

تابع الباحث Jung وآخرون في العام 2019 دراسة الخصائص الغذائية لمتفرعات القرون وفقاً لتوزع العوالق الحيوانية في المياه الساحلية لكوريا الجنوبية، وقد وجدوا أن من أهم استراتيجيات التغذية عند متفرعات القرون البحرية لتعويض الطاقة المصروفة على عملية الترشيح لجسيمات الغذاء في الطبقات المائية الفقيرة بالغذاء يكون من خلال النقص الواضح في أبعاد الجسم [15].

اهتم الباحث Han وآخرون في العام 2020 بدراسة التغذية الاصطفائية للعوالق الحيوانية على العوالق النباتية، ولقد أوضحوا أنه على الرغم من أن متفرعات القرون البحرية لم تحدث نجاحاً بيئياً واضحاً في البيئية البحرية إذ لا يوجد سوى 8 أنواع بحرية حقيقية منها، إلاّ أنها تشكل ركن هام في جماعات العوالق الحيوانية البحرية في العديد من البيئات الساحلية وخاصة في الفصول الدافئة لتلعب دوراً مهماً في شبكات الغذاء البحرية[14].

مما تقدم من الدراسات السابقة يظهر لنا بوضوح تام وجلي أهمية متفرعات القرون في النظم البيئية البحرية، وأن لمعظم أفرادها التغذية النباتية حيث تعمل كمرشحات تقوم بتصفية وعزل العوالق النباتية الأصغر حجماً منها وخاصة السوطيات والدياتومات، ولابدّ من الإشارة إلى أن بعض أنواعها يتغذى على الهدبياتCiliata ولكن بأعداد قليلة جداً وذلك لقدرة الهدبيات على الهروب من التيارات التي تحدثها حركة الأرجل الصدرية عند متفرعات القرون.

2- هدف البحث:

- يهدف البحث إلى :

دراسة الطيف الغذائي للنوع *Evadne spinifera* في الطبقات المائية المختلفة وتحديد محتوى المعي من الغذاء ودراسة شكل وتركيب الفقيم عنده وذلك تحت تأثير بعض العوامل البيئية، مما يشكل قاعدة أساسية تسهل عملية التنبؤ بحالة مثل هذه الأنواع من حيث الانتاجية كونها ذات أهمية اقتصادية وتشكل الغذاء الرئيس للأسماك والقشريات العليا والعديد من الكائنات البحرية الأخرى.

3-طرائق العمل:

- تتضمن طريقة البحث مرحلتين أساسيتين:

المرحلة الأولى تتضمن تحديد مناطق الاعتيان بدقة مع احداثياتها الجغرافية والقيام بعملية جمع عينات النوع المذكور أعلاه من المحطات المحددة مع أخذ القياسات الهيدروفيزيائية والهيدروكيائية، أما المرحلة الثانية فيتم فيها نقل العينات إلى مخابر البحث العلمي ودراسة بنية الفقيم ومحتوى المعي من الغذاء على الأعماق المختلفة، واستخلاص النتائج المطلوبة.

3-1 المرحلة الأولى:

أولاً: تحديد مناطق الدراسة:

جمعت عينات النوع *E. spinifera* من مناطق الدراسة الثلاث التي تم اختيارها في المياه الشاطئية لمدينة بانياس والتي تختلف عن بعضها البعض من الناحية البيئية كما يظهر في الشكل(1) وهي:

- منطقة الصرف الصحي: رمزها(A) :

35°12′09″N 35°57′08″E

تقع مقابل مستشفى بانياس الوطني، حيث تصب مجارير الصرف الصحي التابعة للمستشفى ولأحياء المروج في خط إسالة موحد (خط صرف صحي رئيس)، حيث ينتهي مصبه في المياه الشاطئية للمدينة، ويبعد هذا الشاطئ عن المنطقة الثانية (منطقة المحطة الحرارية) مسافة 7 كم.

2- منطقة المحطة الحرارية:(مصب مياه تبريد المحطة):رمزها(B).

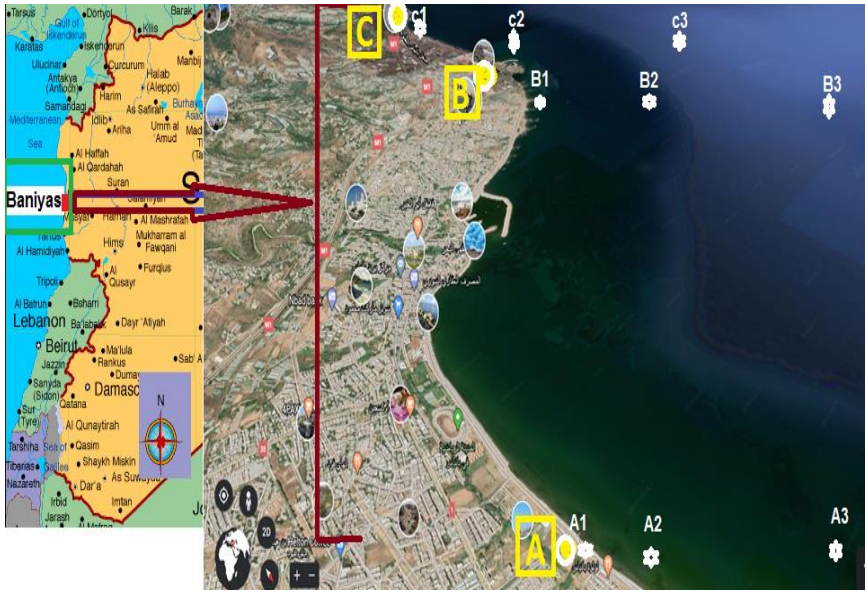
35°10′13″N 35°55′21″E

تقع هذه المنطقة مقابل المحطة الحرارية لتوليد الطاقة الكهربائية في بانياس وهي إحدى محطّات الطاقة الخمس المسؤولة عن تزويد البلاد بالطاقة الكهربائية، وتبعد المحطة الحرارية مسافة 5 كم عن المنطقة الثالثة النظيفة نسبياً، وتصب المياه الحرارية الناتجة عن تبريد المحطة وبخار المراجل الذي يتحد معها في المياه البحرية.

3- منطقة شاليهات شاطئ الأمير:رمزها(C).

35°09′02″N 35°55′20″E

شاطئ شاليهات الأمير، الذي أقيم عليه منتجع وشاليهات الأمير ويبعد هذا الشاطئ الجميل 1 كم عن موقع برج الصبي الأثري، وهذا الشاطئ منطقة نظيفة نسبياً وغير معرضة للتلوث، ولذلك فهو مقصد للسياحة والاصطياف.



الشكل (1): مناطق الدراسة في المياه الشاطئية لمدينة بانياس.

ثانياً: جمع عينات العوالق الحيوانية القشرية:

- بداية تم استخدام مركب بحري مجهز بكافة الامكانيات المطلوبة للعمل من جهاز GPS وجهاز مخصص لسبر الأعماق وتحديد نوعية القاع مع وجود بكرة معدة لرفع الشبكة الكمية من البحر.
- قسمت كل منطقة إلى ثلاثة مواقع(محطات) :
- المنطقة A: المحطات:A3-A2-A1.
- المنطقة B: المحطات:B3-B2-B1.
- المنطقة C: المحطات:C3-C2-C1.
- تمت عملية جمع عينات العوالق في كل موقع على الشكل التالي :

1. الموقع الأول: (50–0)م،(50–25)م،(25–0)م.
2. الموقع الثاني: (100–0)م،(100–50)م،(50–25)م،(25–0)م.
3. الموقع الثالث:(200–0)م،(200–100)م،(100–50)م،
(50–25)م،(25–0)م.

- تم إجراء قياسات العوامل البيئية الرئيسة مثل:(درجة الحرارة(t)،الملوحة (s)، تركيز الأوكسجين المنحل، درجة الحموضة pH، والشفافية) واستخدمت لعملية الجمع شبكة جمع العوالق الحيوانية العالمية ذات جهاز الإغلاق، وذات ثقوب 200 µ ومن النمط WP2 Closing Net.
- استخدمت العدسة الغاطسة ذات التكبير x100 في دراسة النوع من حيث التعرف على محتوى المعي ودراسة تركيب الفقيم، كما استخدمت كاميرا ديجتال حديثة HD نوع Olympus ذات تكبير 14 ميغابيكسل في عملية االتصوير.
- تم الاعتماد على المراجع التالية:

(William and Munger,2010), (Mona et al.,2009) في تحديد العوالق النباتية التي وجدت في المعي جدول(1).

4- النتائج والمناقشة:

4-1 الوضع التصنيفي والوصف العام:

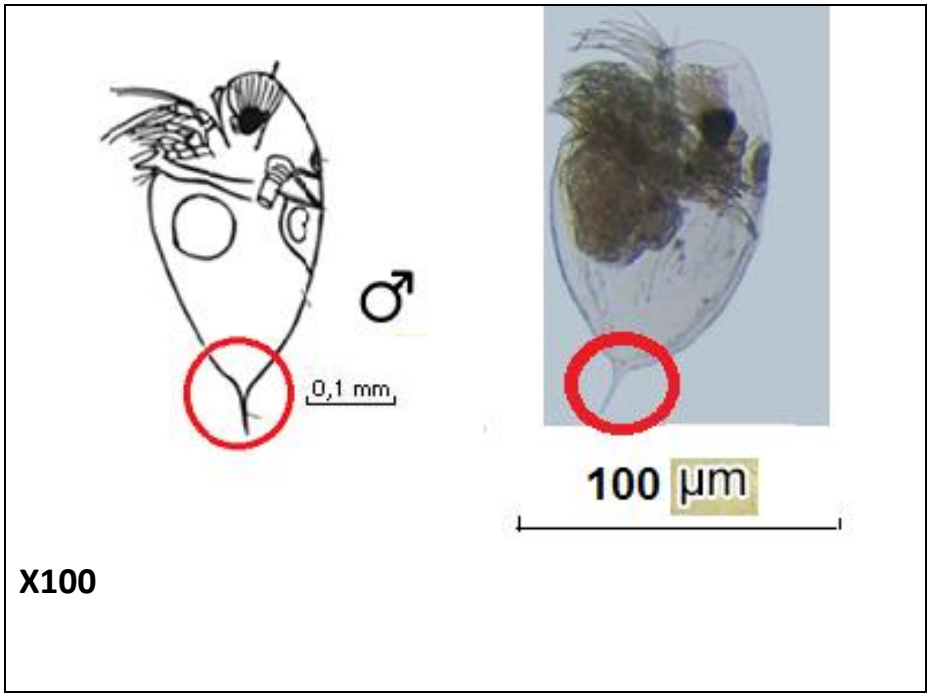
4-1-1.الوضع التصنيفي والوصف العام للنوع *Evadne spinifera* :

4-1-1-2.الوضع التصنيفي:

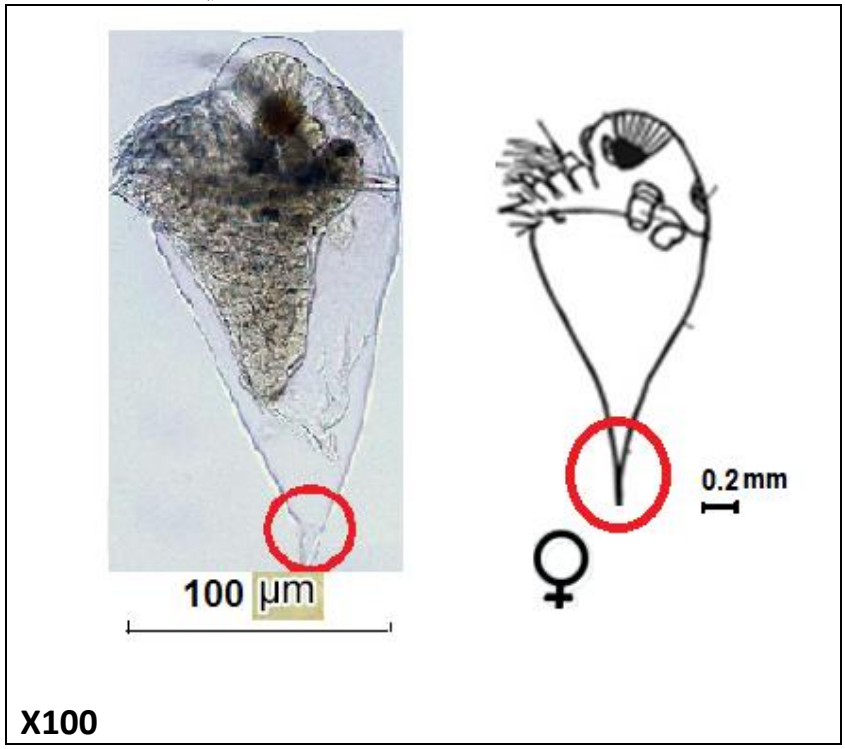
شعبة: مفصليات الأرجل	Phylum: Arthropoda
تحت شعبة: القشريات	Subphylum: Crustacea
صف: غلصميات الأرجل	Class :Branchiopoda
رتبة: متفرعات القرون	Order :Cladocera
الفصيلة	Family: Podonidae
الجنس	Genus :Evadne
النوع	Species: *Evadne spinifera* (Müller, 1867)

4-1-3.الوصف العام:

يتراوح الطول المرجعي للذكر ما بين(0.6-1.2mm) الشكل(2)، في حين يبلغ طول الأنثى(0.7-1.4mm) الشكل(3)، حيث يتحول الرأس عند هذا النوع إلى قوقعة دون انخفاض قفوي، كما تمتد القوقعة على القمة على شكل نصل وأحياناً يكون ذو طول كبير، كذلك تتميز عضلات قرون الاستشعار الثاني بأنها متباعدة، كما نلاحظ وجود شعرتين على الرجيلة الخارجية للشفع الثالث من الأرجل [2-3].



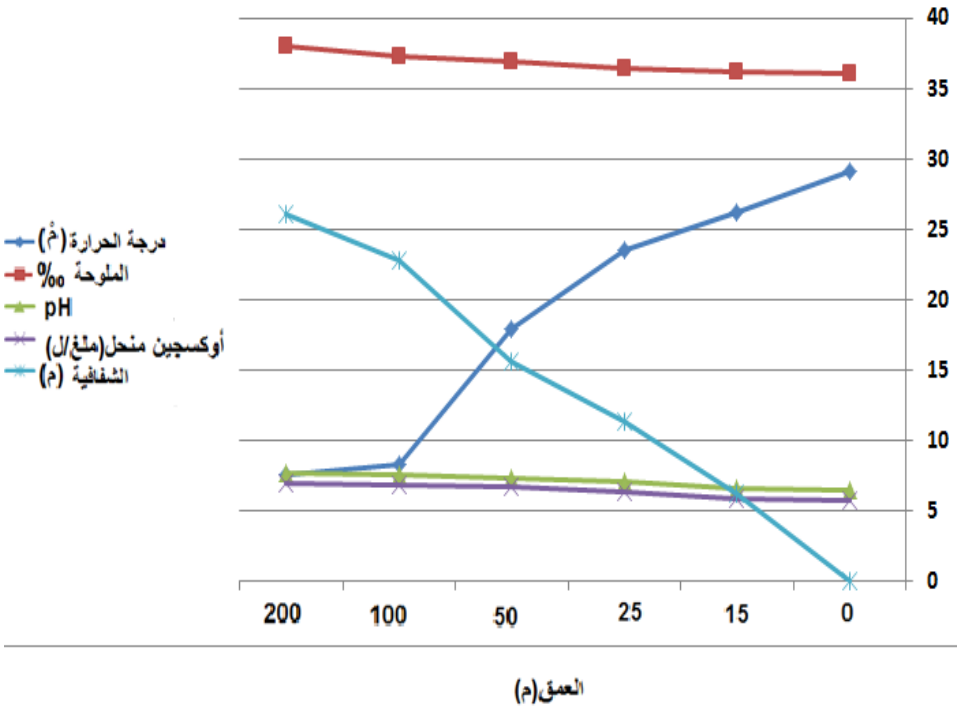
الشكل (2): الشكل العام للذكر مع الشوكة الطويلة في نهاية القوقعة .



الشكل (3): الشكل العام للأنثى مع الشوكة الطويلة في نهاية القوقعة .

4-2. الطيف الغذائي للنوع *Evadne spinifera* تحت تأثير بعض العوامل البيئية المختلفة:

ظهر النوع *Evadne spinifera* في جميع مناطق الدراسة ومحطاتها وعلى الأعماق المختلفة وهذا يدل على أنه ذو تكيف بيئي واسع Eurybiont مع قيم العوامل البيئية [10]الشكل(4)، حيث تراوحت القيم المتوسطة لدرجة الحرارة مابين(7.63-29.16)مْ، في حين كانت القيم المتوسطة للملوحة مابين(36.01-38.03)‰، أما الشفافية فقد تراوحت القيم المتوسطة لها مابين(6.21-26.12)م، حيث نلحظ أن القيمة المتوسطة الأدنى لها سجلت في المحطات الشاطئية ويعود السبب في ذلك إلى غزارة العوالق النباتية [13-14]، وبالتالي كان الوجود الأكبر للنوع المذكور أعلاه في الطبقات ذات العمق(50-0)م و(25-0)م، ولذلك نجد أنه يفضل العيش غالباً في المناطق الشاطئية، بالرغم من وجوده أيضاً في عرض البحر وفي الأعماق، وقد توافقت هذه النتيجة السابقة مع دراسة الباحثين[4-6-9]، وقد لعبت العوامل البيئية وخاصةً درجة الحرارة ،الملوحة والشفافية دوراً مهماً في تنوع الطيف الغذائي عند النوع *E. spinifera* ، فدرجة الحرارة المرتفعة والملوحة المنخفضة وقيم الشفافية المنخفضة أيضاً ساهمت مجتمعة كلها في غزارة العوالق النباتية في المحطات الشاطئية وفي الأعماق المختلفة (50-0)م و(50-25)م ولذلك فإن النوع السابق وجد بغزارة وتكيف للعيش في الأعماق السابقة وتغذّى على (9)أنواع و(7) أجناس منها(1) نوع واحد و(1) جنس واحد من الهدبيات، وقد جاءت هذه النتيجة متوافقة مع أبحاث[1-11-12]، وبالتالي فإن التغيرات الواضحة في قيم العوامل البيئية الشكل(4)، وبالأخص درجة الحرارة والملوحة إضافة إلى حركة الأمواج والتيارات البحرية والتي تشهدها الطبقات (50-0)م و(25-0)م، كان لها الدور الكبير في غنى الطبقات السابقة بالمغذيات مما ساهم في ازدهار العوالق النباتية والذي انعكس بشكل ايجابي على استراتيجية التغذية عند النوع *E. spinifera* وهذا ما نجده متوافقاً تماما مع دراسات[8-17-18].



الشكل(4): تغيرات متوسطات قيم العوامل البيئية خلال فترة ظهور النوع *Evadne spinifera* .

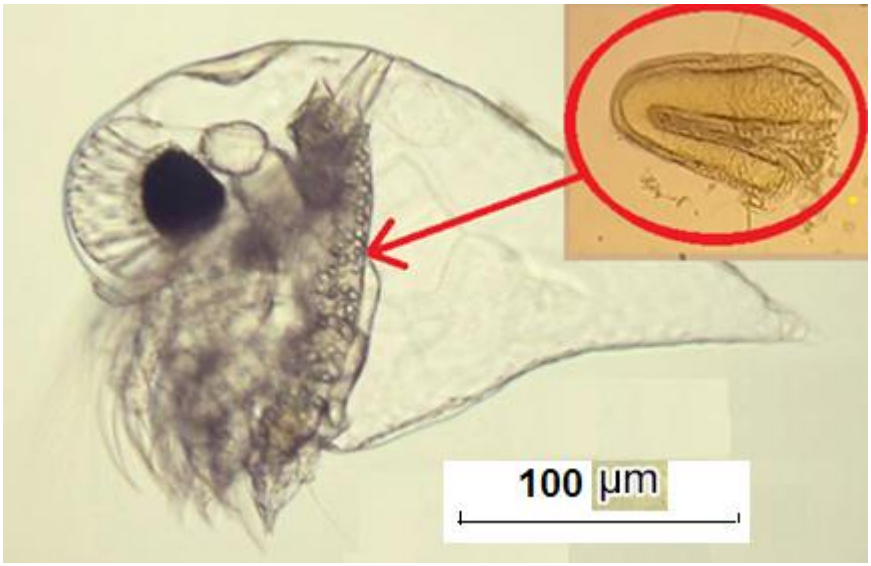
من خلال دراسة بنية المعي الشكل(5)، تبين أن أهم أنواع العوالق النباتية التي اعتمد عليها النوع *E. spinifera* في تغذيه هي أنواع السوطيات **Dinophyceae** الجدول(1)، إذ بلغ مجموع متوسط عدد أفرادها في المعي (1388) فرداً، تلتها المشطورات**Bacillariophyceae** حيث بلغ مجموع متوسط عدد أفرادها(1264) فرداً، في حين بلغ مجموع متوسط عدد أفراد**Cryptophyceae** (117)فرداً، وقد توافقت هذه النتيجة مع[5-7]، أما بالنسبة للهدبيات **Ciliata** فقد بلغ مجموع متوسط عدد أفرادها في المعي(173) فرداً، وبالتالي فإن النوع السابق هو من الكائنات القارتة **Omnivorous** لحد ما.

الجدول(1): متوسط عدد الأفراد في المعي للأنواع التي شكلت غذاء النوع *E.spinifera* خلال فترة الدراسة.

الصف	النوع	متوسط عدد الأفراد في المعي
Bacillariophyceae	*Coscinodiscus sp*	109
	Chaetoceros socialis	240
	leptocylindrus minimus	114
	Rhizosolenia Sp.	312
	Licmophora sp	89
	Nitzschia longissima	203
	Thalassionema nitzschioides	197
Dinophyceae	*Dinophysis acuminata*	312
	Dinophysis acuta	298
	Alexandrium sp.	325
	Ceratium furca	287
	Protoperidinium sp.	93
	prorocentrum micans	73
Cryptophyceae	*Rhodomonas sp.*	117
Ciliata	*Pseudokeronopsis flava*	67
	Strombidium sp.	106

إن الوجبة الغذائية الرئيسة للنوع *E.spinifera* هي من العوالق النباتية بسبب غزارة العوالق النباتية في الطبقات القليلة العمق وفي المحطات الشاطئية وهي البيئة المفضلة لوجود النوع المذكور أعلاه[2-3]، حيث ساهمت التيارات البحرية وحركة الأمواج والعوامل البيئية الملائمة من درجة الحرارة المرتفعة والملوحة المنخفضة في ازدهار أنواع السوطيات والمشطورات مما ساهم في زيادة شدة التغذية والتي لعبت الدور الأساس في

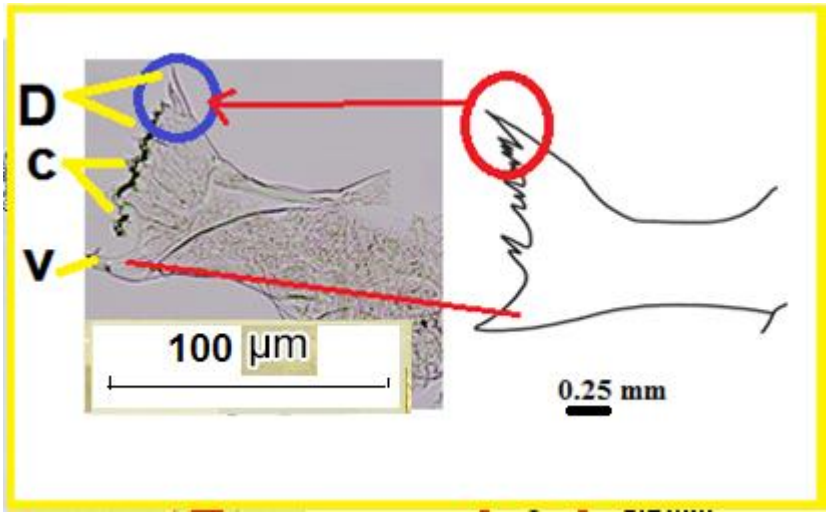
تأمين الطاقة اللازمة لعملية التصفية(الترشيح) Filtration والتي تعد التكيف الرئيس الأهم في استراتيجية التغذية عند النوع المدروس، وهذه النتيجة كانت متوافقة تماماً مع دراسات[16-19].



الشكل(5):الشكل العام للمعي عند النوع *Evadne spinifera* .

لوحظ من خلال دراسة بنية الفقيم الشكل(6) عند النوع *E. spinifera* بأنه يملك جهازاً ترشيحياً أي يتغذى النوع المذكور بطريقة الترشيح Filter feeding ،حيث يقوم بتصفية وعزل العوالق النباتية من المياه البحرية بمساعدة الحركات المعقدة للأرجل الصدرية، بحيث ينجم عن هذه الحركات تيار مستمر من الماء يقوم بدفع جسيمات الغذاء باتجاه الفم ليتم طحنها بين أسنان الفقيم، وقد كانت هذه النتائج متوافقة بشكل كبير مع نتائج دراسات[9–15]. من ناحية أخرى تعمل أشعار التصفية Filter bristlesالموجودة على الشفع الثالث والرابع للأرجل الصدرية كمجاذيف لخلق التيارات المائية، كما يستفاد من هذه الشعيرات في ابعاد جسيمات الغذاء الغير مرغوب بها أو الغير ملائمة من حيث الحجم وفقاً لآلية انتقائية معقدة[14] ، كما تبين من خلال دراسة بنية الفقيم بأنه يتكون من قاعدة قوية تتوضع عليها أسنان منحنية وظيفية تكيفت لطحن جسيمات الغذاء ولعل الأمر الأكثر أهمية بأن هذه الأسنان تحتوي في تركيبتها على السيليكا وهذا ما يفسر قدرتها على تحطيم هياكل المشطورات بسهولة[12]، كذلك فإن

القواعد القوية والثابتة لأسنان الفقيم لعبت دوراً هاماً في تثبيت عناصر الغذاء أثناء عملية الطحن، حيث تساهم الأسنان المركزية في تثبيت عناصر الغذاء وتؤدي الأسنان الظهرية والسن البطني(**V**) الدور الأهم في تحطيم عناصر الغذاء، وهذا يعتبر أيضاً من العوامل المهمة في استراتيجية التغذية لدى النوع المدروس، وقد توافقت هذه النتيجة إلى حد كبير مع نتائج دراسات [1–11–19].



الشكل(6): بنية الفقيم،D: أسنان ظهرية،C : أسنان مركزية،V: السن البطني عند النوع*Evadne spinifera* .

من ناحية أخرى، تبين من خلال دراسة محتوى المعي بأن النوع *E.spinifera* قد تغذى على الهدبيات من خلال وجود نوعين في المعي لديه وهما:

Strombidium sp. و *Pseudokeronopsis flava* ولعل قلة تغذيه على الهدبيات يعود إلى قدرتها على الهروب من التيارات البحرية التي تحدثها حركة الأرجل الصدرية، وقد جاءت هذه النتيجة متوافقة مع نتيجة دراسة[13].

لقد تنوعت الوجبات الغذائية للنوع المدروس طيلة فترة الدراسة وذلك على الأعماق المختلفة الجدول(2)، ولوحظ بأن التنوع الكبير والهائل في الوجبة الغذائية له كان في الطبقات المائية القلية العمق(0–50)م ،(0–25)م و(25–50)م[8-9-14]، فكانت الأنواع التي تغذى عليها في مختلف الطبقات هي على الشكل التالي حيث تم تصنيف

الأجناس والأنواع جميعها بالاعتماد على المراجع والمفاتيح التصنيفية العالمية وهي(William and Munger,2010), (Mona et al.,2009) :

في الطبقات (25–0)م و(50–25)م كان غذاءه متنوعاً ووجبته الغذائية شاملة لجميع الأنواع والأجناس المفضلة لديه في الوسط والتي بلغت (9)أنواع و(7)أجناس بما فيها الهدبيات:

Coscinodiscus sp, ***leptocylindrus minimus***, ***Chaetoceros socialis***,

Licmophora sp., ***Rhizosolenia Sp.***, ***Nitzschia longissima***, ***Thalassionema nitzschioides***, ***Dinophysis acuta***, ***Dinophysis acuminate***, ***Ceratium furca***, ***Alexandrium sp.***, ***prorocentrum micans***, ***Protoperidinium sp.***, ***Rhodomonas sp.***, ***Pseudokeronopsis flava, Strombidium sp.*** .

في الطبقة (0–50)م كان عدد الأنواع والأجناس التي تغذى عليها (8) أنواع و(5) أجناس وهي:

leptocylindrus minimus, ***Chaetoceros socialis***, ***Rhizosolenia Sp.***, ***Nitzschia longissima***, ***Pseudokeronopsis flava, Strombidium sp.***, ***prorocentrum micans***, ***Protoperidinium sp.***, ***Rhodomonas sp.***, ***Dinophysis acuminate***, ***Ceratium furca***, ***Alexandrium sp.***, ***Dinophysis acuta***.

بينما في الطبقة (100–0)م اعتمد النوع المدروس في غذاءه على(5) أنواع و(3) أجناس وهي:

prorocentrum micans, ***Protoperidinium sp.***, ***Rhodomonas sp.***, ***Nitzschia longissima***, ***Pseudokeronopsis flava, Strombidium sp.***, ***leptocylindrus minimus***, ***Chaetoceros socialis***.

وفي الطبقة(100–50)م تغذى على (3) أنواع و(2) جنسين هي:

Dinophysis acuminate, ***Ceratium furca***, ***Rhodomonas sp.***, ***Strombidium sp.***, ***Pseudokeronopsis flava***.

أما في الطبقة(200–0)م فقد تغذى على(2)نوعين و(2) جنسين فقط وهي:

Coscinodiscus sp, ***leptocylindrus minimus***, ***Chaetoceros socialis***, ***Licmophora sp***. .

وأخيراً في الطبقة(200–100)م تغذى على(2) نوعين فقط وهما:

***Thalassionema nitzschioides*, *Dinophysis acuta*.**

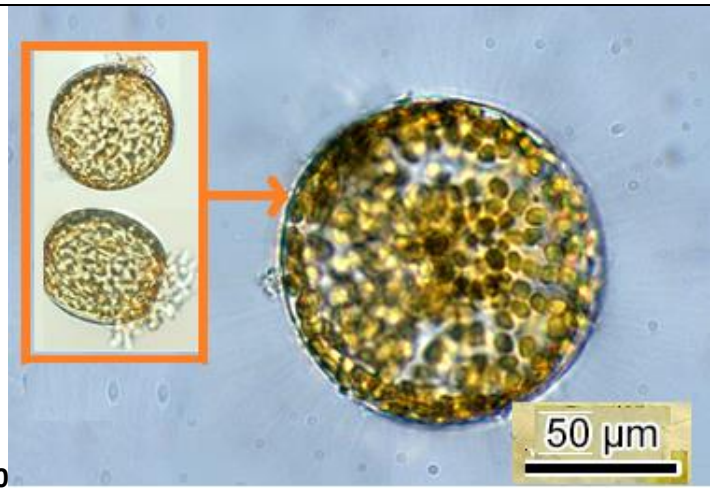
وقد جاءت النتائج السابقة متوافقة مع نتائج دراسات[5-11-15-18].

بالتالي كلما ازداد العمق كلما أصبحت الوجبة الغذائية للنوع المذكور مقتصرة على عدد قليل من الأنواع والأجناس بسبب ندرة وجود العوالق النباتية، كما هو الحال في الطبقات ذات العمق(200–0)م (200–100)م[6]، لذلك فإن الاستراتيجية الغذائية للنوع المدروس في تلك الطبقات العميقة والفقيرة بالغذاء كانت من خلال التغذي على أكبر قدر ممكن من أفراد النوع الواحد من العوالق النباتية لتعويض النقص في عدد الأنواع مقارنة مع الطبقات السطحية، وقد توافقت هذه النتائج مع دراسة[17].

أما في طبقة الإنتاجية الأولية (25–0)م والتي تكون غنية بالغذاء وتزدهر فيها السوطيات والمشطورات، حيث يكون الضوء مناسباً لقيامها بعملية التركيب الضوئي، كذلك درجة الحرارة المرتفعة والملوحة المنخفضة مقارنة مع الأعماق، فإن استراتيجية النوع *E.spinifera* تكون في زيادة شدة التغذية من خلال التغذي على أكبر قدر ممكن من الأنواع وذلك لتعويض فقدان الطاقة المصروفة على عملية ترشيح جسيمات الغذاء، وهذه النتيجة متوافقة مع دراسات[10-16] .

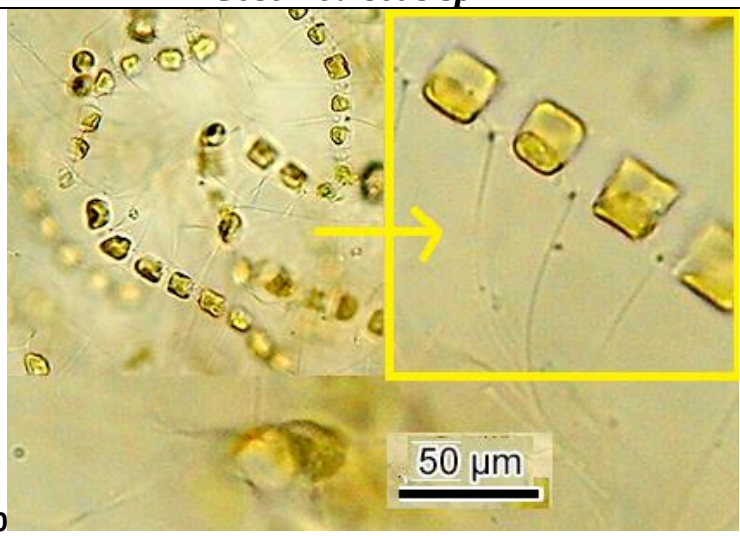
الجدول(2): الأنواع التي شكلت غذاء النوع *E.spinifera* خلال فترة الدراسة.

Bacillariophyceae



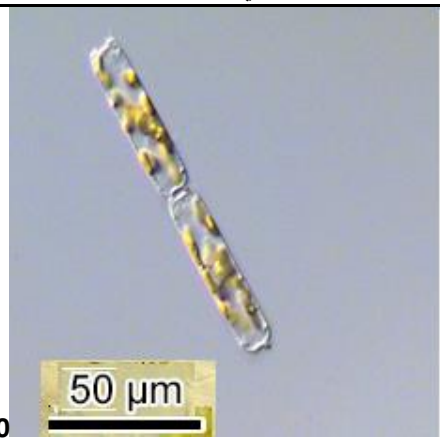
X100

Coscinodiscus sp



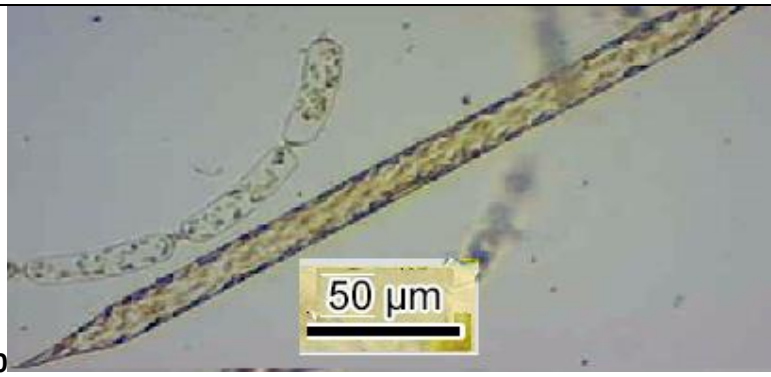
X100

Chaetoceros socialis



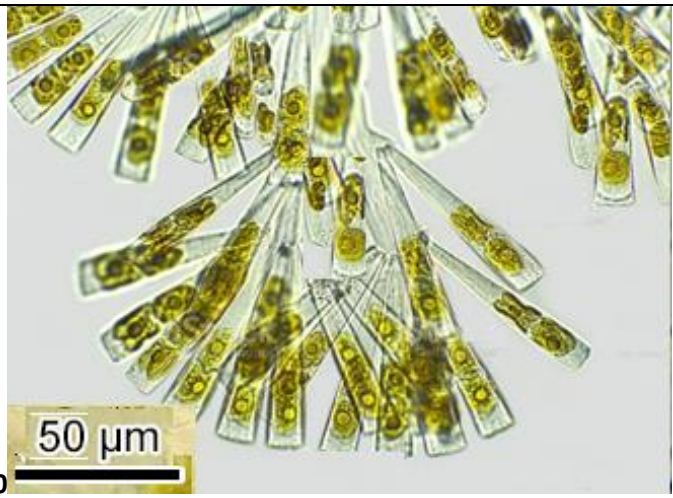
X100

leptocylindrus minimus

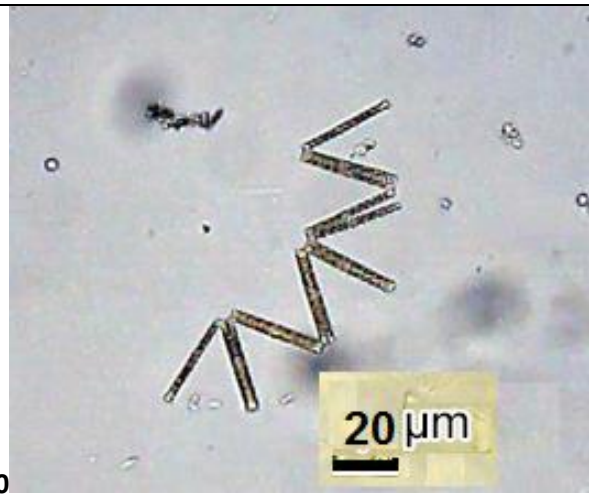


X100

Rhizosolenia Sp.



X100

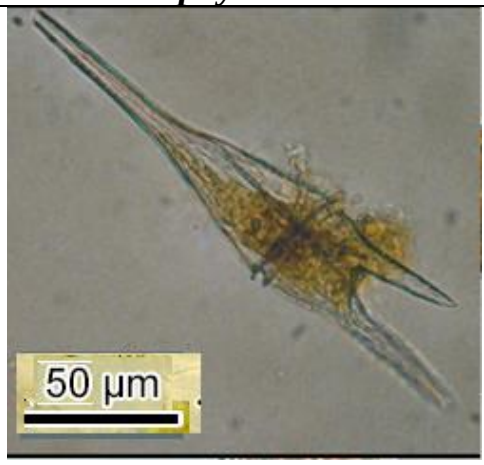
Licmophora sp.
 X40 ***Nitzschia longissima***
 X40 ***Thalassionema nitzschioides***
Dinophyceae

X40

Dinophysis acuta

X40

Dinophysis acuminata



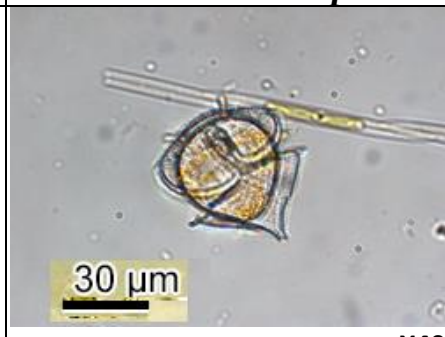
X100

Ceratium furca

X40

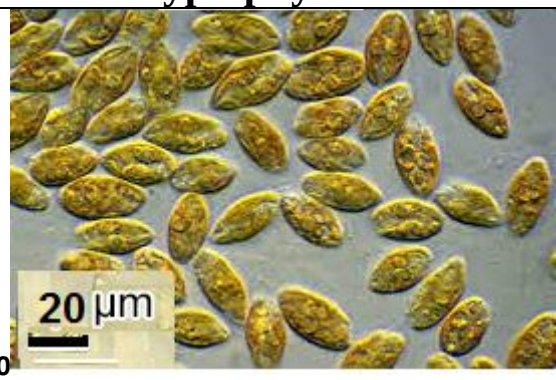
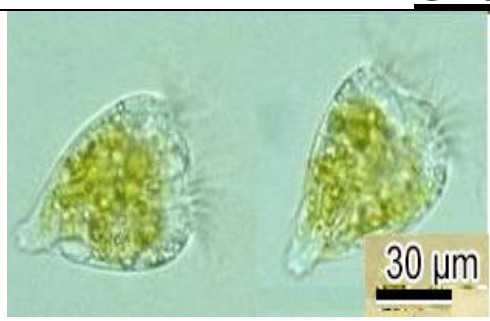
Alexandrium sp.

X40



X40

Protoperidinium sp.

prorocentrum micans	
Cryptophyceae	
 X100 ***Rhodomonas sp.***	
Ciliata	
 X40 ***Strombidium sp.***	 X100 ***Pseudokeronopsis flava***

لقد استطاع النوع *E.spinifera* أن يحدث توازناً هاماً بين معدلات ابتلاع الفرائس الطبيعية ومعدلات النمو لديه مما ساهم في إعطائه كفاءة نمو عالية وساهم في نجاح الاستراتيجية الغذائية لديه عوضاً عن عوامل أخرى ساهمت أيضاً في نجاح استراتيجيته الغذائية مثل عمر الجيل القصير والتكاثر البكري، وهذا بدورة ساعده في لعب دور هام

في شبكات الغذاء البحرية ليشكل مع بقية متفرعات القرون البحرية أحد المجموعات الهامة من العوالق الحيوانية القشرية في النظم البيئية البحرية[7-8-14-15].

أخيراً، يمكن القول بأن الدور البيئي الذي يلعبه أي كائن حي من العوالق الحيوانية القشرية في النظم البيئية البحرية يحدده موقعه وأهميته في شبكات الغذاء البحرية، لذلك تعتبر التغذية من أهم العمليات بالنسبة للعوالق الحيوانية البحرية لأنها تزودها بالمتطلبات اللازمة للحفاظ على إنتاجها ونشاطها واستمرارية بقائها، وهي أيضًا الطريق الرئيس لنقل الطاقة والمواد من المستويات الغذائية الأدنى إلى المستويات الأعلى، لذلك، من أجل فهم ديناميكيات شبكات الغذاء البحرية عند العوالق الحيوانية القشرية ، كان لابد من معرفة الطيف الغذائي ودراسة استراتيجيات التغذية عندها تحت تأثير العوامل البيئية المختلفة.

5-الاستنتاجات والتوصيات:

5-1. الاستنتاجات:

1- انخفاض تعداد أنواع العوالق النباتية الداخلة في غذاء *Evadne spinifera* مع العمق، مرتبطاً بتباين العوامل البيئية.

2- أسنان الفقيم ذات حواف قصيرة وحادة وذات تراكيب معقدة ثلاثية الأبعاد قادرة على تحطيم عناصر الغذاء الأكثر قساوة .

3- استراتيجية النوع *E.spinifera* تتجلى من خلال التغذي على أكبر قدر ممكن من الأنواع لتعويض فقدان الطاقة المصروفة على عملية ترشيح جسيمات الغذاء.

5-2.التوصيات:

الاستمرار في مثل هذا النوع من الأبحاث والدراسات بشكل دوري وذلك بهدف تحديد المتطلبات الغذائية للأنواع ذات الأهمية الاقتصادية كونها تشكل الغذاء الرئيس للأسماك والقشريات العليا والعديد من الكائنات البحرية الأخرى.

المراجع:

[1] A. KATECHAKIS.E.,H.STIBOR.,2004 "Feeding selectivities of the marine cladocerans ,Penilia avirostris,Podon intermedius and Evadne nordmanni",**Marine Biology**,pp:145-529.

[2] AL-HANOUN. K.S., ZAENI.A.,2017" Zooplankton, Directorate of University Books and Publications**"**, **Tishreen University publications**, ,pp. 17-295.

[3] AL-HANOUN .K.S.,ZAENI.A.,2020 "Practical Zooplankton - Second Edition, Directorate of University Books and Publications", **Tishreen University publications** ,pp.276 .

[4] BROGLIO. E., SAIZ .E., CALBET. A., TREPAT. I., ALCARAZ. M .,2004" Trophic impact and prey selection by crustacean zooplankton on the microbial communities of an oligotrophic coastal area(NW Mediterranean Sea**)**". **Aquat Microb Ecol**.pp: 35-65 .

[5] CHONG KIM WONG ,AXUE-JUNLIUA,YUEN YUSIUA ,JIANG-SHIOU HWANG,2020" Study of selective feeding in the marine cladoceran Penilia avirostris by HPLC pigment analysis" **Journal of Experimental Marine Biology and Ecology,** Volume 331, Issue 1, 4 April 2006, pp: 21-32.

[6] D'ALELIO.D.; LIBRALATO.S., WYATT.T., RIBERA.D., ALCALA.M., 2016" Ecological-network models link diversity, structure and function in the plankton food-web".**Sci. Rep**.

[7] EFETURI OGHENEKARO , PAULINUS CHIGBU,2019" Population Dynamics and Life History of Marine Cladocera in the Maryland Coastal Bays, U.S.A." **Journal of Coastal Research**, Vol. 35, No. 6, pp: 1225-1236.

[8] ERIC ZEUS RIZO, SHAOLIN XU, QUEHUI TANG, REY DONNE , HENRI. J. DUMONT, SONG. S. QIAN, BO.PING HAN,2019" A

global analysis of cladoceran body size and its variation linking to habitat, distribution and taxonomy" **Zoological Journal of the Linnean Society**, Volume 187, Issue.4, pp: 1119–1130, https://doi.org/10.1093/zoolinnean/zlz053.

[9] FLÓRIÁN TÓTH, KATALIN ZSUGA ,ÉVA KEREPECZKI, LÁSZLÓ BERZI,2020" The Effect of Feed Composition on the Structure of Zooplankton Communities in Fish ponds"**Journal of Experimental Marine Biology and Ecology,** Volume .331, Issue. 1**,**pp: 21-32.

[10] KIM. S.W., ONBÉ .T., YOON. Y.H., 1989 " Feeding habits of marine cladocerans in the Inland Sea of Japan:. **Mar Biol 100**,pp:313 – 318.

[11] LIU.H.,CHEN.M., SUZUKI.K., CHONG. K.W., CHEN. B.,2010" Mesozooplankton selective feeding in subtropical coastal waters as revealed by HPLC". **pigment analysis.Mar. Ecol. Prog**.,407,pp: 111–123.

[12] LIU. H., TANG. C., WONG. C.,2014" Microzooplankton grazing and selective feeding during bloom periods in the Tolo Harbour area as revealed by HPLC". **pigment analysis.J. Sea Res**.,90,pp: 83–94.

[13] MARAZZO. A., VALENTIN. J.L., 2001" Spatial and temporal variations of Penilia avirostrisand Evadne tergestina(Crus-tacea, Branchiopoda) in a tropical bay, Brazil". **Hydrobiolo-gia** ,445,pp:133–139.

[14] MENGQI HAN, Chenchen Dong, Jingyi Jia, Jianwu Chen, Chong Kim Wong and Xiangjiang Liu.,2020" Mesozooplankton Selective Feeding on Phytoplankton in a Semi-Enclosed Bay as Revealed by HPLC", **The Chinese University of Hong Kong, New Territories, Hong Kong, China, Water Journal**,12, pp.2031.

[15] MIN JUNG, SEOK HYUN YOUN, JIN YEONG KIMAND, CHUL WOONG., 2019 "Feeding Characteristics Of Cladocera, Engraulis

Japonicas According To The Distribution Of Zooplankton In The Coastal Waters Of Southern Korea ", **Oceanography of the East Sea (Japan Sea),Korean Journal of Environmental Biology** , Volume 31, Issue 4,pp: 275-287.

[16] MONA HOPPENRATH., MALTE ELBRÄCHTER., GERHARD DREBES.,2009 " Marine Phytoplankton Selected microphytoplankton species from the North Sea around Helgoland and Sylt", **ISBN 978-3-510-61392-2, paperback**, 264 p.

[17] S. NIVAL, S. RAVERA, 1979"Morphological study of the appendages of the marine cladoceran Evadne spinifera Muller by means of the scanning electron microscope" **Journal of Plankton Research**, Rio de Janeiro, Brazil. Revta bras. Zoo. 17 .(4),pp: 1101 -1102.

[18] TURNER. J.T., HOPCROFT .R.R., LINCOLN. J.A., HUESTIS. C.S., TESTER. P.A.,ROFF. J.C., 1998" Zooplankton feeding ecology: grazing bymarine copepods and cladocerans up on phytoplankton and cyanobacteria from Kingston Harbour, Jamaica."**PSZN I: Mar Ecol** ,19,pp:195–208.

[19] WILLIAM .T. KERSEY AND SAMUEL. P. MUNGER.,2010" Guide of Marine Phytoplankton".**Nova Science Publishers, ,Col & b/w figs, tabs,**ISBN: 9781607410874,Hardback,382.p.

دراسة التقارب المطلق لمتسلسلة معاملات فوريه – هاآر المضاعفة في صف معمم W

د. منير مخلوف [1]

ملخص البحث

ندرسُ في هذا البحث التقارب المطلق لمتسلسلة معاملات فوريه – هاآر المضاعفة في صف معمم W، وتحديد الشروط الكافية التي تضمن هذا التقارب .

وقد تمَّ الإثبات على صحة المبرهنة الآتية:

- **مبرهنة (1)** : لتكن الدالة $f(x_1,x_2)$ معرفة على I^2 وتنتمي إلى الصف W ، وبفرض أن $\beta \geq 1$ والمتسلسلات الآتية متقاربة:

$$\sum_{n_1=1}^{\infty}\sum_{n_2=1}^{\infty}\left[\frac{\left[E_{n_1,\infty}^{(2)}(f,H)\right]^2+\left[E_{\infty,n_2}^{(2)}(f,H)\right]^2-\left[E_{n_1,n_2}^{(2)}(f,H)\right]^2}{n_1 n_2}\right]^{\frac{1}{2}}$$

$$\sum_{n_1=1}^{\infty}\frac{E_{n_1,\infty}^{(2)}(f,H)}{\sqrt{n_1}} \quad , \quad \sum_{n_2=1}^{\infty}\frac{E_{\infty,n_2}^{(2)}(f,H)}{\sqrt{n_2}}$$

عندئذ تتقارب المتسلسلة : $\sum_{n_1=0}^{\infty}\sum_{n_2=0}^{\infty}\left|c_{n_1,n_2}(f,H)\right|^{\beta}$

حيث $c_{n_1,n_2}(f,H)$ معاملات فوريه – هاآر للدالة $f(x_1,x_2)$.

[1] ـ أستاذ مساعد في كلية العلوم – جامعة البعث.

Studing absolute Convergence of the Double Series of Fourier - Haar coefficients in the generalized class W

Dr. Moner . M. Makhlouf [1]

Abstract

In this paper we study the absolute convergence of the double Series Of Fourier- Haar coefficients in the generalized class W

The following 0n theorem will be proved:

Theorem (1): *Let* $f(x_1,x_2)\in W$, $\beta\geq 1$, *and convergence of series* :

$$\sum_{n_1=1}^{\infty}\sum_{n_2=1}^{\infty}\left[\frac{\left[E^{(2)}_{n_1,\infty}(f,H)\right]^2+\left[E^{(2)}_{\infty,n_2}(f,H)\right]^2-\left[E^{(2)}_{n_1,n_2}(f,H)\right]^2}{n_1n_2}\right]^{\frac{1}{2}}$$

$$\sum_{n_1=1}^{\infty}\frac{E^{(2)}_{n_1,\infty}(f,H)}{\sqrt{n_1}} \quad , \quad \sum_{n_2=1}^{\infty}\frac{E^{(2)}_{\infty,n_2}(f,H)}{\sqrt{n_2}}$$

:*Then the series* **:**

$$\sum_{n_1=0}^{\infty}\sum_{n_2=0}^{\infty}\left|c_{n_1,n_2}(f,H)\right|^{\beta}$$

convergence , where : $c_{n_1,n_2}(f,H)$ *the Fourier - Haar coefficeints of function* $f(x_1,x_2)$.

[1]- **De Pr. of Mathematics, Faculty of Science Al- Baath University , Homs, Syria**

1- مقدمة البحث:

بدأ العالم هآار (Haar) في عام1910 م البحث في تقارب متسلسلات هآار للدوال الحقيقية ، وقد أثبت أنَّ هذه المتسلسلات تتقارب بانتظام من دالة مستمرة وتتقارب تقريباً في كل مكان من دالة جموعية على المجال [0,1]. (انظر [1] ,[2])

ودرس التقارب المطلق وغير المشروط تقريباً في كل مكان لمتسلسلات فوريه – هآار، حيث التقارب يتم في مجموعة جزئية E من [0,1] مقيسة لوبيغياً وذات قياس موجب، كما أنّه حدّد العلاقة بين هذين التقاربين. [3]

بعد ذلك اهتمّ بدراسة التقارب غير المشروط لمتسلسلات هآار بشكل عام في الفضاءات $L^p(0,1)$, $1 \le p < +\infty$.

كان ب. ل. أوليانوف من السباقين في دراسة تقارب متسلسلات هآار ومتسلسلة المعاملات في جملة هآار ضمن مجموعات مقيسة لوبيغياً وذات قياس موجب واهتم أيضاً بدراسة قابلية جمع متسلسلات هآار وفق طرائق تجميع خطية وخطية نظامية. (انظر [4])

ولقد قام ب. ي. كالوبوف بدراسة تقارب متسلسلات فوريه – هآار لدوال ثابتة وتحديد الشروط التي تضمن هذا التقارب. (انظر [6] , [7])

ثم عمّم هذه الدراسة ف. غ. كروتوف من خلال دراسة تقارب هذا النوع من المتسلسلات لأجل دالة ما ذات مشتقة مستمرة على [0,1] ربما باستثناء مجموعة عدودة. (انظر [8])

وبعد ذلك عمّم هذه المسألة غ. آ. تشخايدزه بدراسة تقارب وقابلية جمع متسلسلات هآر وفق طرائق تجميع خطيّة نظامية (مثل: سيزارو وآبل وغيرها) في الفضاء $\mathbb{R}^n (n \geq 2)$. (انظر [12])

أثبتَ برنشتاين (C . N . Brenshtain) أنه إذا كانت الدالة $f(x)$ مستمرة ودورية بدور قدره 2π ، فإنه من تقارب المتسلسلات:

$$\sum_{n=1}^{\infty} \frac{E_n(f)}{\sqrt{n}} \quad , \quad \sum_{n=1}^{\infty} \frac{\omega\left(f, \frac{1}{n}\right)}{\sqrt{n}}$$

ينتج التقارب المطلق لمتسلسلة معاملات فوريه للدالة $f(x)$.

حيث إن : $E_n(f)$ قيمة أفضل تقريب وسطياً للدالة f بكثيرة حدود درجتها أقل من n أو تساويها ، و $\omega\left(f, \frac{1}{n}\right)$ معامل الاستمرار للدالة f . (انظر [3,2])

لقد أثبت غريغوريان (*Grigorian .M .G*) بأنه لكل $0 < \varepsilon < 1$ توجد مجموعة مقيسة لوبيغياً $E \subset [0,1]$ بحيث يكون : $|E| > 1 - \varepsilon$ ، ولكل دالة مثل: $f(x) \in L^1[0,1]$ يمكن إيجاد دالة أخرى $g(x) \in L^1[0,1]$ تطابق $f(x)$ عل ى E ومتسلسلة فوريه– هآر لها متقاربة مطلقاً في الفضاء $L^p[0,1], 0 < p < 1$. (انظر [13])

2- **هدف البحث:**

نقوم في هذا البحث بدراسة التقارب المطلق لمتسلسلات معاملات فورييه – هاآر (*Haar*) المضاعفة وذلك باستخدام طريقة التقريب بكثيرات حدود هاآر في صف معمم W ، ونحدد الشروط الكافية التي تضمن هذا النوع من التقارب، علماً أن هذه المتسلسلات يمكن أن تختلف من حيث الجوهر عن المتسلسلات المثلثية.

ويمكن ذلك من خلال إثبات صحة المبرهنة الآتية :

- **مبرهنة(*1*):** لتكن الدالة $f(x_1,x_2)$ معرفة على المربع$I^2=[0,1]\times[0,1]$ وتنتمي إلى الصف W، وبفرض أن المتسلسلات الآتية متقاربة :

$$\sum_{n_1=1}^{\infty}\sum_{n_2=1}^{\infty}\left[\frac{\left[E_{n_1,\infty}^{(2)}(f,H)\right]^2+\left[E_{\infty,n_2}^{(2)}(f,H)\right]^2-\left[E_{n_1,n_2}^{(2)}(f,H)\right]^2}{n_1n_2}\right]^{\frac{1}{2}}$$

$$\sum_{n_1=1}^{\infty}\frac{E_{n_1,\infty}^{(2)}(f,H)}{\sqrt{n_1}} \quad , \quad \sum_{n_2=1}^{\infty}\frac{E_{\infty,n_2}^{(2)}(f,H)}{\sqrt{n_2}}$$

عندئذ تتقارب المتسلسلة : $\beta\geq 1$,

$$\sum_{n_1=1}^{\infty}\sum_{n_2=1}^{\infty}\left|c_{n_1,n_2}(f,H)\right|^{\beta}$$

حيث $c_{n_1,n_2}(f,H)$ معاملات فورييه – هاآر للدالة $f(x_1,x_2)$.

لنستعرض الآن بعض المفاهيم الأساسية والتعاريف و الرموز التي نحتاج إليها في هذا البحث :

- **تعريف (1)**[2,3,15]: الفضاء $L_2(I^2)$ هو مجموعة كل الدوال المقيسة والمحدودة $f(x_1,x_2)$ المعرفة على المربع: $I^2=[0,1]\times[0,1]$ والمحققة للشرط الآتي: $\int_0^1\int_0^1 |f(x_1,x_2)|^2 dx_1dx_2 <\infty$.

(وهذا يتحقق بحكم الاستمرار أو الاستمرار تقريباً في كل مكان ، وبالتالي تكون مقيسة حسب ليبيغ على I^2 ومحدودة عليه والتي تعتبر من الشروط الأساسية لوجود تكامل ليبيغ المضاعف) .

- **تعريف (2)**: إن جملة الدوال المعرفة على المربع: $I^2=[0,1]\times[0,1]$ بالشكل: $\{H_{n_1}(x_1)\times H_{n_2}(x_2): n_\mu=0,1,2,....,\ (\mu=1,2)\}$

تسمى جملة هآ ر (Haar) المضاعفة والتي تمثل جملة متعامدة نظامية وتامة. (انظر [5,14 ,15]) ، حيث:

$$H_{n_\mu}(x_\mu)=H_{k_\mu}^{(m_\mu)}(x_\mu)=$$
$$=\begin{cases}2^{\frac{k_\mu}{2}} & , \quad if \quad x_\mu\in\Delta_{k_\mu+1}^{\left(2^{m_\mu-1}\right)}\\ -2^{\frac{k_\mu}{2}} & , \quad if \quad x_\mu\in\Delta_{k_\mu+1}^{\left(2^{m_\mu}\right)}\\ 0 & , \quad if \quad x_\mu\notin\Delta_{k_\mu}^{-(m_\mu)}\end{cases}$$

إذ إن : $\bar{\Delta}_{k_\mu}^{(m_\mu)} = \left[\frac{m_\mu - 1}{2^{k_\mu}}, \frac{m_\mu}{2^{k_\mu}}\right] \quad , n_\mu = 2^{k_\mu} + m_\mu$

$1 \leq m_\mu \leq 2^{k_\mu} \; ; \; \mu = 1,2 \; ; \; k_\mu = 0,1,2,\ldots ; \; (m_1 = i \; ; m_2 = j \,)$

- **تعريف** (3) (انظر[3]): ليكن النشر المعطى بالشكل :

$$
\begin{aligned}
& a_{0,0}^{(0,0)} H_0^{(0)}(x_1) H_0^{(0)}(x_2) \\
& \quad + \sum_{m_1=0}^{\infty} \sum_{i_1=1}^{2^{m_1}} a_{m_1,0}^{(i_1,0)} H_{m_1}^{(i_1)}(x_1) H_0^{(0)}(x_2) \\
& \quad + \sum_{m_2=0}^{\infty} \sum_{i_2=1}^{2^{m_2}} a_{0,m_2}^{(0,i_2)} H_0^{(0)}(x_1) H_{m_2}^{(i_2)}(x_2) \\
& \quad + \sum_{m_1=0}^{\infty} \sum_{m_2=0}^{\infty} \sum_{i_1=1}^{2^{m_1}} \sum_{i_2=1}^{2^{m_2}} a_{m_1,m_2}^{(i_1,i_2)} H_{m_1}^{(i_1)}(x_1) H_{m_2}^{(i_2)}(x_2) \qquad (1)
\end{aligned}
$$

حيث إن : $a_{m_1,m_2}^{(i_1,i_2)}$ أعداد حقيقية و $H_{m_\mu}^{(i_\mu)}$, $(\mu = 1,2)$ دوال هاآر.

هذا النشر يسمى نشر هاآر، وإذا احتوى فقط الحدود ذات الدرجات:

$m_2, m_1 \;\; k_2, k_1,$ ، حيث : $\left(1 \leq k_2 \leq 2^{m_2} \;\; , \; 1 \leq k_1 \leq 2^{m_1}\right)$ فإنه يؤول إلى كثيرة الحدود $P_{m_1,m_2}^{(k_1,k_2)}$ التي تسمى كثيرة حدود هاآر .

وتجدر الإشارة إلى أنه عند تغيير المعاملات $a_{m_1,m_2}^{(i_1,i_2)}$ نحصل على نشور مختلفة والذي ينتج عنه أيضاً كثيرات حدود هاآر $P_{m_1,m_2}^{(k_1,k_2)}(x_1, x_2)$ مختلفة .

- **تعريف**(4)(انظر[3,7]): لتكن $f(x_1, x_2) \in L_2(I^2)$ ،وبفرض أن: $n_2 \, , n_1$

أي عددين طبيعيين ، عندئذ :

$$S_{n_1,n_2}^{(2)}(f,H)=\inf_{a_{\mu_1,\mu_2}^{(i_1,i_2)}}\left\|f(x_1,x_2)-P_{m_1,m_2}^{(k_1,k_2)}(x_1,x_2)\right\|_{L_2}$$

يسمى أفضل قيمة تقريبية كلية وسطياً للدالة $f(x_1,x_2)$ بكثيرات حدود هآر حيث: $a_{\mu_1,\mu_2}^{(i_1,i_2)}$ هي معاملات كثيرة الحدود $P_{m_1,m_2}^{(k_1,k_2)}$ والأعداد $m_2,\ m_1\ k_2,\ k_1,$ تؤخذ بحيث يكون : $n_1=2^{m_1}+k_1\,,n_2=2^{m_2}+k_2$.

وبصورة خاصة ، إذا كان :

$$P_{m_1,\infty}^{(k_1)}(x_1,x_2)=$$
$$=a_0^{(0)}(x_2)H_0^{(0)}(x_1)+\sum_{\mu_1=0}^{m_1}\sum_{i_1=0}^{2^{\mu_1}}a_{\mu_1}^{(i_1)}(x_1)H_{\mu_1}^{(i_1)}(x_1)+$$
$$+\sum_{i_1=0}^{k_1}a_{m_1+1}^{(i_1)}(x_2)H_{m_1+1}^{(i_1)}(x_1)$$

حيث إن المعاملات $a_{\mu_1}^{(i_1)}(x_1)$ تنتمي إلى الفضاء L_2 والعدد k_1 يحقق المتباينة : $1\le k_1\le 2^{m_1}$ ، فإننا نسمي القيمة:

$$S_{n_1,\infty}^{(2)}(f,H)=\inf_{a_{\mu_1}^{(i_1)}(x_2)}\left\|f(x_1,x_2)-P_{m_1,\infty}^{(k_1)}(x_1,x_2)\right\|_{L_2}$$

أفضل قيمة تقريبية جزئية وسطياً للدالة $f(x_1,x_2)$ بكثيرات حدود هآر بالنسبة للمتغير x_1.

- **تعريف(5) :** [2,3,4 ,6] إن الصف Lip_α $(0<\alpha<1)$ هو مجموعة كل الدوال $f(x_1,x_2)$ المعرفة على I^2 التي تحقق الشرط:

$$\left\|f(x_1+h,x_2+\lambda)-f(x_1,x_2)\right\|_c=O\left(h^2+\lambda^2\right)^{\frac{\alpha}{2}}$$

وسوف نرمز بـ$C(I^2)$ لفضاء كل الدوال $f(x_1,x_2)$المضاعفة المستمرة على I^2 والمزود بالنظيم:

$$\|f\|_c = \max_{(x_1,x_2)\in I^2} |f(x_1,x_2)|$$

- **تعريف(6):** [7,10] تسمى الدالة الحقيقية : $f : [0,1]\times[0,1]\to\mathbb{R}$ محدودة التغير جزئياً على I^2 إذا وجد ثابت موجب k بحيث أنه لأجل أي تجزئتين مختلفتين :

$$\Delta_1 = \{0 \le x_0 < x_1 < x_2 < \cdots < x_n \le 1\}$$
$$\Delta_2 = \{0 \le y_0 < y_1 < y_2 < \cdots < y_m \le 1\}$$

يكون:

$$V_1(f)_2 = \sup_{0\le y\le 1} \sup_{\Delta_1} \sum_{j=0}^{n-1} |f(x_i,y) - f(x_{i+1},y)|^2 \le k$$

$$V_2(f)_2 = \sup_{0\le x\le 1} \sup_{\Delta_2} \sum_{j=0}^{m-1} |f(x,y_i) - f(x,y_{j+1})|^2 \le k$$

وسوف نرمز لفضاء كل الدوال المحدودة التغير جزئياً على I^2 بـ $PBV_2\,(I^2)$.

- **تعريف(7):**[2,3,5] لتكن الدالة $f \in L_2(I^2)$ ، وبفرض أن: $0 < \delta_m < 1$ $(m = 1,2)$. عندئذ المعامل الجزئي المتكامل للاستمرارية البحت والمختلط للدالة $f(x_1,x_2)$ بالنسبة لـx_2, x_1 يعطى بالشكل :

$$\omega_1(f,\delta_1)_2 = \sup_{(x_1,x_2)\in I^2}\{\|f(x_1+u_1,x_2) - f(x_1,x_2)\|_{L_2}\}$$

$$\omega_{\ 2}(f,\delta_2)_2 = \sup_{(x_1,x_2)\ \in\ I^2}\{\|f(x_1,x_2+u_2)-f(x_1,x_2)\|_{L_2}\}$$

$$\omega_{\ 1,2}(f,\delta_1,\delta_2)_2 = \sup_{(x_1,x_2)\ \in\ I^2}\{\|f(x_1+u_1,x_2+u_2)- f(x_1+u_1,x_2)\ -f(x_1,x_2+u_2)+f(x_1,x_2)\|_{L_2}\}$$

على الترتيب . حيث : $|u_m| \le \delta_m \quad ,(m=1,2)$

- **تعريف (8):** إن الصف المعمم W معرف كما يلي :

$$W = \{f(x_1,x_2)\ :\ f\ \in L_2(I^2)\ or\ f \in PBV_2(I^2)\}$$

وسوف نرمز بـ: $H_{m_\mu}^{(k_\mu)}(x_\mu) = H_{n_\mu}(x_\mu)\ ,\ E_{m_1,m_2}^{(k_1,k_2)}(f) = E_{n_1,n_2}(f,H)$

$$E_{\infty,m_2}^{(k_2)}(f) = E_{\infty,n_2}(f,H)\ \ ,\ E_{m_1,\infty}^{(k_1)}(f) = E_{n_1,\infty}(f,H)$$

$$n_\mu = 2^{m_\mu} + k_\mu\ ,(m_\mu = 0,1,2,3,\dots.;\ 1 \le k_\mu \le 2^{m_\mu}\ ;\mu = 1,2)$$

والتي تمثل على الترتيب دوال هآر، وقيمة أفضل تقريب كلي وسطياً، وقيمة أفضل تقريب جزئي وسطياً بالنسبة للمتغيرين x_2, x_1 الموافقة للدالة :

$$f(x_1,x_2) \in W(I^2)\ \ ,\ \ I^2 = [0,1]\times[0,1]$$

مع الأخذ بالحسبان أن:

$$E_{\infty,n_2}(f,H) = \lim_{n_1 \longrightarrow \infty} E_{n_1,n_2}(f,H)$$
$$E_{n_1,\infty}(f,H) = \lim_{n_2 \longrightarrow \infty} E_{n_1,n_2}(f,H)$$

3- **المناقشة والنتائج** : لإثبات المبرهنة (1) نحتاج إلى التمهيدية الآتية :

تمهيدية (1): (انظر [8]) إذا كان: $f \in PBV_2(I^2)$ فإن :

$$\omega_{\mu}(f,\delta)_2 \le \sqrt{3\delta}\ V_{\mu}(f)_2 \quad (\mu=1,2) \quad ,0<\delta<1$$

حيث : $V_{\mu}(f)_2$ هو التغير الجزئي للدالة f بالنسبة للمتغير x_{μ}.

إثبات المبرهنة (1) : إذا كان $f \in W(I^2)$ ، فإننا نميز حالتين :

الحالة الأولى: إذا كان $f \in L_2(I^2)$ ، فإنه حسب مساواة بارسيفال يكون لدينا:

$$\begin{aligned}
&\int_0^1\int_0^1 \left[f(x_1,x_2)-E_{n_1,n_2}(f,H)\right]^2 dx_1dx_2 \\
&\quad=\sum_{i_1=n_1+1}^{\infty}\sum_{i_2=0}^{n_2} c_{i_1,i_2}^2(f,H)+\sum_{i_1=0}^{n_1}\sum_{i_2=n_2+1}^{\infty} c_{i_1,i_2}^2(f,H) \\
&\quad+\sum_{i_1=n_1+1}^{\infty}\sum_{i_2=n_2+1}^{\infty} c_{i_1,i_2}^2(f,H) \\
&\quad=\sum_{i_1=n_1+1}^{\infty}\sum_{i_2=0}^{\infty} c_{i_1,i_2}^2(f,H)+\sum_{i_1=0}^{\infty}\sum_{i_2=n_2+1}^{\infty} c_{i_1,i_2}^2(f,H) \\
&\quad-\sum_{i_1=n_1+1}^{\infty}\sum_{i_2=n_2+1}^{\infty} c_{i_1,i_2}^2(f,H) \qquad (1)
\end{aligned}$$

ومن جهة ثانية على اعتبار أنه يمكن إيجاد من بين كثيرات حدود هاآر واحدة على الأقل أفضل تقريب وسطياً لها والتي تمثل مجاميع فوريه – هاآر الجزئية للدالة $f(x_1,x_2)$ فإن:

$$\begin{aligned}
&\left[E_{n_1,n_2}^{(2)}(f,H)\right]^2= \\
&\qquad=\int_0^1\int_0^1 \left[f(x_1,x_2)-S_{n_1,n_2}(f,H)\right]^2 dx_1dx_2 \qquad (2)
\end{aligned}$$

$$\left[E^{(2)}_{n_1,\infty}(f,H)\right]^2 = \int_0^1\int_0^1 \left[f(x_1,x_2) - S_{n_1,\infty}(f,H)\right]^2 dx_1 dx_2$$

$$\left[E^{(2)}_{\infty,n_2}(f,H)\right]^2 = \int_0^1\int_0^1 \left[f(x_1,x_2) - S_{\infty,n_2}(f,H)\right]^2 dx_1 dx_2 \qquad (3)$$

الآن حسب العلاقة (3) ومساواة بارسيفال نستطيع أن نكتب :

$$\left[E^{(2)}_{n_1,\infty}(f,H)\right]^2 = \sum_{i_1=n_1+1}^{\infty}\sum_{i_2=0}^{\infty} c^2_{i_1,i_2}(f,H)$$

$$\left[E^{(2)}_{\infty,n_2}(f,H)\right]^2 = \sum_{i_1=0}^{\infty}\sum_{i_2=n_2+1}^{\infty} c^2_{i_1,i_2}(f,H) \qquad (4)$$

الآن لو أخذنا بالحسبان العلاقات (2), (4) و المتراجحة (1) نحصل على:

$$\sum_{i_1=n_1+1}^{\infty}\sum_{i_2=n_2+1}^{\infty} c^2_{i_1,i_2}(f,H) = \left[E^{(2)}_{n_1,\infty}(f,H)\right]^2 + \left[E^{(2)}_{\infty,n_2}(f,H)\right]^2 - \left[E^{(2)}_{n_1,n_2}(f,H)\right]^2 \qquad (5)$$

لإتمام الإثبات نحتاج إلى تقارب المتسلسلة :

$$\sum_{i_1=0}^{\infty}\sum_{i_2=0}^{\infty}\left|c_{i_1,i_2}(f,H)\right| = \sum_{i_1=0}^{1}\sum_{i_2=0}^{1}\left|c_{i_1,i_2}(f,H)\right| + \sum_{i_1=2}^{\infty}\sum_{i_2=0}^{1}\left|c_{i_1,i_2}(f,H)\right| + \sum_{i_1=0}^{1}\sum_{i_2=2}^{\infty}\left|c_{i_1,i_2}(f,H)\right| + \sum_{i_1=2}^{\infty}\sum_{i_2=2}^{\infty}\left|c_{i_1,i_2}(f,H)\right| \quad (6)$$

لكن يمكن التحقق من أن:

$$\sum_{i_1=2}^{\infty}\sum_{i_2=2}^{\infty}\left|c_{i_1,i_2}(f,H)\right| = \sum_{i_1=2}^{\infty}\sum_{i_2=2}^{\infty}\sum_{n_1=1}^{i_1-1}\sum_{n_2=1}^{i_2-1}\frac{\left|c_{i_1,i_2}(f,H)\right|}{(i_1-1)(i_2-1)}$$

$$= \sum_{n_1=1}^{\infty}\sum_{n_2=1}^{\infty}\sum_{i_1=n_1+1}^{\infty}\sum_{i_2=n_2+1}^{\infty}\frac{\left|c_{i_1,i_2}(f,H)\right|}{(i_1-1)(i_2-1)}$$

$$\le \sum_{n_1=1}^{\infty}\sum_{n_2=1}^{\infty}\left[\sum_{i_1=n_1+1}^{\infty}\sum_{i_2=n_2+1}^{\infty}\frac{1}{(i_1-1)^2(i_2-1)^2}\right]^{\frac{1}{2}}\cdot\left[\sum_{i_1=n_1+1}^{\infty}\sum_{i_2=n_2+1}^{\infty}c_{i_1,i_2}^2(f,H)\right]^{\frac{1}{2}}$$

$$\le 0(1)\sum_{n_1=1}^{\infty}\sum_{n_2=1}^{\infty}\frac{1}{\sqrt{n_1 n_2}}\left[\sum_{i_1=n_1+1}^{\infty}\sum_{i_2=n_2+1}^{\infty}c_{i_1,i_2}^2(f,H)\right]^{\frac{1}{2}}$$

الآن لو أخذنا بالحسبان الفرض و العلاقة (5) نجد أن :

$$\sum_{i_1=2}^{\infty}\sum_{i_2=2}^{\infty}\left|c_{i_1,i_2}(f,H)\right| \le$$

$$\le 0(1)\sum_{n_1=1}^{\infty}\sum_{n_2=1}^{\infty}\left[\frac{\left[E_{n_1,\infty}^{(2)}(f,H)\right]^2+\left[E_{\infty,n_2}^{(2)}(f,H)\right]^2-\left[E_{n_1,n_2}^{(2)}(f,H)\right]^2}{n_1 n_2}\right]^{\frac{1}{2}} < \infty \quad (7)$$

وبمناقشة مماثلة وحسب العلاقة (4) نستطيع أن نكتب :

$$\sum_{i_1=2}^{\infty}\sum_{i_2=0}^{1}\left|c_{i_1,i_2}(f,H)\right| = \sum_{i_1=2}^{\infty}\sum_{i_2=0}^{1}\sum_{n_1=1}^{i_1-1}\frac{\left|c_{i_1,i_2}(f,H)\right|}{i_1-1} = \sum_{n_1=1}^{\infty}\sum_{i_2=0}^{1}\sum_{i_1=n_1+1}^{\infty}\frac{\left|c_{i_1,i_2}(f,H)\right|}{i_1-1}$$

$$\le 0(1)\sum_{n_1=1}^{\infty}\frac{1}{\sqrt{n_1}}\left[\sum_{i_1=n_1+1}^{\infty}\sum_{i_2=0}^{\infty}c_{i_1,i_2}^{2}(f,H)\right]^{\frac{1}{2}}$$

$$= 0(1)\sum_{n_1=1}^{\infty}\frac{E_{n_1,\infty}^{(2)}(f,H)}{\sqrt{n_1}} < \infty \qquad (8)$$

ومن جهة أخرى لدينا:

$$\sum_{i_1=0}^{1}\sum_{i_2=2}^{\infty}\left|c_{i_1,i_2}(f,H)\right| = \sum_{i_2=2}^{\infty}\sum_{i_1=0}^{1}\sum_{n_2=1}^{i_2-1}\frac{\left|c_{i_1,i_2}(f,H)\right|}{i_2-1}$$

$$= \sum_{n_2=1}^{\infty}\sum_{i_1=0}^{1}\sum_{i_2=n_2+1}^{\infty}\frac{\left|c_{i_1,i_2}(f,H)\right|}{i_2-1}$$

$$\le 0(1)\sum_{n_2=1}^{\infty}\frac{1}{\sqrt{n_2}}\left[\sum_{i_1=0}^{\infty}\sum_{i_2=n_2+1}^{\infty}c_{i_1,i_2}^{2}(f,H)\right]^{\frac{1}{2}}$$

$$= 0(1)\sum_{n_2=1}^{\infty}\frac{E_{\infty,n_2}^{(2)}(f,H)}{\sqrt{n_2}} < \infty \qquad (9)$$

ومن هذا كله نحصل على تقارب المتسلسلة :

$$\sum_{n_1=0}^{\infty}\sum_{n_2=0}^{\infty}\left|c_{n_1,n_2}(f,H)\right|$$

وبهذا يكتمل إثبات المبرهنة (1) في هذه الحالة.

الحالة الثانية: نفرض أن $f \in PBV_2(I^2)$: , $\beta > 1$ عندئذ يكون:

$$\sum_{n_1=0}^{\infty}\sum_{n_2=0}^{\infty}\left|c_{n_1,n_2}(f,H)\right|^{\beta} < \infty$$

وذلك بملاحظة أن المتسلسلة : $\sum_{n_1=0}^{\infty}\sum_{n_2=0}^{\infty}\left|c_{n_1,n_2}(f,H)\right|^{\beta}$

تكتب بالصورة :

$$\sum_{n_1=0}^{\infty}\sum_{n_2=0}^{\infty}\left|c_{n_1,n_2}(f,H)\right|^{\beta} = \sum_{n_1=0}^{\infty}\left|c_{n_1,0}(f,H)\right|^{\beta} + \sum_{n_2=0}^{\infty}\left|c_{0,n_2}(f,H)\right|^{\beta} + \sum_{n_1=1}^{\infty}\sum_{n_2=1}^{\infty}\left|c_{n_1,n_2}(f,H)\right|^{\beta} \qquad (10)$$

الآن لتكن : $n_1 = 2^{k_1} + i$, $k_1 = 0,1,..$, $1 \le i \le 2^{k_1}$

$n_2 = 2^{k_2} + j$, $k_2 = 0,1,..$, $1 \le j \le 2^{k_2}$

فإنه باستخدام متراجحة هولدر والتمهيدية (1) نجد أن :

$$\sum_{i=1}^{2^{k_1}}\left|c_{2^{k_1}+i,0}(f,H)\right|^2 =$$

$$= 2^{k_1}\sum_{i=1}^{2^{k_1}}\left|\int_0^1\left(\int_{\frac{2i-2}{2^{k_1+1}}}^{\frac{2i-1}{2^{k_1+1}}}\left[f\left(x_1+\frac{1}{2^{k_1+1}},x_2\right)-f(x_1,x_2)\right]dx_1\right)dx_2\right|^2 \le$$

$$\le 2^{k_1}\sum_{i=1}^{2^{k_1}}\left[\int_0^1\left(\int_{\frac{2i-2}{2^{k_1+1}}}^{\frac{2i-1}{2^{k_1+1}}}\left|\Delta_{\frac{1}{2^{k_1+1}}}f(x_1,x_2)_1\right|dx_1\right)dx_2\right]^2$$

$$\le 2^{k_1}\sum_{i=1}^{2^{k_1}}\left[\left(\int_0^1\left(\int_{\frac{2i-2}{2^{k_1+1}}}^{\frac{2i-1}{2^{k_1+1}}}\left|\Delta_{\frac{1}{2^{k_1+1}}}f(x_1,x_2)_1\right|^2dx_1\right)dx_2\right)^{\frac{1}{2}}\left(\int_0^1\left(\int_{\frac{2i-2}{2^{k_1+1}}}^{\frac{2i-1}{2^{k_1+1}}}1dx_1\right)dx_2\right)^{\frac{1}{2}}\right]^2$$

$$\le \int_0^1\int_0^1\left|\Delta_{\frac{1}{2^{k_1+1}}}f(x_1,x_2)_1\right|^2dx_1dx_2 \le \omega_1^2\left(\frac{1}{2^{k_1+1}},f\right)_2$$

$$\le 3.\frac{1}{2^{k_1}}V_1^2(f)_2 \le c.2^{-k_1}.V_1^2(f)_2 \qquad (11)$$

الآن من أجل $\left(\frac{4}{3}<\beta<2\right)$ ، وباستخدام متراجحة هولدر التكاملية والعلاقة (11) يكون لدينا:

$$\sum_{i=1}^{2^{k_1}}\left|c_{k_1,0}^{(i)}(f,H)\right|^\beta \le \left(\sum_{i=1}^{2^{k_1}}\left|c_{k_1,0}^{(i)}(f,H)\right|^2\right)^{\frac{\beta}{2}}2^{k_1\left(1-\frac{\beta}{2}\right)} \le$$

$$\le 2^{k_1\left(1-\frac{\beta}{2}\right)}\left(c.2^{-k_1}.V_1^2(f)_2\right)^{\frac{\beta}{2}} \le$$

$$\le \alpha.2^{k_1(1-\beta)} \qquad (12)$$

حيث : $\alpha=\left(cV_1^2(f)_2\right)^{\frac{\beta}{2}}$ ثابت موجب.

من العلاقة (12) ومن الفرض الوارد في المبرهنة نجد أن:

$$\sum_{n_1=2}^{\infty}\left|c_{n_1,0}(f,H)\right|^{\beta} =$$

$$=\sum_{k_1=0}^{\infty}\sum_{i=1}^{2^{k_1}}\left|c^{(i)}_{2^{k_1}+i,0}(f,H)\right|^{\beta} \le \sum_{k_1=0}^{\infty}\alpha.2^{k_1(1-\beta)} < \infty$$

وبصورة مماثلة تماماً يمكن الإثبات على أنه من أجل $(1<\beta<2)$ يكون :

$$\sum_{n_2=1}^{\infty}\left|c_{0,n_2}(f,H)\right|^{\beta} < \infty$$

أيضاً اعتماداً على متراجحة هولدر والعلاقة (10) والتمهيدية (1) نجد أن :

$$\sum_{i=0}^{2^{k_1}-1}\sum_{j=0}^{2^{k_2}-1}\left|\int_{\frac{2i}{2^{k_1}}}^{\frac{i+1}{2^{k_1}}}\int_{\frac{2j}{2^{k_2}}}^{\frac{j+1}{2^{k_2}}} f(x_1,x_2)H_{2^{k_1}+i}(x_1)H_{2^{k_2}+j}(x_2)dx_1dx_2\right|^2 \le$$

$$\le 2^{k_1+k_2}\sum_{i=0}^{2^{k_1}-1}\sum_{j=0}^{2^{k_2}-1}\left[\int_{\frac{2i}{2^{k_1+1}}}^{\frac{2i+1}{2^{k_1+1}}}\int_{\frac{2j}{2^{k_2+1}}}^{\frac{2j+1}{2^{k_2+1}}}\left|\Delta_{\frac{1}{2^{k_1+1}},\frac{1}{2^{k_2+1}}} f(x_1,x_2)\right|dx_1dx_2\right]^2$$

$$\le 2^{k_1+k_2}\sum_{i=0}^{2^{k_1}-1}\sum_{j=0}^{2^{k_2}-1}\left[\left(\int_{\frac{2i}{2^{k_1+1}}}^{\frac{2i+1}{2^{k_1+1}}}\int_{\frac{2j}{2^{k_2+1}}}^{\frac{2j+1}{2^{k_2+1}}}\left|\Delta_{\frac{1}{2^{k_1+1}},\frac{1}{2^{k_2+1}}} f(x_1,x_2)\right|^2 dx_1dx_2\right)^{\frac{1}{2}}\times\right.$$

$$\left.\times\left(\int_{\frac{2i}{2^{k_1+1}}}^{\frac{2i+1}{2^{k_1+1}}}\int_{\frac{2j}{2^{k_2+1}}}^{\frac{2j+1}{2^{k_2+1}}}1dx_1dx_2\right)^{\frac{1}{2}}\right]^2 \le \int_0^1\int_0^1\left|\Delta_{\frac{1}{2^{k_1+1}},\frac{1}{2^{k_2+1}}} f(x_1,x_2)\right|^2 dx_1dx_2$$

$$\le \omega_{1,2}^2\left(\frac{1}{2^{k_1+1}},\frac{1}{2^{k_2+1}},f\right)_2$$

$$\le 4\omega_1\left(\frac{1}{2^{k_1+1}},f\right)_2.\omega_2\left(\frac{1}{2^{k_2+1}},f\right)_2$$

$$\le \gamma.2^{-\frac{k_1+k_2}{2}} \qquad (13)$$

الآن ليكن: $\left(\frac{4}{3}<\beta<2\right)$ عندئذ حسب متراجحة هولدر والعلاقة (13) يكون لدينا:

$$\sum_{i=0}^{2^{k_1}-1}\sum_{j=0}^{2^{k_2}-1}\left|c_{2^{k_1}+i,2^{k_2}+j}(f,H)\right|^{\beta}\le\gamma.2^{(k_1+k_2)\left(1-\frac{3\beta}{4}\right)}$$

$$=\gamma.2^{k_1\left(1-\frac{3\beta}{4}\right)}.2^{k_2\left(1-\frac{3\beta}{4}\right)} \qquad (14)$$

فإذاً حسب الفرض والعلاقة (14) نجد أن:

$$\sum_{n_1=1}^{\infty}\sum_{n_2=1}^{\infty}\left|c_{n_1,n_2}(f,H)\right|^{\beta}=$$

$$=\sum_{k_1=0}^{\infty}\sum_{k_2=0}^{\infty}\sum_{i=0}^{2^{k_1}-1}\sum_{j=0}^{2^{k_2}-1}\left|c_{2^{k_1}+i,2^{k_2}+j}(f,H)\right|^{\beta}$$

$$\le\gamma\sum_{k_1=0}^{\infty}2^{k_1\left(1-\frac{3\beta}{4}\right)}.\sum_{k_2=0}^{\infty}2^{k_2\left(1-\frac{3\beta}{4}\right)}<\infty$$

وهذا يعني أن إثبات المبرهنة (1) قد تم .

- **نتائج البحث :**

(1) إذا وضعنا $\beta=1$ (أي : $f\in W\cap L_2(I^2)$) في المبرهنة **(1)** فإن :

$$\sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\left|c_{n,m}(f,H)\right|<\infty$$

(2) إذا وضعنا $\beta = 1$ في المبرهنة **(1)** وإذا كان :

$$\sum_{n_1=1}^{\infty} \frac{\left[E^{(2)}_{n_1,\infty}(f,H)\right]^{\alpha_1}}{\sqrt{n_1}} < \infty \quad , \quad \sum_{n_2=1}^{\infty} \frac{\left[E^{(2)}_{\infty,n_2}(f,H)\right]^{\alpha_2}}{\sqrt{n_2}} < \infty$$

حيث : $\alpha_1 + \alpha_2 = 1 \, , \, \alpha_1 . \alpha_2 > 0$ ، فإن :

$$\sum_{n_1=1}^{\infty} \sum_{n_2=1}^{\infty} \left| c_{n_1,n_2}(f,H) \right| < \infty \qquad (15)$$

إن إثبات هذه النتيجة يمكن الحصول عليه مباشرة وذلك بملاحظة ما يلي:

$$\left[E^{(2)}_{n_1,\infty}(f,H)\right]^2 + \left[E^{(2)}_{\infty,n_2}(f,H)\right]^2 - \left[E^{(2)}_{n_1,n_2}(f,H)\right]^2 \le \left[E^{(2)}_{n_1,\infty}(f,H)\right]^{2\alpha_1} . \left[E^{(2)}_{\infty,n_2}(f,H)\right]^{2\alpha_2}$$

ثم من المتراجحة :

$$\sum_{n_1=1}^{\infty} \sum_{n_2=1}^{\infty} \left\{ \frac{\left[E^{(2)}_{n_1,\infty}(f,H)\right]^2 + \left[E^{(2)}_{\infty,n_2}(f,H)\right]^2 - \left[E^{(2)}_{n_1,n_2}(f,H)\right]^2}{n_1 n_2} \right\}^{\frac{1}{2}} \le$$

$$\le \sum_{n_1=1}^{\infty} \frac{\left[E^{(2)}_{n_1,\infty}(f,H)\right]^{\alpha_1}}{\sqrt{n_1}} . \sum_{n_2=1}^{\infty} \frac{\left[E^{(2)}_{\infty,n_2}(f,H)\right]^{\alpha_2}}{\sqrt{n_2}}$$

ينتج تقارب المتسلسلة (15) .

مع الأخذ بالحسبان أنه من أجل: $(\mu = 1,2) \, , \, \alpha_\mu = 0$.

$(\alpha_1 = 0$ أو $\alpha_2 = 0)$ ، تكون المتسلسلة (15) متباعدة .

(3) إذا كان : $\beta > \frac{4}{3}$ أي: $\left(f \in W \cap PBV_2\left(I^2\right)\right)$ فإنه من المبرهنة **(1)** يكون:

$$\sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\left|c_{n,m}(f,H)\right|^{\beta} < \infty$$

(4) إذا كان $f(x_1,x_2) \in W$ فإنه من أجل $\left(\beta = 1, \lambda < -\frac{1}{4}\right)$ تتقارب المتسلسلة الآتية :

$$\sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\left[(n+1)(m+1)\right]^{\lambda}.\left|c_{n,m}(f,H)\right|^{\beta}$$

وتجدر الإشارة على أنه فيما عدا ذلك ليس بالضرورة أن يكون التقارب المطلق لهذا النوع من المتسلسلات محققاً.

- **التوصيات :**

1) محاولة إنجاز هكذا عمل وذلك من خلال دراسة تقارب متسلسلة معاملات فوريه–هاآر المكررة n مرة ($n > 2$) أي في فضاءات ذات n بعد مع تحديد الشروط الكافية لذلك إن أمكن.

2) محاولة دراسة قابلية جمع متسلسلات معاملات فوريه –هاآر في فضاءات ذات n بعد وفق طرائق تجميع خطية بشكل عام أو طرائق تجميع خطية نظامية بشكل خاص وهذا الأمر مهم تحديداً لأجل المتسلسلات المتباعدة.

المراجع (*REFERENCES*):

[1]- A. Haar ,Zur ,Theorieder orthogonalen Function en system,Math,Ann,69(1910),331-371.

[2]- BARY. N. K,1961 – Trigonometric series. Moscow. Government Puplishing Hause. 201P.

[3]- ZYGMUND. A., 1965 – Trigonometric series. Vol. 1. Moscow Peace, 615P.

[4]- P.L . Ulyanov ,on the series with respect to Haar system (Rssian), Math,sb,63:3,1964,356-391 .

[5] - B .S .Kashin ,A . A .Saakyan ,orthogonal series ,AFTS ,M ,1999 ,1st ed. Transl Math. Monogr .v.75 ,1989,451pp.

[6]-KOLMOGORAPH, A. N., FOMIN, C. V., 1989 – Elements of the theory functions and functional analysis . Moscow , 623P.

[7]- U . Goginava . on the absolute convergence of the series of Fouier- Haar coefficients ,Bull .Georgian Acad.Sci.164(1):21-23,2001

[8]- Z . A .Chanturia ,on the absolute convergence of the series of Fouier – Haar coefficients ,comment ,Math ,Special,Issc,2:25-35,1979 .

[9]- L .D . Gogoladze ,V. SH Tsagareishvili ,the absolute convergence of the Fourier – Haar series for two dimensional functions,Tbilisi,380028,Gorgia,2007.

[10]- S .Yu .Galkina ,, on the Fourier – Haar series coefficients of functions of several variables with

Bounded Vitali Variation,, Mathematical Notes Vol.70 Issue 5 ,pp 733-743, 2001 .

[11]- M.G. Plotnikov ,,Coefficients of convergent multiple Haar series ,, Russian Mathematics ,vol . 56 ,Issue 1,pp 61-65 ,2012

[12] - ЧХАИДЗЕ, Г. А, 1972 –О кратных рядах по системе Хаара. Сообщения АН ГССР, 35. N1, 541-544.

[13]-Grigorian . M.G ,,On the absolute convergence of Fourier – Haar series in the metric $L^p(0,1), 0 < p < 1$,, Akad. Nauk.SSSR. St.0025,Yerevan ,Armenia,2018 .

[14– مخلوف منير، 2015 "دراسة تقارب متسلسلات هآر ذات المعاملات المطردة الحقيقية" ،مجلة جامعة البعث ، مجلد (37).

[15] - مخلوف منير ،2017، " تقارب متسلسلات فورييه – هآر لدوال مشتقاتها مستمرة" مجلة جامعة البعث ، مجلد 39.

دراسة حول استخدام تركيب التوابع لتهجين بعض خوارزميات التشفير

احمد شاهين[1] وَ أ.م. د. محمد فراس الحلبي[2]

قسم الرياضيات – كليّة العلوم – جامعة دمشق– سوريا

المُلخّص

لا يخفى على أحد الدور الكبير للتشفير في شتى مجالات حياتنا اليومية، وعليه تعددت خوارزميات التشفير. لقد ركزت معظم الخوارزميات التي طُورت في هذا المجال على هدف واحد كتعقيد فك تشفير النص. لم تقدم أي دراسة آلية رياضية واضحة تعطي خوارزميات تشفير عددية جديدة تعمم وتدمج خوارزميات التشفير العددية المعروفة. قمنا في هذا البحث بدراسة التوابع العددية التشفيرية لعدة أهداف. هذه الأهداف تتمثل في تقديم النموذج الرياضي الكامل لوصف شفرات عائلة فيجينير (الكاملة – تلقائية المفتاح – طويلة المفتاح)، بالإضافة لزيادة الأعداد المحتملة الكلية اللازمة لكسر مفاتيح التوابع التشفيرية. بهدف زيادة هذه الأخيرة قمنا بتقديم مقترحين الأول آلية جديدة لتوسيع جدول المقابلات العددي، والثاني دراسة إمكانية تركيب التوابع التشفيرية التي تشكل آلية فعالة لتعميم ودمج خوارزميات التشفير العددية. اقترحنا خوارزمية تشفير عددية مبنية على التركيب تعطي تعميماً لبعض خوارزميات التشفير المعروفة مع جدول مقابلات عددي معدل. للتحقق من صحة ما توصلنا إليه قمنا بدراسة الحالات الخاصة للخوارزمية المقترحة وفق شروط محددة. كما قمنا بدراسة الأعداد المحتملة الكلية اللازمة لكسر مفاتيح تشفير الطريقة المقترحة. أخيراً قمنا ببرمجة الطريقة المقترحة مع جدول المقابلات العددي المعدل باستخدام لغة البرمجة #C.

الكلمات المفتاحية: تابع تشفيري، تابع مركب، تحويلات تابع، أعداد محتملة، محارف محتملة، تعميم خوارزمية، كسر التشفير، جدول مقابلات عددية، عائلة شفرات فيجينير.

[1] طالب ماجستير – قسم الرياضيات – كليّة العلوم –جامعة دمشق.

[2] الدكتور المشرف – قسم الرياضيات – كليّة العلوم – جامعة دمشق.

A Study about using Functions Composition for Mixing some Cryptographic Algorithms

Ahmad Shaheen[3] and Prof. Mohamad Firas Al-halabi [4]
Department of Mathematics - Faculty of Science - Damascus University –Syria

Abstract

Nowadays cryptography plays an important role in many areas. Therefore, many cryptography algorithms were developed, but most of them focus on one goal, such as the decryption complexity. Indeed, no study proposes a clear mathematical technique that produces new cryptographic algorithms aiming at generalizing and mixing some cryptographic algorithms in a form of cryptographic functions. In this paper, we study the functions of cryptography for multi goal. In one side, we propose a complete mathematical model allow to describe the Vegener family. In another side, we increase the possible total numbers needed to break the cryptographic function keys. In order to achieve this, we introduce two proposals: (i) a new technique for expanding the table of numerical interviews; (ii) study the possibility of composition cryptographic functions that constitute an effective technique for generalizing and mixing function cryptography algorithms. We propose a new cryptographic algorithm based on a cryptographic functions composition. This gives generalization to some well-known cryptographic algorithms with a modified numerical interview table. To verify the validity of our results, we study a special cases of the proposed algorithm for specific conditions. We also study the possible total numbers needed to breakdown the proposed algorithm encryption keys. Finally, we implement the proposed algorithm with the modified numerical interview table using C # programming language.

Keywords: Cryptographic function, Compound function, Function transformation, Possible numbers, Possible chars, generalization algorithm, table numerical interviews, breaking the encryption, family of Vigener cipher.

[3] Master student - Damascus University - Faculty of Science.
[4] Associate Professor- Damascus University - Faculty of Science.
[4] Dr-mfalh@scs-net.org

1. مقدمة

استُخدمَ علم التشفير قديماً من قبل الفراعنة. كما استخدم الصينيون طرائق عديدة في علم التشفير لنقل الرسائل أثناء الحروب [2]. لكن مع تطور الوسائل التقنية والنمو الكبير للشبكات وبخاصة الشبكة العالمية الأنترنت التي تشكل الوسط الأضخم لنقل المعلومات وتبادلها [3]، كان لابد من الحفاظ على سرية الرسائل المبثوثة عبر قنوات الاتصال المختلفة، بإيجاد خوارزميات تعمية تواكب هذا التقدم [12]. نال التشفير اهتمام العديد من الباحثين خلال الفترة الأخيرة. وجدنا أن الدراسات تتجه نحو التوابع العددية لسهولة التعامل معها وتطبيقها حاسوبياً وقد قدمت عدة دراسات في هذا المجال. من أبرز التوابع العددية التشفيرية قيصر[2] وَ أتباش[13] وَ الإزاحة[9] وَ الضرب[9] وَ أفاين[1] وَ فيجينير الكاملة[2] وَ RSA[5] وَ ROT13[2] وَ طريقة RSA – Affine المطورة بالتابع المركبة [11] وعلاقة فيثاغورث المولدة لثلاثية عددية أولية [12]. من جهة أخرى في [10] وَ [8] تم الدمج بين خوارزميتي تشفير إحداها RSA. الدراسات السابقة تعتبر دافعاً مهماً لطرح العديد من التساؤلات التي تحدد أهداف هذا البحث والتي سنقوم بعرضها في الفقرة التالية.

2. الهدف من البحث

تعتبر عملية دمج خوارزميات التشفير طريقة فعالة في زيادة قوة الشيفرة، وعليه تعددت خوارزميات التشفير القائمة على الدمج. لكن عند التعامل مع خوارزميات التشفير العددية فمن الضروري عند تشفير نص ما ضمان إمكانية فك التشفير. العديد من الأسئلة يمكن طرحها هنا نذكر منها ما يلي:

1. هل يمكن الحصول على عدد لانهائي من خوارزميات التشفير العددية؟
2. هل يمكن تركيب التوابع التشفيرية العددية؟
3. هل يمكن الوصول الى خوارزمية عددية تشكل تعميماً لكل من شفرات: قيصر وأتباش والإزاحة والضرب وأفاين فيجينير الكاملة و RSA و ROT13 وطريقة RSA – Affine المطورة بالتابع المركبة ؟

4. هل يمكن زيادة الأعداد المحتملة الكلية اللازمة لكسر مفاتيح تابع تشفيري؟
5. هل يمكن توسيع جدول المقابلات العددي؟
6. هل تختلف توابع شيفرات عائلة فيجينير (الكاملة–تلقائية المفتاح–طويلة المفتاح)؟

سنحاول في هذا البحث الإجابة عن هذه الأسئلة.

3. مواد وطرق البحث

في الواقع بعض خوارزميات التشفير تعتمد على نظرية الأعداد (Number Theory). لنقوم بعرض بعض المفاهيم المتعلقة بعلم التشفير وبعض دوال خوارزميات التشفير العددية [7][3][2].

3.1 قابلية القسمة

ليكن a, b عددين صحيحين بحيث $a \neq 0$، نقول إن a يقسم b إذا وجد عدد صحيح ثالث c بحيث $b = a.c$ ونشير إلى ذلك بالرمز $a|b$. نقول عن عدد ما إنه أولي إذا كان له قاسمان فقط هما العدد 1 والعدد نفسه.

3.2 القاسم المشترك الأكبر (The greatest common divisor)

القاسم المشترك الأكبر لعددين صحيحين x, y هو أكبر عدد صحيح موجب يقسم العددين x, y معاً. نرمز له بالرمز $\gcd(x, y)$ أي:

$$\gcd(x, y) = \max_{a}\{\, a \in Z^{+} ; a|x \ \wedge a|y \,\}$$

نقول عن عددين x, y إنهما أوليان فيما بينهما إذا تحقق: $\gcd(x, y) = 1$

3.3 تابع اويلر φ (Euler Function)

ليكن n عدداً صحيحاً. ولتكن المجموعة $M_n = \{x \in \mathbb{N} ; \gcd(x, n) = 1\}$ عندئذٍ يُعرف تابع اويلر بأنه عدد عناصر المجموعة M_n ويرمز له بالرمز $\varphi(n)$.

3.4 التطابق(Congruent)

ليكن العدد الصحيح $n \geq 1$. نقول عن العددين الصحيحين a و b إنهما متطابقان(Congruent) بالقياس(Module) n إذا كان: $n|(a - b)$ ونكتب:

$$a \equiv b \ mod \ n$$

3.5 مبرهنة

ليكن العدد الصحيح $n \geq 1$. إذا كان $a_1 \equiv b_1 \ mod \ n$ و $a_2 \equiv b_2 \ mod \ n$ فإن:

$$a_1 \pm a_2 \equiv (b_1 \pm b_2) mod \ n \ \ \& \ \ a_1 . a_2 \equiv (b_1 . b_2) mod \ n .$$

3.6 النظير الضربي (Multiplicative Inverse)

ليكن $n \geq 1$ و x عددين صحيحين حيث $\gcd(x, n) = 1$ نقول إن y هو النظير الضربي للعدد x بالقياس n إذا تحقق: $x.y \equiv 1 \ mod \ n$، نرمز للنظير الضربي بالقياس n بالرمز x^{-1}. من الواضح أن: $(-1)^{-1} \equiv -1 \ mod \ n$ لأن:

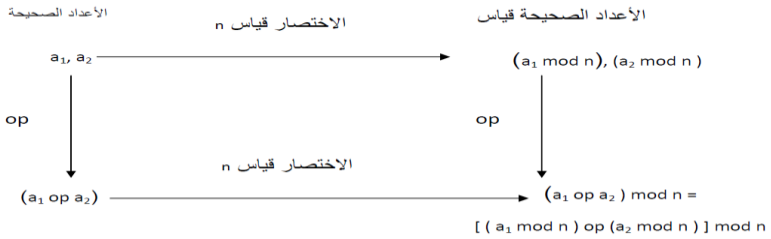
$(-1).(-1) \equiv 1 \ mod \ n$ وَ $(1)^{-1} \equiv 1 \ mod \ n$ لأن:

$$(1).(1) \equiv 1 \ mod \ n$$

3.7 مبرهنة

بفرض أن a_1, a_2 عددان صحيحان وبفرض أن op تمثل إحدى العمليات $+, -, \times$، عندها يكون التحويل قياس n هو هوموморفيزم من حلقة الأعداد الصحيحة إلى حلقة الأعداد الصحيحة قياس n (الشكل 1). يمكن التعبير عن هذا الهوموморفيزم كما يلي:

$$(a_1 \text{op} \ a_2) mod \ n = [(a_1 mod \ n) \text{op} (a_2 mod \ n)] mod \ n$$



الشكل 1: مبدأ هوموморفيزم التحويل قياس n.

3.8. النص الأصلي (Plain Text) [2]

هو الرسالة الواضحة (المفهومة) أو المعطيات التي تشكل دخل عملية التشفير.

3.9. التشفير (Encryption) [14]

هو عملية تحويل النص الأصلي (Plain Text) إلى النص المشفر (Cipher text).

3.10. المفتاح (key)[14]

قيمة صغيرة من المعلومات تستخدم لتحويل النص الأصلي (Plain Text) إلى النص المشفر (Cipher text) أو بالعكس.

3.11. النص المشفر(Cipher text) [14]

هو النص الناتج عن عملية التشفير (Encryption) بواسطة بعض أنظمة التشفير (Cryptosystem).

3.12. فك التشفير (Decryption)[14]

هي عملية تحويل النص المشفر (Cipher text) إلى النص الأصلي (Plain Text).

3.13. أنواع مفاتيح التشفير (Types of encryption keys)[4]

3.13.1 المفتاح العام (Public-Key)

يستخدم المفتاح العام في تشفير الرسائل، ويكون من أساسيات عملية التشفير ومعروف من قبل أي شخص. لكن لا يستطيع أحد فك التشفير باستخدام المفتاح العام فقط لأنه يحتاج إلى المفتاح الخاص لإتمام عملية فك التشفير والحصول على المعلومات المطلوبة.

3.13.2 المفتاح الخاص (Private-Key)

المفتاح الخاص هو المفتاح المكمل للمفتاح العام. يمكن من خلاله فك أي معلومة مشفرة على أساس المفتاح العام. لهذا السبب يجب الاحتفاظ بالمفتاح الخاص بشكل سري.

3.14 الجزء الصحيح [6]

إذا كان $x \in \mathbb{R}$ فيوجد عدد صحيح وحيد $\lfloor x \rfloor$ يحقق العلاقة :

$$\lfloor x \rfloor = \max \{z \in \mathbb{Z} \, ; \, z \leq x\}$$

نسمي $\lfloor x \rfloor$ الجزء الصحيح للعدد x.

3.15 بعض توابع التشفير العددية

التوابع العددية لخوارزميات التشفير تجعل من السهل التعامل معها وتطبيقها حاسوبياً. نذكر هنا بعضاً من تلك التوابع.

3.15.1 تابع شيفرة قيصر [2] (Caesar Cipher)

هي طريقة قديمة ابتكرها القيصر يوليوس لتشفير الرسائل بين قطاعات الجيش وقد أثبتت فاعليتها في عصره. تتميز شيفرة قيصر ببساطتها ويعيبها سهولة كسرها. يتم فيها أولاً مقابلة الأحرف الأبجدية بأعداد من 0 إلى 25. كما في الجدول 1.

الجدول 1: جدول المقابلات العددية.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

يمكن أن نعبر عن خوارزمية قيصر العددية (للتشفير وفك التشفير) بالعلاقات التالية:

$$y = f(x) = (x + 3) mod\ 26 \quad \dots (1$$
$$x = f^{-1}(y) = (y - 3) mod\ 26 \quad \dots (2$$

حيث x يرمز للمقابل العددي للمحرف قبل التشفير، y يرمز للمقابل العددي للمحرف بعد التشفير. يمكن توسيع تابع شيفرة قيصر لتتعامل مع أكثر من 26 محرفاً، وذلك باستبدال الجدول 1 بجدول مقابلات عددية يحوي n محرف. عندئذٍ نقوم باستبدال 26 بـ n في العلاقتين 1 و2.

3.15.2 تابع شيفرة الضرب(Product Cipher)[4][9]

يعتمد تابع شيفرة الضرب على عملية الضرب بشكل أساسي، حيث تتم مقابلة الأحرف الأبجدية بأعداد ضمن جدول مقابلات عددية يحوي n محرف. تعطى التوابع العددية (للتشفير وفك التشفير) لشيفرة الضرب بالعلاقات التالية:

$$y = f(x) = (a.x)\ mod\ n \quad \dots (3$$

بشرط أن يتحقق: $\gcd(a, n) = 1$ حتى نتمكن من فك التشفير(حتى نضمن أن يكون للعدد a نظير ضربي)

$$x = f^{-1}(y) = (a^{-1}.y)\ mod\ n \quad \dots (4$$

حيث x يرمز للمقابل العددي للمحرف قبل التشفير،y يرمز للمقابل العددي للمحرف بعد التشفير،a عدد صحيح يستخدم كمفتاح.

3.15.3 تابع شفيرة الازاحة (Shift Cipher)[9]

في هذه الطريقة يتم إزاحة كل حرف من النص الأصلي بمقدارcوذلك بعد مقابلة الأحرف الأبجدية بأعداد ضمن جدول مقابلات عددية، يحوي n محرف، يمكن أن نعبر عن ذلك بالعلاقات التالية:

$$y = f(x) = (x + c)\ mod\ n \quad \dots (5$$
$$x = f^{-1}(y) = (y - c)\ mod\ n \quad \dots (6$$

حيث x يرمز للمقابل العددي للمحرف قبل التشفير، y يرمز للمقابل العددي للمحرف بعد التشفير، c عدد صحيح يستخدم كمفتاح.

3.15.4 تابع شيفرة أتباش [13] (Atbash Cipher)

على الرغم من اقتراح شيفرة أتباش في الأصل للغة العبرية، لكن يمكن استخدام المفهوم مع باقي اللغات. تقوم هذه الشيفرة على مقابلة الأحرف الأبجدية بأعداد ضمن جدول مقابلات عددية، يحوي n محرف. تعطى تابع شيفرة أتباش (التشفير وفك التشفير) بالعلاقات التالية:

$$y = f(x) = ((n-1) - x) \bmod n \quad \dots (7$$
$$x = f^{-1}(y) = ((n-1) - y) \bmod n \quad \dots (8$$

حيث x يرمز للمقابل العددي للمحرف قبل التشفير، y يرمز للمقابل العددي للمحرف بعد التشفير.

3.15.5 تابع شيفرة أفاين [13][1] (Affine Cipher)

تسمى شيفرة أفاين أيضاً بالتشفير المختلط لأنها تدمج بين شيفرة الإزاحة وشيفرة الضرب. في هذه الشيفرة يتم مقابلة الأحرف الأبجدية بالأعداد ضمن جدول مقابلات عددية، يحوي n محرف. يعطى تابع شيفرة أفاين (التشفير وفك التشفير) بالعلاقات التالية:

$$y = f(x) = (a.x + b) \bmod n \quad \dots (9$$
$$x = f^{-1}(y) = (a^{-1}.(y - b)) \bmod n \quad \dots (10$$

بشرط أن يتحقق: $\gcd(a, n) = 1$ حتى نتمكن من فك التشفير (حتى نضمن أن يكون للعدد a نظير ضربي). حيث x يرمز للمقابل العددي للمحرف قبل التشفير، y يرمز للمقابل العددي للمحرف بعد التشفير، a عدد صحيح يستخدم كمفتاح أول، b عدد صحيح يستخدم كمفتاح ثانٍ.

3.15.6 تابع شيفرة فيجينير الكاملة [2](The Full Vegenere Cipher)

في شيفرة فيجينير الكاملة مقابلة أحرف النص الأصلي والمفتاح بالأعداد ضمن جدول مقابلات عددية، يحوي n محرف. يعطى التابع العددية (للتشفير– فك التشفير) بالعلاقات:

$$z = f(x, y) = (x + y) \bmod n \quad \dots (11$$
$$x = f^{-1}(z, y) = (z - y) \bmod n \quad \dots (12$$

حيث x يرمز للمقابل العددي للمحرف قبل التشفير، y يرمز للمقابل العددي للمحرف في المفتاح النصي، z يرمز للمقابل العددي للمحرف بعد التشفير.

3.15.7 تابع شيفرة RSA [10][5]

تعتبر شيفرة RSA من أهم خوارزميات المفتاح العام. يرجع سبب تسميتها لأسماء العلماء الذين أوجدوها وهم (Rivest – Shamir – Adleman). تقوم RSA على إيجاد العوامل الأولية لعدد صحيح. يتم في هذه الخوارزمية مقابلة أحرف النص الأصلي فقط بأعداد ضمن جدول مقابلات عددية. يمكن توضيح آلية عمل هذه الخوارزمية كما يلي:

اولاً: توليد المفتاح

1. نختار عددين أوليين p, q.
2. نحسب ناتج جداء العددين وهو n أي $n = p * q$.
3. نحسب $\varphi(n) = (p-1)(q-1)$.
4. نختار المفتاح العام (key public)

$$k \in \{1, 2, 3, \ldots .., \varphi(n)-1\}; \gcd(k, \varphi(n)) = 1$$

ويكون المفتاح العام: $\text{Key}_{\text{public}} = (k, n)$

5. نختار المفتاح الخاص (key private)

$$d \in \mathbb{Z}^+ ; d * k \bmod \varphi(n) = 1$$

ويكون المفتاح الخاص: $\text{Key}_{\text{private}} = (d, n)$

ثانياً: التشفير (Encryption): يتم وفق العلاقة:

$$y = f(x) = x^k \bmod n \quad \ldots\ldots (13$$

حيث x يرمز للمقابل العددي لمحرف النص الأصلي قبل التشفير، y يمثل ناتج تشفير المحرف x وهو عدد صحيح.

ثالثاً: فك التشفير (Decryption): يتم وفق العلاقة:

$$x = f^{-1}(y) = y^d \bmod n \quad \ldots\ldots (14$$

حيث y عدد صحيح ما في النص المشفر، x يرمز للمقابل العددي لمحرف النص الأصلي قبل التشفير المرتبط بالعدد y.

4. النتائج ومناقشتها

بعد دراسة التوابع العددية لبعض خوارزميات التشفير المعروفة، تبين أنه من الضروري إعطاء نموذج رياضي كامل لوصف عائلة شفرات فيجينير، ذلك لا يقل أهمية عن دراسة الأعداد المحتملة الكلية لتحويلات[5] بعض توابع التشفير العددية. قمنا بدايةً بصياغة النموذج الرياضي الكامل لعائلة شفرات فيجينير، ثم أجرينا دراسة للأعداد المحتملة الكلية لتحويلات بعض توابع التشفير العددية التي تمكننا من حساب العدد الكلي المحتمل لكسر مفاتيح التشفير لتلك التوابع. كما قمنا بإجراء مقارنة العدد الكلي المحتمل لكسر مفاتيح التشفير للتوابع المدروسة وتبين لنا أن العدد الكلي المحتمل لكسر مفاتيح التشفير لتابع يزداد من خلال توسيع جدول المقابلات العددي من جهة، وتركيب التوابع التشفيرية من جهة أخرى. بناءً على ذلك قدمنا آلية جديدة لتوسيع جدول المقابلات العددي. كما قدمنا آلية جديدة للتشفير باستخدام تركيب التوابع التشفيرية. من أجل تسهيل عملية التركيب القياسي قمنا ببرهان النتيجة (4.6). لنبيّن أن تركيب التوابع يعطي تعميماً للتوابع التي يتم تركيبها اقترحنا إحدى خوارزميات توابع التشفير المركبة مع جدول مقابلات عددي مُعدّل، وضحنا عملها من خلال مثال. أخيراً قمنا بدراسة الحالات الخاصة التي يمكن الوصول لها وفق شروط محددة. قمنا بحساب العدد الكلي المحتمل لكسر مفاتيح التشفير للخوارزمية المقترحة، وذلك للتحقق من كفاءة وصحة ما توصلنا إليه.

4.1 دراسة في شيفرات عائلة فيجينير

من خلال البحث تبين أنه تم تحويل طريقة فيجينير الكاملة فقط إلى تابع عددية في [2]، كما أن الفرق الوحيد بين عائلة شيفرات فيجينير هو توليد مفاتيح التشفير [1]. انطلاقاً من ذلك، يمكننا أن نطرح **السؤال** التالي:

ما هو النموذج الرياضي الذي بنيت علية شيفرات عائلة فيجينير؟

[5] الأعداد المحتملة الكلية لتحويلات تابع ما هي العدد الكلي الممكن اختياره لكل ثوابت (المفاتيح أو المحارف) التابع من أجل كامل محارف النص الأصلي (عدد مرات استخدام التابع).

أي بمعنى آخر ما هي التابع (التشفير– فك التشفير) العددية لشيفرة فيجينير تلقائية المفتاح؟ ما هي التابع (التشفير– فك التشفير) العددية لشيفرة فيجينير طويلة المفتاح؟ كيف يتم بناء المفاتيح في شيفرات عائلة فيجينير بالطريقة الرياضية؟

سنقوم في هذه الفقرة بالإجابة على هذه الأسئلة. من أجل ذلك نفرض ما يلي:

سلسلة محارف النص الأصلي $X = x_1x_2 \dots x_k$ ، حيث $|X| = k$. سلسلة محارف المفتاح النصي $Y = y_1y_2 \dots y_t$، حيث $|Y| = t$. أما سلسلة محارف النص المشفر $Z = z_1z_2 \dots z_k$ حيث: $|Z| = k$.

4.1.1 نموذج شيفرات عائلة فيجينير الرياضي

قمنا بتوصيف شيفرات عائلة فيجينير وفق عدة مراحل: مرحلة بناء المفاتيح ومرحلتي التشفير وفك التشفير.

- **مرحلة بناء المفاتيح**

الهدف الأساسي في هذه المرحلة هو الحصول على مفتاح نصي:

$$\grave{Y} = \acute{y}_1\acute{y}_2\acute{y}_3 \dots$$

يحقق الشرط $|\grave{Y}| = |X| = k$[6]، بناءً على المفتاح النصي المعطى Y فقط أو على جزء من المفتاح النصي المعطى Y والنص الأصلي X، لنتمكن من التشفير وفك التشفير. يمكننا أن نميز حالتين:

1. **حالة** $(|Y| < |X|)$[7]

في هذه الحالة أيضاً نميز حالتين:

A. **الحالة الأولى:** يتم تشكيل المفتاح النصي الجديد $\grave{Y}$ بتكرار محارف المفتاح النصي Y ليصبح طول مفتاح نصي جديد $\grave{Y}$ مساوياً لطول النص الأصلي X ، وهذا ما يتم في طريقة فيجينير الكاملة [1]. لنعبر عن ذلك رياضياً كما يلي:

$$\grave{Y} = \acute{y}_1\acute{y}_2 \dots \acute{y}_k$$

$$\left(\left\lfloor\frac{k}{t}\right\rfloor = r\right) \&\ (k \bmod t = s)$$

[6] طول المفتاح النصي الجديد $\grave{Y}$ مساوياً لطول النص الأصلي X

[7] طول النص الأصلي أكبر من طول المفتاح النصي

$$\acute{y}_i = \begin{cases} \acute{y}_{i+t.m} = y_i \ ; i = 1,2, \dots, t \ ; m = 0,1, \dots, \mathrm{r}-1 \\ \acute{y}_{i+r.t} = y_i \ ; i = 1,2, \dots, \mathrm{s} \end{cases}$$

B. **الحالة الثانية:** يتم تشكيل المفتاح النصي الجديد $\grave{\mathrm{Y}}$ بتكرار محارف المفتاح النصي Y ثم بعد الإنتهاء يتم تكرار محارف النص الأصليX، ليصبح طول المفتاح النصي الجديد $\grave{\mathrm{Y}}$ مساوياً لطول النص الأصلي X ، وهذا ما يتم في طريقة فيجينير تلقائية المفتاح [1]. لنعبر عن ذلك رياضياً كما يلي:

$$\grave{\mathrm{Y}} = \acute{y}_1 \acute{y}_2 \dots \acute{y}_k$$

$$\acute{y}_i = \begin{cases} \acute{y}_i = y_i \ ; i = 1,2, \dots, t \\ \acute{y}_{i+t} = x_i \ ; i = 1,2, \dots, k-t \end{cases}$$

2. **حالة** $(\boldsymbol{t > k})$

يتم تشكيل المفتاح النصي الجديد $\grave{\mathrm{Y}}$ بأخذ جزء من محارف المفتاح النصي Y، ليصبح طول المفتاح النصي الجديد $\grave{\mathrm{Y}}$ مساوياً لطول النص الأصلي X ، وهذا ما يتم في طريقة فيجينير طويلة المفتاح [1]. لنعبر عن ذلك رياضياً كما يلي:

$$\grave{\mathrm{Y}} = \acute{y}_1 \acute{y}_2 \dots \acute{y}_k$$

$$\acute{y}_i = y_i \ ; i = 1,2, \dots, k$$

- **مرحلتي التشفير وفك التشفير**

بعد بناء المفتاح النصي اللازم لعملية التشفير بأحد الطرق المذكورة في المرحلة الأولى، يمكن التشفير (فك التشفير) بالتوابع العددية لشفرات عائلة فيجينير التي تعطى بالعلاقات:

$$\acute{z} = f(\acute{x}, \acute{w}) = (\acute{x} + \acute{w}) \ mod\, n \quad \dots\dots (1$$

$$\acute{x} = f^{-1}(\acute{z}, \acute{w}) = (\acute{z} - \acute{w}) \ mod\, n \quad \dots (2$$

حيث n عدد محارف الأبجدية المراد التشفير بها، $\acute{x}$ يرمز للمقابل العددي لمحرف النص الأصلي، $\acute{w}$ يرمز للمقابل العددي لمحرف النص المفتاحي، $\acute{z}$ يرمز للمقابل العددي لمحرف النص المشفر.

ملاحظة: الفرق الوحيد بين شيفرات عائلة فيجينير هو توليد مفتاح التشفير ولكن تابع التشفير وتابع فك التشفير نفسها في الطرائق الثلاثة.

4.2 الأعداد المحتملة لتحويلات بعض التوابع العددية

قام الباحثان Hari Om وRahul Patwa في [9] بدراسة الأعداد الكلية المحتملة لتحويلات تابع أفاين(Affine) فقط، التي من خلالها يتم حساب الأعداد المحتملة الكلية اللازمة لكسر مفاتيح شيفرة تابع أفاين(Affine)، وتجدر الإشارة هنا إلى أنه تم حساب الأعداد الكلية المحتملة لتحويلات تابع شيفرة أفاين(Affine) بطريقة غير دقيقة. بين الباحثان أن العدد الكلي من الأعداد المحتملة لتحويلات تابع أفاين(Affine) من أجل k محرف هو $n^k.\varphi(n)^k$ في حين أننا وجدنا أن العدد الصحيح هو $n^k.\varphi(n^k)$.

سنبين ذلك من خلال دراسة الأعداد الكلية المحتملة لتحويلات بعض التوابع التشفيرية ومن ضمنها تابع شيفرة أفاين(Affine) ثم الأعداد المحتملة الكلية اللازمة لكسر مفاتيح تشفير هذه التوابع. لسهولة حساب الأعداد المحتملة لتحويلات بعض التوابع العددية، نفرض سلسلة النص الأصلي $X = x_1x_2 \dots x_k$ مكونة من k محرف. لنعرف التابع $h : \mathbb{N} \to \mathbb{N}\ ; h(k) = v$، حيث v العدد الكلي من الأعداد المحتملة لتحويلات التابع المدروسة، k عدد محارف النص الأصلي. بناءً على ذلك، لندرس فيما يلي الأعداد المحتملة للتحويلات والأعداد المحتملة الكلية اللازمة لكسر مفاتيح بعض التوابع التشفيرية.

4.2.1 الأعداد المحتملة لتحويل تابع شيفرة قيصر

من أجل محرف واحد فإننا نأخذ العدد الطبيعي (3) مرة واحدة ومنه العدد المحتمل لتحويلات تابع قيصر هو 1.

من أجل محرفين فإننا نأخذ العدد الطبيعي (3) مرتين وعلية يكون العدد المحتمل لتحويلات تابع قيصر هو 1.

وبما أن النص الأصلي X مكونة من k محرف، فمن أجل المحرف k نأخذ العدد الطبيعي (3) k مرة والعدد المحتمل لتحويلات تابع قيصر هو1.

أي أن العدد الكلي من الأعداد المحتملة لتحويلات التابع من أجل k محرف هي:

$$h(k) = 1 \quad \dots (1$$

تطبق تابع شيفرة قيصر على كامل النص الأصلي[8]. بناءً على ذلك لحساب الأعداد المحتملة الكلية اللازمة لكسر هذه الشيفرة، نعوض $k = 1$ في العلاقة (1) فنجد أن $h(1) = 1$. أي من أجل كشف النص الأصلي نحتاج إلى مفتاح واحد محتمل فقط. بأسلوب مشابه نجد أن كلاً من دالتي شيفرة أتباش وROT13 تعطيان نفس العدد الكلي من الأعداد المحتملة الكلية لتحويلات تابع قيصر ونفس الأعداد المحتملة الكلية اللازمة لكسر مفتاح شيفرة قيصر.

4.2.2 الأعداد المحتملة لتحويل تابع شيفرة أفاين

من أجل محرف واحد فإننا نستطيع أخذ b أي عدد طبيعي أقل من n :

$$b \in \{0,1,2, \dots, n-1\}$$

كما نستطيع أخذ a أي عدد طبيعي أقل من n و أولي نسبياً مع n أي:

$$a \in \{x: 0 < x < n \,;\, \gcd(x,n) = 1\}$$

وبذلك يكون عدد الأعداد المحتملة الكلية لتحويلات تابع شيفرة أفاين هي $n.\varphi(n)$.

ومن أجل محرفين[9] فإن:

$$b \times b \in \{0,1,2, \dots, n-1\} \times \{0,1,2, \dots, n-1\}$$

و a يمكن أن يأخذ الأعداد:

$$a \times a \in \{x: 0 < x < n \,;\, \gcd(x,n) = 1\} \times \{x: 0 < x < n \,;\, \gcd(x,n) = 1\}$$

ويكون عدد الأعداد المحتملة الكلية لتحويلات تابع شيفرة أفاين المحتملة هي:

$$n^2.\varphi(n)^2.$$

وبما أن النص الأصلي X مكونة من k محرف، فمن أجل k محرف يكون عدد الأعداد المحتملة الكلية لتحويلات تابع أفاين هي:

$$n^k.\varphi(n)^k$$

أي أن العدد الكلي من الأعداد المحتملة لتحويلات التابع من أجل k محرف هو:

$$h(k) = n^k.\varphi(n)^k \quad \dots (2$$

[8] يتم تشفير كامل النص الأصلي دفعة واحدة بشيفرة قيصر

[9] بفرض المحارف مستقلة عن بعضها البعض

تطبق تابع شيفرة أفاين أيضاً على كامل النص الأصلي. بناءً على ذلك لحساب الأعداد المحتملة الكلية اللازمة لكسر هذه الشيفرة نعوض $k = 1$ في العلاقة (2) فنحصل على:

$$h(1) = n.\varphi(n)$$

أي من أجل كشف النص الأصلي نحتاج إلى $n.\varphi(n)$ مفتاح(عدد) محتمل.

4.2.3 عدد المحارف المحتملة الكلية لتحويلات تابع عائلة شفرات فيجينير

لنفرض أن النص المفتاحي $Y = y_1y_2 \dots y_t$ في عائلة شفرات فيجينير مكون من t محرف. وبما أن النص الأصلي X مكونة من k محرف. بأسلوب مشابه لما سبق نجد أن عدد المحارف المحتملة الكلية لتحويلات تابع عائلة شفرات فيجينير من أجل k محرف هي $h(k) = n^k$ ... (3

تطبق تحويلات مختلفة على تابع عائلة شفرات فيجينير وتعتمد على طريقة التعامل مع المفتاح(طويلة – تلقائية – كاملة).

من أجل حساب العدد المحتمل الكلي من المحارف المحتملة لكسر المفتاح النصي[10] لعائلة شفرات فيجينير نميز الحالات:

1. **طريقة فيجينير الكاملة** : نعوض $k = t$ (عدد محارف المفتاح) في العلاقة (3) فنحصل على: $h(t) = n^t$

   أي من أجل كشف النص الأصلي نحتاج إلى n^t محرف محتمل.

2. **طريقة فيجينير تلقائية المفتاح** : نعوض $k = t$ في العلاقة (3) فنجد:

$$h(t) = n^t$$

   أي من أجل كشف النص الأصلي نحتاج إلى n^t محرف محتمل.

3. **في طريقة فيجينير طويلة المفتاح** : يكون طول المفتاح النصي مساوياً لطول النص الأصلي k ، وبالتالي: $h(k) = n^k$

أي من أجل كشف النص الأصلي نحتاج إلى n^k محرف محتمل.

يمكن ملاحظة أن المحارف المحتملة الكلية لكسر المفتاح النصي في طريقة فيجينير طويلة المفتاح أكبر من المحارف المحتملة الكلية لكسر المفتاح النصي في كلا طريقتي فيجينير الكاملة وتلقائية المفتاح.

[10] كسر المفتاح النصي يعني كسر الشيفرة أو بمعنى أخر كشف النص الأصلي

بأسلوب مماثل يمكن الحصول من عدد الأعداد الكلية المحتملة من التحويلات، التي يمكن من خلالها حساب عدد الأعداد المحتملة الكلية اللازمة لكسر مفاتيح تشفير بعض التوابع العددية، كما هو موضح في الجدول 2.

الجدول 2 :العدد المحتمل من التحويلات والأعداد الكلية اللازمة لكسر مفاتيح التشفير

الشيفرة	الأعداد المحتملة الكلية من التحويلات	الأعداد المحتملة الكلية اللازمة لكسر مفاتيح الشيفرة
RSA	$\varphi(\varphi(n))^s$	$\varphi(\varphi(n))$
الضرب	$\varphi(n)^s$	$\varphi(n)$
الإزاحة	n^s	n
RSA-Affine	$n^s\varphi(n)^s\varphi(\varphi(n))^s$	$n.\varphi(n)\varphi(\varphi(n))$

4.3 مقارنة الأعداد المحتملة الكلية اللازمة لكسر مفاتيح تشفير بعض التوابع العددية

سنقوم بتقييم بعض خوارزميات التشفير المحولة الى توابع عددية عن طريق استخدام الأعداد المحتملة الكلية اللازمة لكسر مفاتيح التشفير، حيث أجرينا عملية المقارنة بين بعض خوارزميات التشفير العددية مرتبة بشكل تصاعدي عن طريق الأعداد المحتملة الكلية اللازمة لكسر مفاتيح التشفير، كما في الجدول 3 التالي.

الجدول 3 : مقارنة الأعداد المحتملة الكلية لكسر مفاتيح التشفير لبعض توابع التشفير العددية

الشيفرة		الأعداد المحتملة الكلية اللازمة لكسر مفاتيح التشفير
قيصر–أتباش–ROT13		1
RSA		$\varphi(\varphi(n))$
الضرب		$\varphi(n)$
الإزاحة		n
أفاين		$n.\varphi(n)$
RSA-Affine		$n.\varphi(n)\varphi(\varphi(n))$
فيجينير	الكاملة	n^t
	تلقائية المفتاح	n^t
	طويلة المفتاح	n^k

من خلال الجدول 3، نلاحظ ما يلي:

1. لتابع شيفرة فيجينير طويلة المفتاح عدد أكبر من الأعداد المحتملة الكلية اللازمة لكسر مفتاح تشفيرها من الأعداد المحتملة الكلية لكسر مفتاح تشفير باقي التوابع المذكورة.
2. لتابع شيفرة أفاين عدد أكبر من الأعداد المحتملة الكلية اللازمة لكسر مفتاح شيفرتها من الأعداد المحتملة الكلية اللازمة لكسر مفتاح شيفرة كل من تابعي شفرتي الضرب والإزاحة، علماً أن تابع أفاين يمثل تابع مركبة من تابع شيفرة الإزاحة وتابع شيفرة الضرب.
3. للتابع المركب RSA-Affine عدد أكبر من الأعداد المحتملة الكلية اللازمة لكسر مفتاح تشفيرها من الأعداد المحتملة الكلية للازمة لكسر مفتاح التوابع التي تم تركيبها (RSA وAffine).
4. الأعداد المحتملة الكلية للازمة لكسر مفاتيح كل من تابعي شيفرة فيجينير الكاملة وتلقائية المفتاح يعتمد على طول المفتاح النصي المختار.

يمكننا أيضاً ملاحظة أن الأعداد المحتملة الكلية اللازمة لكسر مفاتيح التشفير تزداد بزيادة عدد المحارف n أي بتوسيع جدول المقابلات العددي.

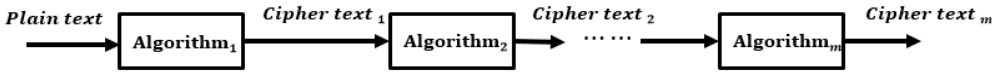
بناءً على كل ما سبق قمنا بتوسيع جدول المقابلات العددي. كما اقتراحنا فكرة تركيب التوابع في الفقرات اللاحقة.

4.4 الحروف ومقابلاتها العددية

قمنا بالبحث عن آلية جديدة من أجل توسيع جدول المقابلات العددي. تمكنا عن طريق برنامج Excel 2016 من نافذة صيغ بالحصول على محارف ASCCII وبعض الرموز الأخرى التي يمكن استخدام البعض منها في التشفير عن طريق تعليمة UNICHAR(.) للإنتقال إلى المحارف الموجودة. وشكّلنا من مخرجات تلك التابع الجدول (2) جدول مقابلات عددي أسميناه بجدول المقابلات العددي المعدل في الملحق.

4.5 التشفير باستخدام تركيب التوابع العددية

بهدف الإستفادة من مزايا الطرائق المذكورة وزيادة الأعداد المحتملة لكسر الشيفرة، طرحنا فكرة تركيب التوابع. في عملية تركيب التوابع نقوم بتشفير النص الأصلي (plain text) بالتابع التشفيري الأول فنحصل على النص المشفر الأول ويتم تشفير هذا النص المشفر بالتابع التشفيري الثاني فنحصل على النص المشفر الثاني ويتم تشفير هذا النص المشفر الثاني بالتابع التشفيري الثالث فنحصل على النص المشفر الثالث وهكذا... تتم العملية لتشكل النص المشفر النهائي ويعبر عن ذلك بالشكل 2.



الشكل 2: التشفير المركب.

بما أن التوابع التشفيرية هي توابع تقابل (غامرة ومتباينة) بشكل عام [2]. بما أن ناتج تركيب توابع متباينة هي تابع متباينة وناتج تركيب توابع غامرة هي تابع غامرة، وبالتالي فإن التوابع الناتجة عن تركيب توابع تشفيرية هي توابع تشفيرية حكماً. يمكن التعبير عن ذلك عددياً على الشكل التالي: إذا كان لدينا سلسلة النص الأصلي $X = \grave{x}_1\grave{x}_2 \dots .\grave{x}_n$، حيث $\grave{x}_i \; ; i = 1,2, \dots , n$ المقابلات العددية للمحارف $x_i \; ; i = 1,2, \dots , n$ على الترتيب والتوابع التشفيرية $f_k(x_i) \; ; k = 1,2, \dots , m \& i = 1,2, \dots , n$ فإنه يمكن أجراء عملية التشفير باستخدام تركيب التوابع كما يلي:

$$y_i = h(x_i) = f_m{}^{\circ} f_{m-1}{}^{\circ} f_{m-2}{}^{\circ} \dots {}^{\circ} f_2{}^{\circ} f_1(x_i) = f_m\big(f_{m-1}(f_{\dots}(\dots f_1(x_i)))\big)$$

لتسهيل عملية تركيب التوابع التشفيرية. قمنا ببرهان النتيجة التالية.

4.6 نتيجة

بفرض أن a_1, a_2 عددان صحيحان وبفرض أنop يمثل أحد العمليات $+, -, \times$ ،عندها يحقق التحويل قياس n العلاقة:

$$(a_1 mod\ n \ \text{op}\ a_2) mod\ n = (a_1 \text{op}\ a_2) mod\ n$$

الاثبات

لننطلق من الطرف الأول:

$$l_1 = (a_1 mod\ n \ \text{op}\ a_2) mod\ n$$

بالاعتماد على المبرهنة (3.7) ينتج:

$$l_1 = [((a_1 mod\ n) mod\ n) \text{op} (a_2 mod\ n)] mod\ n$$

ولكن: $a_1 \equiv a_1 mod\ n$ وبالتالي ينتج:

$$l_1 = [(a_1 mod\ n) \text{op} (a_2 mod\ n)] mod\ n$$

وحسب المبرهنة (3.7) ينتج:

$$l_1 = (a_1 \text{op}\ a_2) mod\ n = l_2$$

بناءً على ما سبق اقترحنا إحدى طرق التوابع المركبة التي تشكل تعميماً لبعض التوابع التشفيرية في الفقرة التالية.

4.7 الطريقة المقترحة باستخدام تركيب تابع فيجينير مع تابع RSA مع أفاين

ركزت الدراسات مؤخراً على دمج خوارزمية RSA مع خوارزميات تشفير أخرى. ففي [11] قدمت طريقة جديدة تقوم بإجراء تشفير النص تشفيراً أولياً منفصلاً عن خوارزمية RSA ثم دمجها مع خوارزمية RSA للحصول على خوارزمية RSA المدمجة (Mixed RSA Algorithm). في [8] تم دمج طريقتي(RSA) و(Knapsack). بينما اقتراحنا طريقة تقوم بالدمج ولكن بتركيب التوابع التشفيرية. الطريقة التي قمنا باقتراحها تعتمد على تركيب شيفرة فيجينير الكاملة عدداً من المرات c واستخدام هذا العدد بصفته مفتاحاً عاماً، ثم تشفير الناتج باستخدام شيفرة RSA، وأخيراً تشفير ناتج المرحلتين السابقتين باستخدام شيفرة أفاين.

فيما يلي نبين الخطوات الأساسية للخوارزمية المقترحة:

أولاً: توليد المفاتيح

1. اختيار جدول مقابلات عددي للمحارف التي يتم التشفير بها وليكن n عدد محارف ذلك الجدول.
2. حساب $\varphi(n)$
3. إيجاد المفاتيح العامة (key public)

A. نختار $k \in \{1, 2, 3, \ldots, \varphi(n) - 1\}$ ويحقق:

$$\gcd(k, \varphi(n)) = 1$$

ويكون المفتاح العام العددي الاول: $\text{Key}_{\text{public}_1} = (k, n)$

B. نختار المفتاح العام الثاني a يحقق العلاقة: $\gcd(a, n) = 1$ حتى نتمكن من فك التشفير (حتى نضمن ان يكون للعدد a نظير) ويكون المفتاح العام العددي الثاني $\text{Key}_{\text{public}_2} = (a, n)$.

C. نختار المفاتيح العددية العامة الثالث والرابع $c, b \in \mathbb{Z}$

D. نختار المفتاح النصي Y. بالتالي جملة المفاتيح العامة

$$\text{Key}_{\text{public}} = (k, a, b, c, Y, n)$$

4. إيجاد المفتاح الخاص (key private)

نحسب d من العلاقة $d \times k \bmod \varphi(n) = 1$.

ويكون المفتاح الخاص: $\text{Key}_{\text{private}} = (d, n)$

ثانياً: التشفير: يتم وفق العلاقة:

$$z = h(x, y) = (a(x + c.y)^k + b) \bmod n \ldots (5$$

ثالثاً: فك التشفير: يتم وفق العلاقة:

$$x = h^{-1}(y, z) = \left(\left(a^{-1}.(z - b)\right)^d - cy\right) \bmod n \ldots (6$$

مثال تطبيقي

لنوضح خطوات الخوارزمية المقترحة من خلال تشفير النص" Star Gate " بالاعتماد على الجدول المقترح (في الملحق). سنستخدم المفاتيح العددية التالية $a = 3 \;\&\; b = 5 \;\&\; c = 4 \;\&\; k = 5$ والمفتاح النصي" Damascus ".

1. عدد المحارف في الجدول المقترح $n = 619$
2. $\varphi(n) = 618$
3. كما أن: $\gcd(k, \varphi(n)) = \gcd(5,618) = 1$

وبالتالي يوجد المفتاح الخاص d لفك التشفير بحيث يتحقق:

$$d \times k \; mod \; \varphi(n) = 1$$
$$d \times 5 \; mod \; 618 = 1$$
$$d = 371$$

4. بما أن: $\gcd(a, n) = \gcd(3,619) = 1$، يوجد نظير ضربي لفك التشفير بحيث يحقق: $a \times a^{-1} \; mod \; n = 1$

$$3 \times a^{-1} \; mod \; 619 = 1$$
$$a^{-1} = 413$$

نعوض في العلاقتين 5 و6 (في الخوارزمية المقترحة) فنجد أن:

$$z = (3(x + 4y)^5 + 5) \; mod \; 619 \quad \ldots (7$$
$$x = \left(\left(413 \times (z - 5)\right)^{371} - 4y\right) mod \; 619 \ldots (8$$

<u>للتشفير</u>: نضع المقابل العددي للنص الأصلي وفق الجدول المقترح:

	S	t	a	r	G	a	t	e
x_i	138	142	87	137	107	87	142	99

نضع المقابل العددي للنص المفتاحي وفق الجدول المقترح:

	D	a	m	a	s	c	u	s
y_i	96	87	123	87	139	93	144	139

وبتطبيق العلاقة (7) أعلاه نجد أن:

z_i	340	595	420	478	547	331	168	583

نضع المقابل الحرفي للأعداد وفق الجدول المقترح فنجد أن:

z_i	340	595	420	478	547	331	168	583
	⚸	⛏	輪	⚵	♻	⚸	Φ	♂

ومنه النص المشفر: " ⚸⛏輪⚵ ♻⚸Φ♂ ".

لفك التشفير: نضع المقابل العددي للنص المشفر وفق الجدول المقترح:

	⌘	⛏	輪	⍟	♻	⌘	Φ	♂
z_i	340	595	420	478	547	331	168	583

نضع المقابل العددي للنص المفتاحي وفق الجدول المقترح:

	D	a	m	a	s	c	u	s
y_i	96	87	123	87	139	93	144	139

بتطبيق العلاقة (8) نجد أن:

x_i	138	142	87	137	107	87	142	99

نضع المقابل الحرفي للأعداد وفق الجدول المقترح فنجد أن:

138	142	87	137	107	87	142	99
S	t	a	r	G	a	t	e

وبالتالي يكون النص الأصلي هو: " Star Gate ".

4.8 دراسة الحالات الخاصة

إن الخوارزمية المقترحة تشكل تعميماً لبعض التوابع التشفيرية العددية، لأنها تعطي عند اختيار مفاتيح معينة التوابع العددية لبعض الشيفرات، ومنها:

الحالة الأولى: لنأخذ فقط المفتاح $c = 0$ في الطريقة المقترحة فنجد أن علاقتي (التشفير وفك التشفير):

$$z = (a.x^k + b)\ mod\ n$$
$$x = (a^{-1}.(z - b))^d\ mod\ n$$

بأخذ $n = 255$ وجدول ASCII كجدول مقابلات عددية بحذف المحرف الأخير.

هذه التوابع تشكل التشفير باستخدام طريقة $RSA - Affine$ المطورة بالتابع المركبة والتي قدمت في [12].

الحالة الثانية: 1. لنأخذ جدول مقابلات عددية يحوي n محرف.

2. بما أن $k \in \{1, 2, 3, \ldots, \varphi(n) - 1\}$

يمكن اختيار المفتاح $k = 1$ ، لأن : $\forall\, n \in \mathbb{Z} : \gcd(1, n) = 1$

وبالتالي فإن $\forall\, n \in \mathbb{Z} : \gcd(1, \varphi(n)) = 1$

3. حساب d

$$d * k \bmod \varphi(n) = 1 \Longrightarrow d * 1 \bmod \varphi(n) = 1 \Longrightarrow d = 1$$

نعوض في علاقتي (التشفير وفك التشفير) للطريقة المقترحة فنجد أن:

$$z = f(x, y) = (a(x + cy) + b) \bmod n \ldots (9$$

$$x = f^{-1}(z, y) = (a^{-1}(z - b) - cy) \bmod n \ldots (10$$

هنا نميز عدة حالات:

1. باختيار المفاتيح $a = 1 \;\&\; c = 0 \;\&\; b = 3$ تصبح العلاقتان 9 و10:

$$z = f(x) = (x + 3) \bmod n$$

$$x = f^{-1}(z) = (z - 3) \bmod n$$

هذه الأخيرة تمثل التوابع العددية لشيفرة قيصر.

2. باختيار المفاتيح $a = -1 \;\&\; c = 0 \;\&\; b = n - 1$ تصبح العلاقتان 9 و10:

$$z = f(x) = (-x + n - 1) \bmod n$$

$$x = f^{-1}(z) = (-z + n - 1) \bmod n$$

وهي تمثل التوابع العددية لشيفرة أتباش.

3. باختيار المفتاح $c = 0$ في العلاقتان 9 و10 فنجد أن:

$$z = f(x) = (ax + b) \bmod n$$

$$x = f^{-1}(z) = a^{-1}(z - b) \bmod n$$

وتمثل التوابع العددية لشيفرة أفاين.

4. باختيار المفاتيح $a = 1 \;\&\; c = 1 \;\&\; b = 0$ تصبح العلاقتان 9 و10:

$$z = f(x, y) = (x + y) \bmod n$$

$$x = f^{-1}(z, y) = (z - y) \bmod n$$

وتمثل التوابع العددية لشفرات عائلة فيجينير.

5. باختيار المفاتيح $a = 1 \;\&\; c = 0 \;\&\; b = 13$ تصبح العلاقتان 9 و10:

$$z = f(x) = (x + 13) \bmod n$$

$$x = f^{-1}(z) = (z - 13) \bmod n$$

وهي التوابع العددية لـ(ROT13).

6. باختيار المفاتيح $a = 1 \ \& \ c = 0$ فتصبح العلاقتان 9 و10:

$$z = f(x) = (x + b) \ mod \ n \ \forall \ b \in \mathrm{Z}$$
$$x = f^{-1}(z) = (z - b) \ mod \ n$$

وهي التوابع العددية لـشيفرة الإزاحة.

7. باختيار المفاتيح $b = 0 \ \& \ c = 0$ فتصبح العلاقتان 9 و10:

$$z = f(x) = (a.x) \ mod \ n \ ; \gcd(a, n) = 1$$
$$x = f^{-1}(z) = (a^{-1}.z) \ mod \ n$$

وهي التوابع العددية لـشيفرة الضرب.

<u>الحالة الثالثة</u>: باختيار جدول مقابلات عددية للنص الأصلي فقط ، وأخذ المفاتيح التالية $a = 1 \ \& \ b = 0 \ \& \ c = 0$ في الطريقة المقترحة فنجد أن علاقتي (التشفير وفك التشفير):

$$z = x^k \ mod \ n \ ; \ \gcd\big(k, \varphi(n)\big) = 1$$
$$x = z^d \ mod \ n$$

وهي تشكل شيفرة RSA.

4.9 الأعداد المحتملة لكسر مفاتيح الشيفرة المقترحة

ذكر الباحثان Mohamad Nour Shamma وَSamir Karaman في [11] أن عدد المفاتيح اللازمة لكسر الشيفرة بطريقة $\mathrm{RSA} - \mathrm{Affine}$ المطورة هو:

$$NUM(n) = \varphi\big(\varphi(n)\big).\varphi(n).n$$

وهي ذاتها الأعداد المحتملة لكسر مفاتيح الشيفرة التي قمنا باستنتاجها في الفقرة (4.2.3). كما استخدم الباحثان المحارف في نظام ASCII المعدل بحذف المحرف الأخير، وقاما بحساب عدد المفاتيح اللازمة لكسر الشيفرة بطريقة $\mathrm{RSA} - \mathrm{Affine}$ المطورة من أجل محارف ASCII المعدل بحذف المحرف، فنتج لديهما العدد 522240. ننوه هنا أن هذا العدد تم حسابه بشكل غير دقيق، والعدد الفعلي هو 2088960.

يمكن أن نجد بسهولة أن الأعداد المحتملة الكلية لكسر مفاتيح شيفرة الطريقة المقترحة هي $NUM(n) = \varphi\big(\varphi(n)\big).\varphi(n).n^{t+2}$ ، حيث t طول المفتاح النصي.

لنقوم بمقارنة الطريقة المقترحة وطريقة $RSA-Affine$ المطورة من حيث الأعداد المحتملة لكسر مفاتيح التشفير، عن طريق جدول المقابلات المبني على محارف ASCII بحذف المحرف الأخير الذي تم عرضه في [8]، وجدول المقابلات العددي المقترح (بفرض أن لدينا مفتاحاً نصياً طوله $t = 1$)، ينتج لدينا الجدول 4.

الجدول 4: الأعداد المحتملة الكلية لكسر مفاتيح تشفير الخوارزمية المقترحة RSA-Affine

عدد المحارف	الأعداد المحتملة الكلية للازمة لكسر الشيفرة	
n	RSA-Affine	Proposed Algorithm
255	2088960	135834624000
619	78038568	29901335753448

من خلال الجدول 4، نلاحظ ما يلي:

1. الأعداد المحتملة الكلية اللازمة لكسر مفاتيح تشفير الخوارزمية المقترحة من أجل مفتاح نصي بمحرف واحد$(t = 1)$ أكبر بكثير من الأعداد المحتملة الكلية للازمة لكسر مفاتيح تشفير خوارزمية $RSA-Affine$ في حال استخدمنا أي جدول مقابلات عددي[11].
2. جدول المقابلات العددي المقترح زاد الأعداد المحتملة الكلية اللازمة لكسر مفتاح تشفير كلاً من الخوارزميتين بشكل كبير.

يمكننا القول إنه لكسر مفاتيح التشفير بالطريقة المقترحة نحتاج إلى كسر مفاتيح التشفير في خوارزمية RSA-Affine علاوة على ذلك نحتاج كسر مفتاح التشفير الذي يستخدم في خوارزمية فيجينير الكاملة والمفتاح الذي قمنا باقتراحه[12].

[11] محارف ASCII بحذف المحرف الأخير أو جدول المقابلات العددية المقترح

[12] يمثل عدد مرات استخدام خوارزمية فيجينير الكاملة

5. الاستنتاجات

كما هو معروف تم التركيز في الآونة الأخيرة على التشفير بالتوابع العددية. كما تم تحويل بعض خوارزميات التشفير إلى توابع عددية. يمكن من خلال تلك التوابع الوصول إلى خوارزمية تشفير تشكل تعميماً لتلك الخوارزميات. في هذا البحث قدمنا آلية للوصول إلى خوارزميات تشفير جديدة، تعِمم خوارزميات التشفير العددية، وذلك بالاعتماد على فكرة تركيب التوابع. كما قمنا بطرح آلية لتوسيع جدول المقابلات العددية، وقد تمكنا من الحصول على حلول مجدية. بناءً على ما سبق وفي ضوء المناقشة والمقارنة التي قمنا بإجرائها يمكن أن نورد الاتي:

- التوابع التشفيرية المركبة تشكل تعميماً للتوابع التي يتم تركيبها ضمن شروط محددة.
- التوابع التشفيرية المركبة تعطي عدداً أكبر من الأعداد المحتملة الكلية اللازمة لكسر مفاتيح تشفير التوابع التشفيرية التي يتم تركيبها.
- توسيع جدول المقابلات العددي زاد عدد الأعداد المحتملة الكلية اللازمة لكسر مفاتيح التشفير بشكل أكبر.
- عملية التركيب فتحت الباب أمام طرائق جديدة ومتنوعة في التشفير.

6. التوصيات

قمنا بدراسة حالة واحدة من التركيب وبما أن عملية التركيب ليست تبديلية فإنه يمكن التركيب بترتيب آخر، فمثلاً: دراسة تركيب تابع فيجينير الكاملة باستخدام النص المفتاحي Y نفسه $(c-1)$ مرة مع تابع أفاين مع تابع شيفرة RSA. كما يمكن توسيع جدول المقابلات العددي إلى رموز قد تصل إلى حوالي 52800 رمز عن طريق برنامج Excel 2016 من نافذة صيغ عن طريق تعليمة (.)UNICHAR للانتقال إلى الرموز الموجودة. يمكن تعديل مرحلة بناء المفتاح في شفرات عائلة فيجينير والحصول على خوارزميات جديده مشابهه لشفرات عائلة فيجينير من حيث عمليتي التشفير وفك التشفير. يمكن استخدام نوع آخر من التركيب وهو تركيب التوابع التي تتعامل مع المعاملات المنطقية مثل XOR وعمليات الإزاحة shift. كما يمكن تطبيق عملية التركيب على

نوعين من التوابع التشفيرية الأولى عددية والثانية تتعامل مع المعاملات المنطقية مثل XOR وعمليات الإزاحة shift بترتيب محدد.

7. المراجع:

[1] ABDALREHEM, W., (2007). Introduction in Classical Cryptographic. Al Masirah House for Publishing and Distribution and Printing, Second Printing, Jordan, pp:119.

[2] AL-KAMHA, R., SHAMMA, M.N., NADAWI, M., (2018). Study the Conversion of some Classical Cryptographic Algorithms into Numerical Functions. Master Thesis, Damascus University, Damascus.

[3] AL-NAJJAR, H., SHAAR, A., AL-MOHAMMAD, M., (2011). Investigating an Improvement on AES Through using EC Mathematics in its Transformation. PhD Thesis, Aleppo University, Aleppo.

[4] HAMANDOUSH, M., DABABSH, M., DABABO, D., (2020) use Complex Mathematical Minions and Apply Encryption Algorithms in Literal Strings based on Mathematical Modeling. Tishreen University Journal for Research and Scientific Studies - Basic Sciences Series, Vol. 24 No.2, PP:91-100.

[5] HIDAREY, R., DAHER, M., (2018). Develop Algorithm RSA of Ensure Authentication and Smooth Flow Data. Journal of Hama University vol.1, pp:53-66.

[6] Järpe, E., (2020). An Alternative Diffie-Hellman Protocol. Journal cryptography. pp:1-10.

[7] KOBLITS, N., (1994)- A Course in Number Theory and Cryptography, Springer- Varlag.

[8] MOHAMMAD, K.S., HUSSEIN, A., (2014). Hybrid Public-Key Cryptosystem. Journal of Al-Turath University College, Vol.16 pp: 1-9.

[9] OM, H., PATWA, R., (2008). Affine Transformation in Cryptography. Journal of Discrete Mathematical Sciences and Cryptography, Vol:11, pp: 59-65.

[10] SAREM, A., (2020). Improving RSA Encryption Algorithm and Applying it in Digital Signal Processing. Master Thesis, Tishreen University, Lattakia.

[11] SHAMMA ,M.N. , KARAMAN, S., (2018) Encryption using RSA_Affine Function $f(x) = (a\,x^e + b) mod\ (n)$,Journal of Natural Sciences and Mathematics (jnm) ,Vol.40 No.27,pp: 41-53.

[12] SHAMMA, M.N., AL-KHATIB, A., (2016) The Encryption using Special Pythagorean Function, Journal of Natural Sciences and Mathematics (jnm) Vol.38 No.12, pp:113-131.
[13] SHAMMA, M.N., AL-LAHAM, M., (2017). Merging Cryptography for Broadcast Letters by Social Media. Master Thesis, Syrian Virtual University, Damascus.
[14] VENKATESWARAN, R., SUNDARAM, V., (2010), Information Security: Text Encryption and Decryption with Poly Substitution Method and Combining the Features of Cryptography, International Journal of Computer Applications, Vol.3 No. 7, pp: 28-31.

المُلحق

يتضمن هذا المُلحق بعض المحارف التي تمكنا من الحصول عليها عن طريق برنامج Excel 2016 من نافذة صيغ، عن طريق تعليمة (.)UNICHAR للانتقال إلى المحارف الموجودة. كما شكّلنا من مخرجات تلك التابع جدول دعوناه بجدول المقابلات العددي المعدل (الجدول 2).

الجدول2 : جدول المقابلات العددي المعدل.

الرمز	المقابل العددي	الرمز	المقابل العددي	الرمز	المقابل العددي	الرمز	المقابل العددي	الرمز	المقابل العددي
♔	508	克	381	Ꚍ	254	o	127	✍	0
♕	509	出	382	Ꚏ	255	ô	128	✾	1
♖	510	勒	383	Ꚑ	256	Ö	129	✿	2
♗	511	吉	384	Ꚓ	257	Œ	130	❀	3
♘	512	名	385	Ꚕ	258	œ	131	!	4
♙	513	含	386	Ꚗ	259	P	132	ⵣ	5
♚	514	吾	387	Ꚙ	260	p	133	#	6
♛	515	哦	388	Ꚛ	261	Q	134	$	7
♜	516	場	389	ꚝ	262	q	135	%	8
♝	517	娜	390	ꚟ	263	R	136	&	9
♞	518	字	391	ꚡ	264	r	137	(	10
♟	519	尔	392	ꚣ	265	S	138	)	11
♠	520	尺	393	ꚥ	266	s	139	*	12
♡	521	屁	394	ꚧ	267	Ș	140	,	13
♢	522	平	395	ꚩ	268	T	141	،	14
♣	523	开	396	ꚫ	269	t	142	.	15
♤	524	弗	397	ꚭ	270	™	143	/	16
♥	525	德	398	ꚯ	271	u	144	:	17
♦	526	提	399	ꚱ	272	U	145	;	18
♧	527	斯	400	ꚳ	273	Ù	146	?	19
♨	528	杰	401	ꚵ	274	Û	147	@	20
♩	529	東	402	ꚷ	275	Ü	148	[	21
♪	530	比	403	ꚹ	276	Ü	149	ⵛ	22
♫	531	治	404	ꚻ	277	v	150	]	23
♬	532	漢	405	ꚽ	278	V	151	^	24
♭	533	煙	406	ꚿ	279	w	152	_	25

26	`	153	W	280	ሜ	407	片	534	ᛋ
27	{	154	x	281	ም	408	直	535	ᛐ
28	|	155	X	282	ሞ	409	私	536	ᛏ
29	}	156	y	283	ሟ	410	维	537	ᛏ
30	~	157	Y	284	ሠ	411	艾	538	♲
31	¦	158	z	285	ሡ	412	草	539	♲
32	¨	159	Z	286	ሢ	413	莨	540	♲
33	¯	160	Б	287	ሣ	414	表	541	♲
34	´	161	Ж	288	ሤ	415	西	542	♲
35	¸	162	З	289	ሥ	416	诶	543	♲
36	¸	163	И	290	ሦ	417	豆	544	♲
37	¦	164	Й	291	ሧ	418	贝	545	♲
38	?	165	К	292	ረ	419	贼	546	♲
39	‘	166	Л	293	ሩ	420	輪	547	♻
40	’	167	П	294	ሪ	421	迪	548	♻
41	,	168	Ф	295	ራ	422	送	549	♻
42	“	169	Ц	296	ሬ	423	金	550	♾
43	”	170	Ч	297	ር	424	马	551	♿
44	„	171	Ш	298	ሮ	425	魚	552	⊡
45	‹	172	Щ	299	ሯ	426	➳	553	⊡
46	›	173	Ъ	300	ሰ	427	➘	554	⚃
47	¢	174	Ы	301	ሱ	428	➵	555	⚃
48	£	175	Э	302	ሲ	429	➶	556	⚃
49	¤	176	Ю	303	ሳ	430	➘	557	⚅
50	¥	177	Я	304	ሴ	431	➵	558	⊙
51	€	178	ウ	305	ስ	432	➶	559	⊙
52	ॐ	179	う	306	ሶ	433	→	560	●
53	+	180	キ	307	ሷ	434	➙	561	●
54	<	181	き	308	ሸ	435	➵	562	⚐
55	=	182	ギ	309	ሹ	436	➽	563	⚑
56	>	183	ぎ	310	ሺ	437	⇛	564	⚒
57	±	184	ク	311	ሻ	438	☀	565	⚓
58	«	185	コ	312	ሼ	439	☁	566	⚔
59	»	186	こ	313	ሽ	440	☂	567	⚕
60	×	187	シ	314	ሾ	441	☃	568	☔
61	÷	188	し	315	ሿ	442	☄	569	⚗
62	§	189	す	316	ቀ	443	★	570	⚘
63	©	190	ソ	317	ቁ	444	☆	571	⚙

64	¬	191	バ	318	ቂ	445	☇	572	⚕
65	®	192	ば	319	ቃ	446	☈	573	⚛
66	°	193	フ	320	ቄ	447	☉	574	⚜
67	µ	194	マ	321	ቅ	448	☊	575	⚝
68	¶	195	み	322	ቆ	449	☋	576	⚞
69	·	196	も	323	ቇ	450	☌	577	⚟
70	…	197	ヨ	324	ቈ	451	☍	578	⚠
71	†	198	よ	325	ቊ	452	☎	579	⚡
72	‡	199	ラ	326	ቋ	453	☏	580	⚢
73	•	200	リ	327	ቌ	454	☔	581	⚣
74	‰	201	り	328	ቍ	455	☕	582	⚤
75	○	202	ロ	329	ቐ	456	☖	583	⚥
76	¼	203	ワ	330	ቑ	457	☗	584	⚦
77	½	204	わ	331	ቒ	458	☘	585	⚧
78	¾	205	ン	332	ቓ	459	☙	586	⚨
79	২	206	ん	333	ቔ	460	☚	587	⚩
80	৩	207	ء	334	ቕ	461	☛	588	⚽
81	৫	208	ا	335	ቖ	462	☜	589	⚾
82	৬	209	إ	336	ቘ	463	☝	590	⚿
83	৭	210	أ	337	ቚ	464	☞	591	☸
84	৮	211	آ	338	ቛ	465	☟	592	☹
85	৯	212	ب	339	ቜ	466	☠	593	☺
86	A	213	پ	340	ቝ	467	☡	594	☻
87	a	214	ة	341	በ	468	☢	595	⛏
88	à	215	ت	342	ቡ	469	☣	596	⛐
89	â	216	ٹ	343	ቢ	470	☤	597	⛑
90	B	217	ث	344	ባ	471	☥	598	⛒
91	b	218	ج	345	ቤ	472	☦	599	⛓
92	C	219	چ	346	ብ	473	☧	600	⛔
93	c	220	ح	347	ቦ	474	☨	601	⛕
94	ç	221	خ	348	ቧ	475	☩	602	⛗
95	Ç	222	د	349	ቨ	476	☪	603	⛟
96	D	223	ڈ	350	ቩ	477	☫	604	⛱
97	d	224	ذ	351	ቪ	478	☬	605	⛲
98	E	225	ر	352	ቫ	479	☭	606	⛳
99	e	226	ڑ	353	ቬ	480	☮	607	⛴
100	é	227	ز	354	ቭ	481	☯	608	⛵
101	è	228	ژ	355	ቮ	482	◌	609	⛷
102	ê	229	س	356	ቯ	483	◍	610	⛸

103	ë	230	ش	357	ሥ	484	◎	611	🚸
104	F	231	ص	358	ሦ	485	●	612	🛴
105	f	232	ض	359	ሧ	486	◐	613	🚲
106	*f*	233	ط	360	ረ	487	◑	614	🛩
107	G	234	ظ	361	ሩ	488	◒	615	🚘
108	g	235	ع	362	ሪ	489	◓	616	🚚
109	Ğ	236	غ	363	ራ	490	◔	617	🚛
110	H	237	ف	364	ሬ	491	◕	618	🚜
111	h	238	ق	365	ር	492	◖		
112	I	239	ك	366	ሮ	493	◗		
113	i	240	ک	367	ሯ	494	◘		
114	î	241	گ	368	ሰ	495	◙		
115	ï	242	ل	369	ሱ	496	◚		
116	J	243	م	370	ሲ	497	◛		
117	j	244	ں	371	ሳ	498	⛽		
118	K	245	ن	372	ሴ	499	◜		
119	k	246	⏭	373	ስ	500	◝		
120	L	247	ه	374	ሶ	501	◞		
121	l	248	و	375	ሷ	502	◠		
122	M	249	ۇ	376	ሸ	503	◡		
123	m	250	ى	377	ሹ	504	◢		
124	N	251	ي	378	ሺ	505	◣		
125	n	252	ے	379	ሻ	506	◤		
126	O	253	ئ	380	ሼ	507	◥		

استخدام قانون التحويل التنسوري في التشفير

الباحث الدكتور: باسل حمدو العرنوس

مدرّس في قسم الرياضيات – كليّة العلوم – جامعة البعث

الملخص

قمنا في هذا البحث باستخدام التّحليل التّنسوري في التشفير، وذكرنا التعاريف الأساسيّة اللازمة لذلك، وعرّفنا ترتيب مركّبات تنسور، وتطابق التّنسورات بالمقاس n.

أثبتنا أنّ تشفير كل نص واضح P (من الحروف ASCII) من خلال استخدام قانون التّحويل التّنسوري بالمفتاح $C\left(C_n,p,q\right)$ يتم بشكلٍ وحيد. و أنّ فك التتشفير عن كل نص مشفّر C (من الحروف ASCII) من خلال استخدام قانون التّحويل التّنسوري بالمفتاح $C\left(C_n,p,q\right)$ يتم بشكلٍ وحيد.

الكلمات المفتاحيّة:

تنسور – قانون التحويل التنسوري – مصفوفة هل – مفتاح التشفير – تشفير – النّص الواضح – النّص المشفّر.

Using The Law of Transformation Tensor in Cryptography

.Dr. Basel Hamdo Al-Arnous

Department Of Mathematics - Faculty of Sciences - Al- Baath University

Abstract

We used in this paper Tensor analysis in cryptography and mentioned some fundamental definitions as the order of tensor components and congruence of tensors mod n.

we proved that the cryptography of any clear text P from ASCII characters , using the law of tensor transformation by a key $C\left(C_n, p, q\right)$, is unique. we can decrypt any encrypted text C from ASCII characters using the law of tensor transformation by a key $C\left(C_n, p, q\right)$ in a unique manner.

Key Words:

Tensor - Law of Transformation Tensor – Hill matrix - The Cryptography key – Cryptography - Plaintext ,Ciphertext .

1.مقدّمة

يُقصد بالتّشفير هو ذلك العلم الذي يدرس تحويل الرّسائل والمعلومات إلى شكل، غير قابل للفهم من قبل جميع الأشخاص غير المصرّح لهم. وبالتّالي فهو عمليّة إخفاء المعلومات باستخدام الخوارزميّات ومفاتيح سريّة [3−1].

يتطوّر علم التّشفير باستمرار من حيث الآليّة المستخدمة في التّشفير، ودرجة التّعقيد التي تجعل الشّيفرة أكثر أماناً.

نقوم في هذا البحث على تطوير طريقة هيل [9],[1] في التّشفير بالاعتماد على جدول الـ$ASCII$، حيث تعتمد طريقة هيل على مفتاح وهو عبارة عن مصفوفة A من المرتبة $n \times n$ محدّدها أوّليّ نسبيّاً مع 256 (عدد عناصر جدول الـ$ASCII$). وتتلخّص الطّريقة بالخطوات الآتية.

- تُرتّب حروف ورموز النّص الأصلي في مصفوفة X من المرتبة $n \times k$.
- تُقابل الحروف والرّموز بما يقابلها من جدول $ASCII$.
- تُضرب المصفوفة النّاتجة بالمصفوفة A بالمقاس 256.
- تُرجع الأرقام إلى ما يُقابلها من حروف أو رموز في جدول $ASCII$ للحصول على النّص المشفّر.

قمنا باستبدال المصفوفة X بتنسور، وبدلاً من الضّرب بالمفتاح قمنا باستخدام قانون التّحويل التّنسوري من قاعدة إلى أخرى، وذلك من خلال مصفوفة الانتقال، ومن ثمّ الحصول على النّص المشفّر.

2. هدف البحث

يهدف البحث إلى استخدام قانون التّحويل التّنسوري في الحصول على النّص المشفّر، ودراسة قابليّة العكس بحيث نحصل على النّص الأصل من نص مشفّر.

3. أهميّة البحث:

تهدف كل طرق التّشفير إلى زيادة أمان الشّيفرة، وتغيير آليّة التّشفير، وتعمل على ذلك باستمرار. لذا فإنّ استخدام مركّبات تنسور ما في التّشفير يحقّق أماناً أعلى ممّا تحقّقه طريقة هيل، نظراً لصعوبة العمليّات الحسابيّة وتعدّد المفاتيح وكثرة الخيارات في اعتماد نوع التّنسور المستخدم.

4. المناقشة و النّتائج

4 – 1: تعاريف أساسيّة: [4,7]

تعريف1:

ليكن n عدداً طبيعيّاً وأكبر تماماً من 1، وليكن $1 \le a < n$ ، نقول عن العدد a إنه أولي نسبياً مع العدد n إذا كان: $\gcd(a,n) = 1$.

تعريف2:

ليكن n عدداً طبيعيّاً وأكبر تماماً من 1، نرمز بالرّمز M_n إلى مجموعة جميع الأعداد الأوّليّة نسبيّاً مع العدد n، أي أنّ:

$$M_n = \{a \in \mathbb{Z} ; 1 \le a < n \ , \ \gcd(a,n) = 1\}$$

تعريف3:

مصفوفة هيل: هي مصفوفة عدديّة مربّعة من المرتبة k $\left(k \in \mathbb{N}^{*}\right)$ نرمز لها بالرّمز C_k، وتحقّق:

$$\det\left(C_k\right) \in M_{256} \qquad (1)$$

مثال1:

إنّ المصفوفة $\begin{pmatrix} 4 & 3 \\ 1 & 4 \end{pmatrix}$ هي مصفوفة هيل، بينما $\begin{pmatrix} 4 & 2 \\ 0 & 4 \end{pmatrix}$ ليست كذلك.

تعريف 4:[10]

لتكن $W, V_1, \ldots, V_s$ فضاءات متّجهيّة حقيقيّة ، نسمّي التطبيق :

$$F : V_1 \times \ldots \times V_s \to W$$

متعدّد الخطيّة إذا كان F خطيّاً بالنسبة لكل مركّبة.

ملاحظة 1:

سنتعامل مع ترميز آينشتاين للتّنسورات، وهو ترميز يهدف إلى تبسيط التّعبير عن مجموع، حيث نقوم بالاستغناء عن الرّمز Σ . وعلى سبيل المثال:

$$x^i e_i = \sum_{i=1}^{n} x^i e_i$$

تعريف 5: [10]

ليكن V_n فضاءً متّجهيّاً حقيقيّاً ، و V_n^{*} فضاءه الثنوي، و ليكن p,q عددين صحيحين موجبين، بحيث $(p,q) \neq (0,0)$ ، نسمّي تنسوراً من النوع $\begin{pmatrix} p \\ q \end{pmatrix}$ فوق

الفضاء V_n ، أيّة متعدّد الخطيّة:

$$T : (V_n)^p \times (V_n{}^*)^q = V_n \times ... \times V_n \times V_n{}^* \times ... \times V_n{}^* \to \square$$

معرّفة بالشكل:

$$\begin{aligned} T(x_1,...,x_p,\xi^1,...,\xi^q) &= T(x_1^{\,j_1} e_{j_1},...,x_p^{\,j_p} e_{j_p},\xi_{i_1}^1 e^{i_1},...,\xi_{i_q}^q e^{i_q}) \\ &= T(e_{j_1},...,e_{j_p},e^{i_1},...,e^{i_q}) x_1^{\,j_1} ... x_p^{\,j_p} .\xi_{i_1}^1 .. \xi_{i_q}^q \\ &= T_{j_1...j_q}^{i_1...i_p} x^{j_1} ... x^{j_p} \xi_{i_1} ... \xi_{i_q} \end{aligned} \qquad (2)$$

حيث $\left(i = \overline{1,p}\right) x_i = x_i^{\,j_1} e_{j_1}$ متجهات من V_n و $\left(j = \overline{1,q}\right)$ $\xi^j = \xi_{j_1}^j e^{j_1}$ أشكال خطية من $V_n{}^*$ شريطة أن تكون الدالة T خطيّة في كل متغير.

نسمي الأعداد $T_{j_1...j_q}^{i_1...i_p}$ مركبات التنسور T بالنسبة للقاعدة (e_i) ، وكما هو واضح أنَّ عددها n^{p+q}.

نسمي العدد p مرتبة مخالف التغير ، والعدد q مرتبة موافق التغير.

4 – 2: قانون التّحويل التّنسوري: [10]

ليكن T تنسوراً من النّوع $\begin{pmatrix} p \\ q \end{pmatrix}$ في الفضاء V_n، مرّكّباته من الشّكل: $T_{j_1...j_q}^{i_1...i_p}$ في القاعدة (e_i)، ولتكن $(e_{i'})$ قاعدة جديدة للفضاء المذكور، بحيث تكون المصفوفة C_j^i : مصفوفة الانتقال من القاعدة (e_i) إلى القاعدة $(e_{i'})$. عندئذٍ تكون مركّبات التّنسور T بالنّسبة للقاعدة الجديدة، هي من الشّكل:

$$T'^{\,k_1...k_p}_{\,l_1...l_q} = T_{j_1...j_q}^{i_1...i_p} C_{l_1}^{j_1} ... C_{l_q}^{j_q} .B_{i_1}^{k_1} ... B_{i_p}^{k_p} \qquad (3)$$

حيث B_j^i هي مصفوفة الانتقال من القاعدة $(e_{i'})$ إلى القاعدة (e_i)، إنّ:

$$B_j^i = \left(C_j^i\right)^{-1}$$

نسمي العلاقة **(3)** ، قانون التحويل التنسوريّ وهي تحدّد العلاقة بين مركّبات تنسور بالنسبة لقاعدتين مختلفتين.

إنّ مركبات التنسور $T\begin{pmatrix} p \\ q \end{pmatrix}$ بالنسبة للقاعدة (e_i) هي:

$$T'^{\,i_1\ldots i_p}_{\;j_1\ldots j_q} = T^{\,k_1\ldots k_p}_{\;l_1\ldots l_q}\, B^{\,l_1}_{\;j_1}\ldots B^{\,l_q}_{\;j_q}\, C^{\,i_1}_{\;k_1}\ldots C^{\,i_p}_{\;k_p} \qquad (4)$$

ملاحظة 2:

يتّضح من العلاقة **(3)** أنّه إذا كانت مركبات تنسور معدومة بالنسبة لقاعدة ما ، فإنّها تكون كذلك بالنسبة لأيّة قاعدة أخرى في الفضاء V_n نفسه.

مبرهنة 1: [8]

من أجل أي عددين صحيحين موجبين p,q يوجد في الفضاء V_n ذي القاعدة (e_i) تنسوراً من النوع $\begin{pmatrix} p \\ q \end{pmatrix}$ بالنسبة لهذه القاعدة.

4 – 3: التّطابق

تعريف 6: $[10]$

نقول عن تنسورين T,S إنّهما متساويان، ونكتب اختصاراً $T = S$ ، إذا كانا من النّوع ذاته $\begin{pmatrix} p \\ q \end{pmatrix}$ ومركّباتهما متطابقة بالنّسبة لأي قاعدة مفروضة، فإذا كانت مركّباتهما بالنسبة للقاعدة (e_i) هي على الترتيب: $T^{\,i_1\ldots i_p}_{\;j_1\ldots j_q}$ ، $S^{\,i_1\ldots i_p}_{\;j_1\ldots j_q}$ فنقول إنّهما متطابقان إذا كانت:

$$S_{j_1\dots j_q}^{i_1\dots i_p} = T_{j_1\dots j_q}^{i_1\dots i_p} \qquad (5)$$

لكل $i_1,\dots,i_p, j_1,\dots,j_q$ حيث:

$$1 \le i_k \le n,\ k = 1,\dots,p \quad , \quad 1 \le j_l \le n \quad , \ l = 1,\dots,q$$

نتيجة 1:

نستنتج من العلاقة **(3)** أنَّ خواص تطابق التنسورين المشار إليهما بالتعريف السابق لا تتغير بالانتقال من قاعدة ما إلى أي قاعدة أخرى.

تعريف 7:

ليكن m عدداً طبيعيّاً يحقّق: $m > 1$، وليكن T, S تنسورين من النّوع $\begin{pmatrix} p \\ q \end{pmatrix}$ في الفضاء V_n ، ولنفرض أنّ:

$$S_{j_1\dots j_q}^{i_1\dots i_p}, T_{j_1\dots j_q}^{i_1\dots i_p} \in \square \ ; \ i_1,\dots,i_p, j_1,\dots,j_q \in \{1,\dots,n\}$$

نقول عن التّنسورين T, S إنّهما متطابقان بالمقاس m، ونكتب اختصاراً $T \equiv S \pmod m$ ، إذا كانت مركّباتهما متطابقة بالمقاس m بالنّسبة لأي قاعدة مفروضة، فإذا كانت مركّباتهما بالنسبة للقاعدة (e_i) هي على الترتيب: $T_{j_1\dots j_q}^{i_1\dots i_p}$ ، $S_{j_1\dots j_q}^{i_1\dots i_p}$ فنقول إنّهما متطابقان بالمقاس m، إذا كانت:

$$S_{j_1\dots j_q}^{i_1\dots i_p} \equiv T_{j_1\dots j_q}^{i_1\dots i_p} \pmod m \ ; \quad ; \ i_1,\dots,i_p, j_1,\dots,j_q \in \{1,\dots,n\} \qquad (6)$$

تعريف 8:

ليكن m عدداً طبيعيّاً يحقّق: $m > 1$، وليكن T تنسوراً من النّوع $\begin{pmatrix} p \\ q \end{pmatrix}$ في الفضاء V_n ، ولنفرض أنّ:

$$T_{j_1\dots j_q}^{i_1\dots i_p} \in \square \ ; \ i_1,\dots,i_p, j_1,\dots, j_q \in \{1,\dots,n\}$$

نعرّف **تنسور الممثّلات الرّئيسيّة للتّنسور** T **بالمقاس** m **ونرمز له بالرّمز** ${}^{(m)}T$ بأنّه تنسور من النّوع $\begin{pmatrix} p \\ q \end{pmatrix}$ ويحقّق:

$$\begin{aligned} &1) \quad {}^{(m)}T_{j_1\dots j_q}^{i_1\dots i_p} \in \square_m \ ; \ i_1,\dots,i_p, j_1,\dots, j_q \in \{1,\dots,n\} \\ &2) \quad {}^{(m)}T \equiv T \pmod m \end{aligned} \tag{7}$$

مثال2:

ليكن T تنسوراً من النّوع $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ في الفضاء $\square^2$، حيث:

$$T_1^{\,1} = -312 \ , \ T_1^{\,2} = 425 \ , \ T_2^{\,1} = 211 \ , \ T_2^{\,2} = 1012$$

إنّ تنسور الممثّلات الرّئيسيّة لهذا التّنسور بالمقاس 256 هو التّنسور ${}^{(256)}T$ من النّوع $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$، ومركّباته:

$${}^{(256)}T_1^{\,1} = 200 \ , \ {}^{(256)}T_1^{\,2} = 169 \ , \ {}^{(256)}T_2^{\,1} = 211 \ , \ {}^{(256)}T_2^{\,2} = 244$$

4 – 4: الترتيب

لسهولة العمل بإجراء تقابل بين المحارف ومركّبات تنسور ما، نعتمد طريقة لترتيب مركّبات التّنسور.

تعريف 9:

لتكن $a_1,\dots,a_n,b_1,\dots,b_n$ أعداداً حقيقيّة، نقول إنّ الترتيبة $(a_1,\dots,a_n)$ تأتي بعد الترتيبة $(b_1,\dots,b_n)$، إذا تحقّق أحد الشّرطين الآتيين:

- إذا كان $a_1 > b_1$.
- إذا كان $a_i > b_i$ و $a_j = b_j$ لكل $j < i$ حيث $1 < i \le n$.

مثال3 :

الترتيبة $(2,1,3,4)$ تأتي بعد الترتيبة $(1,5,2,4)$، والترتيبة $(2,1,3,4)$ تأتي بعد الترتيبة $(2,1,2,4)$.

تعريف 10:

ليكن T تنسوراً من النّوع $\begin{pmatrix} p \\ q \end{pmatrix}$ في الفضاء V_n، نقول إنّ المركّبة $T^{i_1 \dots i_p}_{j_1 \dots j_q}$ تأتي بعد المركّبة $T^{r_1 \dots r_p}_{s_1 \dots s_q}$، إذا كانت الترتيبة $(i_1,\dots,i_p,j_1,\dots,j_q)$ تأتي بعد التّرتيبة: $(r_1,\dots,r_p,s_1,\dots,s_q)$

مثال 4:

ليكن T تنسوراً من النّوع $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ في الفضاء $\mathbb{R}^3$، إنّ ترتيب مركّباته هو كالآتي:

$$T^1_{11},T^1_{12},T^1_{13},T^1_{21},T^1_{22},T^1_{23},T^1_{31},T^1_{32},T^1_{33},T^2_{11},T^2_{12},T^2_{13},T^2_{21},T^2_{22},T^2_{23},T^2_{31},T^2_{32},T^2_{33}$$

$$T^3_{11},T^3_{12},T^3_{13},T^3_{21},T^3_{22},T^3_{23},T^3_{31},T^3_{32},T^3_{33}$$

4 – 5: التّنسور المقابل للنّص

4 – 5 – 1 تنسور النّص الواضح:

ليكن لدينا P النص الواضح (Plaintext) المكوّن من α محرفاً، نختار نوع التّنسور T وفقاً لعدد المحارف ولنوع مصفوفة هيل. ثمّ نأخذ المقابل العددي لكل محرف في

النّص من جدول $ASCII$، ونسند هذه الأعداد إلى مركّبات التّنسور المختار بنفس ترتيب المحارف، فنحصل على تنسور النّص الواضح.

4 – 5 – 2 تنسور النّص المشفّر:

ليكن لدينا C النص المشفّر(Ciphertext) المكوّن من α محرفاً، نتّبع نفس الطريقة السّابقة لنحصل على تنسور النّص المشفّر R.

4 – 5 – 3 اختيار نوع التّنسور:

إنّ عدد مركّبات تنسور T من النّوع $\begin{pmatrix} p \\ q \end{pmatrix}$ في الفضاء V_n، هو: n^{p+q}. ليكن P النّص الواضح وعدد محارفه α، ولتكن m هي مرتبة مصفوفة هيل. نختار من بين قوى العدد m أوّل قوّة أكبر أو تساوي α ولتكن m^{β}. عندئذٍ نختار تنسور في الفضاء الذي بُعده m ومن النّوع $\begin{pmatrix} p \\ q \end{pmatrix}$ حيث $p+q=\beta$.

مثال 5:

ليكن لدينا النّص الواضح P هو: $Law-of-Transformation$ ولتكن مصفوفة هيل من المرتبة الثّالثة. واضح أنّ عدد المحارف هو 21 وأوّل قوّة لـ3 أكبر أو تساوي 21 هو القوّة 3^3.

وبالتّالي نأخذ تنسوراً في الفضاء $\square^3$ من أحد الأنواع الآتية:

$$\begin{pmatrix} 0 \\ 3 \end{pmatrix},\begin{pmatrix} 1 \\ 2 \end{pmatrix},\begin{pmatrix} 2 \\ 1 \end{pmatrix},\begin{pmatrix} 3 \\ 0 \end{pmatrix}$$

4 – 6: التشفير باستخدام قانون التّحويل التنسوري

استخدام قانون التّحويل التنسوري

هي إبدال كل حرف ASCII في الرسالة المبثوثة بحرف آخر من ASCII من خلال استخدام قانون التّحويل التّنسوري على تنسور النّص الواضح.

نعتمد في هذه الطّريقة على مصفوفة هيل واعتمادها كمصفوفة انتقال من قاعدة إلى أخرى على تنسور النّص الواضح. لذا يلزمنا من أجل استخدام هذه الطّريقة:

- مصفوفة هيل من المرتبة n .
- نوع التّنسور المستخدم وليكن $\begin{pmatrix} p \\ q \end{pmatrix}$.

فإذا كان عدد حروف النص الأصلي أقل من n^{p+q} نملئ أماكن الحروف الناقصة بالمحرف $(-)$.

تعريف 11:

مفتاح التشفير: نرمز بالرّمز $C(C_n, p, q)$ إلى التشفير باستخدام المصفوفة C_n كمصفوفة انتقال على تنسور النّص الواضح T والذي هو من النّوع $\begin{pmatrix} p \\ q \end{pmatrix}$. ويبقى المفتاح ذاته في العمليّة المعاكسة.

إذا كان T هو تنسور النّص الواضح فإنّ الرّمز $F(T)$ يدل على استخدام قانون التّحويل التّنسوري على التّنسور T للحصول على التّنسور R تنسور النّص المشفّر.

خوارزمية التشفير باستخدام التّحليل التّنسوري:

إذا كان لدينا نص واضح P والمراد تشفيره باستخدام المفتاح $C(C_n, p, q)$:

- نكتب مركّبات تنسور النّص الواضح T مرتّبةً كما بيّنا في التعريف 10، ونسند إليها الأعداد المقابلة لمحارف النّص الواضح في جدول ASCII.
- نستخدم قانون التّحويل التّنسوري على التّنسور T فنحصل على:

$$R = F(T)$$

- نوجد تنسور الممثّلات الرّئيسيّة للتّنسور R بالمقاس 256، أي: نوجد التّنسور $R^{(256)}$.
- نكتب مركّبات التّنسور $R^{(256)}$ بشكل مرتّب.
- نستبدل مركّبات التّنسور $R^{(256)}$ بالحروف المقابلة لها في جدول ال $ASCII$ فنحصل على النص المشفر **C** المطلوب .

مبرهنة 2 :

إن تشفير كل نص واضح P (من الحروف ASCII) من خلال استخدام قانون التّحويل التّنسوري بالمفتاح $C(C_n, p, q)$ يتم بشكلٍ وحيد.

الإثبات :

لتكن P, P' رسالتين مختلفتين من الحروف ASCII وليكن T, T' هما تنسوري النّصّين P, P' على التّرتيب، $R = F(T), R' = F(T')$ ولنثبت أن :

$$R' \neq^{(256)} R.$$

بما أنّ $P_1 \neq P_2$ فإنّه حسب جدول الحروف ومقابلاتها العددية:

$$T' \neq T$$

وباستخدام قانون التّحويل التّنسوري على التّنسورين T', T وحيث إنّ تطبيق التّحويل التّنسوري على تنسور يُعطي تنسوراً وحيداً، فإنّ:

$$F(T') \neq F(T)$$

وبالتّالي:

$$R' \neq R$$

نفرض جدلاً أنّ : $R \overset{(256)}{=} R'$، أي أنّ:

$$R' \pmod{256} \equiv R \pmod{256}$$

وبالتّالي يكون:

$$R'^{k_1 \ldots k_p}_{l_1 \ldots l_q} \equiv R^{k_1 \ldots k_p}_{l_1 \ldots l_q} \bmod(256) \; ; \; k_1, \ldots, k_p, l_1, \ldots, l_q \in \{1, \ldots, n\}$$

وبالتالي :

$$T'^{i_1 \ldots i_p}_{j_1 \ldots j_q} C^{j_1}_{l_1} \ldots C^{j_q}_{l_q} . B^{k_1}_{i_1} \ldots B^{k_p}_{i_p} \equiv T^{i_1 \ldots i_p}_{j_1 \ldots j_q} C^{j_1}_{l_1} \ldots C^{j_q}_{l_q} . B^{k_1}_{i_1} \ldots B^{k_p}_{i_p} \pmod{256}$$

لننظر إلى خواص التّطابقات، ولا سيّما إلى الخاصّتين الآتيتين:

- إذا كان $a \equiv b \pmod{m}$ و $k \in \mathbb{Z}$ فإنّ: $k.a \equiv k.b \pmod{m}$.
- إذا كان $a \equiv b \pmod{m}$ و $k \in \mathbb{Z}$ فإنّ: $k + a \equiv k + b \pmod{m}$.

وبالنّظر إلى بنية قانون التّحليل التّنسوري، فإنّه بتطبيق قانون التّحويل العكسيّ نجد:

$$T'^{i_1 \ldots i_p}_{j_1 \ldots j_q} \equiv T^{i_1 \ldots i_p}_{j_1 \ldots j_q} \pmod{256} \; ; \; i_1, \ldots, i_p, j_1, \ldots, j_q \in \{1, \ldots, n\}$$

وبالتّالي:

$$T' \equiv T \pmod{256}$$

وبالتّالي يكون:

$$T' = T$$

وهذا مخالف للفرض ، إذاً $R \overset{(256)}{\neq} R'$ وبالتالي ، تشفير كل رسالة باستخدام قانون التّحويل التّنسوري يتم بشكلٍ وحيد .

مبرهنة3:

إن فك التتشفير عن كل نص مشفّر C (من الحروف ASCII) من خلال استخدام قانون التّحويل التّنسوري بالمفتاح $C\left(C_n, p, q\right)$ يتم بشكلٍ وحيد.

الإثبات :

يتمّ الإثبات بطريقة مماثلة للإثبات السّابق.

مثال 6:

لنحوّل الجملة الآتية: " $Basel\ Alarnous$ " إلى شيفرة باستخدام التّحليل التّنسوري مستخدمين المفتاح $C\left(C_4, 1, 1\right)$، حيث:

$$C = \begin{pmatrix} 6 & 0 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -2 & 3 & 2 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

بما أنّ المصفوفة C من المرتبة الرّابعة فسنستخدم تنسور من النّوع $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ في الفضاء الرّباعي. سننظّم الجدول الآتي:

الحرف	B	a	s	e	l	–	A	l

ASCII	66	97	115	101	108	95	65	108
مركّبة التّنسور	$T_1^{\,1}$	$T_2^{\,1}$	$T_3^{\,1}$	$T_4^{\,1}$	$T_1^{\,2}$	$T_2^{\,2}$	$T_3^{\,2}$	$T_4^{\,2}$
الحرف	*a*	*r*	*n*	*o*	*u*	*s*	–	–
ASCII	97	114	110	111	117	115	95	95
مركّبة التّنسور	$T_1^{\,3}$	$T_2^{\,3}$	$T_3^{\,3}$	$T_4^{\,3}$	$T_1^{\,4}$	$T_2^{\,4}$	$T_3^{\,3}$	$T_4^{\,4}$

سنستخدم مصفوفة الانتقال للحصول على الشيفرة.

تعطى قاعدة التحويل التّنسوري لتنسور من النّوع $\begin{pmatrix}1\\1\end{pmatrix}$ في الفضاء الرّباعي من خلال العلاقة:

$$R_{\beta}^{\alpha}=T_{j}^{i}C_{\beta}^{j}B_{i}^{\alpha}\quad;\ \alpha,\beta,i,j=\overline{1,4}$$

حيث:

$$C=\begin{pmatrix}1&-4&-2&1\\-2&9&4&-1\\-3&14&7&-3\\2&-10&-5&3\end{pmatrix}=\begin{pmatrix}C_1^1&C_2^1&C_3^1&C_4^1\\C_1^2&C_1^2&C_1^2&C_1^2\\C_1^3&C_2^3&C_3^3&C_4^3\\C_1^4&C_2^4&C_3^4&C_4^4\end{pmatrix}$$

$$B=C^{-1}=\begin{pmatrix}6&0&1&-1\\1&1&-1&-1\\1&-2&3&2\\1&0&1&1\end{pmatrix}=\begin{pmatrix}B_1^1&B_2^1&B_3^1&B_4^1\\B_1^2&B_1^2&B_1^2&B_1^2\\B_1^3&B_2^3&B_3^3&B_4^3\\B_1^4&B_2^4&B_3^4&B_4^4\end{pmatrix}$$

نقوم بحساب مركّبات التّنسور $R\begin{pmatrix}1\\1\end{pmatrix}$.

$$R_1^1 = T_j^i C_1^j B_i^1 = T_j^1 C_1^j B_1^1 + T_j^2 C_1^j B_2^1 + T_j^3 C_1^j B_3^1 + T_j^4 C_1^j B_4^1$$
$$= \left(T_1^1 C_1^1 + T_2^1 C_1^2 + T_3^1 C_1^3 + T_4^1 C_1^4\right) B_1^1 +$$
$$+ \left(T_1^2 C_1^1 + T_2^2 C_1^2 + T_3^2 C_1^3 + T_4^2 C_1^4\right) B_2^1 +$$
$$+ \left(T_1^3 C_1^1 + T_2^3 C_1^2 + T_3^3 C_1^3 + T_4^3 C_1^4\right) B_3^1 +$$
$$+ \left(T_1^4 C_1^1 + T_2^4 C_1^2 + T_3^4 C_1^3 + T_4^4 C_1^4\right) B_4^1$$
$$= -1657$$

$$R_2^1 = T_j^i C_2^j B_i^1 = T_j^1 C_2^j B_1^1 + T_j^2 C_2^j B_2^1 + T_j^3 C_{12}^j B_3^1 + T_j^4 C_2^j B_4^1$$
$$= \left(T_1^1 C_2^1 + T_2^1 C_2^2 + T_3^1 C_2^3 + T_4^1 C_2^4\right) B_1^1 +$$
$$+ \left(T_1^2 C_2^1 + T_2^2 C_2^2 + T_3^2 C_2^3 + T_4^2 C_2^4\right) B_2^1 +$$
$$+ \left(T_1^3 C_2^1 + T_2^3 C_2^2 + T_3^3 C_2^3 + T_4^3 C_2^4\right) B_3^1 +$$
$$+ \left(T_1^4 C_2^1 + T_2^4 C_2^2 + T_3^4 C_2^3 + T_4^4 C_2^4\right) B_4^1$$
$$= 7375$$

قمنا بصياغة برنامج بلغة التربو باسكال لحساب باقي القيم (البرنامج 1) فوجدنا :

$$R_1^1 = -1657 \quad R_2^1 = 7375 \quad R_3^1 = 3397 \quad R_4^1 = -454$$
$$R_1^2 = 115 \quad R_2^2 = -553 \quad R_3^2 = -258 \quad R_4^2 = 81$$
$$R_1^3 = -1282 \quad R_2^3 = 5801 \quad R_3^3 = 2661 \quad R_4^3 = -395$$
$$R_1^4 = -718 \quad R_2^4 = 3224 \quad R_3^4 = 1449 \quad R_4^4 = -85$$

نوجد تنسور الممثّلات الرّئيسيّة للتنسور R بالمقاس 256.

$$^{(256)}R_1^1 = 135 \quad ^{(256)}R_2^1 = 207 \quad ^{(256)}R_3^1 = 69 \quad ^{(256)}R_4^1 = 58$$
$$^{(256)}R_1^2 = 115 \quad ^{(256)}R_2^2 = 215 \quad ^{(256)}R_3^2 = 254 \quad ^{(256)}R_4^2 = 81$$
$$^{(256)}R_1^3 = 254 \quad ^{(256)}R_2^3 = 169 \quad ^{(256)}R_3^3 = 101 \quad ^{(256)}R_4^3 = 117$$
$$^{(256)}R_1^4 = 50 \quad ^{(256)}R_2^4 = 152 \quad ^{(256)}R_3^4 = 169 \quad ^{(256)}R_4^4 = 171$$

وبالتالي نستطيع تنظيم الجدول الآتي:

مركبة التنسور	$^{(256)}R_1^1$	$^{(256)}R_2^1$	$^{(256)}R_3^1$	$^{(256)}R_4^1$	$^{(256)}R_1^2$	$^{(256)}R_2^2$	$^{(256)}R_3^2$	$^{(256)}R_4^2$
ASCII	135	207	69	58	115	215	254	81
الحرف	‡	د	*E*	:	*s*	×		*Q*
مركبة التنسور	$^{(256)}R_1^3$	$^{(256)}R_2^3$	$^{(256)}R_3^3$	$^{(256)}R_4^3$	$^{(256)}R_1^4$	$^{(256)}R_2^4$	$^{(256)}R_3^4$	$^{(256)}R_4^4$
ASCII	254	169	101	117	50	152	169	171
الحرف		©	e	u	2	ک	©	«

فيكون النّص بعد التشفير هو:

‡دE:s× Q ©eu2ک©«

وبالعكس لنقوم بفك تشفير النّص المشفّر الذي حصلنا عليه:

ننتقل من التّنسور $R\begin{pmatrix}1\\1\end{pmatrix}$ إلى التّنسور $T\begin{pmatrix}1\\1\end{pmatrix}$

تعطى قاعدة التحويل التّنسوري لتنسور من النّوع $\begin{pmatrix}1\\1\end{pmatrix}$ في الفضاء الرّباعي من خلال العلاقة:

$$T_{\beta}^{\alpha} = R_j^i B_{\beta}^j C_i^{\alpha} \quad ; \quad \alpha,\beta,i,j = \overline{1,4}$$

وبالحساب كما السابق، نحصل على:

$$T_1^{\,1}=-6846 \quad T_2^{\,1}=1121 \quad T_3^{\,1}=-3213 \quad T_4^{\,1}=-667$$
$$T_1^{\,2}=15724 \quad T_2^{\,2}=-2721 \quad T_3^{\,2}=7745 \quad T_4^{\,2}=1900$$
$$T_1^{\,3}=24929 \quad T_2^{\,3}=-3982 \quad T_3^{\,3}=11630 \quad T_4^{\,3}=2415$$
$$T_1^{\,4}=-17291 \quad T_2^{\,4}=2675 \quad T_3^{\,4}=-7841 \quad T_4^{\,4}=-1441$$

نوجد تنسور الممثّلات الرّئيسيّة للتنسور T بالمقاس 256.

$$^{(256)}T_1^{\,1}=66 \quad ^{(256)}T_2^{\,1}=97 \quad ^{(256)}T_3^{\,1}=115 \quad ^{(256)}T_4^{\,1}=101$$
$$^{(256)}T_1^{\,2}=108 \quad ^{(256)}T_2^{\,2}=95 \quad ^{(256)}T_3^{\,2}=65 \quad ^{(256)}T_4^{\,2}=108$$
$$^{(256)}T_1^{\,3}=97 \quad ^{(256)}T_2^{\,3}=114 \quad ^{(256)}T_3^{\,3}=110 \quad ^{(256)}T_4^{\,3}=111$$
$$^{(256)}T_1^{\,4}=117 \quad ^{(256)}T_2^{\,4}=115 \quad ^{(256)}T_3^{\,4}=95 \quad ^{(256)}T_4^{\,4}=95$$

وبالتالي نستطيع تنظيم الجدول الآتي:

مركبة التنسور	$^{(256)}T_1^{\,1}$	$^{(256)}T_2^{\,1}$	$^{(256)}T_3^{\,1}$	$^{(256)}T_4^{\,1}$	$^{(256)}T_1^{\,2}$	$^{(256)}T_2^{\,2}$	$^{(256)}T_3^{\,2}$	$^{(256)}T_4^{\,2}$
ASCII	66	97	115	101	108	95	65	108
الحرف	*B*	*a*	*s*	*e*	*l*	–	*A*	*l*
مركبة التنسور	$^{(256)}T_1^{\,3}$	$^{(256)}T_2^{\,3}$	$^{(256)}T_3^{\,3}$	$^{(256)}T_4^{\,3}$	$^{(256)}T_1^{\,4}$	$^{(256)}T_2^{\,4}$	$^{(256)}T_3^{\,4}$	$^{(256)}T_4^{\,4}$
ASCII	97	114	110	111	117	115	95	95
الحرف	*a*	*r*	*n*	*o*	*u*	*s*	–	–

فيكون النّص الأصلي هو:

$$Basel-Alarnous--$$

نستطيع استخدام طريقة أخرى وذلك وفقاً لقاعدة التّحويل التّنسوري المُعطاة. يتّضح ذلك من خلال المثال الآتي:

لنحوّل الجملة الآتية: " $Basel\ Alarnous$ " إلى شيفرة باستخدام التّحليل التّنسوري مستخدمين المفتاح $C\,(C_2,2,2)$، حيث:

$$C=\begin{pmatrix}1 & 2\\ 1 & 3\end{pmatrix}$$

سننظّم الجدول الآتي:

الحرف	B	a	s	e	l	–	A	l
$ASCII$	66	97	115	101	108	95	65	108
مركّبة التّنسور	T_{11}^{11}	T_{12}^{11}	T_{21}^{11}	T_{22}^{11}	T_{11}^{12}	T_{12}^{12}	T_{21}^{12}	T_{22}^{12}
الحرف	a	r	n	o	u	s	–	–
$ASCII$	97	114	110	111	117	115	95	95
مركّبة التّنسور	T_{11}^{21}	T_{12}^{21}	T_{21}^{21}	T_{22}^{21}	T_{11}^{22}	T_{12}^{22}	T_{21}^{22}	T_{22}^{22}

سنستخدم مصفوفة الانتقال للحصول على الشيفرة.

تعطى قاعدة التحويل التّنسوري لتنسور من النّوع $\begin{pmatrix}2\\2\end{pmatrix}$ في الفضاء الثّنائي من خلال العلاقة:

$$R_{\gamma\delta}^{\alpha\beta}=T_{kl}^{ij}C_{\gamma}^{k}C_{\delta}^{l}B_{i}^{\alpha}B_{j}^{\beta}\quad ;\ \alpha,\beta,\gamma,\delta,i,j,k,l=\overline{1,2}$$

حيث:

$$C=\begin{pmatrix}1 & 2\\ 1 & 3\end{pmatrix}=\begin{pmatrix}C_1^1 & C_2^1\\ C_1^2 & C_2^2\end{pmatrix}$$

$$B=C^{-1}=\begin{pmatrix}3 & -2\\ -1 & 1\end{pmatrix}=\begin{pmatrix}B_1^1 & B_2^1\\ B_1^2 & B_2^2\end{pmatrix}$$

نقوم بحساب مركّبات التّنسور $R\begin{pmatrix}2\\2\end{pmatrix}$.

$$
\begin{aligned}
R_{11}^{11} &= T_{kl}^{ij}C_1^kC_1^lB_i^1B_j^1 = T_{kl}^{i1}C_1^kC_1^lB_i^1B_1^1 + T_{kl}^{i2}C_1^kC_1^lB_i^1B_2^1 \\
&= T_{kl}^{11}C_1^kC_1^lB_1^1B_1^1 + T_{kl}^{21}C_1^kC_1^lB_2^1B_1^1 + T_{kl}^{12}C_1^kC_1^lB_1^1B_2^1 + \\
&\quad + T_{kl}^{22}C_1^kC_1^lB_2^1B_2^1 \\
&= T_{k1}^{11}C_1^kC_1^1B_1^1B_1^1 + T_{k2}^{11}C_1^kC_1^2B_1^1B_1^1 + T_{k1}^{21}C_1^kC_1^1B_2^1B_1^1 + \\
&\quad + T_{k2}^{21}C_1^kC_1^2B_2^1B_1^1 + T_{k1}^{12}C_1^kC_1^1B_1^1B_2^1 + T_{k2}^{12}C_1^kC_1^2B_1^1B_2^1 + \\
&\quad + T_{k1}^{22}C_1^kC_1^1B_2^1B_2^1 + T_{k2}^{22}C_1^kC_1^2B_2^1B_2^1 \\
&= T_{11}^{11}C_1^1C_1^1B_1^1B_1^1 + T_{21}^{11}C_1^2C_1^1B_1^1B_1^1 + T_{12}^{11}C_1^1C_1^2B_1^1B_1^1 + \\
&\quad + T_{22}^{11}C_1^2C_1^2B_1^1B_1^1 + T_{11}^{21}C_1^1C_1^1B_2^1B_1^1 + T_{21}^{21}C_1^2C_1^1B_2^1B_1^1 + \\
&\quad + T_{12}^{21}C_1^1C_1^2B_2^1B_1^1 + T_{22}^{21}C_1^2C_1^2B_2^1B_1^1 + T_{11}^{12}C_1^1C_1^1B_1^1B_2^1 + \\
&\quad + \left(+T_{21}^{12}C_1^2C_1^1B_1^1B_2^1\right) + T_{12}^{12}C_1^1C_1^2B_1^1B_2^1 + T_{22}^{12}C_1^2C_1^2B_1^1B_2^1 + \\
&\quad + T_{11}^{22}C_1^1C_1^1B_2^1B_2^1 + T_{21}^{22}C_1^2C_1^1B_2^1B_2^1 + T_{12}^{22}C_1^1C_1^2B_2^1B_2^1 + \\
&\quad + T_{22}^{22}C_1^2C_1^2B_2^1B_2^1 = 251
\end{aligned}
$$

(نلاحظ هنا تعقيد العمليّات الحسابيّة ، ممّا يُعطي أماناً أكثر لعمليّة التّشفير)

وباستخدام لغة التربو باسكال (البرنامج 2) نتمكن من حساب باقي المركّبات، فنجد أنّ:

$$
\begin{array}{cccc}
R_{11}^{11}=251 & R_{12}^{11}=556 & R_{21}^{11}=842 & R_{22}^{11}=1767 \\
R_{11}^{12}=11 & R_{12}^{12}=67 & R_{21}^{12}=-45 & R_{22}^{12}=53 \\
R_{11}^{21}=67 & R_{12}^{21}=201 & R_{21}^{21}=115 & R_{22}^{21}=420 \\
R_{11}^{22}=-7 & R_{12}^{22}=-34 & R_{21}^{22}=-2 & R_{22}^{22}=-67
\end{array}
$$

نوجد تنسور الممثّلات الرّئيسيّة للتنسور R بالمقاس 256.

$$^{(256)}R_{11}^{11}=251 \quad ^{(256)}R_{12}^{11}=44 \quad ^{(256)}R_{21}^{11}=74 \quad ^{(256)}R_{22}^{11}=231$$
$$^{(256)}R_{11}^{12}=11 \quad ^{(256)}R_{12}^{12}=67 \quad ^{(256)}R_{21}^{12}=211 \quad ^{(256)}R_{22}^{12}=53$$
$$^{(256)}R_{11}^{21}=67 \quad ^{(256)}R_{12}^{21}=201 \quad ^{(256)}R_{21}^{21}=115 \quad ^{(256)}R_{22}^{21}=164$$
$$^{(256)}R_{11}^{22}=249 \quad ^{(256)}R_{12}^{22}=222 \quad ^{(256)}R_{21}^{22}=254 \quad ^{(256)}R_{22}^{22}=189$$

وبالتالي نستطيع تنظيم الجدول الآتي:

مركبة التنسور	$^{(256)}R_{11}^{11}$	$^{(256)}R_{12}^{11}$	$^{(256)}R_{21}^{11}$	$^{(256)}R_{22}^{11}$	$^{(256)}R_{11}^{12}$	$^{(256)}R_{12}^{12}$	$^{(256)}R_{21}^{12}$	$^{(256)}R_{22}^{12}$
ASCII	251	44	74	231	11	67	211	53
الحرف	û	′	J	ç		C	س	5
مركبة التنسور	$^{(256)}R_{11}^{21}$	$^{(256)}R_{12}^{21}$	$^{(256)}R_{21}^{21}$	$^{(256)}R_{22}^{21}$	$^{(256)}R_{11}^{22}$	$^{(256)}R_{12}^{22}$	$^{(256)}R_{21}^{22}$	$^{(256)}R_{22}^{22}$
ASCII	67	201	115	164	249	222	254	189
الحرف	C	ة	s	¤	ù	ق		½

فيكون النّص بعد التشفير هو:

Û'Jç Cس5Cةs¤ùق ½

وبالعكس لنقوم بفك تشفير النّص المشفّر الذي حصلنا عليه:

ننتقل من التّنسور $R\begin{pmatrix}2\\2\end{pmatrix}$ إلى التّنسور $T\begin{pmatrix}2\\2\end{pmatrix}$

تعطى قاعدة التحويل التّنسوري لتنسور من النّوع $\begin{pmatrix}2\\2\end{pmatrix}$ في الفضاء الرّباعي من خلال العلاقة:

$$T_{\gamma\delta}^{\alpha\beta}=R_{kl}^{ij}B_{\gamma}^{k}B_{\delta}^{l}C_{i}^{\alpha}C_{j}^{\beta} \quad ; \quad \alpha,\beta,\gamma,\delta,i,j,k,l=\overline{1,2}$$

وبالحساب كما السابق، نحصل على:

$$T_{11}^{11}=4418 \quad T_{12}^{11}=-1951 \quad T_{21}^{11}=-1677 \quad T_{22}^{11}=613$$
$$T_{11}^{12}=5740 \quad T_{12}^{12}=-2465 \quad T_{21}^{12}=-1983 \quad T_{22}^{12}=620$$
$$T_{11}^{21}=6241 \quad T_{12}^{21}=-2702 \quad T_{21}^{21}=-2450 \quad T_{22}^{21}=879$$
$$T_{11}^{22}=8565 \quad T_{12}^{22}=-3725 \quad T_{21}^{22}=-3233 \quad T_{22}^{22}=119$$

نوجد تنسور الممثّلات الرّئيسيّة للتّنسور T بالمقاس 256.

$$^{(256)}T_{11}^{11}=66 \quad ^{(256)}T_{12}^{11}=97 \quad ^{(256)}T_{21}^{11}=115 \quad ^{(256)}T_{22}^{11}=101$$
$$^{(256)}T_{11}^{12}=108 \quad ^{(256)}T_{12}^{12}=95 \quad ^{(256)}T_{21}^{12}=65 \quad ^{(256)}T_{22}^{12}=108$$
$$^{(256)}T_{11}^{21}=97 \quad ^{(256)}T_{12}^{21}=114 \quad ^{(256)}T_{21}^{21}=110 \quad ^{(256)}T_{22}^{21}=111$$
$$^{(256)}T_{11}^{22}=117 \quad ^{(256)}T_{12}^{22}=115 \quad ^{(256)}T_{21}^{22}=95 \quad ^{(256)}T_{22}^{22}=95$$

وبالتالي نستطيع تنظيم الجدول الآتي:

مركبة التنسور	$^{(256)}T_{11}^{11}$	$^{(256)}T_{12}^{11}$	$^{(256)}T_{21}^{11}$	$^{(256)}T_{22}^{11}$	$^{(256)}T_{11}^{12}$	$^{(256)}T_{12}^{12}$	$^{(256)}T_{21}^{12}$	$^{(256)}T_{22}^{12}$
ASCII	66	97	115	101	108	95	65	108
الحرف	*B*	*a*	*s*	*e*	*l*	–	*A*	*l*
مركبة التنسور	$^{(256)}T_{11}^{21}$	$^{(256)}T_{12}^{21}$	$^{(256)}T_{21}^{21}$	$^{(256)}T_{22}^{21}$	$^{(256)}T_{11}^{22}$	$^{(256)}T_{12}^{22}$	$^{(256)}T_{21}^{22}$	$^{(256)}T_{22}^{22}$
ASCII	97	114	110	111	117	115	95	95
الحرف	*a*	*r*	*n*	*o*	*u*	*s*	–	–

فيكون النّص الأصلي هو:

$$Basel-Alarnous--$$

5. النتائج:

تمّ تعميم طريقة هيل في التشفير و إدخال التّنسورات عوضاً عن المصفوفات في التشفير، من خلال اعتماد قانون التّحويل التّنسوري، وتمّ التوصّل إلى إثبات صحّة المبرهنتين:

مبرهنة2:

إن تشفير كل نص واضح P (من الحروف ASCII) من خلال استخدام قانون التّحويل التّنسوري بالمفتاح $C\left(C_n, p, q\right)$ يتم بشكلٍ وحيد.

مبرهنة 3:

إن فك التتشفير عن كل نص مشفّر C (من الحروف ASCII) من خلال استخدام قانون التّحويل التّنسوري بالمفتاح $C\left(C_n, p, q\right)$ يتم بشكلٍ وحيد.

6. المقترحات والتّوصيات:

إنّ التعميم باستخدام التّنسورات في التشفير يفتح آفاقاً جديدة لتطوير التشفير وزيادة أمانه، وذلك بتحميل محارف النص الواضح على مركّبات تنسور، لذلك يمكن العمل في المرحلة اللاحقة على استبدال مصفوفة هيل بتنسور يحقّق شروطاً تجعل عمليّة التشفير العكسيّة عمليّة ممكنة.

7. الملحقات:

7 – 1 برنامج رقم 1

```
Program Basel1;
Uses crt;
var
T,B,C,B: array [1..2,1..2] of integer;
I,j,k,l:integer;
Begin
for i:=1 to 2 do
for j:=1 to 2 do
begin
write('C[',i,j,']=');readln(C[i,j]);
end;
readln;
for i:=1 to 2 do
for j:=1 to 2 do
begin
write('B[',i,j,']=');readln(B[i,j]);
end;
readln;
for i:=1 to 2 do
for j:=1 to 2 do
begin
write('T[',i,j,']=');readln(T[i,j]);
```

```
end;
readln;
for k:=1 to 4 do
for l:=1 to 4 do
begin
R[k,l]:=0
for i:=1 to 2 do
for j:=1 to 2 do
R[k,l]:= R[k,l]+T[i,j]*C[j,l] *B[k,i];
End;
for i:=1 to 2 do
for j:=1 to 2 do
write('R[',i,j,']=',R[i,j]);
readln;
end.
```

7 – 2 برنامج رقم 2

```
Program Basel2;
Uses crt;
var
T,R: array [1..2,1..2,1..2,1..2] of integer;
C,B: array [1..2,1..2] of integer;
lup,jup,kdown,ldown,l,j,k,l:integer;
Begin
```

```
for i:=1 to 2 do
for j:=1 to 2 do
begin
write('C[',i,j,']='); readln(C[i,j]);
end;
readln;
for i:=1 to 2 do
for j:=1 to 2 do
begin
write('B[',i,j,']=');readln(B[i,j]);
end;
readln;
for i:=1 to 2 do
for j:=1 to 2 do
for k:=1 to 2 do
for l:=1 to 2 do
begin
write('T[',i,j,k,l,']=');readln(T[i,j,k,l]);
end;
readln;
for iup:=1 to 2 do
for jup:=1 to 2 do
for kdown:=1 to 2 do
for ldown:=1 to 2 do
```

```
begin
R[iup,jup,kdown,ldown]:=0
for i:=1 to 2 do
for j:=1 to 2 do
for k:=1 to 2 do
for l:=1 to 2 do
R[iup,jup,kdown,ldown]:=
R[iup,jup,kdown,ldown]+T[l,j,k,l]*C[k,kdown]*C[l,ldown]*B[iup,
i]*B[jup,j];
End;
for i:=1 to 2 do
for j:=1 to 2 do
for k:=1 to 2 do
for l:=1 to 2 do
write('R[',i,j,k,l,']=',R[i,j,k,l]);
readln;
end.
```

8. المراجع:

1. Lester S. Hill public son article "Cryptography in an Algebraic Alphabet", dans American Mathematical Monthly, 36, pp. 306-312, 1929
2. H.S.A. Rose, Course in number theory. Oxford Sciences Publication. (Clarendon), 1988.
3. B. Schneier , Applied cryptography. Second edition, protocols, algorithms and source coding C(John Wiley\& Sons), 1996.
4. M. I. Sowalle, Introduction to cryptology, Dist. Center, (Arabic version)Riyadh, 1996.
5. D. Welsh, Codes and Cryptography, Oxford Science publications ,1988.
6. F. A. Zoukair, and A. Samhan, Introduction to number theory , Pub. Dist. Center, Riyadh, (Arabic version), 2001
7. Swapan Kumar Sarkar ,A Text book of Discrete mathematics S.CHAND & COMPANY LTD, A TEXTBOOK OF DISCRETE MATHEMATICS RAMNAGAR,NEW DELHI-110055, 2008.
8. Moravitz Martin, Tensor Decompositions Workshop Discussion. University of Cornell (2004).

9. د. عبد الباسط الخطيب ، د. محمدنور شمه ، 2008 ، **التشفير العربي المطور "التشفير المطورة"**، مجلة جامعة البعث للعلوم الهندسية ، مجلد 30، العدد 17.

10.باسل العرنوس، 2015 ، التطبيقات الجيوديزيّة بين فضاءات ريمان ، رسالة ماجستير ، جامعة البعث.

دراسة مطيافية الأشعة تحت الحمراء لمركب أكسيد القصدير النقي والمشاب بالحديد (x=0.00,0.04)

أ.د.أحمد خضرو[1] د.برهان دالاتي[2]

,, **قسم الفيزياء–كلية العلوم–جامعة تشرين** 2,1

الملخص

تعتبر دراسة الأكاسيد الشفافة (TCO) ذات أهمية علمية كبيرة نظراً لتطبيقاتها العلمية الواسعة. لذلك ، توصلت دراستنا إلى بعض الخصائص الفيزيائية لمركبات كل من أكسيد القصدير النقي وأكسيد القصدير المشاب بالحديد. من خلال قياس طيف الأشعة تحت الحمراء لأكسيد القصدير النقي ، وجد أن هناك خمسة ترددات اهتزازية ، وهي: (cm^{-1} 415.585 – 574.683 – 1641.13 – 2125.3 – 3432.67) ولأكسيد قصدير المشاب بالحديد (cm^{-1} 580.49–1384.64 – 1640.16 – 3431.71) .أظهرت الدراسة أن أكبر قيمة للامتصاصية ولمعامل الامتصاص كانت في العينة النقية على التوالي A = 0.725، α = 16.687 cm^{-1} المقابل للعدد الموجي υ = 574.683cm^{-1}.

الكلمات المفتاحية: أكسيد القصدير – طيف الأشعة تحت الحمراء – الامتصاصية – قرينة الانكسار – الناقلية الضوئية

Studying the Infrared spectroscopy of the pure tin oxide and iron doped tin oxide compounds ;(x= 0.00,0.04)

Ahmad Khoudro[1] Burhan Dalati[2]

1.Professor, Department of Physics, Faculty of science, Tishreen University, Syria.
2.Assistant Professor, Department of Physics, Faculty of science, Tishreen University, Syria.

Abstract

The study of transparent oxides (TCO) is of great scientific importance due to its wide scientific applications. Therefore, our study came to some of the physical properties of the compounds of both pure tin oxide and iron doped tin oxide. By measuring the infrared spectrum of pure tin oxide, it is found that there are five vibratory frequencies, namely:415.585 - 574.683 - 1641.13 – 2125.3- 3432.67) cm^{-1} and for iron doping tin oxide (580.49-1384.64-1640.16-3431.71) cm^{-1} . the study showed that the greatest value of the absorbance and absorption coefficient was in pure sample respectively $A = 0.725$, $\alpha = 16.687\ cm^{-1}$ corresponding to the wavenumber $\upsilon = 574.683 cm^{-1}$.

Keywords: Tin Oxide - infrared spectrum - absorbance - absorption coefficient - refractive index - optical conductivity.

1.Introduction:

The crystals of metal oxides semiconductor have attracted a great interest due to their intriguing properties, which are different from those of their corresponding bulk state.Tin Oxide (SnO_2) is one of the important metal oxides due to its many useful properties such as its wide band gap (E_g = 3.64 eV, 330 K), n-type conductivity, high transparency in the visible range (>80 %).

It crystallizes in the tetragonal rutile structure with space group P42/mnm , with lattice parameters $a = b$ = 4.738 Å and c = 3.187 Å , and can be synthesized in variety of shapes and sizes using different low cost synthesis techniques relevant for a wide range of applications such as solid-state gas sensors, flat panel displays, solar energy cells [1-3] .

Its unit cell contains two tin and four oxygen atoms as is shown in figure (1) . The tin atom is at the center of six oxygen atoms placed at the corners of a regular octahedron. Every oxygen molecule is surrounded by three tin atoms at the corners of an equilateral triangle [4].

Some properties can be drastically changed by the addition of adequate dopants. For instance, undoped stoichiometric SnO_2 is an insulator .

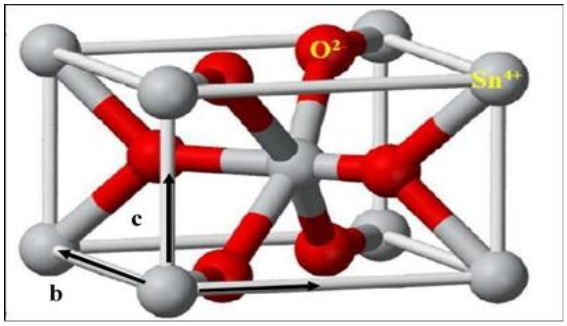


Fig (1) : Unit cell of the crystal structure of SnO_2 [5].

2.Infrared spectroscopy:

Infrared is electromagnetic waves and it has all the basic properties of light, which are represented by the phenomena of diffusion, reflection, refraction, interference, diffraction and polarization. They are invisible thermal waves emitted by the sun or from

artificial sources and have a high penetration ability as well as from our bodies and their frequency is lower than the red ray frequency in the visible electromagnetic spectrum. The infrared spectrum is located between the visible spectrum and the microwave radiation spectrum. It is divided into three zones, as follows:

- Near infrared (NIR): It is the closest to the visible rays, namely the red colour, and it lies within the range [4000 -12000] cm^{-1} .
- Middle Infrared MIR: located between the two preceding zones within the range [200 -4000] cm^{-1} .
- Infrared spectroscopy is one of the basic methods of studying materials. It enables us to identify the structure of the material without affecting its properties. It depends on the study of the spectra absorbed by the sample, and its field is limited to [20 -1400] cm^{-1} .

Red radiation energy is not enough to cause electronic excitation in most materials, but it is sufficient to cause elasticity vibrations and flexion in the bonds. All types of these bonds respond to this amount of energy in which vibrations of this type occur. Therefore, they are absorbed in the zone beneath the red under the condition that absorption leads to a change in the polar moment, and these vibrations are quantized, and their occurrence means that the compound absorbs infrared energy in a specific part of the spectrum. [6]

Most spectroscopic analysis occur in the central infrared zone [20 – 1400] cm^{-1} where the most molecular vibrations occur to determine the molecular structure of the studied compounds.

3.Infrared spectroscopy principle

Natural molecules vibrate according to all their vibrating patterns, but with very weak amplitudes. However, the photon has a sinusoidal electric component. If the frequency of the photon corresponds to the frequency of the vibrations of the normal patterns of the molecule, the molecule will enter the resonance and vibrate at very large amplitudes. In other words the photon whose energy is Equal to the energy necessary for the molecule to pass from a low energy state to an excited state is absorbed and its energy is transformed into a vibration energy as in Figure (2).

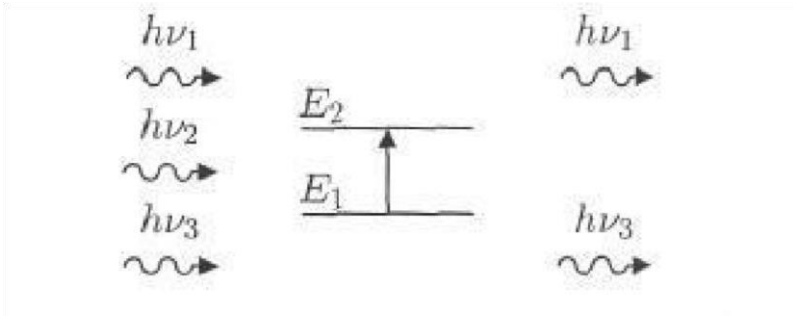


Figure (2) Infrared absorption

Only the photon whose energy (hv) equals to the transmission energy (E_2-E_1) is absorbed and thus the emission of the emitted radiation is impaired. As the absorption of some of the incoming photons leads to the appearance of the lines of compatibility of the photons that were not emitted in the curve of the infrared spectrum of the molecule. This absorption distinguishes the bonds between the atoms, since each vibration pattern corresponds to the single movement of the molecule, so there is a direct correspondence between the frequency of the absorbed radiation and the structure of the molecule [7].

Research objective:

This work aims to determine the field of absorption frequencies, that is the vibrations samples frequencies of the infrared spectra of pure tin oxide and iron doped tin oxide by (4wt%), and then finding the absorbance, reflectance , absorption coefficient, extinction coefficient, refractive index, optical length and optical conductivity to improve the physical properties of tin oxide.

Research materials and methods:

The following materials have been used in preparing the samples:

- Tin oxide SnO_2 (99% purity, TITAN BIOTECH LTD, origin India).
- Iron Fe (99% purity, TITAN BIOTECH LTD, origin India).

Devices and tools used:

1- Sensitive scale type (SARTORIUS) with an accuracy of (10^{-4}) gr is available in the Faculty of Science - Physics Department.
2- Small agate mortar.
3- High temperature thermal Oven (700°C) with a Temperature Regulator.

4- Preparing the samples:

The samples are prepared by the solid state reaction method. Accordingly the weights of the powders required for each sample are mixed and calculated using the molecular weight method in order to obtain the compounds required for the study where $Sn_{1-x}Fe_xO_2$; (x=0.0- 0.04). Then grinding these materials in the agate mortar perfectly well to make the mixture homogeneous and sifting it with a sieve of 90 µm. Then it is put it in a container and we add distilled water to increase the mixing process and homogeneity of the powder. Then we put it on a heater for 3 hours at a temperature of 100° C and the mixing and homogeneity process of the powder occurs by stirring.

After that, the powder is placed on a heater with direct contact with the air, then the water evaporates and then we perform a preliminary roasting process inside the oven (pre-sinter) to increase the degree of homogeneity of the mixture. We fix the oven temperature at 700°C for three hours, then we turn off the oven, which means to stop the roasting process and leave the sample inside the oven until it cools and reaches room temperature, thus we get rid of impurities that evaporate at high temperatures.

Then we grind the powder resulting from the roasting process in its first stage. Then we perform the second roasting process where we fix the oven temperature at 100° C for an hour and then we raise the temperature 50°C every 15min until we reach the

temperature of 700°C where we fix the oven temperature at it for 3 hours In order to get the crystal structure in its correct form.

To study the infrared spectra, we use an infrared spectroscopy device, which is a simple device whose main components are an infrared source, a sample holder and a detector. This device is considered one of the best spectroscopic devices used to identify the chemical composition of the compounds. It is available in the Faculty of Science - Tishreen University works at the range [400-4000] cm^{-1}.

The spectrometer is characterized by a computer memory that analyzes the waves gathered on the detector, computerizes them, and draws the spectrum resulting from absorption. Or a vibratory transmission of the atoms occurs relative to each other in the molecule, which leads to a periodic change in the length of chemical bonds or a change in the angles between the chemical bonds in the molecule. Each vibrational motion results from the movement of two atoms, or it may include a group of its constituent atoms. The wavelength or frequency at which this absorption occurs depends on several factors, including the mass of the atom, the strength of the bonds that make up the molecule, and the geometry of the atoms in the molecule.

5- Results and discussion:

The IR spectrum of pure tin oxide and iron doped tin oxide was measured using the spectrometer **asco** type **FT / IR-460 plus** available in the central laboratory of the Faculty of Science - Tishreen University, working in the range [400-4000] cm^{-1}. Where the transmittance T was measured by the frequency function υ , the absorbance A, the reflectance R, the absorption coefficient α, the extinction koefficient K, the refractive index n and optical conductivity $\boldsymbol{\sigma_{opt}}$ were calculated:

1- **Transmittance T**: It is defined as the ratio between the intensity of the penetrating radiation to the intensity of the

incident radiation, it has been taken from the device itself and then by using the appropriate mathematical equations, other optical parameters have been calculated.

2- **Absorbency A**: is the ratio between the intensity of the absorbed radiation and the intensity of the inciden radiation, calculated from the equation [8]:

$$A = \log\left(\frac{100}{T\%}\right) = \log\left(\frac{1}{T}\right) \qquad (1)$$

T represents Permeability.

3- **Reflectance R** : is the ratio between the intensity of the reflected radiation and the intensity of the incident radiation , calculated from the equation [9] :

$$R+T+A=1 \qquad (2)$$

4- **Absorption coefficient α**: defined as the ratio between the decrease in the flow of the incident radiation energy to the unit of distance towards the spread of the incident light wave within the field, and is calculated from the equation [10] :

$$\alpha = 2.303\frac{A}{d} \qquad (3)$$

A represents absorbency , d = 1mm the thickness of the material

5- **The extinction coefficient k**: is defined as the amount of energy absorbed by the electrons of the studied material from the energy of the radiation photons that fall on it, and is calculated from the equation [11]:

$$k = \frac{\alpha}{4\pi\nu} \qquad (4)$$

6- **Refractive index n**: which is the ratio between the speed of light in the vacuum to its speed in the field, and it is calculated from the equation [12] :

$$n = \left[\left(\frac{1+R}{1-R}\right)^2 - (K^2 + 1)\right]^{1/2} + \frac{1+R}{1-R} \qquad (5)$$

R represents reflectance .

7- **Optical length L**: the inversion of the absorption coefficient [10]:

$$L = \frac{1}{\alpha} \qquad (6)$$

8- **Optical conductivity σ_{opt}**: optical conductivity is related to the refractive index and the extinction coefficient according to the following equation [13]:

$$\sigma_{opt} = \frac{1}{30} nk\nu \qquad (7)$$

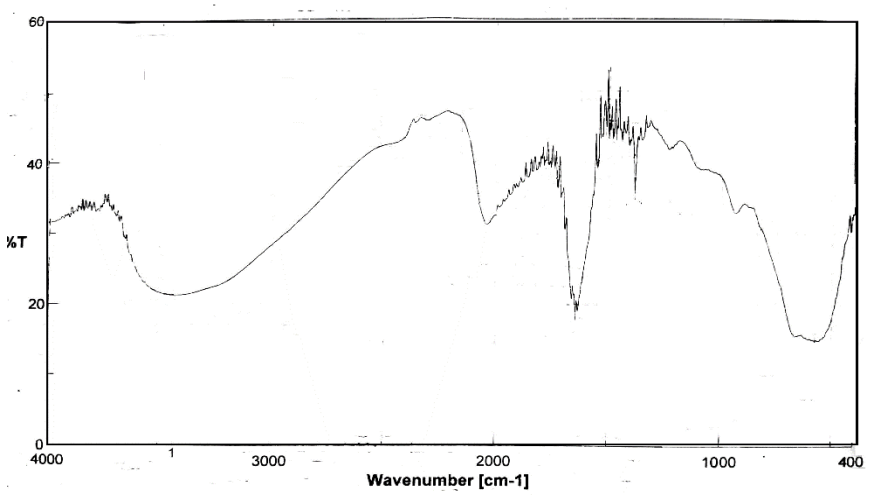


Figure (3): Represents the FTIR spectrum for pure tin oxide.

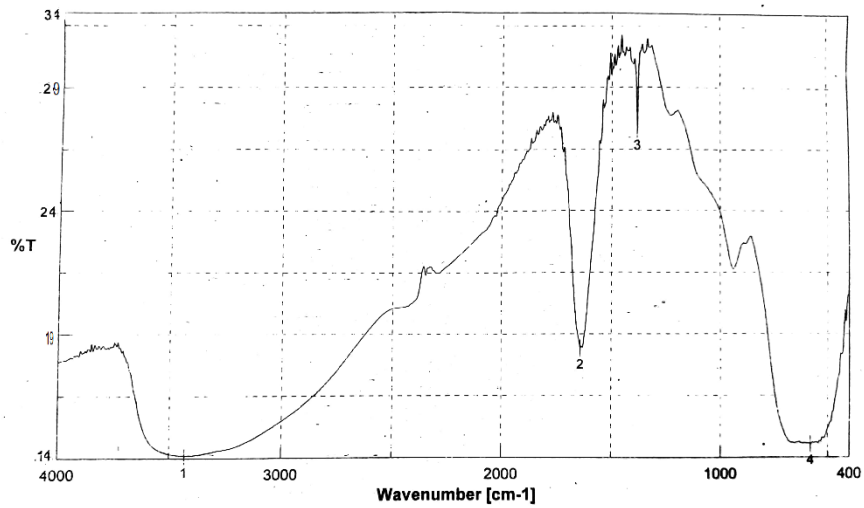


Figure (4): represents FTIR spectrum of iron doped tin oxide by (4wt%).

FTIR is a technique used to obtain information regarding chemical bonding and functional groups in a material. In the transmission mode, it is quite useful to predict the presence of certain functional groups which are adsorbed at certain frequencies; thus, it reveals the structure of the material. The band positions and numbers of absorption peaks depend on the crystalline structure, chemical composition, and also on morphology [6]. To investigate chemical groups on the surface of sintered samples, an FTIR analysis was carried out at room temperature over the wave number range of 400– 4000 cm^{-1}. There are several bands appearing in the wave number range 400–4000 cm^{-1}. The broad absorption band at 3423 cm^{-1}, the peaks at 2977 cm^{-1}, and 1630 cm^{-1} are assigned to the vibration of hydroxyl group due to the absorbed/adsorbed water and show a stretching vibrational mode of O–H group [7]. Absorption peaks observed around 2380 cm^{-1} belong to the stretching vibrations of C–H bonds that could be due to the adsorption and interaction of atmospheric carbon dioxide with water during the firing process [8]. The bands observed in the range of 970–700 cm^{-1} are due to the vibration of Sn=O and Sn–O surface cation oxygen bonds [7]. The very strong absorption bands observed in the range of 420–700 cm^{-1} are attributed to the Sn–O antisymmetric

vibrations. In that region, the peak at 686 cm^{-1} are assigned to Sn–O–Sn vibrations, respectively . The bands exhibited in the low wave number region 430–620 cm^{-1} are attributed to the Sn–O stretching vibrations [10]. The Fe doping shifts the positions of the absorption bands. It has been previously reported that changes observed in the shape, width, and positions of FTIR peaks are attributed to the variation in the local defects, grain size and shape of the samples [11]. In all samples, the vibrations associated to C–H and O–H bonds are seen. This implies that the surface is highly active and adsorbed these molecules.

Table: (1) shows the vibrations frequency of pure tin oxide with corresponding permeability values for each frequency, absorbance, reflectance , absorption coefficient, extinction coefficient, refractive index, optical length and optical conductivity.

$\nu\ (cm)^{-1}$	T%	A	R	$\alpha\ (cm)^{-1}$	k	n	L(cm)	$\sigma_{(opt)}(\Omega.cm)^{-1}$
3432.670	21.092	0.6758	0.1131	15.54529	0.000361	2.014	0.06430	0.083093
2125.300	27.692	0.5576	0.1654	12.82585	0.000480	2.371	0.07790	0.080712
1641.130	18.841	0.7248	0.0866	16.67261	0.000809	1.834	0.05997	0.081178
574.683	18.813	0.7255	0.0863	16.68746	0.002312	1.832	0.05992	0.081140
415.585	20.188	0.6949	0.1032	15.98285	0.003062	1.946	0.06250	0.082572

Table: (2) shows the vibrations frequency of the iron doped tin oxide by (4 wt%) with corresponding permeability values for each frequency, absorbance , reflectance, absorption coefficient,

$\nu\ (cm)^{-1}$	T%	A	R	$\alpha\ (cm)^{-1}$	k	n	L(cm)	$\sigma_{(opt)}(\Omega.cm)^{-1}$
3431.71	14.1154	0.8503	0.0085	19.5570	0.00045	1.2036	0.0511	0.0624
1640.16	19.4074	0.7120	0.0938	16.3767	0.00079	1.8835	0.0610	0.0818
1384.64	27.3105	0.5636	0.1632	12.9644	0.00074	2.3557	0.0771	0.0810
580.49	14.5440	0.8373	0.0172	19.2582	0.00264	1.3023	0.0519	0.0665

extinction coefficient, refractive index, optical length and optical conductivity.

Figure (5) shows the change in the absorbance of pure and iron doped tin oxide , we note that the largest absorbance value corresponds to the pure tin oxide at the value 0.7255 corresponding to the wavenumber (574.683) cm $^{-1}$, and the smallest value of absorbance corresponds to the Fe doped tin oxide at the value 0.5636 corresponding to the wavenumber (1384.64) cm^{-1}.

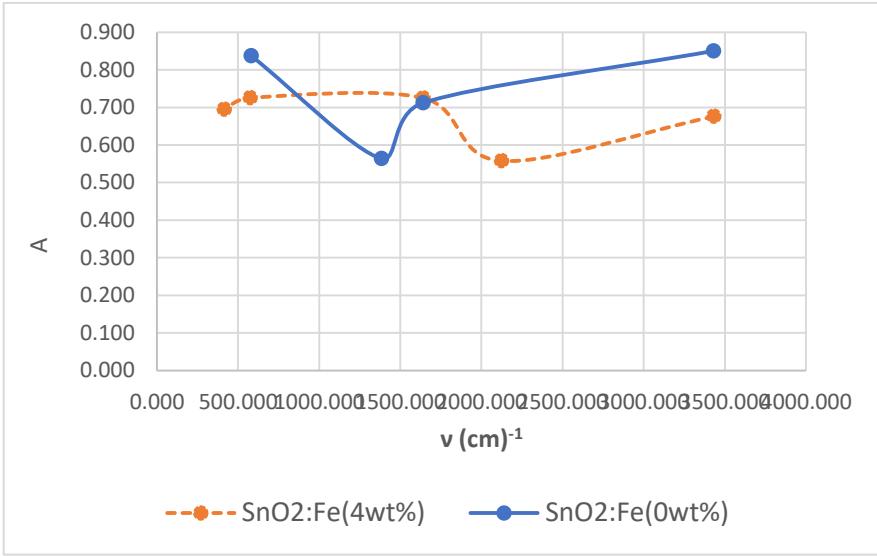


Figure (5): the absorbance by the wavenumber function of pure SnO_2 and Fe doped SnO_2 powder by (4wt%) .

The absorption coefficient variations have been studied by the frequency function as in Figure (6), and that the largest value absorption coefficient corresponds to the pure tin oxide at the value 16.6874 cm^{-1} corresponding to the wavenumber 574.683cm $^{-1}$, and the smallest value of absorption coefficient corresponds to the Fe doped tin oxide at the value 12.9644 cm^{-1} corresponding to the wavenumber 1384.64 cm^{-1}.

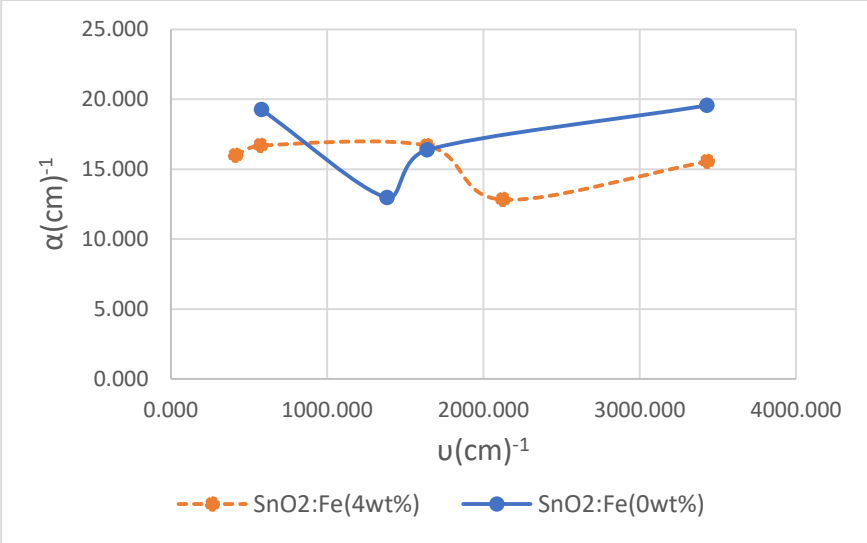


Figure (6): the absorption coefficient by the wavenumber function of pure SnO_2 and Fe doped SnO_2 powder by (4 wt%) .

Figure (7) shows the optical conductivity of the pure tin oxide and Fe doped tin oxide by (4 wt%) powder , where the values of the optical conductivity in the pure sample ranges between [0.0807-0.0830] $(\Omega cm)^{-1}$. where the highest value was corresponds to the Fe doped tin oxide at 0.0818 $(\Omega cm)^{-1}$ corresponding to the wave number (1640.16) cm^{-1} for Fe doped SnO_2 , and the smallest value corresponds to the Fe doped tin oxide at the value 0.0624 $(\Omega cm)^{-1}$ corresponding to the wavenumber (3431.71) cm^{-1}.

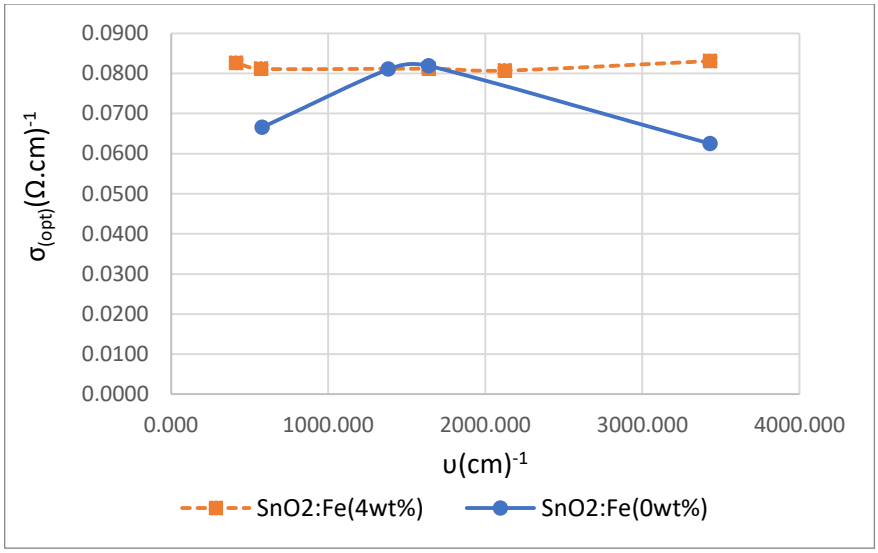


Figure (7): the optical conductivity by the wavenumber function of pure SnO_2 and Fe doped SnO_2 powder by (4wt%) .

Conclusions:

1. The pure tin oxide FTIR spectrum has shown some vibrational frequencies within the range [400-4000] cm^{-1} which are (415.585 - 574.683 - 1641.13 – 2125.3- 3432.67) cm^{-1}

2. The FTIR spectrum of the iron doped tin oxide by 4wt% showed vibrational frequencies within the range [400-4000] Cm-1, the most notably are: (3431.71-1640.16-1384.64-580.49) cm^{-1}

3. The absorbance value for the pure sample varies within the range [0.557 – 0.725], and for the doped sample, the absorbance value varies within the range [0.5630 – 0.8503].

4. The absorption coefficient value varies within the range of the pure sample [12.825 – 16.687] cm^{-1} , and for the doped sample, the absorption coefficient value varies within the range [12.9644 – 19.5570]cm^{-1}.

5. The optical conductivity value σ_{opt} for the pure sample varies within the range [0.0807 – 0.0830]$(\Omega cm)^{-1}$, for the doped sample, the value of the optical conductivity varies in the range [0.0624 – 0.0818] $(\Omega cm)^{-1}$.

8. The Fourier transformed infrared (FTIR) spectrum showed a band O – Sn – O and Sn – O stretching vibration

REFERANCE:

[1] - Z. Ying, Q. Wan, Z. Song, S. Feng, (2004) Nanotechnology , 15 No 11, 1682.
[2] G. McCarthy, J. Welton , (1989) , Powder Diffraction, 4, 156.
[3] A. Singh, U. Nakate, (2013), Adv. Nanoparticles 2, 66.
[4] - Jarzebski Z. & Marton J. (1976), "Physical Properties of SnO2 Materials", Journal of the Electrochemical Society, 199-205.
[5] W. Hamd, (2009), "Elaboration par voie sol-gel et étude microstructurale de gels et de couches minces de SnO2", Thèse de doctorat, Univ de Limoges,.
[6]- ROUESSAC.F, ROUESSAC,A,(2004), Analyse Chimique Méthodes et Techniques Instrumentals Modernes, Dunod, Paris.
[7]- MAGET.V,(2005), Développement de Méthodes de traitement de signauxspectroscopiques: estimation de linge de base et du spectre de raie, Univ Henri Poicré.
[8] SAKNI.L. ,(2017), '' Studying the structural of Fe doped tin oxide*"*, Master thesis , Alwadi university .
K. L. Chopra, (1985), " Thin Film Phenomena ", Mc. Graw-Hill, New York ,. [9]
[10] AlJAWAD , S. (2016), '' Studying effect of doping on the structural and optical properties of tin oxide thin films'' , Journal of engineering and technology , Vol.34.
[11] MANSOUR, M, (2012),'' Studying the structural and optical properties of ZnO:Cu thin films by APCVD method'' , Vol.5.
[12] S.S Al-Rawi, S. J. Shakir and Y N. Husan, (1990), "Solid State Physics",Pbpublishing of Mousal University Arabic Version .
[13] ZAID, A, (2012), ''Studying the structural and optical properties of NiO thin films'' , Master thesis , Dyala University .