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:

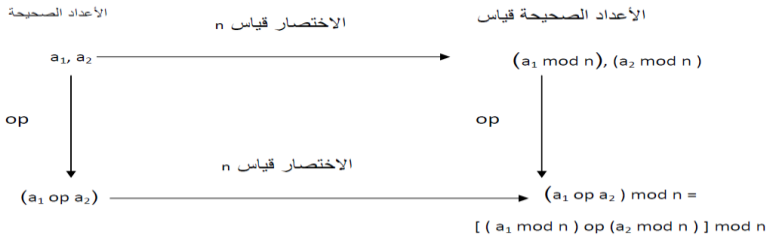
$(-1).(-1) \equiv 1 \ mod \ n$ وَ $(1)^{-1} \equiv 1 \ mod \ n$ لأن:

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

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.

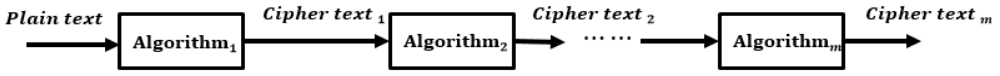
بناءً على كل ما سبق قمنا بتوسيع جدول المقابلات العددي. كما اقتراحنا فكرة تركيب التوابع في الفقرات اللاحقة.

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: $\gcd(\mathrm{k}, \varphi(\mathrm{n})) = \gcd(5,618) = 1$

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: $\gcd(\mathrm{a}, \mathrm{n}) = \gcd(3,619) = 1$، 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:

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

للتشفير: 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
	⺶	⛏	輪	☬	♻	⚳	Φ	⚥

ومنه النص المشفر : " ⺶⛏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.

المقابل العددي	الرمز	المقابل العددي	الرمز	المقابل العددي	الرمز	المقابل العددي	الرمز	المقابل العددي	الرمز
0	✍	127	o	254	ሂ	381	克	508	♔
1	✾	128	ô	255	ሃ	382	出	509	♕
2	✿	129	Ö	256	ሄ	383	勒	510	♖
3	❀	130	Œ	257	ህ	384	吉	511	♗
4	!	131	œ	258	ሆ	385	名	512	♘
5	ጀ	132	P	259	ሇ	386	含	513	♙
6	#	133	p	260	ለ	387	吾	514	♚
7	$	134	Q	261	ሉ	388	哦	515	♛
8	%	135	q	262	ሊ	389	場	516	♜
9	&	136	R	263	ላ	390	娜	517	♝
10	(	137	r	264	ሌ	391	字	518	♞
11	)	138	S	265	ል	392	尔	519	♟
12	*	139	s	266	ሎ	393	尺	520	♠
13	,	140	Ş	267	ሏ	394	屁	521	♡
14	ˎ	141	T	268	ሐ	395	平	522	♢
15	.	142	t	269	ሑ	396	开	523	♣
16	/	143	™	270	ሒ	397	弗	524	♤
17	:	144	u	271	ሓ	398	德	525	♥
18	;	145	U	272	ሔ	399	提	526	♦
19	?	146	Ù	273	ሕ	400	斯	527	♧
20	@	147	Û	274	ሖ	401	杰	528	♨
21	[	148	Ü	275	ሗ	402	東	529	♩
22	ሺ	149	Ü	276	መ	403	比	530	♪
23	]	150	v	277	ሙ	404	治	531	♫
24	^	151	V	278	ሚ	405	漢	532	♬
25	_	152	w	279	ማ	406	煙	533	♭

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	ョ	324	ቈ	451	☍	578	⚠
71	†	198	ょ	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	০	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	◥		