جامعة دمشق
Damascus University

كلية العلوم
Faculty of sciences

قسم الرياضيات
Department of Mathematics

# دراسة حول تطبيقات نظرية الأعداد في التشفير

**A Study *about applications of number theory in* cryptography**

**رسالة أُعدت لنيل درجة الماجستير في الرياضيات اختصاص جبر وهندسة**

**إعداد**

**الطالب : سليمان زغيَر**

**إشراف**

**الدكتور: يحيى قطيش**

1439هـ –2018 م

# شكر وتقدير

**أشكرك ربي على نعمك التي لا تُعد ، وآلائك التي لا تُحد ، أحمدك ربي وأشكرك على أن يسرت لي إتمام هذا العمل على الوجه الذي أرجو أن ترضى به عني.**

**ولِّما كان من تمام شكره سبحانه شكر أولي الفضل فإني أتقدم بأسمى آيات الشكر والتقدير وعظيم الامتنان إلى أستاذي ومشرفي الفاضل الدكتور يحيى قطيش الذي أكرمني الله بشرف أبوَّته العلمية فلم يألُ جهداً في توجيهي وإمدادي بما احتجت إليه و تقديم النصح والإرشاد مع طول نفس ورحابة صدر ، أجزل الله له المثوبة ونفع به ورفع مقامه.**

**كما وأتقدم بخالص شكري وتقديري إلى أساتذتي الموقرين في لجنة الحكم**

**أ.م.د. شوقي الراشد و أ.م.د. محمد فراس الحلبي**

**لتفضُّلهم علي بقبول مناقشة هذه الرسالة على كثرة شواغلهما وضيق وقتهما فهم أهل لسد خللها وتقويم معوجها والإبانة على مواطن القصور فيها سائلاً الله أن يُثيبهم عني خيراً وأن يأجرهما ويرفع درجتهُما.**

**ويوجب علي الاعتراف بالفضل أن أشكر جميع أساتذتي الفضلاء في قسم الرياضيات في كلية العلوم بجامعة دمشق.**

**ولا يفوتني أن أتقدم بالشكر والامتنان لكل من ساهم في مساعدتي فلهم في النفس منزلة وإن لم يسعف المقام لذكرهم.**

# الإهداء

إلى من بلغ الرسالة وأدى الأمانة ... ونصح الأمة ... إلى نبي الرحمة ونور العالمين .

"سيدنا محمَّد صلى الله عليه وأله وصحبه وسلَّم"

إلى اللذين أسديا لحياتي بعد وجودي أكبر معروف ... إلى اللذين أيقظا في عقلي ما كان غافياً ، وأضاءا في قلبي ما كان مظلماً ، إلى من في كل أمري أقتدي بِهما وأتحرك في فلكِهما نجماً يقتبس من الشمس نورها ومن القمر ضياءه طالباً بذلك رضاهما متوجهاً به إلى رضاء الله راجيه أن يطيل عمريهما ويبارك لهما عملِهما...

"أبي وأمي الغاليين"

إلى سندي وقوتي ... إلى من آثرني على نفسه ومنحني الأمل والتفاؤل ...

أخي محمد أبو حمزة

إلى من ساندوني لحظة بلحظة، إلى مصدر قوتي .... إلى أزهار الياسمين التي تفيض حباً ونقاءً وعطراً

"إخوتي وأخواتي الغاليات"

إلى توأم روحي ورفيقة دربي ، إلى صاحبة القلب الطيب والنوايا الصادقة ،إلى من رافقتني في السراء الضراء .... زوجتي الغالية

إلى ملائكتي الصغار ،الوجوه المفعمة بالبراءة ، إلى من أرى الأمل في عيونهم

أولادي سفيان ومحمد أمين

إلى من تحلوا بالإخاء وتميزوا بالوفاء إلى ينابيع الصدق الصافي إلى من معهم سرت وسعدت ...

"أصدقائي"

إلى هؤلاء جميعاً أتوجه بهذا الإهداء يحتويه ويحيطه فضلُ الله فهو سبحانه صاحب الفضل الأول وصاحب المِنَّة العظمى وإليه يرجع الأمر كله وهو يهدي السبيل.

سليمان

**Damascus University**

**Faculty of sciences**

**Department of Mathematics**

# A Study *about applications of number theory in* cryptography

**A Dissertation Submitted In Partial Fulfillment Of**

**The Requirements For The Master Degree In**

**Mathematics**

**By**

**Suleiman Zgheer**

**Supervision By**

**Dr. Yahia Qtaesh**

1439-2018

# الفهرس

# المُلَخَّصُ

تمَّ في هَذه الرسالةِ بناءُ خوارزميةٍ لحلِّ معادلةِ ديوفانتس الخطيةِ باستخدامِ نظامِ العدِّ الثلاثيِّ من أجلِ ($x_i \in \{0, 1, 2\}$) وذلك بإضافةِ شروطٍ خاصةٍ على معاملاتها ، وقد جُمعتْ هذه الشروطُ في المتَّجِهِ المتعامِدِ المضاعَفْ الذي قُمْنا بتعريفهِ وإضافته لهذا العمل .

فضلاً عن ذلك، فقد تمَّ بناءُ نظامِ التشفيرِ SY في حالةِ استُخدمَ المتَّجِهُ المتعامِدُ المضاعَفُ ونظامُ العدِّ الثلاثيِّ ، حيثُ اعتَمد هذا النظامُ على الخوارزميةِ التي تحلُّ معادلة ديوفانتس والمتَّجِهَ المتعامِدَ المضاعف ونظامَ العدَّ الثلاثيِّ ، وأخيراً قَدَّمنا مثالاً تطبيقياً عن هذا النظام .

الكلمات المفتاحية: التشفير ، معادلة ديوفانتس الخطية ، المفتاح العام ، نظام العد الثلاثي المتجه المتعامد .

# ABSTRACT

In this paper , we will build an algorithm to solve the Diophantine equation with this vector in ternary number system ($x_i \in \{0 ,1 ,2 \}$)and develop special conditions for it .
These conditions have been combined in a multiple orthogonal vector that defined in above .
then we will present a new public key cryptosystem based on algorithm and on multiple orthogonal vector with an example to illustrate the system.



Keywords : Linear Diophantine equation ,cryptography, public key , ternary number system, orthogonal vector

## مقدمة:

إنَّ الهدفَ الأساسيُّ في هذا البحث هو محاولة الوصولِ إلى نتائجَ جديدةٍ في هذا المجال بعد دراسةُ تطبيقاتِ نظريةِ الأعدادِ في التشفير، حيثُ قسَّمنا العملَ إلى أربعةِ فصولٍ ، قدمنا في الفقرة الأولى من الفصلِ الأولِ أساسيات نظرية الأعداد ، ومنها العمليات بالمقاس n وبعضَ التعاريف والمبرهنات الأساسية كمبرهنة اولر وفيرما ، والبواقي الصينية ، ومفاهيم الكسور المستمرة ، والبواقي والمصفوفات .

أمّا الفقرةُ الثانيةُ من هذا الفصل ،فقد خُصصت لعرض أساسياتِ علم التعمية أو التشفير ،والتعاريف الأساسية ، وفي الفقرة الثالثةِ من هذا الفصل فقد درسنا التشفير الكلاسيكي ،الذي اعتمد على تشفير كتلةِ بحرف واحد أو حرفين ،وتشفير المصفوفاتِ ، وتوضيحِ مفهوم التشفيرِ بالمفتاح العام ، وأهم خوارزمياتهِ (RSA) ،ووضحنا ذلك بأمثلةٍ مناسبةٍ.

- أمّا الفصلُ الثاني فقد تمَّت فيه دراسةُ تطبيقِ مبرهنات اولر وفيرما في التشفير الأسِّي ، حيثُ استخدمنا الأسَّ القياسيَّ كما استخدمنا هذه المبرهنات في تشفير المفتاح العام ،وخاصة في الخوارزمية (RSA) وانتقلنا من التشفير الكلاسيكي الذي يستخدم حرفاً إلى التشفيرِ المتقدمِ الذي استخدم محارفَ وكلماتٍ وهنا استخدمنا جدول ASCII .

وفي الفقرة الثانية من الفصل الثاني ، عرضنا تطبيقاتَ البواقيِ التكعيبية ، والتي استخدمت الأس القياسي وقدمنا بعضَ الخوارزميات المستخدمة ، ومثال على كل منها .

- والفصل الثالث تضمنَ فقرتين ، الأولى خُصصتْ لعرض تطبيقاتِ نظريةِ البواقي الصينية (CRT) في التشفير ، حيث استُخدمت في المشاركة السريةِ بشكل مباشر وفي مخططات العتبة بالإضافة لأنظمة استخدمت (CRT) كنظام Cao-Li .

أما الفقرة الثانية من الفصل الثالث فقد خصصت لدراسة الكسور المستمرة واستخدامها في القيمة الأسية الصغرى وكذلك في اختراق خوارزمية RSA والحصول على المفتاح الخاص انطلاقاً من معلومات المفتاح العام وهذا ما عُرف باسم هجمات (Winer) .

- وأخيراً في الفصل الرابع تمت دراسة أنظمة تشفير بالاعتماد على مسألة حقيبة السارق

(حقيبة الظهر) (Knapsack) في الحالتين التي تكون فيها المعاملات متزايدة أو متعامدة .

وفي الفقرة الثانية من هذا الفصل قمنا بتعريف متجه جديد والذي ضم ثلاثة شروط وهو المتجه مضاعف التعامد بالإضافة إلى وضع خوارزمية لحل أي معادلة ديوفانتس خطية بمعاملات تحقق

شروطَ المتجه مضاعف التعامد ، كما قمنا ببناء نظامِ تشفيرٍ يحاكي نظام Hellman أسميناه نظام التشفير SY ، ولكنَّه تميزَ ببعض الخواص ومنها استخدامُ المتجهِ مضاعف التعامد ، واستخدام نظام العد الثلاثي بدلاً من الثنائي ، وبهذا النظام نكون قد عممنا مسألة حقيبة السارق التي حلولها {1, 0} إلى معادلة ديوفانتس الخطية التي حلولها {0,1,2} ، ونأمل أنَ تكونَ هذه الخواصُ التي أضفناها تزيد من قوة دفاعات هذا النظام ضد الهجمات بعد أن تتم برمجتهِ .

أخيراً , لا بد من ذكر النتائج التي تم التوصل إليها في هذه الرسالة وهي كالآتي:

- جميعُ نتائج الفصل الرابع جديدةٌ.

هذا فإننا نأمل أن نكونَ قد وفقنا في هذا العمل إلى إضافة بصمةٍ جديدةٍ تساهمُ في تطُّور هذا العلم.

في النهاية لابد من شكرِ كلّ مّن ساهمَ في إنجازِ هذا العملِ بهذه الصورة ، ونخصُّ بالشكرِ والتقدير قسمَ الرياضيات في كلية العلوم بجامعة دمشق ممثلاً بجميع أعضائه لما قدموه لنا في رحلة إعداد هذه الرسالة.

دمشق في 2018

# الفصلُ الأَوَّلُ

## مفاهيمٌ أساسيَّةٌ في نظريةِ الأعدادِ والتَشْفيرِ

نقدِّمُ في هذا الفصلِ بعضَ المفاهيمِ الأساسيَّةِ في نظريةِ الأعدادِ بالإضافةِ للمفاهيمِ الأساسيَّةِ للتشفيرِ والَّتي تُعتبرُ حجرَ الأساسِ لهذا البحثِ ، وسنستخدمُ الأحرفَ اللاتينيَّةَ الصغيرةَ للدلالةِ على الأعدادِ الصحيحة ،كما سنستخدمُ الأعدادَ $P_1, P_2, P_3, \dots$ للدلالةِ على الأعدادِ الأوليِّةِ ، وسنستخدمُ حروفَ اللغــة الانكليزيَّةِ للتعبيرِ عن نصِ الرسالــةِ ،والرمزَ $P$ للرسالةِ الصريحةِ ،والرمزَ $C$ ليدلَّ على الرسالةِ المشفَّرةِ .

### 1−1 تعاريف ومفاهيم أساسية في نظرية الأعداد :[1]

**(1−1−1) تعريف:** نقولُ إنَّ $a, b$ متطابقَيْنِ بالمقاسِ $n$ إذا وفقط إذا كان $n|(a-b)$

ونكتبُ التطابقَ $a \equiv b(\ mod\ n)$ ، وإذا لمْ يتحقّق ذلك نقولُ إنَّ $a$ لا يطابقُ $b$ بالمقاسِ $n$ .

**(1−1−2) مبرهنة:** إذا كانَ $c \equiv d(\ mod\ n)$ , $a \equiv b(\ mod\ n)$ .عندئذٍ يكونُ

$$ac \equiv bd(\ mod\ n) \quad \text{و} \quad a + c \equiv b + d\ (mod\ n)$$

**(1−1−3) تعريف صف التكافؤ:[1]**

كلُّ العناصرِ الَّتي تكافئُ $a$ بالمقاسِ $n$ تدعى صفَّ تكافُؤْ $a$ ،ويُرْمزُ لها بـــ $[a]$

ويمكنُ أن يُرَمزَ لها بـــ $\bar{a}$

مثال صفَّ التكافؤ 0 بالمقاسِ 5 هو $[0] = \{\dots, -10, -5, 0, 5, 10, \dots\}$

**(1−1−4) نتيجة:** من تعريفِ التطابقِ ينتجُ ، إنه إذا كان $a \equiv b(\ mod\ n)$ ،فهذا يعني إن $a, b$ ينتميانِ إلى صفِّ تكافؤٍ واحدٍ من صفوفِ البواقي بالمقاسِ $n$ .

تدعى المجموعة $\mathbb{Z}_n = \{0,1,2,3, \dots, (n-1)\}$ مجموعةَ البواقي التامَّةِ ،ونَعرِفُ عليها عمليتَيْنِ $(\cdot_n), (+_n)$

### (1−1−5) تعريف الجمع بالمقاس n (the addition Modulo n) :[1]

أياً كان $[a] \in \mathbb{Z}_n, [b] \in \mathbb{Z}_n$ نعرِفُ الجمعَ على $\mathbb{Z}_n$ كالتالي $[a]+_n[b] = [a+b]$

وهي عمليةٌ تبديليةٌ وتجميعيَّةٌ و $[0]$ هو الحياديُّ فيها وفيها :

$$\exists\, [-a] \in \mathbb{Z}_n \;; [a]+_n[-a] = [0]$$

### (1−1−6) تعريف الضرب بالمقاس n (the Multiplication Modulo n): [1]

أياً كان $[a], [b] \in \mathbb{Z}_n$ فإننا نعرفُ الضرب على $\mathbb{Z}_n$ كما يلي :

$$[a] \cdot_n [b] = [a \cdot b]$$

**(1−1−7) نتائج:** 1− الضربُ المقاسيُّ هو عمليةٌ تبديليةٌ وتجميعيَّةٌ والعنصرُ $[1]$ هو الحياديُّ ويحقِّقُ

$$\exists [0] \in \mathbb{Z}_n \;; [a] \cdot_n [0] = [0]$$

$$\forall [a], [b], [c] \in \mathbb{Z}_n \;; [a] \cdot_n \{[b]+_n[c]\} = \{[a] \cdot_n [b]\}+_n\{[a] \cdot_n [c]\}$$ - 2

3− إذا كان العددانِ $a, b$ أَوَّليَّانِ نسبِّياً فيما بينهما أي $gcd(a,b) = 1$

ونعرِّف المجموعةَ

$$\mathbb{Z}_n^* = U_n = \{m : m \in \mathbb{N}^* \;\; m < n \,, \gcd(m,n) = 1\}$$

**مثال 1 :**

$$\mathbb{Z}_4^* = U_4 = \{[1], [3]\}$$

$$\mathbb{Z}_7^* = U_7 = \{[1],, [2], [3], [4], [5], [6]\}$$

### (1−1−8) مبرهنة:

$[a] \in \mathbb{Z}_n$ يملِكُ نظيرَ ضَرْبَيْ $[b]$ إذا وفقط إذا كان $gcd(n,a) = 1$

أيْ $[a].{}_n [b] \equiv [1]\ (mod\ n)$

**(1−1−9) تعريف:** نقولُ إنَّ الصفوفَ $[a],[b]$ قواسمٌ للصفر إذا كان $[a][b]=[0]$ وكلاً من $[a],[b]$ غيرَ صفريٍّ.

**(1−1−10) تعريف:** نقولُ إنَّ العدَد $a\in\mathbb{Z}_n$ هو واحديٌّ إذا كان يوجدُ $b\in\mathbb{Z}_n$ بحيثُ يكون

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

**(1−1−11) تعريف دالة اولر(Eulers function) : [1]**

نعرِّفُ دالة اولر بأنها عددُ الأعدادِ الواحدية في $\mathbb{Z}_n$ ويُرْمَزُ لها $\phi(n)$ أي أن $\phi(n)=|U_n|$

مثال: $\phi(7)=|U_7|=6$

**(1−1−12) مبرهنة لاغرانج (Lagrangestheorm):[ 22]**

إذا كانت $G$ زمرةٌ منتهيةٌ و $H$ زمرةً جزئيَّةً من $G$ عندئذٍ مرتبةُ $(H:1)$ تقسمُ $(G;1)$

**نتيجة:** إذا كانت $G$ زمرةً منتهيةً ،وكان $a$ عنصراً من $G$ عندئذٍ $|a|\,|\,|G|$

**(1−1−13) مبرهنة اولر(Eulerstheorm):[1]**

إذا كان $(a,n)=1$ فإنَّ $a^{\phi(n)}\equiv 1\ (modn)$

الإثبات: بما أنَّ $(U_n\ ,\cdot_n)$ زمرةٌ ولكونِ $|U_n|$ هو عددُ العناصرِ في $U_n$ عندئذٍ وحَسْبَ لاغرانج $[a]^{|U_n|}=[1]$ (لأجل كل $[a]\in U_n$ ) وبالتالي $a^{\phi(n)}\equiv 1(\ mod\ n)$

**مثال 2 :**

$$U_8=\{1,3,5,7\}\Longrightarrow\phi(8)=U_8=4$$

ومنه $1^4=1\ ,3^4=81\equiv 1(mod\ 8),5^4=625\equiv 1(mod\ 8)$

$$7^4=2401\equiv 1(mod\ 8)$$

**(1−1−14) نتيجة:** إذا كان $\mathrm{p},\mathrm{q}$ عددينِ صحيحَيْنِ موجبَيْنِ أوليينِ فيما بينهما .عندئذٍ:

$$\emptyset(\mathrm{p}.\mathrm{q})=\emptyset(\mathrm{p}).\emptyset(\mathrm{q})$$

الاثبات: ليكن $p, q$ عَدَدَيْنِ أوليَيْنِ عندئذٍ الأعدادُ الأصغرُ من $p.q$ وليست أوليةً مع $p$ هي $\{p, 2p, 3p, \dots, (q-1)p\}$ عددها $(q-1)$

والأعدادُ الأصغرُ من $p.q$ وليستْ أوليةً مع $q$ هي :

$\{q, 2q, 3q, \dots, (p-1)q\}$ عددها $(p-1)$

للحصولِ على $\emptyset(pq)$ نطرحُ من الجداءِ $(pq)$ عددَ الأعدادِ التي ليست أوليةً مع $p$ وليست أوليةً مع $q$ ومنه

$$\begin{aligned}\emptyset(pq) &= pq - 1 - (p-1) - (q-1)\\ &= pq - 1 - p + 1 - q + 1\\ &= pq - p - (q-1) = p(q-1) - (q-1)\\ &= (q-1)(p-1) = \emptyset(q).\emptyset(p)\end{aligned}$$

**(1−1−15) نتيجة**: الدالَّةُ $\emptyset$ دالَّةٌ زوجيَّةٌ من أجلِ $n \geq 3$

الإثبات: ليكن $n$ عدداً صحيحاً نميِّزُ حالتَيْنِ

1)- إذا كان $n$ أولياً $\Leftarrow \quad \emptyset(n) = n - 1$

2)- إذا كان $n$ ليس عدداً أولياً فهو يُكْتَبُ على شكلِ جداءِ قوى لــ أعدادٍ أوليَّةٍ (حَسْبَ المبرهنةِ الأساسيةِ في الحسابِ) $n = p_1^{k_1}.p_2^{k_2}.\dots.p_n^{k_n}$

وكونَ الدالةِ $\emptyset$ ضربيَّةً فإن :

$$\emptyset(n) = P_1^{K_1-1}P_2^{K_2-1}\dots P_n^{k_n-1}(p_1-1)(p_2-1)\dots(p_n-1)$$

وهو جداءُ أعدادٍ زوجيَّةٍ ومنه $\emptyset$ دالَّةٌ زوجيةٌ.

## (1−1−16) نتائج من مبرهنة اولر:[1]

☒ ليكن $p$ عدداً أولياً عندئذٍ $a^p \equiv a(mod\ p)$ لأجلِ أيِّ عددٍ صحيحٍ $a$ و $(a, p) = 1$

مثال 3: $4^5 = 1024 \equiv 4(\text{mod } 5), 3^5 = 243 \equiv 3(\text{mod } 5)$

☒ إذا كان $n$ عدداً أولياً ،عندئذٍ $a^{n-1} \equiv 1(mod\ n)$ لأجل كلِّ $[a] \in U_n$

**مثال 4:** $U_5 = \{1,2,3,4\}$ ومنه

$$1^4 = 1, 2^4 = 16 \equiv 1(\text{mod } 5), 3^4 = 81 \equiv 1(\text{mod } 5)$$

$$4^4 = 256 \equiv 1(\text{mod } 5)$$

☒ إذا كانَ $n = p_1^{k_1}.p_2^{k_2}.\dots.p_n^{k_n}$ عندئذٍ :

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_m}\right)$$

**(1−1−17) مبرهنة البواقي الصينيَّة:[1]** إذا كانتِ المقاساتُ $m_1, m_2, \dots, m_k$ أوليَّةً مثنى مثنى ، فإنَّهُ يوجَدُ لجملةِ التطابقاتِ الخطيَّةِ:

$$x \equiv a_1\ mod\ m_1$$

$$x \equiv a_2\ mod\ m_2$$

$$\vdots \qquad \vdots$$

$$x \equiv a_k\ mod\ m_k$$

حلٌّ وحيدٌ بالمقاسِ $m = m_1.m_2 \dots m_k$ .

**(1−1−18) تعريف: [3]** لِتكنْ $G =< g >$ زمرةً دوَّارةً منتهيَةً ، لأجلِ كلِّ عنصرٍ $g \in G$ يوجَدُ عُنصرٌ أصغريٌّ $a \in N_0$ بحيثُ $g^a = y$ نسمي $a$ اللوغاريتمَ المميَّزَ (discrete logarithm) للعنصرِ $y$ بالأساسِ $g$ وحسابِ المقدارِ $a = log_g y$ حيث $a, y$ عددَينِ صحيحَينِ تُدْعى بمسألةِ اللوغاريتمِ المميَّزِ (DLP)

**(1−1−19) البواقي التربيعيَّة (Squaring modulo):[3]**

الشكلُ العامُّ للتطابقاتِ التربيعيةِ هو $ax^2 + bx + c \equiv 0(\text{ mod } p)$ ويمكنُ أن نكتبَها بالشكلِ النموذجيِّ $x^2 \equiv a(\ mod\ p)$ ، وعندها نقولُ إن $a$ باقٍ تربيعيٌّ إذا وفقط إذا وجُدِ للتطابق حلٌّ.

ويمكنُ أنْ نعبَّرَ عن التربيعِ من خلالِ التطبيقِ :

$$q_n: \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* \to \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$$

$$x \mapsto x^2$$

والذي يحقِّقُ الخواصَ التاليةَ :

1) إذا كان $n = p$ عدداً أولياً فإن

- $\ker(q_n) = \{\mp 1\}$
- إذا كان $p > 2$ فإنهُ يوجَدُ بالضبط $\frac{p-1}{2}$ باقي تربيعٍ في $(\frac{\mathbb{Z}}{p\mathbb{Z}})^*$

2) إذا كان $n = pq$ جداءَ عددْينِ أوليْينِ فرديَّيْنِ مختلفيْنِ عندئذٍ:

- $\ker(q_n)$ تتكوَّنُ من أربعةِ عناصرٍ
- يوجَدُ بالضبطِ $\frac{\Phi(n)}{4}$ باقي تربيعٍ في $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$

**(1−1−20) تعريف رمز لوجاندر:[ 3]** ليكن $p$ عدداً أولياً يُعرفُ رمزُ لوجندر كالآتي

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & if\ \ a \equiv b^2\ (mod\ p) \\ 0 & if\ \ p|a \\ -1 & if\ \ other\ wise \end{cases}$$

**(1−1−21) مبرهنة Euler:[ 3]** ليكن $P > 2$ عدداً أولياً فردياً فإن $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}\ (mod\ p)$ . وهذه المبرهنةُ تُستخدمُ لحسابِ رمزِ لوجاندر على سبيلِ المثالِ النتيجةِ التاليةِ :

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1\ if\ p \equiv 1\ (mod\ 4) \\ -1\ if\ p \equiv 3(\ mod\ 4) \end{cases}$$

**(1−1−22) تعريف رمز جاكوبي (Jacobi symbol):[3]**

ليكن العددُ الطبيعيُّ $n = p_1^{k_1}.p_2^{k_2}.\dots.p_n^{k_n} > 1$ ولأجلِ $a \in \mathbb{Z}$ عندئذٍ يكون رمزُ جاكوبي :

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{\alpha_1} \dots \left(\frac{a}{p_r}\right)^{\alpha_r} \in \{-1,0,1\}$$

وفي حالةِ: $n = 1$ سيكونُ $\left(\frac{a}{1}\right) := 1$

ورمزُ جاكوبي يمكنُ حسابهُ دونَ الحاجةِ إلى تحليلِ $n$ إلى عواملِه.

**(1−1−23) تعريف:[3]** إذا كان $\left(\frac{a}{n}\right) = -1$ يعني أنَّ $a$ ليس باقياً تربيعياً بالمقاسِ $n$

وإذا كان $\left(\frac{a}{n}\right) = 1$ و $a$ ليسَ باقياً تربيعيّاً بالمقاسِ $n$ عندها نسمي $a$ باقياً زائفاً بالمقاسِ $n$ (pseudo-square modulo n).

**مثال 6** : عين الباقي الزائفِ من أجل $n = 5$ $n = 15$

$n = 5$:

| $a$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $a^2$ | 1 | 4 | 4 | 1 |
| $\left(\frac{a}{n}\right)$ | 1 | -1 | -1 | 1 |

$n = 15$:

| $a$ | 1 | 2 | 4 | 7 | 8 | 11 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|
| $a^2$ | 1 | 4 | 1 | 4 | 4 | 1 | 4 | 1 |
| $\left(\frac{a}{n}\right)$ | 1 | 1 | 1 | -1 | 1 | -1 | -1 | -1 |

لذلك تكونُ 8,2 بواقياً مزيفةً بالمقاسِ 15.

**(1−1−24) تعريف:[3]** نعرفُ المجموعاتِ التاليةَ

**1- مجموعةُ البواقي التربيعيةُ بالمقاسِ $n$**

$$Q_n := \left\{a \in \left(\frac{\mathbb{Z}}{a\mathbb{Z}}\right)^* : \exists b \in \frac{\mathbb{Z}}{n\mathbb{Z}} : a \equiv b^2 (mod n)\right\} = \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^2$$

**2- مجموعةُ البواقي غيرَ التربيعيةِ بالمقاسِ $n$**

$$\overline{Q_n} := \left\{a \in \left(\frac{\mathbb{Z}}{a\mathbb{Z}}\right)^* : \nexists b \in \frac{\mathbb{Z}}{n\mathbb{Z}} : a \equiv b^2\right\}$$

مثال 7 : $Q_5 = \{1,4\}$ , $\overline{Q_5} = \{2,3\}$

**(1−1−25) تعريف:[13]** ليكن m عدداً صحيحاً موجباً يحقق $m \geq 2$ ، نقول إنَّ العددَ الصحيحَ a باقٍ تكعيبيٌّ بالمقاسِ m إذا كان التطابقُ $x^3 \equiv a(\text{mod } m)$ يملكُ حلاًّ أمَّا إذا كان التطابقُ لا يملكُ أيَّ حلٍّ عندها نقولُ إن العددَ a ليس باقياً تكعيبياً بالمقاس m.

**مثال 8 :**

أيُّ عددٍ فرديٍّ $a$ هو باقٍ تكعيبيٌّ بالمقاسِ 2 لأنَّ التطابقَ $x^3 \equiv a(\text{mod } 2)$ يقبلُ جميعَ الأعدادِ الفرديةِ حلولاً له.

**(1−1−26) تعريف: [3]** ليكن $n \in \mathbb{N}$ نسمِّي هذا العددَ عددَ بلوم (Blum) إذا كان $n = p_1 p_2$ حيثُ $p_1, p_2$ أوليانِ مختلفانِ ويحققانِ أنَّ $p_i \equiv 3(\ mod\ 4)$ $\quad i = 1,2$

**(1−1−28) تعريف: [2]** الكسورُ البسيطةُ المستمرةُ المنتهيةُ هيَ كسورٌ من الشكلِ

$$\frac{A}{B} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-2} + \cfrac{1}{a_{n-1} + \frac{1}{a_n}}}}}}$$

ويُرْمَزُ له بـــ $\frac{A}{B} =< a_1, a_2, \dots, a_n >$ $\quad a_1 \in \mathbb{Z} \quad i = 2, .., n \quad a_i \in \mathbb{Z}^+$

**مثال 9 :**

$$\frac{-5}{4} = -2 + \frac{3}{4} = -2 + \frac{1}{\frac{4}{3}} = -2 + \frac{1}{1 + \frac{1}{3}} =< -2,1,3 >$$

$$\frac{32}{19} = 1 + \frac{13}{19} = 1 + \frac{1}{\frac{19}{13}} = 1 + \frac{1}{1 + \frac{6}{13}} = 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{6}}} =< 1,1,2,6 >$$

نسمي العددَ $c_k$ النسبةَ الجزئيَّةَ من المرتبةِ $k$ وإذا توقفْنَا بالكسرِ عند النسبةِ الجزئيَّةِ فإننا نحصلُ على التقريبِ $c_k$ من المرتبةِ $k$ .

## (1-1-29) المصفوفات :[16]

إذا كانت لدينا مصفوفةٌ 2×2 بمدخلاتٍ حقيقيةٍ $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ومتجه $\begin{pmatrix} x \\ y \end{pmatrix}$ في المستوي فإن جداءَ

المصفوفةِ بالمتجهِ يعطينا متجهاً جديداً

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$$ وهذا يكافئ $$\begin{matrix} ax+by=e \\ cx+dy=f \end{matrix}$$

ويكتبُ بالشكل $AX = B$ ولحلِّ المعادلةِ المصفوفيةِ $AX = B$ علينا إيجادُ $A^{-1}$ معكوسِ

المصفوفةِ $A$ ويكون الحل $X = A^{-1}B$

والمصفوفةُ $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ تملكُ معكوساً إذا وفقط إذا كان المحددُ غيرَ معدومٍ أي :

$D = \det(A) = ad - bc \neq 0$ والمعكوسُ في هذه الحالةِ يكون

$$A^{-1} = \frac{1}{\mathrm{D}}\begin{pmatrix} \mathrm{d} & -\mathrm{b} \\ -\mathrm{c} & \mathrm{a} \end{pmatrix} = \begin{pmatrix} \mathrm{D}^{-1}\mathrm{d} & -\mathrm{D}^{-1}\mathrm{b} \\ -\mathrm{D}^{-1}\mathrm{c} & \mathrm{D}^{-1}\mathrm{a} \end{pmatrix}$$

**مثال** 10 : $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2(\frac{Z}{26Z})$ ولنجدْ المعكوسَ

$D = 2 \times 8 - 3 \times 7 = -5 \equiv 21(\,mod\ 26)$ , (21,26)=1

ومنه للمصفوفةِ A لها معكوسٌ

$$A^{-1} = \begin{pmatrix} 5 \times 8 & -5 \times 3 \\ -5 \times 7 & 5 \times 2 \end{pmatrix} = \begin{pmatrix} 40 & -15 \\ -35 & 10 \end{pmatrix} \equiv \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} (mod\ 26)$$

## (1-1-30) مبرهنة: [16]

لتكن $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\frac{Z}{NZ})$ و $N\rangle 1$ و $D = ad - bc$ عندئذٍ القضايا التاليةٌ متكافئةٌ:

1. $gcd\,(D, N) = 1$
2. المصفوفةُ A تملك معكوساً
3. إذا كان $x, y$ ليس كلاهما معدوماً في $\frac{Z}{NZ}$ عندئذٍ $A\begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$
4. يوجدُ تَقابلٌ من $\left(\frac{Z}{NZ}\right)^2$ إلى $\left(\frac{Z}{NZ}\right)^2$ (تقابلُ واحدٌ إلى واحدٍ) .

**مثال 11** : حلُّ جملةِ التطابقاتِ التاليةِ:

$$a)\ \begin{matrix}2x+3y\equiv 1\ (mod26)\\ 7x+8y\equiv 2\ (mod26)\end{matrix} \quad b)\ \begin{matrix}x+3y\equiv 1\ (mod26)\\ 7x+9y\equiv 2\ (mod26)\end{matrix} \quad c)\ \begin{matrix}x+3y\equiv 1\ (mod\ 26)\\ 7x+8y\equiv 1\ (mod\ 26)\end{matrix}$$

الحل: للتطابقِ $(a)$ المصفوفةُ $A=\begin{pmatrix}2 & 3\\ 7 & 8\end{pmatrix}$ وهي المصفوفةُ المستخدمةُ في المثالِ السابقِ لذلك يكونُ حلُ الجملةِ

$$X=A^{-1}B=\begin{pmatrix}14 & 11\\ 17 & 10\end{pmatrix}\begin{pmatrix}1\\ 2\end{pmatrix}=\begin{pmatrix}10\\ 11\end{pmatrix}(\ mod\ 26)$$

المصفوفةُ في الجملتينِ (c), (b) لا تملكُ معكوساً وذلك لأن محدَّدها 14 ليسَ أولياً مع 26 أي (14,26)=2 لذلك نستطيعُ حلَ الجملةِ في المقاسِ 13 والتي تعطينا نفسَ الحلولِ

لدينا $A=\begin{pmatrix}1 & 3\\ 7 & 9\end{pmatrix}$ ومنه $D=\det(A)=14$ وبالتالي

$$A^{-1}=\begin{pmatrix}9 & -3\\ -7 & 1\end{pmatrix}=\begin{pmatrix}9 & 10\\ 6 & 1\end{pmatrix}(mod13)$$

ولدينا مصفوفةُ الثوابتِ $\begin{pmatrix}e\\ f\end{pmatrix}$ في الجملةِ (b) هي $\begin{pmatrix}1\\ 2\end{pmatrix}$ وبالتالي الحلُ سيكونُ $\begin{pmatrix}x\\ y\end{pmatrix}=\begin{pmatrix}3\\ 8\end{pmatrix}$

## (2−1) التشفير

**(1−2−1) الأبجدية** $(Alpha\ pets)$**:[16]** الأبجديَّةُ هي مجموعةٌ غيرُ خاليةٍ منتهيةُ A وعناصرُها هي الحروفُ وتدعى $|A|$ قدرةُ المجموعةِ A وهي عددُ عناصرِ المجموعةِ A .

العنصرُ $w=(w_1,w_2,\dots,w_n)\in A^n$ كلمةٌ من الأبجدية A من الطول $l(w)=n$ بحيث يكون $w=w_1w_2\dots w_n$ وطولُ الكلمةِ الفارغةِ صِفْرٌ

$$A=\{a,b,\dots,z\}\ ;\ crypto\in A^n$$

**(2−2−1) مفهوم التشفير:[10]** هوعمليةُ تحويلِ المعلوماتِ من نصٍّ واضحٍ وصريحٍ إلى شكلٍ مُعمى ( مخفيٍّ) ومن ثُمَّ إرسالُها بحيثُ المستلمُ هو الشخصُ الوحيدُ الذي يستطيعُ إعادتَها للنصِّ الأصليِّ والرسالةُ التي نريدُ إرسالَها تُدْعى النصَ الصريحَ (plain text) والرسالةُ المعالجةُ تدعى النص المشفَّرةَ (cipher text) ،وكلاهما يُكتَبانِ على شكلِ أحرفٍ متقطعةٍ

(alphabet) عمليةُ تحويلِ الرسالةِ الصريحةِ إلى رسالةٍ مشفرةٍ تُدَعى التشفيرُ (encryption) ، وعمليةُ الإعادةِ أو فكُّ التشفيرِ من نصٍّ مشفَّرٍ إلى نصٍ صريحٍ تُدْعى (decryption) والنصُ الصريحُ والمشفَّرُ يُفكَّكَانِ في وحداتِ رسالةٍ (message units) ، ووحدةُ الرسالةِ يمكن أن تكونُ زوجاً من الحروف أَيْ ثنائيةً (digraph) أو ثلاثيةً (triple) أو حتى كتلةً من 50 حرفاً.

### (3-2-1) تطبيق تحويل التشفير(enciphering transformation):[ 10]

هو دالة (تطبيق) تأخذُ أيْ وحدةَ رسالةٍ صريحةٍ وتعطينا وحدةَ رسالةٍ مشفرةٍ أيْ $f: P \to C$ حيثُ $P$ هي كلُ كتلِ النصِّ الصريحِ ، $C$ هي كلُّ وحداتِ الرسالةِ المحتملةِ المشفرةِ من وحداتِ الرسالةِ الصريحةِ ، أما التطبيقُ الذي يحوِّلُ النصَ المشفرَ إلى نصٍ صريحٍ يُدْعى تطبيقَ فكِّ التشفير (the deciphering transformation) $f^{-1}: C \to P$

ويمكن أن نمثِّلَ العلاقةَ بين تطبيقِ التشفيرِ وتطبيقَ فكِ التشفيرِ بالشكل :

$$P \xrightarrow{f} C \xrightarrow{f^{-1}} P$$

قبلْ البدءِ بعمليةِ التشفيرِ نهتمُ بالأشياءِ الرياضيةِ التي تكونُ الدوالُ مبنيةً عليها ، وغالباً ما تكونُ هذه الأشياءُ هيَ أعدادُ صحيحةُ . في البدايةِ نقومُ بتحويلِ الرسالةِ الصريحةِ إلى حروفٍ متقطعةٍ $A, B, \dots, Z$ ثم نقابلُها بالأعدادِ المكافئةِ لهذه الحروفِ وهي $0,1,2, \dots ,25$ ، وتُدْعى بالأعدادِ المكافئةِ للحروفِ المتقطعةِ .

لذلك مكانُ الحرفِ A سوفَ نضعُ الرقمَ 0 ،ومكانُ الحرفِ S سوفَ نضعُ الرقمَ 18 ،ومكانُ X نضعُ 23 ،وهكذا ويمكنُ أن نستخدمَ في وحداتِ الرسائلِ تكونُ ثنائياتٍ من 27 حرفاً وهي الأحرفُ A-Z وبالإضافةِ إلى الفراغِ (blank) ،وربما يكونُ الفراغُ في الأعداد المكافئةِ خارجَ Z فإذا كانَ لدينا الحرفان $x, y$ حيثُ

$$x, y \in \{0,1, \dots ,26\}$$
$$27x + y \in \{0,1, \dots ,728\}$$

- فمثلا :الثنائيةُ No تقابلُ 27×13+14=365

وإذا استخدمنا ثلاثيَة (ثلاثةَ أحرفٍ) ،فإننا نستخدمُ الصيغةَ

$$729x + 27y + z \in \{0,1, \dots ,19682\}$$

ويمكنُ أن نعمِّمَ ذلك لأكثرَ من ثلاثةِ أحرفٍ.

وسنقومُ في هذا الفصلِ بدراسةِ بعضِ طرقِ التشفيرِ الكلاسيكيةِ ، ومنها طريقةُ تشفيرِ قَيْصر والتشفيرِ بالكتلِ وطريقةُ $hill$ ، والتشفيرِ بالمصفوفاتِ من ثم ننتقلُ لأنظمةٍ حديثةٍ في التشفيرِ ومنها نظامُ المفتاحِ العامِ ونظامُ رابين ، ودراسةُ بعضِ الخوارزمياتِ التي هي نواةٌ لأنظمةٍ جديدةٍ .

## (1−2−4) طريقةُ تشفير قيصر (Julius Caesar) : [16]

هذه الطريقةُ استخدمها قيصرُ الرومِ لحمايةِ رسائلهِ في الحروب ، حيثُ استخدم الحروفُ المتقطعةِ الـــ 26 في الانكليزية A-Z مع الأعداد المكافئة لها 0-25 أي : $P \in \{0,1, \dots ,25\}$

لنحصلَ على وحدةِ الرسالةِ المشفرةِ ، ففيها نعرفُ التطبيقَ $f$ من المجموعةِ P إليها نفسَها من خلال قاعدةِ الربط التالية:

$$f: P \to P$$

$$f(p) = \begin{cases} p + 3 \; ; x < 23 \\ p - 23 \; ; x \geq 23 \end{cases}$$

بكلماتٍ أخرى: $f$ يضيفُ 3 بالمقاسِ 26 أي $f(p) \equiv (p + 3)(mod\ 26)$

**مثال 12 :** لنشِّفرَ كلمةَ (yes) أولاً نقومُ بتحويلِها إلى الأعدادِ المكافئةِ لها فتصبحُ 18 4 24 ، ومن ثم نضيفُ 3 بالمقاس 26 لتصبحَ 21 ,7 ,1 ، ثم تتحول إلى (BHV) وهي الرسالةُ المشفرةُ ، ولفكِ الرسالةِ المشفرةِ والرجوعِ للرسالةِ الأصليةِ نطرحُ 3 بالمقاسِ 26 ، نحول الرسالة (BHV) لأعدادٍ مكافئةٍ 21 ,7 ,1 ومن ثم نطرحُ 3 بالمقاسِ 26 لنحصلَ على 18 4 24 وهي حروفُ الرسالةِ الأصليةِ .

وهذا النوعُ من أنظمةِ التشفيرِ بسيطٌ جداً وهو سهلُ الاختراقِ ، لذا من المهمِ أن نَستخدم نوعاً أكثرَ تعميماً وهو الذي يستخدمُ التحويلَ الأفينيَّ (affine map) حيثُ تكونُ دالة الرسالةُ المشفرةُ فيه

$$C \equiv aP + b(\ mod\ N)$$

علماً أن $a\ ,\ b$ أعدادٌ صحيحةٌ (وكلاهما من مفتاحِ التشفيرِ) ولنأخذُ مثالاً على هذا التعميمِ.

**مثال 13** : شَفِرُ الرسالةِ (pay meow) مستخدمٌ التحويلَ الأفينيَّ في شيفرةِ قيصر ، ومفتاح تشفيرٍ مناسبٍ بالمقاسِ 26

الحل : باستخدام التحويلِ الافينيِّ مع مفتاحِ التشفيرِ a=7 , b=12 ، نكتبُ الأعدادَ المكافئةَ للرسالةِ لنحصلَ على

$$15\ 0\ 24\ 12\ 4\ 13\ 14\ 22 \rightarrow 13\ 12\ 24\ 18\ 14\ 25\ 6\ 10$$

وهذه الأرقامُ تكافئُ كلمةَ (nmgsozyk) ، وهي الرسالةُ المشفرةُ.

لفكِ تشفيرِ رسالةٍ اُستخدم فيها التحويلُ الأفينيُّ $C \equiv aP + b(\ mod\ N)$

لنحصلَ على الرسالةِ الصريحةِ P من C من خلالِ $P \equiv a`C + b`(\ mod\ N)$

حيثُ $a`$ هو معكوسُ $a$ بالمقاسِ N و b` هو $-a^{-1}b$ أي $b` = -a^{-1}b$ وهذا الكلامُ محقَّقٌ فقط عندما يكونُ $gcd(a, N) = 1$ خلافَ ذلك لا يجوز.

## (1-2-5) طريقةُ التشفيرِ بالكتلِ Block Ciphers : [16]

في هذهِ الفقْرة سوفَ نقومُ بتبديلِ كلِّ كتلةٍ مكوَّنَةٍ من حرفينِ من النصِ الصريحِ بكتلةٍ من حرفَيْنِ من النصِ المشفَّرِ ، وللتوضيحِ ذلك سنأخذُ مثالاً حيثُ تبدأُ الطريقةُ بتقسيمِ الرسالةِ إلى كتلٍ من حرفيْنِ وإضافةُ الحرفِ X للكتلةِ الأخيرةِ من الرسالةِ في حالِ عدم اكتمالها (لذلك حتماً آخرُ كتلةٍ ستحوي على حرفيْنِ) وتكونُ فكرةُ هذا النظامِ هي استخدامُ كتلٍ من الحروفِ وليس حرفاً واحداً .

**مثال 14:** لِنشفرَ النصَ التاليَ

THE GOLD IS BURIED IN ORONO

أولاً تُقسم الرسالةُ إلى كتلٍ من حرفين:

TH EG OL DI SB UR IE DI NO RO NO

ومن ثُمَّ نقومُ بتحويلِ هذه الحروفِ إلى الأرقامِ المكافئةِ لكلِّ حرفٍ فنحصلَ على:

19 7 4 6 14 11 3 8 l8 1 20 7

8 4 3 8 13 14 17 14 13 1 4

كلُ كتلةٍ من النصِ الصريحِ مثل $P_1\,P_2$ حُولِّت لــ كتلةٍ من النصِّ المشفرِ $C_1\,C_2$ من خلال التطابقِ

$$C_1 \equiv 5P_1 + 17P_2 (\text{mod } 26)$$

$$C_2 \equiv 4P_1 + 15P_2 (\text{mod } 26)$$

لتوضيحِ الكتلةِ الأولى مثلاً 19 7 حُولِّت إلى 25 6 وذلك لأنَّ :

$$C_1 \equiv 5.19 + 17.7 \equiv 6 (\text{mod } 26)$$

$$C_2 \equiv 4.19 + 15.7 \equiv 6 (\text{mod } 26)$$

وبتطبيقِ نفسِ الإجراءاتِ على كلِّ كتلةٍ من النصِ الصريحِ نحصلُ على كتلِ النصِّ المشفرِ من الأعدادِ المكافئةِ وهي :

25 6 18 2 23 13 21 2 3 9 25 23

4 14 21 2 17 2 11 18 l7 2

وعندما نُرجعُ هذهِ الكتلَ إلى الحروفِ المقابلةِ لها نحصلُ على :

GZ SC XN VC DJ ZX EO VC RC LS RC

أمّا عمليةُ فكِ التشفيرِ لهذا النصِ باستخدامِ التشفيرِ الكتليِّ ولإيجادِ كتلةِ النصِّ الصريحِ $P_1\,P_2$ المقابلةِ للنصِّ المشفرِ $C_1\,C_2$ نستخدمُ العلاقاتِ:

$$P_1 \equiv 17\,C_1 + 5\,C_2 (\text{mod } 26)$$

$$P_2 \equiv 18\,C_1 + 23\,C_2 (\text{mod } 26)$$

ويمكنُ أن نجدَ لهذا النظامِ توصيفاً آخراً عن طريقِ المصفوفاتِ

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} \equiv \begin{pmatrix} 5 & 17 \\ 4 & 15 \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} (mod\ 26)$$

ومنه نجدُ أنَّ المصفوفةَ $\begin{pmatrix} 17 & 5 \\ 18 & 23 \end{pmatrix}$ هيَ معكوسُ المصفوفةِ $\begin{pmatrix} 5 & 17 \\ 4 & 5 \end{pmatrix}$ بالمقاسِ 26

إنَّ عمليةِ فكِ التشفيرِ يمكنُ أن تعملَ من خلالِ استخدامِ العلاقةِ:

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} \equiv \begin{pmatrix} 17 & 5 \\ 18 & 23 \end{pmatrix} \begin{pmatrix} C_1 \\ C_2 \end{pmatrix} (mod\ 26)$$

### (1−2−6) طريقةُ تشفير $Hill$ : [16]

هذهِ الطريقةُ تعميمٌ للتشفيرِ بالكتلِ وفيها اعتمدَ Hill على تجزئةِ النصِ الصريح إلى كتلٍ مؤلفةٍ من n حرفِ تُحولُّ إلى أعدادٍ مكونةٍ من n عددٌ مكافئٌ ونحصلُ على النصِ المشفر من العلاقة

$C \equiv AP\ (mod 26)$ حيث A هي مصفوفةٌ مربعةٌ من المرتبةِ n وتحققُ :

$$C = \begin{bmatrix} C_1 \\ C2 \\ : \\ : \\ : \\ C_n \end{bmatrix} \qquad P = \begin{bmatrix} P_1 \\ P2 \\ : \\ : \\ : \\ P_n \end{bmatrix}$$

$C_1,\ C_2, \dots ,\ C_n$ كتلٌ من النصِ المشفرِ المقابلةِ لكتلِ النصِ الصريحِ $P_1,\ P_2, \dots ,P_n$، أخيراً كتلُ النصِ المشفرِ من الأعدادِ تُحولُّ إلى حروفِ فنحصلُ بذلك على رسالةٍ مشفرةٍ .

أمّا لعمليةِ فكِ التشفيرِ سوفَ نستخدمُ المصفوفةَ $A^{-1}$ والتي هي معكوسُ المصفوفةِ A بالمقاسِ 26 وبالتالي $A^{-1}A \equiv I(mod\ 26)$

ولدينا $A^{-1}C \equiv A^{-1}(AP) \equiv (A^{-1}A)P \equiv P\ (mod\ 26)$

لذلك نحصلُ على علاقةٍ بينَ النصِ الصريحِ و النصِ المشفرِ باستخدامِ التطابقِ

$A^{-1}C \equiv P(mod\ 26)$ وسوفَ نوضّحُ هذا التعميمَ من خلالِ المثالِ والذي استخدمنا فيه التشفيرَ بالكتلِ والمصفوفاتِ لأجلِ $n = 3$ ومصفوفةِ التشفيرِ $A = \begin{pmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{pmatrix}$

$$det\ A \equiv 5\ (mod\ 26) \qquad (detA, 26) = 1$$

ولتشفير النصِ الصريحِ بكتلٍ طولُ كلٍّ منها 3 سوفَ نستخدمُ العلاقةَ

$$\begin{pmatrix} C_1 \\ C_2 \\ C3 \end{pmatrix} = A^{-1} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} mod\ 26$$

**مثال 15** : شفرُ الرسالةِ *STOP PAYMENT* مستخدماً طريقةَ Hill

الحل : أولاً نجزئُ الرسالةَ إلى كتلٍ من ثلاثِ حروفٍ ونضيفُ للكتلةِ الأخيرةِ الحرفَ X لنكملَها إلى ثلاثِ حروفٍ فتصبحَ *STO PPA YME NTX*

نكتبُ الحروفَ المكافئةَ لنجدَ 18 19 14 15 15 0 24 12 4 13 19 23

فنحصلَ على أوَّلِ كتلةٍ من النصِ المشفرِ من خلالِ التطابقِ :

$$\begin{pmatrix} C1 \\ C2 \\ C3 \end{pmatrix} = \begin{pmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{pmatrix} \begin{pmatrix} 18 \\ 19 \\ 14 \end{pmatrix} (mod\ 26) \equiv \begin{pmatrix} 8 \\ 19 \\ 13 \end{pmatrix} (mod\ 26)$$

وبالقيامِ بنفسِ الخطواتِ لكلِّ كتلةٍ من الكتلِ نحصلُ على كتلِ النصِ المشفرِ وهي

8 19 13 13 4 15 0 2 22 20 11 0

وبعدَ التحويلِ تكونُ الرسالةُ المشفرةُ

*TTN NEP ACW ULA*

أمّا عمليةُ فكِ التشفيرِ للحصولِ على كتلِ النصِ الصريحِ من كتلِ النصِ المشفرِ ، فإننا نحصلُ عليها من خلالِ التحويلِ الآتي :

$$\begin{pmatrix} P_1 \\ P_2 \\ P3 \end{pmatrix} = A \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} (mod\ 26)$$

$A^{-1}$ هي معكوسُ A بالمقاسِ 26 وهي :

$$A^{-1} = \begin{pmatrix} 6 & -5 & 11 \\ -5 & -1 & -10 \\ -7 & -3 & 7 \end{pmatrix}$$

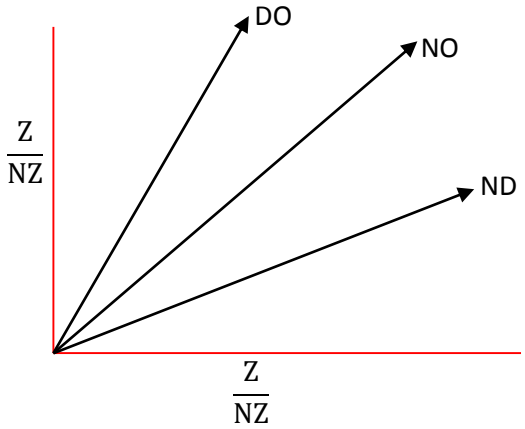
### (7−2−1) التشفير بالمصفوفات (Enciphering Matrices):[16]

بفَرضِ لدينا N حرفٌ متّقطعٌ فإنه يمكنُ أن نُرسلَ ثنائيةً كما في الفقرةِ السابقةِ ، أو نقومَ بمقابلةِ كلِّ ثنائيةٍ بمتجهٍ أو زوجٍ من الأعدادِ الصحيحةِ $\binom{x}{y}$ حيث كلٌّ من x , y مأخوذٌ بالمقاسِ N

على سبيلِ المثالِ إذا كان لدينا 26 حرفاً متقطعاً A-Z وتقابلُ الأعدادُ المكافئةُ 0-25 فإنّ الثنائيةَ (NO) تقابلُ المتجهَ $\binom{13}{14}$

حيث صورنا الثنائيةَ P على أنها نقطةٌ من المربعِ المنتظمِ $N \times N$

حيث $\frac{z}{NZ}$ منطبقٌ على مستقيمِ الأعدادِ ، والمستوي الذي كان يُرمزُ له $R^2$ هنا يُشيرُ إلى $\left(\frac{Z}{NZ}\right)^2$




نَرى من المبرهنةِ (1−1−30) أنه يمكنُ الحصولُ على تحويلِ التشفيرِ بالمتجهاتِ الثنائيةِ باستخدامِ المصفوفةِ المربعةِ درجة ثانيةً $A \in M_2(\frac{Z}{NZ})$ والتي لا تملكُ عاملاً مشتركاً مع $N$ أي

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad D = ad - bc, \qquad gcd(D, N) = 1$$

خاصةً أنَّ $P = \binom{x}{y}$ تعطينا كتلةَ نصٍ مشفَّرٍ $C = \binom{x`}{y`}$

من خلال القاعدةِ: $C = AP$ أي :

$$\begin{pmatrix} x` \\ y` \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

ولفك تشفيرِ الرسالةِ فإننا نطبقُ معكوسَ المصفوفةِ من خلال القاعدةِ

$$P = A^{-1}AP = A^{-1}C \implies \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \mathrm{D}^{-1}\mathrm{d} & -\mathrm{D}^{-1}\mathrm{b} \\ -\mathrm{D}^{-1}\mathrm{c} & \mathrm{D}^{-1}\mathrm{a} \end{pmatrix} \begin{pmatrix} x` \\ y` \end{pmatrix}$$

**مثال 16 :** باستخدامِ الحروفِ المتقطعةِ الإنكليزيةِ وباستخدامِ المصفوفة A المستخدمةِ في شيفرةِ HILL ، شفرُ وحدة الرسالة "NO".

الحل:

$$AP = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} 13 \\ 14 \end{pmatrix} = \begin{pmatrix} 68 \\ 203 \end{pmatrix} = \begin{pmatrix} 16 \\ 21 \end{pmatrix}$$

**توضيح:** لتشفيرِ متتاليةٍ من k ثنائية أي $P = P_1P_2 \dots P_K$ فإننا نكتب الــ k ثنائيةً (متجه) على شكلِ أعمدةٍ لمصفوفةٍ من المرتبةِ 2×k والتي أيضاً نرمزُ لها بالرمزِ P لنحصلَ بالنتيجةِ على رسالةٍ مشفرةٍ C من المرتبةِ 2×k حيث C=AP وهي الرسالةُ المشفرةُ للمتجهاتِ الثنائيةِ.

**مثال 17 :** شفّر الرسالة "*NO ANSWER*" مستخدماً التشفيرَ بالمصفوفاتِ

الحل: الأعدادُ المكافئةُ والمقابلةُ للرسالةِ المطلوبةِ كمتجهاتٍ ثنائيةٍ هي:

$$\begin{pmatrix} 13 \\ 14 \end{pmatrix} \begin{pmatrix} 0 \\ 13 \end{pmatrix} \begin{pmatrix} 18 \\ 22 \end{pmatrix} \begin{pmatrix} 4 \\ 17 \end{pmatrix}$$

وبالتالي سيكونُ

$$C = AP = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} 13 & 0 & 18 & 4 \\ 14 & 13 & 22 & 17 \end{pmatrix} = \begin{pmatrix} 68 & 39 & 102 & 59 \\ 203 & 104 & 302 & 164 \end{pmatrix}$$

$$\implies C = \begin{pmatrix} 16 & 13 & 247 \\ 21 & 0 & 168 \end{pmatrix}$$

وهي تقابلُ الرسالةَ المشفرةَ *(QVNAYQHI)*

**مثال 18** : بنفس معطياتِ المثَالينْ السابقَيْنِ فكَّ تشفيرِ الرسالةِ ( *FWMDIQ* )

الحل:

$$P = A^{-1}C = \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix}\begin{pmatrix} 5 & 12 & 8 \\ 22 & 3 & 16 \end{pmatrix} = \begin{pmatrix} 0 & 19 & 2 \\ 19 & 0 & 10 \end{pmatrix}$$

وهي الرسالةُ الصريحةُ *(ATTACK)* (الهجوم) المقابلةُ للرسالةِ المعطاةِ .

ولنفرضْ بأنّه لدينا معلوماتٌ محددةٌ والتي نريدُ تحليلَها لفكِ تشفيرِ سلسلةِ رسالةٍ مشفرةٍ ، وأننا نعلمُ بأنَّ العدوُ ( المتطفلَ ) يستخدمُ نظامَ المتجهاتِ الثنائيةِ والحروفَ المتقطعةِ التي عددها N ، وتحويلُ التشفيرِ الخطيِّ C=AP ، لكن بأيِّ حالٍ نحنُ لا نملكُ مفتاحَ التشفيرِ (المصفوفةَ A) ولا نملكُ مفتاحَ فكِ التشفيرِ (المصفوفة $A^{-1}$) .

لكن نفرضُ بأننا قادرون على تحديدِ زوجٍ من المتجهاتِ الثنائيةِ من النصِ الصريحِ او المشفَّرِ

$$C_1 = AP_1, C_2 = AP_2$$

وبما أننا حصلْنَا على هذه المعلوماتِ من التحليلِ المتكررِ للمعلوماتِ أو من أيِّ مصدرٍ (أنه أربعةُ حروفِ نصٍ صريحٍ تقابلُ أربعةً من المشفَّرِ) في هذه الحالة يمكنُنَا أن نعالجَ المسألةَ بتحديدِ $A^{-1}, A$ حيثُ نضعُ $P_1, P_2$ في مصفوفةٍ مرتبةٍ من المرتبةِ 2×2 ولتكنْ هذهِ المصفوفةُ $P$ وبشكلٍ مشابهٍ بالنسبةِ للأعمدةِ المشفرةِ $C_1, C_2$ نحصلُ على المصفوفةِ $C$ ، وبالتالي نحصلُ على المعادلةِ المصفوفيةِ من المرتبة 2×2 وهي $C = A$ , والتي يكونُ فيها $P, C$ معلومتَيْنِ لدينا و $A$ غيرَ معلومةٍ ، ويمكنُنَا أن نَحلَّ المعادلةَ والحصولَ على $A$ من خلالِ ضربِ الطرفينِ من اليمينِ بـــ $P^{-1}$ لنحصلَ على

$$A = APP^{-1} = CP^{-1}$$

وبشكلٍ مشابهٍ من المعادلةِ $P = A^{-1}C$ ، نحلُّها نحصلُ على $A^{-1}$ أي $A^{-1} = PC^{-1}$

**مثال 19** : فكُ تشفيرِ الرسالةِ (GFPYJPX?UYXSTLADPLW )

إذا علمتَ أنَّ المصفوفةَ المستخدمةَ للتشفيرِ من مرتبةِ 2×2 مع أبجديةٍ مكَّونةٍ من 29 حرفاً

متقطعاً وهي من $A \to Z$ باستخدامِ الأعدادِ المتكافئةِ والمقابلةِ لها إضافةً إلى $! = 28$ و

$?= 27$ والفراغ $= 26$

وبفرضِ أننا نعلمُ أنه آخرُ خمسةِ حروفٍ من النصِ الصريحِ ، أو توقيعِ الرسالةِ هو (KARLA) .

الحل : طالما أننا لا نعلمُ الحرفَ السادسَ من النصِ الصريحِ ، فإنه يمكنُنا استخدامَ آخرَ أربعةِ حروفٍ فقط لنصنعَ منهم متجهين ثنائيين من النصِ الصريحِ . لذلك يكونُ النصُ المشفرُ DP , LW المقابلُ لــ AR ,LA على الترتيبِ ، وبالتالي المصفوفةُ $P$ المكوَّنةُ من AR,LA والناتجةُ عن ضربِ المصفوفةِ فكِ التشفيرِ $A^{-1}$ بالمصفوفةِ $C$ المكوَّنةِ من DP,LW أي هي :

$$\Rightarrow \begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} = A^{-1} \begin{pmatrix} 3 & 11 \\ 15 & 22 \end{pmatrix}$$

$$\Rightarrow A^{-1} = \begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} \begin{pmatrix} 3 & 11 \\ 15 & 22 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} \begin{pmatrix} 3 & 13 \\ 23 & 17 \end{pmatrix} = \begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix}$$

الرسالةُ الكاملةُ للنصِ الصريحِ هي

$$A^{-1}C = \begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix} \begin{pmatrix} 6 & 15\,9 & 26 & 2724 & 1811 & 3 & 11 \\ 5 & 2415 & 23 & 2023 & 19\,0 & 15 & 22 \end{pmatrix}$$

$$= \begin{pmatrix} 18 & 1710 & 26 & 1913 & 1428 & 0 & 11 \\ 19 & 8\,4 & 0 & 2614 & 1310 & 17 & 0 \end{pmatrix}$$

وهي تقابلُ "*STRIKE AT NOON!KARLA*" (اضْرِبْ عند الظهيرةِ)

**(1-2-8) التطبيق الأفيني والمصفوفات:** لتعميمِ طريقةِ المتجهاتِ الثنائيةِ $P = \begin{pmatrix} x \\ y \end{pmatrix}$

بضربِها بمصفوفةِ $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\frac{Z}{NZ})$ وإضافةِ متجهٍ ثابتٍ $B = \begin{pmatrix} e \\ f \end{pmatrix}$ أي أن

$$C = AP + B \Rightarrow \begin{pmatrix} x` \\ y` \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix} \equiv \begin{pmatrix} ax + by + e \\ cx + dy + f \end{pmatrix}$$

وهذا ما يُسمَّى بالتطبيقِ الأفينيِّ والذي يشابهُ تطبيقَ التشفيرِ $C = aP + b$ الذي دُرست في شيفرةِ قيصر حيث استخدمَ حرفاً واحداً (حيث استخدمنا $\equiv$ لنقصدَ بها العناصرَ المدخلةَ بالمقاسِ $\mathrm{N}^2$)

معكوسَ التحويلِ والذي يعطينا P الذي أوجدناهُ بطرح B من الطرفَيْنِ ومن ثُمَّ الضربُ بــ $A^{-1}$

لكلا الطرفَيْنِ أي:

$$P = A^{-1}C - A^{-1}B$$

وهذا أيضاً تحويلٌ أفينيٌ $P = A`C + B`$ حيثُ $A` = A^{-1}$ , $B` = -A^{-1}B$

إذا افترضنا إننا نريدُ فكَ تشفيرِ رسالةٍ شُفرت بالتحويلِ الأفينيِّ مع المتجهاتِ الثنائيةِ مع N حرفاً متقطعاً ولنحددَ A , B (أو لنحدد $A` = A^{-1}$ , $B` = -A^{-1}B$ ) نحنُ بحاجةٍ على الأقل لثلاثةِ متجهاتٍ ثنائيةٍ من النصِ المشفرِ ولتكن $C_1, C_2, C_3$ المقابلةَ للمتجهاتِ الثنائيةِ للنصِ الصريحِ أي : $P_1, P_2, P_3$

$$P_1 = A`C_1 + B`$$
$$P_2 = A`C_2 + B`$$
$$P_3 = A`C_3 + B`$$

لإيجادِ $A`, B`$ نقومُ بطرحِ المعادلةِ الاخيرةِ من المعادلتين الأولى و الثانية ، ومن ثُم تنتجُ مصفوفةُ $P$ من المرتبةِ 2×2 أعمدتُها $P_1 - P_3, P_2 - P_3$ والمصفوفةُ $C$ التي أعمدتُها $C_1 - C_3, C_2 - C_3$ وبالتالي سوفُ نحصلُ على المعادلةِ المصفوفيةِ $P = A`C$

والتي يمكنُ أن تُحلَّ لأجلِ $A`$ ، كما فعلنا في حالة التحويلِ الخطيِّ مسبقاً ، وأخيراً علينا حسابُ $A` = A^{-1}$ وبالتالي يمكنُ أن نحددَ $B`$ من خلال أي من المعادلاتِ الثلاثةِ أعلاهُ أي

$$B` = P_1 - A`C_1$$

وهذا يماثلُ ما قمنا بهِ في شيفرةِ قيصر ، حيثُ كنا نستخدمُ الأعدادَ الصحيحةَ وهنا أدخلنا التحويلَ الأفينيَّ على المصفوفاتِ ، حيثُ كانت شيفرةُ قيصر

$$C \equiv P + K(mod\ N) \qquad \text{وعكسُه} \qquad P \equiv a^{-1}C + b`(mod\ N)$$

$C$ النصُ المشفَّرُ، $P$ النصُ الصريحُ و $b` = a^{-1}b$ و $a`$ معكوسُ $a$ الضربيُّ والأفينيَّ يكون

$C \equiv aP + b(mod\ N^2)$ وعكسِه $P \equiv a`C + b`(mod\ N^2)$

حيثُ $a` = a^{-1}(mod\ N^2)$ و $b` = a^{-1}b(mod\ N^2)$

أمّا في المصفوفاتِ ، فنحنُ نستخدمُ المتجهاتِ بدلاً من الأعدادِ الصحيحةِ وبالتالي :

$$C \equiv AP + B(mod\ N^2) \text{ أي } C \equiv \begin{bmatrix} a & b \\ c & d \end{bmatrix} P + \begin{bmatrix} e \\ f \end{bmatrix} (modN^2)$$

والعكسُ $P = A^{-1}C - A^{-1}B \equiv A^{-1}(C - B)(mod\ N^2)$

حيثُ $P = \begin{bmatrix} P_1 \\ P_2 \end{bmatrix}$ ومنه $P_i = x_i N + y_i$

$x_i$ القيمةُ المكافئةُ لأولِ حرفٍ $y_i$ القيمةُ المكافئةُ لثاني حرفٍ في الثنائيةِ ، ويمكنُ استخدامُ بالطريقة السابقة الثلاثياتِ $(x, y, z)$ حيث سيكونُ في هذه الحالة

$P = xN^2 + yN + z$ و $x, y, z$ هي القيمُ العدديةُ المكافئةُ للحروفِ في الرسالةِ الصريحةِ

حيث سوفَ يستخدمُ المصفوفةَ المربعةَ من البعد 3×3 لـــ A و 3×1 لـــ B

**مثال 20 :** شفّر الرسالة " HELP MY NOW " مستخدماً التشفيرَ الأفينيَّ والمصفوفاتِ مع مفتاحَيْ التشفيرِ

$$A = \begin{bmatrix} -1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} , B = \begin{bmatrix} 162 \\ 219 \\ 323 \end{bmatrix}$$

الحل: ستُقسمُ الرسالةُ إلى ثلاثياتٍ $P_1(HEL), P_2(PMY), P_3(NOW)$

$$\left.\begin{aligned} P_1 &= 7 \times 26^2 + 4 \times 26 + 11 = 4847 \\ P_2 &= 15 \times 26^2 + 12 \times 26 + 4 = 10456 \\ P_3 &= 13 \times 26^2 + 14 \times 26 + 22 = 9174 \end{aligned}\right\} \Longrightarrow C \equiv AP + B(mod\ N^3)$$

$$C \equiv \begin{bmatrix} -1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 4847 \\ 10456 \\ 9174 \end{bmatrix} + \begin{bmatrix} 162 \\ 219 \\ 323 \end{bmatrix} \equiv \begin{bmatrix} 7825 \\ 2273 \\ 9497 \end{bmatrix} (mod\ 26^3)$$

ومنه

$$\left.\begin{matrix} 7825 = 11 \times 26^2 + 14 \times 26 + 25 = (LOZ) \\ 2273 = 3 \times 26^2 + 9 \times 26 + 11 = (DJL) \\ 9497 = 14 \times 26^2 + 1 \times 26 + 7 = (OAH) \end{matrix}\right\}$$

النصُّ المشفرُ "$LOZDJLOAH$"

ولفكِ التشفيرِ نستخدمُ العلاقةَ : $P \equiv A^{-1}(C - B)(mod\ N^3)$

ويمكنُ التعميمُ حتى نصلَ لمصفوفةٍ من البعد n×n إذا كان بإمكاننا حسابُ المعكوسِ ، حيث سنستخدمُ الخوارزميةَ للتشفيرِ

$$C \equiv \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} P_1 \\ \vdots \\ P_n \end{bmatrix} + \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} (mod\ N^n)$$

على سبيلِ المثال لأجل n=4 مرتباتٌ من أربعِ مساقطَ سيكونُ النصُّ الصريحُ

$P = xN^3 + yN^2 + zN + h$ ولكن في هذه الحالةِ ستكونُ الأعدادُ كبيرةً جداً ، ولكن بالمقابلِ سيكونُ التشفيرُ أكثرَ أمناً ومقاومةً لتحليل الشيفرات .

### (9-2-1) المفتاح العام public key : [16]

في أنظمةِ التشفيرِ السابقةِ على كل مستخدمٍ أن يختارَ زوجاً من المفاتيحِ ( مفتاحِ التشفيرِ وآخرَ لفكِ التشفيرِ يبقى سرِّياً ) ، ولتجنبِ تعيُّنِ مفتاحٍ لكل زوج من المستخدمينِ (والذي يجبُ أن يبقى سرِّياً بالنسبة لبقيةِ المستخدمين) ظهرَ نظامُ التشفيرِ بالمفتاحِ العامِ ( public − key cipher system) والمفتاح العامُ : نشرُ معلوماتٍ عامةٍ للتشفير مع عدمِ قدرةِ أيِّ شخصٍ على قراءةِ هذه الرسائلَ ، في حين يتمُ التكتمُ على المفتاحِ الخاص وإبقائهِ سرِّياً ، والمفتاحُ الخاصُ لا يمكنُ أن يكونَ على علاقةٍ بالمفتاح العام أو متفرِّعاً أو مشابهاً له ، بل يجب أن يبقى مستقلاً استقلالاً تاماً

وبنظامِ التشفيرِ بالمفتاحِ العامِ سيكونُ الشخصُ الذي يملكُ معلوماتِ التشفيرِ لا يمكنُ أن يستَخدمَ مفتاح التشفيرِ لإيجادِ مفتاحِ فكِّ التشفيرِ.

وأقربُ مثالٍ للتشفيرِ بالمفتاحِ العامِّ هو صندوقُ البريدِ في البنايةِ أو الجامعةِ ، فالجميعُ يعلمُ وجودَ رسائلٍ فيه ولكنك أنت وحدَك من يملكُ مفتاحَ هذا الصندوقِ ، وتستطيعُ فتحَهُ واستلامَ رسائلِكَ .

بكلماتٍ أخرى مفتاحُ التشفير $f: P \to C$ هو سهلُ الحسابِ ، أمَّا تابعه العكسيُّ $f^{-1}: C \to P$ فإنَّه من الصعبِ جداً حسابهُ دونَ معرفةِ طولِ الرسالةِ أو معلوماتٍ اضافيةٍ ومثلُ هذا التابعِ يُدْعىَ التابعَ السحريَّ (trapdoor function) ( وهو كلُ تابعٍ يكون سهلاً بالاتجاه المباشرِ $f$ ومن الصعب حسابُ معكوسهِ $f^{-1}$) .

ويوجَدُ مفهومٌ آخرٌ قريبٌ من هذا الاسم وهو ما يُدْعىَ تابعَ الاتجاهِ الواحدِ (one-way function) حيثُ ظهرَ مفهومُ التابعِ السحريِّ لأول مرةٍ عام 1978 مع ظهورِ الخوارزميةِ RSA في حين أن تابعَ الاتجاهِ الواحدِ أقدمُ لحدٍ ما وظهر على يد العالم R.M.Needham في عام 1974 قامَ العالمُ G.Purdy بنشرِ أولِّ بياناتٍ وتفاصيلٍ حولَ تابعِ الاتجاهِ الواحدِ ، حيثُ كلمةُ المرورِ الأصليةُ وصيغةُ التشفيرِ تعتمدُ على أعدادٍ صحيحةٍ بالمقاسِ لعددٍ أوليٍّ كبيرٍ وأنَّ تابعَ الاتجاهِ الواحد $F_P$ أُعطيَ من خلالِ الحدوديةِ $f(x)$ واستخدمَ Purdy القيمةَ $P = 2^{64} - 59$ والحدوديةَ

$$f(x) = x^{2^{24}+17} + a_1 x^{2^{24}+3} + a_2 x^3 + a_3 x^2 + a_4 x + a_5$$

حيث المعاملاتُ $a_i$ تتعينُ بـــ أعدادٍ بـــ 19 منزلةً.

إن عمليةَ إيجادِ $f^{-1}$ دونَ معرفةِ مفتاحِ التشفيرِ هو السببُ الطبيعيُّ للبحثِ في مسائلِ نظريةِ الأعدادِ وإيجادِ مسألةِ العواملِ الأوليةِ لعددٍ صحيحٍ كبيرٍ، حيثُ هذه العواملُ الأوليةُ غيرُ معروفةٍ وهذا النجاحُ ما يُسمَّى بخوارزميةِ (RSA)

## (1-2-10) خوارزمية $RSA$ [16]:

من أهمِ خوارزمياتِ المفتاحِ العامِ والتي تقومُ على إيجادِ العواملِ الأوليةِ لعددٍ صحيحٍ وكبيرٍ وترجعُ سببُ تسميتها لأسماءِ العلماء اللذين أوجدوها وهم (Rivest Shamir Adleman) وسوفُ نناقشُ آليةَ عملِ هذه الخوارزميةِ .

أولاً كلُّ مستخدمٍ يقومُ باختيار عددَيْنِ أوليَيْنِ كبيرَيْنِ لحدٍ ما ومن ثم نضعُ $n = pq$

ومعرفةُ العواملِ لـــ $n$ أمرٌ سهلٌ بحسابِ $\Phi(n) = (p-1)(q-1) = n + 1 - p - q$

ومن ثم المستخدمُ يقومُ بشكلٍ عشوائيٍّ باختيارِ عددِ e محصورٍ بين $1 \le e \le \varphi(n)$ ويحقُق $(\varphi(n), e) = 1$ ، لذلك المستخدمُ A يقومُ باختيار عددَيْنِ أوليَيْنِ $p_A, q_A$ ، من ثم يختارُ بشكل عشوائيٍّ $e_A$ ، والتي لا تملكُ عواملَ أوليةٍ مع $(p_A - 1), (q_A - 1)$ ، ومن ثم يحسبُ

$$n_A = p_A q_A$$

وكذلك $\varphi(n) = n_A + 1 - p_A - q_A$ ومن ثم نحسبُ النظيرَ الضربيَّ (المعكوس ) لـــ $e$ بالمقاسِ $\varphi(n)$ أَيْ $d_A \equiv p^{e_A} \ (mod\ n_A)$ وبذلك يكونُ مفتاح التشفيرِ $K_{E,A} = (n_A, e_A)$ وعلينا إخفاءُ مفتاحِ فكِ التشفيرِ $K_{D,A} = (n_A, d_A)$ وتحويلُ التشفيرِ هو التطبيقُ

$$f: \frac{Z}{n_A Z} \to \frac{Z}{n_A Z}$$

المعرَّفُ بالشكلِ $f(P) \equiv P^{e_A} (mod\ n_A)$

وتحويلُ فكِ التشفيرِ $f^{-1}$ معرَّفٌ بالشكل :

$$f^{-1}(C) \equiv C^{d_A} (mod\ n_A)$$

وإنه ليسَ من الصعبِ التحققُ أن $f, f^{-1}$ كلاً منها معكوسٌ للآخرِ.

يمكن هنا أنْ نستخدمَ في النصِ الصريحِ أو المشفرِ كتلاً مختلفةَ الطولِ وليكنْ النصُ الصريحُ من $k$ كتلةً والنصُ المشفرُ طولَ الكتلةِ $l$ وذلك بشرطِ $(k < l)$ وأنه $N^k < n_A < N^l$ وهذا الشيءُ لم يكنْ محققاً في الفقراتِ السابقة ، بل كان يُستخدمُ في الكتلِ الصريحةِ والمشفرةِ نفسَ الطولِ .

**مثال 21:**

استخدم المقاسَ $N = 26$ حرفاً وإنّ $k = 3, l = 4$ (طول الكتل ) أي النصُ الصريحُ من ثلاثةِ أحرفٍ والمشفرُ من أربعةٍ لإرسالِ الرسالةِ "YES" للمستخدم A مع مفتاح التشفير $(n_A, e_A)$ حيث $(n_A, e_A) = (46927, 39423)$

الحل : أولاً نضعُ الأعدادَ المكافئةَ والمقابلةَ لكلمة "YES" وحسْبَ الخوارزميةِ يكون

$$Y\ 26^2 + E\ 26^1 + S\ 26^0$$

$$\Longrightarrow 24 \times 26^2 + 4 \times 26^1 + 18 = 16346$$

وبالتالي يكونُ $f(P) = 16346^{39423} (mod\ 46927)$

والتي تكونُ $21166 = 1 \times 26^3 + 5 \times\ 26^2 + 8 \times\ 26^1 + 2 \times\ 26^0$

وهذه الأعدادُ تقابلُ الكلمةَ المشفرةَ "BFIC" وهي الرسالةُ المشفَّرةُ المقابلةُ لرسالةِ "YES"

والمستلم A يعلمُ مفتاح فكِّ التشفيرِ $(46927,26767) = K_D(n_A, d_A)$

ومن ثم يحسِبُ $21166\ ^{26767} (mod\ 46927) = 16346$

وهي الأرقامُ المقابلةُ لكلمةِ "YES" ولتوضيحِ كيفَ استطاعَ المستخدمُ A إيجادَ مفتاحهِ؟

أولاً هو ضربُ القيمِ المعروفةِ $P_A = 281$ و $q_A = 167$ لنحصلَ على $n_A$ ومن ثم اختيارُ $e_A$ بشكلٍ عشوائيٍّ بحيثُ يحققُ $gcd(e_A, 280) = gcd(e_A, 166) = 1$ ومن ثم هو أوجدَ $d_e = e_A^{-1} (mod\ 280)$ وأخيراً الأرقامُ $p_A, q_A, d_A$ تبقى سرِّيةً.

ويمكنُ أن نستخدمَ 40 حرفاً مقطعاً وهي الحروفُ A-Z بقيمٍ مكافئةٍ $0 - 25$ وبالإضافة لـــ فراغٍ =26، $27 = .$ , $28 = ?$, $29 = \$$ والأعداد 0-9 بالقيمِ المكافئة لها 30-39 وبفرضَ أن الرسائلَ الصريحةَ ثنائياتٌ والمشفرةَ ثلاثياتٌ أي $k = 2, l = 3$

وأنه $40^2 < n_A < 40^3$ والمطلوبُ:

1. أرسلْ الرسالةَ "SEND$7500" للمستخدمِ الذي مفتاحُ تشفيرهِ $(n_A, e_A) = (2047,179)$
2. فكَّ التشفيرَ باستخدامِ عواملِ $n_A$ وحسابِ مفتاحِ التشفيرِ $(n_A, d_A)$.

## تطبيقاتُ مبرهَنتي اولر وفيرما والبواقي التكعيبيةِ في التشفير

في هذا الفصلِ سندرسُ التشفيرَ الأسِّي والذي يعتمدُ على استخدامِ الدالةِ الأسَّيةِ بالمقاسِ $n$ ، كما سندرسُ التشفيرَ باستخدامِ البواقيِ التكعيبيةِ ومبرهناتِ اولر وفيرما.

**(2-1) التشفير الأسُّي: [16]** في هذه الفقرةِ سوفَ نناقشُ التشفيرَ الذي يعتمدُ على الأسِّ القياسيِ ومبرهنتَيْ اولر و فيرما بالإضافةِ لبعضِ التطبيقاتِ الأخرى ، وسنرى أنَّ هذا التشفيرَ قدَّمَ لنا نظامَ تشفير مقاوماً لتحليلِ الشيفراتِ وتكونُ آليةُ العملِ بهذا النظام وفقَ الآتي :

ليكن $p$ و $e$ أعداداً أوليَّاً ما وليكن $e$ هو مفتاحُ التشفيرِ (enciphering key)

وهو قيمةٌ صحيحةٌ موجبةٌ تُحقِّقُ $(e, p-1) = 1$ ، ولتشفيرِ رسالةٍ أولاً نقومُ بتحويلِ حروفها إلى الأعدادِ المكافئةِ (حيثُ نبدأُ من الصفرِ ونكتبُ كلَّ عددٍ على شكلِ منزلتَينِ ) كما في الجدول الآتي :

| letter | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| numerical equivalent | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

ومن ثم نقسمُ الأعدادَ الناتجةَ إلى كتلٍ مؤلفةٍ من عددٍ زوجيٍّ 2m من المنازلِ وهي أكبرُ قيمةٍ صحيحةٍ موجبةٍ ، بحيث كلُّ الكتلِ من الأعدادِ المكافئةِ تقابل $m$ حرف هي أقل من $p$ وإذا كانَ $2\,5\,2\,5\,2\,5 < p < 2\,5\,2\,5\,2\,5$ عندها يكون $m = 2$ لأجلِ كلِّ كتلةِ $p$ من النصِ الصريحِ وهي كتلةٌ مؤلفةٌ من عددٍ زوجيٍّ من الأعدادِ الصحيحة ، لنحصلَ على الكتلِ المشفرة $c$ باستخدامِ العلاقةِ :

$$c \equiv p^e \ (mod\ p) \quad , 0 \leq c < p$$

والرسالةُ المشفرةُ تتكونُ من الكتلِ المشفرةِ ، والتي هي أعدادٌ صحيحةٌ أقل من $p$ ونبينُ ذلك من خلالِ المثال التالي :

**مثال 1** : ليكن العددُ الأولي $p$ الذي يستخدم أس قياسي $p = 2633$ ، وليكن مفتاحُ التشفير المستخدم في الأس القياسي وهو $e = 29$ ولأن $1 = (e, p-1) = (29,2632)$ ولنشفر الرسالةَ :

**THIS IS AN EXAMPLE OF AN EXPONENTIATION CIPHER**

نقومُ بتحويلِ حروفِ الرسالةِ إلى الأعدادِ المكافئةِ والمؤلفةِ من كتلٍ طولِ كلِّ كتلةٍ أربعُ منازلَ من الأعدادِ فنحصلُ على

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1907 | 0818 | 0818 | 0013 | 0423 | 0012 | 151 1 | 0414 | 0500 |
| 1304 | 2315 | 1413 | 0413 | 0413 | 1908 | 0019 | 0814 | 1302 |
| 0815 | 0704 | 1723 | | | | | | |

ونلاحظُ بأننا أضفنا القيمةَ 23 للكتلةِ الأخيرةِ وهي القيمةُ المقابلةُ للحرف X الذي أضفناه لتكتملَ الكتلةُ الأخيرةُ للطول 4 .

ومن ثم نحوِّلُ الكتلةَ الصريحةَ $p$ إلى كتلةٍ مشفرةٍ $c$ من خلال التحويلِ التالي

$$c \equiv p^{29} \ (mod\ 2633\ ) \quad , \quad 0 \leq C < 2633$$

للتوضيح أكثرَ سنبيِّن كيف توصلنا للكتلةِ المشفرةِ الأولى من خلال حسابِ:

$$c \equiv 1907^{29} \equiv 2199\ (mod\ 2633)$$

وبشكل مماثلٍ نحصلُ على كتلِ النصِ المشفَّرِ من الكتلِ الصريحةِ أي يكون :

| | | | | | | |
|---|---|---|---|---|---|---|
| 2199 | 1745 | 1745 | 1206 | 2425 | 2425 | 1729 |
| 1619 | 0935 | 0960 | 1072 | 1541 | 1701 | 1553 |
| 0735 | 2064 | 1351 | 1704 | 1841 | 1459 | |

ولفكِّ التشفيرِ للكتلة المشفرةِ $c$ ، نحن بحاجةٍ إلى معرفةِ مفتاحِ فكِّ التشفيرِ (deciphering key) وهو قيمةٌ صحيحةٌ $d$ والتي تحققُ

$$de \equiv 1(\ mod\ (p-1)\ )$$

لذلك يكونُ $d$ هو معكوسٌ $e$ بالمقاسِ $p-1$

فإذا رفعنا العددَ المكافئَ للكتلةِ المشفرةِ $c$ للقوى $d$ ، والكلَّ للعددِ $e$ فإننا سوفَ نحصلُ على الكتلةِ الصريحةِ من العلاقة :

$$c^d \equiv (p^e)^d \equiv p^{de} \equiv p^{k(p-1)+1} \equiv p(mod\ p)$$

حيث $de = k(p-1)+1$ و $k$ عددٌ صحيحٌ موجبٌ وذلك لأن أحدَهما معكوسٌ للآخر

حتى نقومَ بفكِّ التشفيرِ لكتلةٍ مولَّدةٍ بالمقاسِ $p = 2633$ ، ومفتاحُ التشفيرِ $e = 29$ نحن بحاجة لمعرفةِ النظيرِ الضربيِّ (المعكوس ) لـــ $e$ بالمقاسِ $p-1 = 2632$ والذي هو

$d = 2269$ ولفك التشفير لكتلة $c$ وإيجادِ الكتلةِ المقابلةِ لها $p$ نستخدمُ العلاقةُ :

$$p \equiv c^{2269}\ (mod\ 2633)$$

وعلى سبيل المثال لنأخذُ الكتلةَ المشفرةَ الأولى 2199 فنجدُ

$$p \equiv 2199^{2269} \equiv 1907(mod\ 2632)$$

وبذلك حصلنا على الكتلةِ الأولى من النصِ الصريحِ .

وبالنتيجة إنَّ عمليةَ التشفيرِ وفكِّ التشفير التي تستخدمُ الأسُّ القياسيَّ تنجزُ بسرعةٍ ، ومن ناحيةٍ أخرى ، فإن تحليلَ الشيفراتِ من قبل (الهكر) على الرسالةِ المشفرةِ باستخدام الأسِّ القياسيِّ بشكلٍ عامٍ لا يمكنُ أن تُنجزَ بسرعةٍ فهي تتطلبُ وقتاً أكثرَ.

لذلك لنفرض إننا نعلم العددَ $p$ الذي استخدمُ كمقاسٍ وأكثر من ذلك لنفرض إننا نعلمُ الكتلةَ الصريحةَ $p$ المقابلةَ للكتلةِ $C$ .

$$c \equiv p^e\ (mod\ p)$$

لتحليلِ شيفراتٍ بشكلٍ ناجحٍ نحنُ بحاجةٍ لمعرفةِ مفتاحِ التشفيرِ $e$ والعلاقةِ الأخيرةِ تبينُ أنَّ $e$ هو لوغاريتم $c$ بالنسبةِ للأساس $p$

إن عمليةَ إيجادِ اللوغارتمياتِ وفقَ مقاسِ عددٍ أوليٍّ $p$ يتطلبُ وقتاً طويلاً جداً على سبيلِ المثال عندما يكونُ $p$ مؤلفاً من 100 منزلةً فإن عمليةَ إيجادِ اللوغارتميات وفقَ المقاس $p$ يتطلبُ تقريباً

74 سنةً و عندما يكون $p$ مؤلفاً من 200 منزلةً عشريةً فإن الوقتَ المتطلبَ لإيجادِ اللوغارتميات تقريباً $3.8 \times 10^9$ سنةً .

وهناك تطبيقاتٌ أخرى للأسّ القياسيِّ منها صناعةُ مفاتيحٍ مشتركةٍ بين المستخدمينَ وأيضاً تدخلُ في التطبيقاتِ المسلّيةِ (لعبة *poker* ).

## (2−2) التشفير بالمفتاح العام (Public-Key Cryptography ): [10]

يختارُ كلُ مستخدمٍ في الأنظمة السابقةِ زوجاً من المفاتيحِ إحداهما سريٌّ هو مفتاحُ فكِّ التشفيرِ ولتجنبِ تعيين مفتاحِ لكل زوج من المستخدمين (والذي يجبُ أن يبقى سرياً بالنسبة لبقية المستخدمين) ظهر نظامُ التشفيرِ بالمفتاح العام (public-key cipher system ) والذي أُدخل حديثاً في هذا النوع من التشفير ، مفاتيحُ التشفير يمكنُ أن تكونَ للعامَّةِ لأنه يحتاجُ الى وقتٍ لإيجادِ مفتاحِ فكِ التشفيرِ من تطبيقِ تحويلِ التشفيرِ ، ولاستخدامِ نظامِ التشفيرِ بالمفتاحِ العامِّ علينا إنشاءُ اتصالٍ آمنٍ للشبكةِ من $n$ مستخدمٍ وكلٌّ مستخدمٍ يحصلُ على مفتاحٍ من نوعٍ خاصٍ ويحتفظُ بمعلوماتٍ خاصةٍ به لإنشاءِ تطبيقِ تحويلِ التشفيرِ $E(k)$ وعندها يكونُ لدينا $n$ مفتاحُ $k_1, k_2, \ldots, k_n$ قد نُشِرت ، عندما يريدُ مستخدمٌ (i) أن يرسلَ إلى آخرَ (j) فإنَّ حروفَ الرسالةِ تُحوَّلُ إلى الأعدادِ المكافئةِ وتوضعُ بكتلٍ بحجمٍ خاصٍّ ومن ثم كلُّ كتلةٍ $p$ تشفَّرُ لنحصلَ على كتلةِ رسالةٍ مشفَّرةٍ والتي حُسبت من خلال التحويلِ $E_{k_j}$.

ولفك تشفير رسالةِ المستخدمِ j يقومُ بتطبيقِ تحويلِ فكِ التشفيرِ $D_{k_j}$ لكلِّ كتلةٍ مشفَّرةٍ $c$ لنحصلَ على الكتلةِ الصريحةِ $p$ أي أن :

$$D_{k_j}(c) = D_{k_j}\left(E_{k_j}(p)\right) = p$$

لا يوجد أي مستخدم آخرُ غيرُ مصرّحٍ له قادرٌ على فكِ تشفيرِ الرسالةِ على الرغمِ أنهم يعرفونَ المفتاحَ $k_j$ وأكثرُ من ذلك فإنّه غيرُ ممكن بالنسبة لمحللي الشيفراتِ (المتطفلين ) لأنه يتطلبُ الكثيرَ من الوقتِ .

ومن أهمِ خوارزمياتِ هذا النظامِ هي خوارزميةُ أو نظامُ التشفير RSA الذي ظهرَ مؤخراً عن طريقِ Rivest, Shamir, and Adleman وهو نظامُ تشفيرِ مفتاحٍ عامٌ يعتمدُ على الأسِّ القياسيِّ ، حيث تكونُ المفاتيحُ فيه عبارةً عن أزواجِ $(e,n)$ على اعتبار أنَّ $e$ هو الأسُّ القياسيُّ و $n$ هو المقاسُ ، والذي هو جداءُ عددينِ أوليينِ كبيرينِ $p,q$ , $n=pq$ يتحققُ $(e,\emptyset(n)) = 1$ ، ولتشفيرِ رسالةٍ أولاً نحوِّلُ حروفَ الرسالةِ إلى الأعدادِ المكافئةِ لها ، ومن ثم إلى كتلٍّ من أكبرِ حجمٍ ممكنٍ (وهو عددٌ زوجيٌّ من المنازل ) ، وأخيراً لتشفيرِ الكتلةِ $p$ الصريحةِ نحصل على كتلةٍ مشفَّرةٍ من خلال :

$$E(p) = c \equiv p^e \ (mod\ n) \qquad 0 < c < n$$

أمّا عمليةُ فكِّ التشفيرِ تتطلبُ منا معرفةَ النظيرِ(المعكوس ) $d$ للعددِ $e$ بالمقاس $\emptyset(n)$ والذي هو موجودٌ طالما أنَّ $(e,\emptyset(n)) = 1$ لذلك لفكِّ تشفيرِ كتلةِ مشفرِ $c$ نستخدمُ العلاقة :

$$D(c) \equiv c^d \equiv (p^e)^d \equiv p^{ed} \equiv p^{k\emptyset(n)+1} \equiv \left(p^{\emptyset(n)}\right)^k p \equiv p\ (mod\ n)$$

$ed = 1(mod\ \emptyset(n))$ لبعض القيم الصحيحة $k$ وذلك لكون $ed = k\emptyset(n) + 1p$

وباستخدامِ نظريةِ اولر لدينا $P^{\emptyset(n)} \equiv 1(mod\ n)$ عندما $(n,p) = 1$ والزوجُ $(e,d)$ هو مفتاحٌ لفكِ التشفيرِ ولتوضيحِ كيف يعملُ هذا النظامُ سنقدِّمُ مثالاً يكونُ فيه المقاسُ هو جداءُ عددينْ أوليينْ.

**مثال 2: [1]** لِيكنْ $p = 59$ , $q = 43$ و $n = 43 \times 59 = 2537$ كمقاسٍ و $e = 13$ الأسَّ لــ RSA ونلاحظُ أنَّ $(e,\emptyset(n)) = 1$ ولْنشفر الرسالةَ

PUBLIC KEY CRYPTOGRAPHY

أولاً نحوِّلُ هذه الحروفَ إلى الأرقامِ المكافئةِ لها ومن ثم تجميعُ هذهِ الأرقامِ في كتلٍّ مؤلفةٍ من أربعةِ منازلَ لنحصلَ على

| | | | | | |
|---|---|---|---|---|---|
| 1520 | 0111 | 0802 | 1004 | 2402 | |
| 1724 | 1519 | 1406 | 1700 | 1507 | 2423 |

علماً أننا أضفنا العددَ X=23 للكتلةِ الأخيرةِ لإكمالها .

نقومُ بتشفيرِ كلِّ كتلةٍ صريحةٍ لنحصلَ على الكتلةِ المشفرةِ المقابلةِ لها من خلالِ التطابقِ

$$c \equiv P^{13} \ (mod\ 2537)$$

كمثال لتشفيرِ الكتلةِ الأولى 1520 لنحصلَ على كتلةٍ مشفَّرةٍ أولى كما يلي :

$$c \equiv (1520)^{13} \equiv 95\ (mod\ 2537)$$

وبالتالي نحصلُ على جميعِ الكتلِ المشفرةِ التاليةِ الناتجةِ عن تشفيرِ الكتلِ الصريحةِ

0095 1648 1410 1299 0811

2333 2132 0370 1185 1457 1084

ولفكِّ التشفيرِ لرسالةٍ تمَّ تشفيرُها باستخدامِ RSA يجبُ علينا إيجادُ النظيرِ $e = 13$ بالمقاس

$\emptyset(n) = 2436$ وذلك من خلالِ حسابٍ بسيطٍ عندها نجد $d = 937$ والذي هو النظيرُ الضربيُّ بالمقاسِ 2436، وبالنتيجة لفكِّ تشفيرِ كتلةٍ والحصولِ على كتلةٍ صريحةٍ نستخدمُ العلاقةَ :

$$p \equiv c^{937}\ (mod\ 2537) \quad 0 \leq p \leq 2537$$

وهذا محققٌ لأنه:

$$c^{937} \equiv (p^{13})^{937} \equiv (p^{2436})^{5} \equiv p\ (mod\ 2537)$$

نلاحظُ استخدامَ مبرهنةَ اولر في الخوارزميةِ العامةِ للمفتاحِ العامِ في أكثرَ من موضعٍ ، وهذا ما يجعلُ الخوارزميةَ أكثرَ بساطةً ومتعةً حيث اعتمدتْ على $p, q$ عَدَدَيْنِ أوليَيْنِ مختلفَيْنِ و فيكونُ $n = p.q$

$$\phi(n) = \phi(p.q) = (p-1)(q-1)$$

ومن ثم نختارُ عدداً أولياً $e$ بحيثُ يكون $(e, \phi(n)) = 1$ وبالتالي الخوارزميةُ تصبحُ

$$M \equiv c^{d}(mod\ n)\ , c \equiv M^{e}(mod\ n)$$

حيث $d$ هو النظيرُ الضربيُّ (المعكوس ) أي $ed \equiv 1(mod\ \phi(n))$

$$\Longrightarrow \phi(n)|(ed-1) \Longrightarrow \phi(n)K + 1 = ed$$

$$M \longrightarrow C^{d} = (M^{e})^{d} = M^{ed} = M^{\phi(n)K+1} = M^{\phi(n)K}.M = M\ (mod\ n)$$

**مثال 3 :** لِيكنْ $n = 77$ ، $p = 7, q = 11$ باستخدامِ الخوارزميةِ السابقةِ ، شفِّر ثم فكَّ تشفيرَ كلمةِ $NO$ .

الحل:

$$\phi(77) = \phi(7 \times 11) = (p-1)(q-1) = 6 \times 10 = 60$$

ولْنفرضْ أننا اخترنا $e$ أصغرَ عددٍ يحققُ $gcd(e, 60) = 1 \Leftarrow e = 7$

$$ed \equiv 1(mod\ 60) \implies d = e^{-1} \implies d = 43$$

لأنَّ $7 \times 403 = 301 \equiv 1(mod\ 60)$

ولْنشفِّرَ الرسالةَ (NO)$\Leftarrow$(13 14)

$$M_1 = 13 \Rightarrow c_1 = M_1^e \equiv 13^7(mod\ 77) \equiv 62 \equiv 10(mod\ 26) \implies K$$
$$M_2 = 14 \Rightarrow c_2 = M_2^e \equiv 13^7(mod\ 77) \equiv 42 \equiv 16(mod\ 26) \implies Q$$

ومنه الرسالةَ المشفرةَ (KQ)

وفكُ التشفيرِ:

$$c_1 = 62 \Rightarrow M_1 \equiv c_1^d(mod\ 77) \equiv 62^{43}(mod\ 77) \equiv 13 \implies N$$
$$c_2 = 42 \Rightarrow M_2 \equiv c_2^d(mod\ 77) \equiv 42^{43}(mod\ 77) \equiv 14 \implies O$$

ومنهُ رَجَعْنَا للرسالةِ الأصلِ (NO).

## (1−2−2) مبرهنة فيرما (Fermatstheorm):

هي حالةٌ خاصةٌ من اولر و تنصُّ "إذا كان $(a, p) = 1$ أولياً نسبياً فإنَّ $a^{p-1} \equiv 1(mod\ p)$ "

تطبيقها في التشفير: استخدمتْ في التشفِّير الأسِّي (Exponential) حيث يتمُ اختيارُ $p$ عدداً أولياً كبيراً وأيَّ عددٍ صحيحٍ $e$ بحيثُ يحققُ $gcd(e, p-1) = 1$ ، وتكونُ خوارزميةُ (تابع) التشفيرَ

$$x \to x^e(mod\ p) \qquad \text{حيث } 0 < x < p$$

ومنهُ $a^{p-1} \equiv 1(mod\ p)$ وهذه هي (Fermats little theorm).

ولتحويلِ فكِّ التشفيرِ علينا حسابُ $d$ حيثُ

$$e.d \equiv 1(mod\ p-1) \Longrightarrow ed = (p-1)x + 1\ ; x \in \mathbb{Z}^+$$

ومنه تحويلُ فكِّ التشفيرِ يصبحُ

$$x \to y^d = (x^e)^d = x^{ed} = x^{(p-1)x+1} = x^{(p-1)x}.x \equiv x(mod\ p)$$

**مثال 4: [1]** شفِّر الرسالةَ "EULER" باستخدامِ الطريقةِ السابقةِ ولأجل $e = 7, p = 31$

$$A = 0, \dots, Z = 25$$

الحل: بما أن $gcd(31,7) = 1$ يمكنُ التشفيرُ وتحويلُ التشفيرِ هو $y \equiv x^7(mod\ 31)$

تحويلُ التشفيرِ $(y \equiv x^7\ mod\ 31)$ ولْنبدأ التشفيرَ

$$E \to (4)^7 = 16384 \equiv 16(mod\ 31) \to Q$$

$$U \to (20)^7 = 1280000000 \equiv 18(mod\ 31) \to S$$

$$L \to (11)^7 = 19487171 \equiv 13(mod\ 31) \to N$$

$$E \to (4)^7 = 16384 \equiv 16(mod\ 31) \to Q$$

$$R \to (7)^7 = 41033673 \equiv 12(mod\ 31) \to M$$

وبالتالي يكونُ تشفيرُ الكلمة "EULER" هو الكلمةُ "QSNQM"

**مثال 5: [1]** فك تشفير "QSNQM"باستخدامِ معكوسِ التابعِ السابقِ لإعادةِ النصِ المشفرِ إلى النصِّ الصريحِ

لدينا $e = 7$ ومنه $d = 13$ معكوسٌ $7 \times 13 = 91 \equiv 1(mod\ 30)$

وبالتالي تابعُ فكِّ التشفيرِ يكون $x \equiv y^{13}(mod\ 31)$

$$Q \to (16)^{13} = (4^7)^{13} = 4^{30\times3+1} = 4^{30\times3} \times 4 \equiv 4(mod\ 31) \to E$$

$$S \to (18)^{13} = (20^7)^{73} = 20^{30\times3+1} = 20^{30\times3} \times 20 \equiv 20(mod\ 31) \to U$$

$$N \to (13)^{13} = (11^7)^{13} = 11^{30\times3+1} = 11^{30\times3} \times 11 \equiv 11(mod\ 31) \to L$$

$$Q \to (16)^{13} = (4^7)^{13} = 4^{30\times3+1} = 4^{30\times3} \times 4 \equiv 4(mod\ 31) \to E$$

$$M \to (12)^{13} = (17^7)^{13} = 17^{30\times3+1} = 17^{30\times3} \times 17 \equiv 17(mod\ 31) \to R$$

والنتيجةُ تكونُ "QSNQM"⟹"EULER"

ويمكنُ أن يتمَّ التعميمُ لأكثرَ من حرفٍ باستخدام RSA ، وهذا باستخدامِ قائمةِ الأرقامِ والحروفِ والرموزِ المعتمدةِ من قبل <<الكودِ الأمريكيِّ القياسيِّ لتبادلِ المعلوماتِ>> أو ما يُسمَّى ASCII (American Standard Cod for Information Interchange) وهي قائمةٌ متضمنةُ الحروفِ وكلِّ الرموزِ والأرقامِ وتبدأُ بأعدادٍ مكافئةٍ لها بالترقيمِ 32 وحتى 126 بحسبِ المرجعِ [4] كما موضحٌ في الجدولِ الآتي :

| Char | Num | Char | Num | Char | Num | Char | Num |
|---|---|---|---|---|---|---|---|
| (space) | 32 | 8 | 56 | P | 80 | h | 104 |
| ! | 33 | 9 | 57 | Q | 81 | i | 105 |
| " | 34 | : | 58 | R | 82 | j | 106 |
| # | 35 | ; | 59 | S | 83 | k | 107 |
| $ | 36 | < | 60 | T | 84 | l | 108 |
| % | 37 | = | 61 | U | 85 | m | 109 |
| & | 38 | > | 62 | V | 86 | n | 110 |
| apostrophe | 39 | ? | 63 | W | 87 | o | 111 |
| L Paren. | 40 | @ | 64 | X | 88 | p | 112 |
| R Paren. | 41 | A | 65 | Y | 89 | q | 113 |
| * | 42 | B | 66 | Z | 90 | r | 114 |
| + | 43 | C | 67 | R Brack. | 91 | s | 115 |
| , | 44 | D | 68 | \ | 92 | t | 116 |
| - | 45 | E | 69 | L Brack. | 93 | u | 117 |
| . | 46 | F | 70 | caret | 94 | v | 118 |
| / | 47 | G | 71 | underscore | 95 | w | 119 |
| 0 | 48 | H | 72 | grave | 96 | x | 120 |
| 1 | 49 | I | 73 | a | 97 | y | 121 |
| 2 | 50 | J | 74 | b | 98 | z | 122 |
| 3 | 51 | K | 75 | c | 99 | { | 123 |
| 4 | 52 | L | 76 | d | 100 | \|\| | 124 |
| 5 | 53 | M | 77 | e | 101 | } | 125 |
| 6 | 54 | N | 78 | f | 102 | tilda | 126 |
| 7 | 55 | O | 79 | g | 103 | | |

**مثال 6: [1]** باستخدامِ جدولِ ASCII والتشفير بالكتلِ:

ولأجل $p = 3181\ ,\ q = 227$ وأنَّ $e = 953$ شفِّر الرسالةَ التالية "161 MAIN STREET" ثم حدّدْ مفتاحَ فكِّ التشفيرِ ، وعُدّ للنصِّ الأصلي.

الحل:

$$n = pq = 3181 \times 227 = 722087$$

$$\phi(n) = (p-1)(q-1) = 718680$$

باستخدامِ جدولِ ASCII تتحولُّ الرسالةُ إلى

49544932776573783283846969 84

نقسمها لخمسِ كتلٍ ...,73783 ,327765 ,495449 ونوجد $y_1, \dots, y_5$

$$y_1 \equiv 495449^{953} (mod\ 722087) \equiv 19929 (mod\ 722087)$$

وهكذا نحصلُ على بقية الكتلِ المشفَّرةِ

199229,251774,33119,578189,24334

وللعودةِ للرسالة الأصلية ، علينا حسابُ $d$ حيث $ed \equiv (mod \phi(n))$

$$\Longrightarrow d \equiv 953^{-1} (mod\ 718680) \Longrightarrow 953.d \equiv 1 (mod\ 718680)$$

$$\Longrightarrow d = 639497$$

(ويمكنُ أن نستخدمَ خوارزميةَ إقليدس لحساب $d$ بطريقةٍ أسرع) وللحصول على الكتلةِ الأولى مثلاً

$$x_1 \equiv 199229^{63497}\ (mod\ 722087) \equiv 495449\ (mod\ 722087)$$

وهي الكتلةُ الصريحةُ الأولى.

وهناك تطبيقاتٌ أخرى لمبرهنة اولر ، منها حسابُ الباقي غيرِ السالب لعددٍ ما.

**مثال7** : أوجدّ الباقي غيرَ السالب للعدد $9^{1346}\ (mod\ 70)$

الحل: لأن $(9,70) = 1$ وحسبُ مبرهنةِ اولر $9^{\phi(70)} \equiv 1\ mod\ 70$

ولكون $70 = 2 \times 5 \times 7$ بالتالي

$$\phi(70) = \phi(2 \times 5 \times 7) = 70\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = 24$$

$$\Longrightarrow 9^{\phi(70)} = 9^{24} \equiv 1\ (mod\ 70)$$

ولكون $1346 = 24 \times 56 + 2$

$$\Longrightarrow 9^{1346} = 9^{(24\times56)} \times 9^2 (mod 70) \equiv 9^2 (mod\ 70)$$

$$9^2 = 81 \equiv 11 (mod\ 70)$$

إذن الباقي هو 11.

## (3-2) اللوغاريتم المميز (Discrete log) (المنفصل):[3]

### (1-3-2) تعريف: [3]

لتكن $G$ زمرةَ دورةٍ منتهيةٍ ، لأجل كلِّ عنصرٍ $g \in G$ يوجدُ عنصرٌ أصغريٌّ $a \in \mathbb{N}$ ، بحيث يكون $g^a = y$ ، نسمي $a$ اللوغاريتمَ المميزَ للعنصر $y$ بالأساس $g$ ، وحساب $a = log_g\, y$ تُدْعى مسألةُ اللوغاريتم المميز (DLP).

أحياناً يكونُ حساب الأسِّ ليس بالأمرِ السهلِ مقارنةً بحسابِ اللوغاريتم ، وعندما يكونُ عملُنا في الزمرِ المنتهيةِ فإنَّ عمليةَ إيجادِ مقلوبِ الأسي تدعى المميزُ (أو المنفصل) (discrete) أي تدعى مسألةَ اللوغاريتم المميز ، لا يوجدُ طريقةٌ تقليديةٌ فعَّالةٌ لحساب اللوغاريتم المميزِ ، وإنما توجدُ خوارزميةُ كميةٍ تعودُ للعالم Peter shor ، ولذلك اعتبرَ أنَّ حسابَ اللوغاريتم المميز غيرُ ممكن حاسوبياً.

### (2-3-2) فرضية Diffe-Hellmon:[3]

تحتَ هذه الفرضيةِ بُني نظامِ تبديلِ المفاتيحِ الجديدُ ، أو ما يدعى نظامَ تبادلِ المفاتيحِ الجديدُ لـــ Diffe-Hellmon وتنصُّ على (لا يمكنُ حسابَ $g^{a.b}$ بمعرفة $g^a$ أو $g^b$ )

بفرضِ مستخدمينَ $A, B$ اتفقوا على مفتاحٍ ، والذي هو عنصرٌ من $\mathbb{F}_q^*$ ، أولاً عليهم أن يضعوا مولداً للمجموعة وليكن $g$ ، ومن ثمَّ المستخدمُ $A$ يختارُ عدداً عشوائياً وليكن $a$ ويحسب $g^a$ ويجعلهُ عاماً والمستخدم $B$ يفعلُ نفسَ الشيءِ باختيار $b$ وحساب $g^b$ ونشرهِ ومن ثمَّ كلاهُما يحسبُ $g^{a.b}$ ، (ولكن تحت فرضية Diffe-Hellmon لا يمكن لأي طرف ثالث حساب $g^{a.b}$ ).

**(3-3-2) نظام تشفير الرسالة المرسلة لــ the Massy-Omura:**

بفرضِ أنَّ كلَّ واحدٍ لديه الحقلُ المنتهِ $\mathbb{F}_q$ ، والذي هو مثبتٌ وعامٌّ (للعموم) (publicy)

كلُّ مستخدمٍ لهذا النظام يختارُ قيمة سرية وعشوائيةً $e$ (من 0 وحتى $q-1$) والتي تحقق $gcd(e, q-1) = 1$ ومن ثم باستخدامِ خوارزمية إقليدس يقومُ بحسابِ المعكوسِ

$d \equiv e^{-1}(mod\ q-1)$ والآن:

إذا أرادَ المستخدم Alice أن يرسلَ رسالةً $p$ لشخصٍ Bob

أولاً عليه إرسالُ $p^{e_A}$ وهذا يعني أنَّه لا يوجدُ أيُّ شخصٍ يعلمُ $d_A$ سوى Alice

ولكن Bob يمكنُ إرسال $p^{e_A.e_B}$ ليرجعَها إلى Alice

وعندما Alice يرفعُ هذا العددَ للقوى $e_A$ ويعيد الرسالة إلى Bob ، وأخيراً Bob يرفعُ العدد للقوى $d_B$ ، الفكرةُ وراءَ هذا النظامِ بسيطةٌ ، وتكمن في أنَّه لا شخصَ يستطيعُ معرفة الرسائلِ إلا إذا كان على علمٍ ودرايةٍ كافيةٍ بمخططِ التواقيعِ الخاص.

**(4-2) نظام التشفير الــ EL Gamal:[3]**

نبدأُ باختيار حقلٍ مثبتٍ منتهٍ كبير $\mathbb{F}_q$ ومولد $g \in \mathbb{F}_q^*$

ولنفرض بأننا نستخدمُ نصَّاً صريحاً (وحدةَ رسالةٍ) مع الأعدادِ المكافئةِ لها $p$ في الحقل $\mathbb{F}_q$ وكلُّ مستخدمِ A يختارُ عشوائياً قيمةَ $a_A$ ، والتي تتراوح $0 < a < q-1$ وهذه القيمةُ الصحيحةُ تبقى سريةً وهي بمثابة مفتاح فكِّ تشفيرٍ ، والمفتاح العامُ للتشفير هو العنصرْ $g^a$

ولإرسالِ رسالةٍ للمستخدم A نختارُ عدداً صحيحاً عشوائياً $k$ ، ومن ثمَّ نرسلُ الرسالةَ من خلال زوجِ العناصر $(g^k, pg^{ak})$

ونلاحظ أننا نستطيعُ حساب $g^{ak}$ من دون معرفة القيمة $a$ ، وذلك من خلال رفعِ $(g^a)$ للقوى $k$

والمستخدمُ A هو الوحيدُ الذي يعلمُ قيمةَ $a$ ويستطيع بها استعادة نصِّ الرسالة $p$ من هذا الزوج من خلال رفعِ العنصرِ الأول وهو $g^k$ للقوى $a$ ومن ثم تقسيمِ الثاني على $g^{ak}$ و النتيجة ستكون العنصر الثاني من الزوج.

ليكن $p$ عدداً أولياً ، $g$ مولد لـــ $\left(\frac{Z}{pZ}\right)^*$ عندئذٍ:

$$ep_g: \left(\frac{Z}{pZ}\right)^* \longrightarrow \left(\frac{Z}{pZ}\right)^*$$

$$x \longmapsto g^x$$

هذه مسألةُ اللوغاريتم المميزُ

ويمكن أن يلخصَ نظامُ الجملِ *(ELGAMAL Cryptosystem)* وفق الآتي:

- $P = \{0,1\}^k \ , C = \{0,1\}^{2(K+1)}$
- $K` = \{(p,d,e);$ أولي $p \ , < g > = \left(\frac{Z}{pZ}\right)^* \ , 2^K < p < 2^{K+1},$
  $a \in \{0, \dots, p-2\}\}$
- $K: (p,g,a) \longrightarrow (p,g,g^a)$

$\{0,1\}^k \subset \left(\frac{Z}{pZ}\right)^* \subset \{0,1\}^{(K+1)}$ ,$\left(\frac{Z}{pZ}\right)^*$ نستبدل $p$ بـــ

$e = (p,g,A = g^a), d = (p,g,a)$ لأجل $\left(\frac{Z}{pZ}\right)^* \times \left(\frac{Z}{pZ}\right)^*$ ونستبدل $C$ بدل

- $\mathrm{E}_e(x) := (g^b, A^b x)$ حيث $b \in \{0, \dots, p-2\}$ (اختيارات عشوائية) ( للتشفير)
- $D_d(y,z) := y^{-a} z$ (فك التشفير)

- ملاحظة: $a$ تُحفظُ بشكلٍ سريٍ
- توضيح $(g^{-a})A^b x = g^{-ba+ab} x = x$

دلالات الرموز : $\boldsymbol{K}$ : تقابلٌ بينَ المفاتيحِ  $\boldsymbol{E_e}$ : تحويلُ التشفير

$\boldsymbol{K`}$ فضاءُ مفتاحِ فك التشفير  $\boldsymbol{D_d}$ : تحويلُ فك التشفير

$\boldsymbol{P} = \{\boldsymbol{0},\boldsymbol{1}\}^{\boldsymbol{k}}$ أبجديةُ النصِّ الصريح  $\boldsymbol{C} = \{\boldsymbol{0},\boldsymbol{1}\}^{\boldsymbol{2(K+1)}}$ :أبجديةُ النصِّ المشفر

**مثال 8 :** لنأخذ $p = 23\ ,\ g = 7\ ,\ a = 6$ ومنه $d(23,7,6)$

نحسب $A = 7^6$ ومنه $A = 7^6 \equiv\ 4\ (mod\ 23)$

$$e = K(d) = (23,7,4)$$

لأجل $P = \left(\frac{Z}{23Z}\right)^* \ni x = 7$ نقومُ بحسابِ $E_e(x)$ كما يلي:

$$b = 3: \quad E_e(x) = (7^3, 4^3.7) = (21,11) \in \left(\frac{Z}{23Z}\right)^* \times \left(\frac{Z}{23Z}\right)^* = C$$

$$b = 2: \quad E_e(x) = (7^2, 4^2.7) = (3,20) \in \left(\frac{Z}{23Z}\right)^* \times \left(\frac{Z}{23Z}\right)^* = C$$

ومنه (فك التشفير)

$$D(21,11) = 21^{-6}.11 \equiv 7\ mod 23 \equiv\ 3^{-6}.20 = D_d(3,20)$$

## (5−2) نظام تشفير Rabin (Rabin cryptosystem) [3]

بنيةُ هذا النظامِ بالشكل الآتي:

- $P = \{0,1\}^k, C = \{0,1\}^{K+1}$
- $K` = \left\{(p,q);\ p,q$ أوليين مختلفين $,\ p,q \equiv 3(mod 4)\ , 2^K < pq < 2^{K+1}\right\}$
- $K: (p,q) \longrightarrow pq \in K = \{n \in \mathbb{N} | 2^K < n < 2^{K+1}$ أعداد $BLUM\}$
- $E_e(x) \coloneqq x^2 (mod n)$
- $D_d(y) \coloneqq n$ بالمقاس $x^2$ أربع جذور تربيعية لـ

**مثال 9 :** باستخدام $p = 3\ ,\ q = 7$ ومنه $n = p.q = 21$ و هو المفتاحُ العامّ في نظامِ Rabin شفرُ النصِ الصريح $10 \in \left(\frac{Z}{21Z}\right)^*$ نقومُ بحساب

$$C = 10^2 = 16\ (mod\ 21)$$

ولفكِ تشفيرِ $C = 16$ باستخدامِ العواملِ الأولية السرية $q = 7\ ,\ p = 3$ نقومُ بحسابِ أربعةِ جذورٍ تربيعيةٍ لـــ 16 بالمقاسِ 21:

$$16^{\frac{p+1}{4}} = 16 \equiv 1(\ mod\ 3\ )\quad and\quad 16^{\frac{q+1}{4}} = 16^2 = 4\ (mod\ 7)$$

هنا $1-, 1$ جذورٌ تربيعيةٌ لـــ 16 بالمقاس 3

و $4-, 4$ جذورٌ تربيعيةٌ لـــ 16 بالمقاس 7

باستخدامِ البواقي الصينيةِ نحصلَ على أربع مركبات

$$(1,4), (1,3), (2,4), (2,3)$$

وبالتالي أربعة جذور تربيعية هي 4,10,11,17

## (6-2) تطبيقات حلول التطابق التكعيبي $\mathbf{x^3 \equiv a(mod\ P)}$ في التشفير الأسي :[23]

في هذه الفقرةِ سنقومُ بعرض حلول التطابقِ التكعيبي في نظرية التشفير ،وسنناقشُ خوارزمياتٍ لتشفيرِ البيانات ، وفقاً لطبيعة العدد الأولي P.

**خوارزمية (1):**

ليكن P عدداً أولياً بحيثُ $P \equiv 4(\mathrm{mod}\ 9)$ أنَّ أحدَ حلولِ التطابق التكعيبية $x^3 \equiv a(\mathrm{mod}\ P)$ يكتبُ بدلالةِ العدد $a$ ، وذلك عندما يكون العدد $a$ باقياً تكعيبياً بالمقاس P ، وهذا الحل هو إمّا $x_0 = a(\frac{P+5}{18})$ أو $x_1 = -a(\frac{P+5}{18})$ ، فيما يلي نقدم خطوات الخوارزمية الأولى لتشفير البيانات المبنيةُ على حلول التطابق التكعيبي السابق ، لنفرض أنَّ T مجموعةُ البواقي التكعيبية بالمقاس $P$ وليكن $K = \{K = (P)\}$ (مفتاح التشفير).

- **خطوات الخوارزمية:**

1) نختار عدداً أولياً $P$ بحيث $P \equiv 4(mod 9)$ و $P \geq 157$ .
2) نوجدُ $T$ مجموعةَ بواقي تكعيبية بالمقاس $P$.
3) نوجدُ $T^2$ حيث $T^2 = \{z^2(mod\ P); z \in T\}$ .

4) نقومُ بتشكيلِ جدولٍ بحيث يقابلُ كلٌّ حرف من أحرف اللغة اللاتينية أحدَ عناصر المجموعة $\boldsymbol{T^2}$ وندعو هذا الجدولَ بجدولِ بواقي تكعيبية.

5) لتشفير أيِّ كلمةٍ نقوم باستبدالِ كلِّ حرفٍ من حروف هذه الكلمةِ بالعدد الذي يقابله في الجدول ، وذلك وفق الترتيبِ الهجائي فينتج لدينا مجموعةٌ من الأعداد ندعوها نصَّ ما قبل التشفير.

6) نقوم بحسابِ دالةِ التشفيرِ $\boldsymbol{f_P(x) \equiv x^{\frac{P+5}{18}}(mod\ P)}$ من أجل كلِّ $\boldsymbol{x}$ من النص ما قبل التشفيرِ ، فينتج لدينا مجموعةٌ أخرى من الأعداد ندعوها نصَّ التشفير.

7) لفك التشفيرِ نحسب دالَّة فكِّ التشفير $\boldsymbol{f_P^{-1}(y) \equiv y^3(mod\ P)}$ لكل $\boldsymbol{y}$ من النص المشفر، عندما نستبدلُ كلَّ عدد بالحرفِ الذي يقابله من جدول البواقي التكعيبية نحصل على النص الأصلي.

الدالتان $f_p(x) \equiv x^{\frac{P+5}{18}}(mod\ P)$ من أجل $x$ من النصِ الأصلي

و $f_P^{-1}(y) \equiv y^3(mod\ P)$ من أجل كل $y$ من النصِ المشفر

تحققان تعريفَ التشفير وذلك لأن:

من أجل أي $x \in T^2$ يوجد $z \in T$ بحيث $x \equiv z^2(mod\ P)$ وبالتالي فإن:

$$\forall x \in T^2: f_P^{-1}\big(f_P(x)\big) \equiv f_P^{-1}\big(f_P(z^2)\big) \equiv f_P^{-1}\left((z^2)^{\frac{P+5}{18}}\right)$$

$$\equiv f_P^{-1}\left(z^{\frac{P+5}{9}}\right) \equiv \left(z^{\frac{P+5}{9}}\right)^3 \equiv z^{\frac{P+5}{3}} \equiv z^{\frac{P-1+6}{3}}$$

$$\equiv z^{\frac{P-1}{3}}.z^{\frac{6}{3}} \equiv 1.z^2 \equiv z^2(mod\ P) = x$$

**ملاحظة:**

في الخطوة الثالثةِ اخترنا المجموعة $T^2$ بدلاً من مجموعة البواقي التكعيبية T ، وذلك لضمان أن دالَتيْ التشفير ، وفك التشفير هي تقابلاتٌ بينَ مجموعةِ محارفِ النص الواضح ومجموعة محارفِ النص المشفر ، لأن حلول التطابق التكعيبي $x^3 \equiv a(mod\ P)$ هي $x_0 = \mp a(\frac{P+5}{18})$ ، وفي الخطوة الرابعة شكلنا جدولاً بحيث يقابل كلَّ حرف من أحرف اللغة اللاتينية أحدَ عناصر المجموعة $T^2$ وعددُ عناصر هذه المجموعة يساوي نصفَ عددِ عناصرِ مجموعةِ البواقي التكعيبية بالمقاس

P وذلك لأنَّ $\forall t \in T\ ;\ t^2 \equiv (-t)^2 (mod\ P)$ ، وبالتالي نحنُ بحاجة إلى أن يكون عددُ عناصر المجموعة $T^2$ أكبرَ أو يساوي 26 (عدد أحرف اللغة اللاتينية) ، وهذا يتحققُ إذا كانت مجموعةُ البواقي التكعيبية بالمقاس P تحتوي على الأقل 52 ، وهذا يتحقق إذا وفقط إذا كان:

$$\frac{P-1}{3} \geq 52 \Leftrightarrow P-1 \geq 156 \Leftrightarrow P \geq 157$$

إذا كان عددُ عناصر المجموعة $T^2$ أكبرَ من 26 نختارُ أصغرَ 26 عنصراً.

**مثال 10 :** شفَر الكلمة SECRET باستخدام الخوارزمية السابقة :

1) نختارُ عدداً أولياً P بحيث $P \geq 157$ و $P \equiv 4(\mathrm{mod}\ 9)$ وليكن 157 (وهذا العددُ هو مفتاحُ التشفير).

2) نوجدُ مجموعةَ البواقي التكعيبية بالمقاس P ، باستخدامِ الحاسوب نجدُ أن مجموعةَ البواقي التكعيبية بالمقاس 157 هي:

$$\mathrm{T} = \{1,2,4,7,8,14,16,23,27,28,29,32,39,41,45,46,49,54,56,58,59,64,65$$
$$,67,75,78,79,82,90,92,93,98,99,101,103,108,111,112,116,$$
$$118,125,128,129,130,134,141,143,149,150,153,155,156\}$$

3) نوجد $T^2$ حيث $\mathrm{T}^2 = \{z^2(\mathrm{mod}\ 157); z \in \mathrm{T}\}$ بالتالي نجد أن:

$$\mathrm{T}^2 = \{1,4,14,16,27,39,46,49,56,58,64,67,75,82,90,93,99,101,$$
$$108,111,118,130,141,143,153,156\}$$

4) نقومُ بتشكيل جدولٍ بحيث يقابلُ كلُّ حرف من أحرف اللغة اللاتينية أحدَ عناصر المجموعة $T^2$ كما هو موضحٌ في الجدول الآتي:

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 4 | 14 | 16 | 27 | 39 | 46 | 49 | 56 | 58 | 64 | 67 | 75 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 82 | 90 | 93 | 99 | 101 | 108 | 111 | 118 | 130 | 141 | 143 | 153 | 156 |

5) تشفيرُ الكلمة SECRET نستبدل كلَّ حرف بالعدد الذي يقابلهُ في الجدول ، وذلك وفق الترتيب الهجائي سنبينُ ذلك من خلال الجدولِ التالي:

| S | E | C | R | E | T |
|---|---|---|---|---|---|

| 108 | 27 | 14 | 101 | 27 | 111 |
|---|---|---|---|---|---|

وبالتالي نحصلُ على الأعداد 111 , 27 , 101 , 14 , 27 , 108 والتي تمثلُ النصَّ قبلَ التشفير.

6) نقومُ بحساب دالةِ التشفير

$$f_P(X) \equiv x^{\frac{p+5}{18}} (\text{mod } P), x \in \{108,27,14,101,27,111\}$$

$$f_P(108) \equiv (108)^{\frac{157+5}{18}} \equiv (108)^9 \equiv 67(\text{mod } 157)$$

$$f_P(27) \equiv (27)^{\frac{157+5}{18}} \equiv (27)^9 \equiv 118(\text{mod } 157)$$

$$f_P(14) \equiv (14)^{\frac{157+5}{18}} \equiv (14)^9 \equiv 16(\text{mod } 157)$$

$$f_P(101) \equiv (101)^{\frac{157+5}{18}} \equiv (101)^9 \equiv 108(\text{mod } 157)$$

$$f_P(27) \equiv (27)^{\frac{157+5}{18}} \equiv (27)^9 \equiv 118(\text{mod } 157)$$

$$f_P(111) \equiv (111)^{\frac{157+5}{18}} \equiv (111)^9 \equiv 64(\text{mod } 157)$$

فينتجُ لدينا النصُ المشفّرُ التالي: 64 , 118 , 108 , 16 , 118 , 67

7) لفكِ التشفير نحسب دالة فك التشفير $f^{-1}(y) \equiv y^3 (\text{mod } P)$ لكل y من النص المشفر.

$$f^{-1}(67) \equiv (67)^3 (\text{mod } 157) \equiv 108(\text{mod } 157)$$

$$f^{-1}(118) \equiv (118)^3 (\text{mod } 157) \equiv 27(\text{mod } 157)$$

$$f^{-1}(16) \equiv (16)^3 (\text{mod } 157) \equiv 14(\text{mod } 157)$$

$$f^{-1}(108) \equiv (108)^3 (\text{mod } 157) \equiv 101(\text{mod } 157)$$

$$f^{-1}(118) \equiv (118)^3 (\text{mod } 157) \equiv 27(\text{mod } 157)$$

$$f^{-1}(64) \equiv (64)^3 (\text{mod } 157) \equiv 111(\text{mod } 157)$$

فتصبحُ لدينا مجموعةُ الأعداد 111 , 27 , 101 , 14 , 27 , 108 والتي تمثلُ النصَّ قبلَ التشفير وباستبدال كل عدد بالحرف الذي يقابلهُ من الجدول ، نحصل على النص الأصلي.

**خوارزمية (2) :**

ليكــن P عدداً أوَّليــاً بحيث $P \equiv 7(\mathrm{mod}\ 9)$ ، نعلــم أنَّ أحــدَ حلــول التطابق التكعيبيــة $x^3 \equiv a(\mathrm{mod}\ P)$ يكتبُ بدلالة العددِ $a$ وذلك عندما يكون العدد a باقياً تكعيبياً بالمقاس P ، وهذا الحلُّ هو $x_0 = a(\frac{P+2}{9})$ ، فيما يلي نقدمُ خطواتِ الخوارزمية الثانية لتشفير البيانات والمبنية على حلول التطابق التكعيبي السابق ، لنفرض أنَّ T مجموعةُ البواقي التكعيبية بالمقاس P وليكن $K = \{K = (P)\}$ (مفتاح التشفير).

- **خطوات الخوارزمية:**

1) نختارُ عدداً أولياً $P$ بحيثُ $P \geq 79$ و $P \equiv 7(mod\ 9)$
2) نوجدُ مجموعةَ البواقي التكعيبية بالمقاس $P$
3) نقومُ بتشكيل جدولٍ بحيثُ يقابلُ كلُّ حرفٍ من أحرف اللغة اللاتينية أحدَ عناصر مجموعة البواقي التكعيبية بالمقاس $P$ ، وندعو هذا الجدول بجدول البواقي التكعيبية.
4) لتشفير أيِّ كلمةٍ نقومُ باستبدال كلِّ حرفٍ من أحرف هذه الكلمةِ بالعددِ الذي يقابلهُ في الجدولِ ،وذلك وفق الترتيبِ الهجائي فينتج لدينا مجموعةُ أعدادٍ ندعوها النصَّ قبل التشفير.
5) نقومُ بحساب دالةِ التشفير $f_P(x) \equiv x^3(mod\ P)$ من أجل كل $x$ من النص ما قبل التشفير ، فينتجً لدينا مجموعةٌ أخرى من الأعداد ندعوها النصَّ المشفر.
6) لفكِّ التشفيرِ نحسبُ دالة فكِ التشفير $f_P^{-1}(y) \equiv y^{\frac{P+2}{9}}(mod\ P)$ لكل $y$ من النصِّ المشفرِ وباستبدال كلِّ عددٍ بالحرف الذي يقابله من جدول البواقي التكعيبية نحصلُ على النص الأصلي

الدالتان $f_P(x) \equiv x^3(\mathrm{mod}\ P)$ من أجلِ كلِّ x من النص الأصلي

و $f_P^{-1}(x) \equiv y^{\frac{P+2}{9}}(\mathrm{mod}\ P)$ من أجلِ كلِّ y من النص المشفر

تحققان تعريفَ التشفير وذلك لأن:

$$\forall x \in T: f_P^{-1}\big(f_P(x)\big) \equiv f_P^{-1}(x^3(\mathrm{mod}\ P)) \equiv (x^3)^{\frac{P+2}{9}}(\mathrm{mod}\ P)$$

$$\equiv (x)^{\frac{P+2}{3}}(\mathrm{mod}\ P) \equiv x^{\frac{P-1+3}{3}} \equiv x^{\frac{P-1}{3}}.x^{\frac{3}{3}}(\mathrm{mod}\ P)$$

$$\equiv 1.x(\text{mod } P) \equiv x(\text{mod } P)$$

**ملاحظة:**

في الخطوة الثالثةِ نشكلُّ جدولاً بحيث يقابل كلُّ حرف من أحرف اللغة اللاتينية ، أحد عناصر مجموعة البواقي التكعيبية بالمقاس P ، وبالتالي نحن بحاجة إلى أن يكونَ عددُ عناصر المجموعة T أكبرَ أو يساوي 26 (عدد أحرف اللغة اللاتينية) ، وهذا يحقق إذا وفقط إذا كان:

$$\frac{P-1}{3} \geq 26 \Leftrightarrow P-1 \geq 78 \Leftrightarrow P \geq 79$$

إذا كان عددُ عناصرِ المجموعة T أكبرَ من 26 نختارُ أصغرَ 26 عنصراً.

سنبين كيفيةَ التشفيرِ بواسطةِ هذه الخوارزمية من خلال المثال التالي:

**مثال 11** : بفرض أنَّ إحدى الكتائبِ أرادت إرسالَ رسالة إلى القيادةِ العامة للجيش مفادُها طلب تعزيزاتٍ إضافيةٍ لمواجهة العدو send more troops فكيف نقوم بتشفير هذه الرسالة؟

الحل:

نختار عدداً أولياً P بحيث يحققُ $P \equiv 7(\text{mod } 9)$ و $P \geq 79$ وليكن P=79

( وهذا العددُ هو مفتاحُ التشفيرِ)

نوجدُ مجموعةَ البواقي التكعيبية بالمقاس P باستخدامِ الحاسوب فنجدُ أنَّ مجموعةَ البواقي التكعيبية بالمقاس 79 هي:

1, 8 , 10 , 12 ,14, 15 ,17 ,18 ,21 ,22,27,33 ,38

,41 ,46, 52 ,57,58 ,61 ,62,64 ,65,67,69 ,71,78.

1) نقومُ بتشكيلِ جدولٍ بحيث يقابل كلُّ حرفٍ من أحرف اللغة الإنكليزية أحدَ عناصر مجموعة البواقي التكعيبية بالمقاس ***P*** كما هو موضحٌ في الجدول الآتي:

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 8 | 10 | 12 | 14 | 15 | 17 | 18 | 21 | 22 | 27 | 33 | 38 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 41 | 46 | 52 | 57 | 58 | 61 | 62 | 64 | 65 | 67 | 69 | 71 | 78 |

2) لتشفير أيِّ كلمةٍ نقوم باستبدالِ كل حرف بالعددِ الذي يقابله في الجدول وذلك وفق الترتيبِ الهجائي سنبين ذلك من خلال الجدول التالي:

| S | E | N | D | M | O | R | E | T | R | E | T | R | O | O | P | S |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 61 | 14 | 41 | 12 | 38 | 46 | 58 | 14 | 62 | 58 | 14 | 62 | 58 | 46 | 46 | 52 | 61 |

3) نقومُ بحسابِ دالة التشفير

$$f(x) \equiv x^3 (\text{mod } 79), x \in \{61,14,41,12,38,46,58,62,52\}$$

$$f(61) \equiv (61)^3 (\text{mod } 79) \equiv 14$$

$$f(14) \equiv (14)^3 (\text{mod } 79) \equiv 58$$

$$f(41) \equiv (41)^3 (\text{mod } 79) \equiv 33$$

$$f(12) \equiv (12)^3 (\text{mod } 79) \equiv 69$$

$$f(38) \equiv (38)^3 (\text{mod } 79) \equiv 46$$

$$f(46) \equiv (46)^3 (\text{mod } 79) \equiv 8$$

$$f(58) \equiv (58)^3 (\text{mod } 79) \equiv 61$$

$$f(14) \equiv (14)^3 (\text{mod } 79) \equiv 58$$

$$f(62) \equiv (62)^3 (\text{mod } 79) \equiv 64$$

$$f(58) \equiv (58)^3 (\text{mod } 79) \equiv 61$$

$$f(46) \equiv (46)^3 (\text{mod } 79) \equiv 8$$

$$f(52) \equiv (52)^3 (\text{mod } 79) \equiv 67$$

$$f(61) \equiv (61)^3 (\text{mod } 79) \equiv 14$$

فينتج لدينا النصُّ المشفَّر التالي:

14 58 33 69 46 8 61 64 61 88 67 14

4) لفكِّ التشفير نحسبُ دالةَ فكِّ التشفيرِ $f^{-1}(y) \equiv yP + 2(mod\ P)$ لكل $y$ من النصِّ المشفر.

$$f^{-1}(14) \equiv (14)^{\frac{79+2}{9}} (\text{mod } 79) \equiv 14^9 \equiv 61 (\text{mod } 79)$$

$$f^{-1}(58) \equiv (58)^{\frac{79+2}{9}} (\text{mod } 79) \equiv 58^9 \equiv 14 (\text{mod } 79)$$

$$f^{-1}(33) \equiv (33)^{\frac{79+2}{9}} (\text{mod } 79) \equiv 33^9 \equiv 41(\text{mod } 79)$$

$$f^{-1}(69) \equiv (69)^{\frac{79+2}{9}} (\text{mod } 79) \equiv 69^9 \equiv 12(\text{mod } 79)$$

$$f^{-1}(46) \equiv (46)^{\frac{79+2}{9}} (\text{mod } 79) \equiv 46^9 \equiv 38(\text{mod } 79)$$

$$f^{-1}(8) \equiv (8)^{\frac{79+2}{9}} (\text{mod } 79) \equiv 8^9 \equiv 46(\text{mod } 79)$$

$$f^{-1}(61) \equiv (61)^{\frac{79+2}{9}} (\text{mod } 79) \equiv 61^9 \equiv 58(\text{mod } 79)$$

$$f^{-1}(58) \equiv (58)^{\frac{79+2}{9}} (\text{mod } 79) \equiv 58^9 \equiv 14(\text{mod } 79)$$

$$f^{-1}(64) \equiv (64)^{\frac{79+2}{9}} (\text{mod } 79) \equiv 64^9 \equiv 62(\text{mod } 79)$$

$$f^{-1}(61) \equiv (61)^{\frac{79+2}{9}} (\text{mod } 79) \equiv 61^9 \equiv 58(\text{mod } 79)$$

$$f^{-1}(8) \equiv (8)^{\frac{79+2}{9}} (\text{mod } 79) \equiv 8^9 \equiv 46(\text{mod } 79)$$

$$f^{-1}(67) \equiv (67)^{\frac{79+2}{9}} (\text{mod } 79) \equiv 67^9 \equiv 52(\text{mod } 79)$$

$$f^{-1}(14) \equiv (14)^{\frac{79+2}{9}} (\text{mod } 79) \equiv 14^9 \equiv 61(\text{mod } 79)$$

فينتج لدينا النصُ 61 52 46 58 62 14 58 46 38 12 41 14 61 وباستبدال كلِّ عددٍ بالحرف الذي يقابلهُ من الجدول ، نحصل على النص الأصلي.

**خوارزمية (3):**

ليكن P عدداً أولياً بحيث $P \equiv 2(\text{mod } 3)$ ، أنَّ أحدَ حلول المتطابقة التكعيبية $x^3 \equiv a(\text{mod } P)$ يكتب بدلالة العدد a باقياً تكعيبياً بالمقاس P ، وهذا الحل هو $x_0 = a^{2n+1}$ حيث n عدداً صحيحاً بحيث $P = 3n + 2$ ، فيما يلي نقدم خطواتِ الخوارزمية الثالثةِ لتشفير البياناتِ والمبنية على حلول التطابق التكعيبي السابق ولنفرضْ أنَّ T مجموعةُ بواقٍ تكعيبية بالمقاس P وليكن $K = \{K = (P)\}$ (مفتاح التشفير).

- **خطوات الخوارزمية:**

1) نختارُ عدداً أولياً $P$ بحيث $P \equiv 2(mod\ 3)$ و $P \geq 27$ .
2) نوجد مجموعة بواقٍ تكعيبيةٍ بالمقاس $P$.
3) نقومُ بتشكيل جدولٍ بحيث يقابلُ كلُّ حرف من أحرف اللغة اللاتينية أحدَ عناصر مجموعة البواقي التكعيبية بالمقاس $P$ وندعو هذا الجدول بجدول البواقي تكعيبية.

4) لتشفير أيِّ كلمةٍ نقومُ باستبدالِ كلِّ حرفٍ من حروفِ هذه الكلمةِ بالعددِ الذي يقابلهُ في الجدول وذلك وفق الترتيبِ الهجائي فينتج لدينا مجموعةٌ من الأعدادِ ندعوها نصَّ ما قبل التشفير.

5) نقومُ بحسابِ دالةِ التشفيرِ $\boldsymbol{f_P(x) \equiv x^3 (mod\ P)}$ من أجل كل $\mathbf{x}$ من النص ما قبل التشفير فينتجُ لدينا مجموعةٌ أخرى من الأعداد ندعوها النصَّ المشفر.

6) لفك التشفيرِ نحسبُ دالة فكِّ التشفير $\boldsymbol{f_P^{-1}(y) \equiv y^{2n+1} (mod\ P)}$ لكل $\mathbf{y}$ من النص المشفر حيث $\boldsymbol{n = \frac{P-2}{3}}$ ، باستبدالِ كلِّ عدد بالحرف الذي يقابلهُ من جدولِ البواقي التكعيبيةِ نحصلُ على النصِّ الأصلي.

الدالتان $f_P(x) \equiv x^3 (\text{mod } P)$ من أجلِ x من النصِّ الأصلي

و $f_P^{-1}(y) \equiv y^{2n+1} (\text{mod } P)$ من أجلِ كل y من النصِّ المشفر.

تحققانِ تعريفَ التشفير وذلك لأن:

$$\forall x \in T: f_K^{-1}\big(f_K(x)\big) \equiv f_K^{-1}\big(x\ (\text{mod } P)\big) \equiv (x^3)^{2n+1} (\text{mod } P)$$
$$\equiv (x)^{6n+3} (\text{mod } P) \equiv x^{3n+2}.x^{3n+1} (\text{mod } P)$$
$$\equiv x^P.x^{P-1} (\text{mod } P) \equiv x.1 (\text{mod } P) \equiv x\ (\text{mod } P)$$

**ملاحظة:** في الخطوةِ الثالثةِ نشكل جدولاً ، بحيث يقابلُ كلُّ حرف من أحرف اللغة اللاتينيةِ أحدَ عناصرِ مجموعةِ البواقي التكعيبية بالمقاس P ، وبالتالي نحنُ بحاجة إلى أن يكونَ عددُ عناصر مجموعة البواقي التكعيبية بالمقاس P أكبر أو يساوي 26 (عدد أحرف اللغة اللاتينية) وهذا يتحقق إذا وفقط إذا كان : $P - 1 \geq 26 \Leftrightarrow P \geq 27$

إذا كان عددُ عناصرِ مجموعةِ البواقي التكعيبية بالمقاس P أكبرُ من 26 نختارُ أصغرَ 26 عنصراً)

# تطبيقات نظرية البواقي الصينية والكسور المستمرة في التشفير

في هذا الفصلِ نعرضُ موضوعَيْن مستقلَيْن الأول يعتمدُ على نظرية البواقي الصينية CRT فيه ندرسُ المشاركةَ السرية (Secret Sharing) وهي أحدُ أهم مواضيع التشفير والتي هي تطبيقٌ مباشرٌ لنظرية البواقي الصينية CRT بالإضافة إلى نظامين من أنظمة المفتاح العامِّ التي تعتمدُ على نظريةِ البواقي الصينية والموضوعُ الثاني يعتمدُ على الكسورِ المستمرة واستخدامها في فك التشفير والوصولِ للمفتاح الخاصِ انطلاقاً من المفتاح العام .

## (3−1) المشاركة السرية والبواقي الصينية (Secret Sharing and CRT): [4]

إن CRT هي بحد ذاتِها مشاركةٌ سريةٌ لو أخذنا $t$ عدداً من الأعداد الصحيحةِ الموجبةِ والأولية مثنى مثنى $m_1, m_2, \dots, m_t$ ، وليكن $m = \prod_{i=1}^{t} m_i$ ولنفرض أنه لدينا قيمةُ سرية $S$ والتي هي قيمةٌ صحيحةٌ تحقق $0 \leq S < m$ هذه السريةُ يمكن أن تُشارك لــ $t$ شخص كالآتي:

بفرض $Y_1, Y_2, \dots, Y_t$ تشير لــ $t$ شخص والذين يشاركون القيمةَ السرية $S$ وتدلّ البواقي $S_i \equiv S \ mod \ m_i$ على المعلوماتِ السرية والتي تكون معروفة فقط لدى الأشخاص $Y_i$ وحسبَ مبرهنةِ البواقي تكون $t$ معلومةً متفرقةً ، و $S_i$ كافيةً لتحديد السرية الأصلية $S$ وأيَّ مجموعة أقلُّ من $t$ من البواقي $S_i$ لا يمكنُ تحديدَ السرية الأصلية $S$ وهذا ما يسمى مخطط المشاركةِ السرية (Secret-Sharing scheme) ولكنهَ ليس مخططَ العتبةِ (threshold scheme) والذي يُعرف كالتالي :

ليكن $t$ شخص و $Y_i$ من المشاركة السرية $S$ والتي تُحقق الخواص التالية:

- كلُّ طرفٍ يملكُ مشاركةَ $S_i$ حول السرية $S$ ، والتي تكونُ غيرَ معروفة بالنسبة لبقيةِ الأطراف.
- هذه السريةُ سهلةُ الحسابِ لأجل $t$ مشاركة $S_i$.
- $t-1$ مشاركةُ $S_i$ (قيمة) لا تعطي أيَّ معلوماتٍ عن السرية $S$.

والآن سوفَ نعرضُ بعضَ مخططاتِ المشاركة السرية ، التي تعتمد على نظرية البواقي CRT:

### (3-1-1) المخطط الأول ( scheme I):

ليكن $m_i$ لأجل $i = 1, \dots, t$ ; أعداداً أوليةً نسبيةً فرديةً وليكن لأجل $1 < K < t$

$$min(K) = min_{1<i_1<\cdots<i_k<t}\, m_{i_1} m_{i_2} \dots m_{i_k}$$

$$max(K-1) = max_{1<i_1<\cdots<i_{k-1}<t}\, m_{i_1} m_{i_2} \dots m_{i_{k-1}}$$

ونختار $w$ أكبرَ قيمةٍ موجبةٍ تحقق

$$w < \frac{min(K)}{max(K-1)} \quad , \qquad gcd(w, m_i) = 1\,, i = 1,2, \dots, t$$

نعرف $m := \min(K)$ في مخططاتِ المشاركةِ السريةِ تكونُ السريةُ هي القيمةُ الموجبة $S$ حيث $0 < S < w$ وبالتالي ستكونُ السريةُ محصورةً بين 0 و $w-1$ والمشاركةُ لأجل $t$ (من المشاركين) تحسب كالتالي:

نختارُ عدداً صحيحاً $a$ يحقق $0 \le s + aw < m$ وليكن $S` = s + aw$

والمشاركةُ تعطى بـــ $S_i \equiv S`(\, mod\, m_i)\; ;\; i = 1,2, \dots, t$

(حيث $S_i$ تشير لمشاركة الفرد $Y_i$).

● والآن لنثبتَ أنه إذا كان لدينا $t-1$ مشاركةً أو أقل فإنَّ هذه المشاركاتِ لا تعطينا معلوماتٍ عن السريةِ ولكن $K$ أو أكثر يمكنُ أن تحددها ، لنفرض $S_1, S_2, \dots, S_h$ مشاركاتِ الأفراد تكون معرفةً لأجل $1 \le h \le t$ وليكن

$M = \prod_{i=1}^{t} m_i$ وأن $\mathrm{M}_j = \frac{M}{m_j}$ لأجل كل $j = 1,2, \dots, n$ ومنه $\mathrm{M}_j, m_j$ أوليانِ نسبياً وحسب خوارزميةِ إقليدس يمكنُ أن نجد $v_j, u_j$ من $\mathbb{Z}$ بحيث تحقق $\mathrm{M}_j u_j + m_j v_j = 1$

وحسب خوارزميةِ البواقي الصينية RSA

$$0 \le S`` < M\,, \qquad S`` = \sum_{j=1}^{h} M_j u_j S_j (mod\ M)$$

إذا كان $h \ge K$ ; $w < m = min(K) \le M$ لذلك حسبِ نظريةِ البواقي الصينية CRT يكون $s`` = s`$ والمشاركة السرية تكون $S \equiv S``\ (mod\ w)$

إذا كان $h = k-1$ فإن $M \le \max(k-1) < \frac{m}{w}$ في هذه الحالة نفرضُ

$$S` = S`` + bM$$

حيث $b$ عددٌ صحيحٌ بحيث يحققُ لأجل $0 \le S` < M$ الآتي :

$$-1 < -\frac{S``}{M} < b < \frac{m - S``}{M}$$

نلاحظُ أنَّ $\frac{m-S``}{M} > \frac{m-M}{M} = \frac{m}{M} - 1 > w - 1$

لذلك لأجلِ أيٍّ $K-1$ أو أقل لا يعطينا معلوماتٍ عن السرية $S$

ملخص: إنَّ النتائجَ أعلاه تثبتُ أن $(K, t)$ هو مخططُ عتبةِ (threshold scheme)

ولتوضيح المخطط أكثرَ سنأخذُ المثال التالي :

**مثال 1 :** نختار $K = 3, t = 4, m_1 = 5, m_2 = 7, m_3 = 11, m_4 = 13$ وحسب المعلومات أعلاه

$$\left.\begin{matrix}\min(K) = m = 385 \\ \max(K-1) = 143\end{matrix}\right\} \Longrightarrow w < \frac{\min(K)}{\max(K-1)} = 2.69$$

في هذا المثال تكون السريةُ أما صفراً أو واحداً (لأن $0 \le S < w = 2$)

ولحساب المشاركةِ لأربعة أشخاص: نختارُ بشكلٍّ عشوائيَّ أيَّ عددٍ صحيحٍ $a$ بحيث يحقق

$0 \le a \le 192$ وليكن $S` = S + 2a$

والمشاركةُ لأربعةِ أشخاصُ تعطى بـــ $S_i \equiv S`(\ mod\ m_i)$

ولنبينَ إذا كان لدينا المشاركتان $S_2 = 5$ , $S_1 = 1$ فإنه لا يمكنُ الحصولُ على معلوماتٍ عن السرية ، ولنفرضْ $M = m_1 m_2 = 35$ لذلك حسبَ خوارزمية إقليدس $M_2 = 5, M_1 = 7$ سنحصلُ على $7 \times (-2) + 5 \times 3 = 1$ وحسب CRA

$$S`` = (7 \times (-2) \times S_1 + 5 \times 3 \times S_2)(mod\ 35) = 26$$

لذلك $S` = 26 + 35b$ حيث $0 \le b \le 10$ و $S$ تأخذ 0 أو 1 ومنه

$$S \equiv S`\ mod\ 2 \equiv b(\ mod\ 2)$$

لذلك فإنَّ مشاركَيْن اثنَيْنِ لا تعطي أيَّ معلوماتٍ عن السرية.

### (3-1-2) أنظمة المفتاح العام بواسطة البواقي الصينية Public-Key systems Via CRT

**☒ نظام Cao-Li والمفتاح العام: [4]**

قدم هذا النظام العالمان Cao و Li كما في المرجع [4] كالآتي:

نختارُ $n$ عدداً أولياً مختلفاً بحيثُ تحقق $m_i \equiv 3(\ mod\ 4)$ ومن ثم نحسب

$$m = \prod_{i=1}^{n} m_i \ \ , M_i = \frac{m}{m_i} \ \ ; i = 1,2, \dots , n$$

ومن ثم حسبِ خوارزمية إقليدس ، نحسب $M`_i$ بحيثُ يحقق $M`_i . M_i \equiv 1 mod m_i$

($M`_i$ معكوس $M_i$ بالمقاس $m_i$ ) وأن $0 < M` < m_i$ لأجل كل $\lambda_i = M`_i M_i, 1 \leq i \leq n$ $i$

$$\Lambda = diag[\lambda_1, \dots , \lambda_n] = \begin{bmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{bmatrix}$$

نختارُ مصفوفةً مربعةً $P$ قابلةَ للعكس وأخرى $P_1$ بحيثُ تحققان هاتين المصفوفتان ما يلي:

- مدخلاتُها أعدادٌ صحيحةٌ موجبةٌ.
- $P(ij) = P_1(ij) = 0$ إذا كان $i < j$.
- كل مُدخلٍ من المدخلات ليس أكبرَ من $B = \min \left[ \sqrt{\frac{m}{i(i+1)d}} \right]$ حيث $d \geq 1$ عدد صحيح موجب اختياري.
- ومن ثم نحسبُ $A = P^T \Lambda P, B = {P_1}^T \Lambda\ P_1$.

المتحولاتُ العامة لهذا النظام هي ( المصفوفة $B-$ والسرية $P, P_1-$ القيم $m_i$).

- تشفيرُ الكتلة من النصِّ الصريح $X = (x_1, \dots , x_n)$ حيث $0 \leq x_i \leq d$ يتمُ وفق حسابِ

$$y = XBX^T$$

ونلاحظُ أنَّ $y = XP_1^T AP_1 X^T = XP_1^T P^T \Lambda P P_1 X^T$

نضعُ $Z = XP_1^T P_1^T$ فتكون: $y = ZZ^T = \lambda_1 z_1^2 + \cdots + \lambda_n z_n^2$

طالما أنَّ $z_i^2 = y(\ mod\ m_i)$ حيث $i = 1,2, \dots, n$

ولأجل كل $i$ نحسبُ الحلَّ $z_i$ ، والتي تحقق $0 \le z_i < \frac{m_i}{2}$

ولفك التشفير كما يلي: $X = Z(P^{-1})^T (P_1^{-1})^T$

ملاحظة: وضعُ الشرطِ $P \equiv 3\ (mod\ p)$ في الخوارزميةِ لتكون أكثرَ فعاليةً ، وللمزيد حول هذا النظام انظر المرجع [4].

## (3-1-3) تطبيق تشفير قاعدة البيانات (data base): [16]

في هذا التطبيقِ يتم فيه تجميعُ عددٍ من ملفات الحاسوبِ أو سجلاتهِ وسنرى كيفيةَ التشفيرِ وفك التشفير والدخول لهذه السجلاتِ كالتالي:

بفرضِ لدينا قاعدةُ بياناتٍ B مكونةٍ من n ملف $F_1, F_2, \dots, F_n$ وطالما أنَّ كلَّ ملف هو سلسلةٌ من أصفارٍ وواحداتِ ، لذلك يمكننا تحديدُ كلِّ ملفٍ بعددٍ ثنائيٍّ .

أولاً علينا اختيارُ n عددٍ أوليٍّ مختلفٍ $m_1, m_2, \dots, m_n$ بحيث $m_j > F_j\ ,\ j = 1,2, \dots, n$

وللتشفير نستخدمُ العددَ الصحيح C الذي يطابقُ $F_j$ بالمقاس $m_j$ $\quad j = 1,2, \dots, n$

ووجود مثلِ هذا العددِ مضمونٌ باستخدام نظريةِ البواقي الصينية ليكن $M = m_1 . m_2 . \dots . m_n$ وأن $\mathrm{M}_j = \frac{M}{m_j}$ وليكن لأجل كل $e_j = M_j y_j$

حيث $y_j$ هو معكوس $M_j$ بالمقاس $m_j$ ، وبالتالي سيكون التشفيرُ

$$C \equiv \sum_{j=1}^{n} e_j F_j (mod\ M)\ \ ; 0 \le C < M$$

الأعدادُ $e_1, \dots, e_n$ تكون مفتاحاً جزئياً للتشفيرِ وللتوضيح أكثرَ سنأخذُ مثالاً على هذا التطبيق

**مثال2 :** بفرض أنَّ قاعدةَ البيانات مؤلفةٌ من أربعةِ ملفات $F_1, F_2, F_3, F_4$ ممثلةً بالنظام الثنائي $(0111)_2, (1001)_2, (1100)_2, (1111)_2$ أو بالترميزِ العشريّ $F_1 = 7, F_2 = 9, F_3 = 12, F_4 = 15$

نضعُ أربعةَ أعدادٍ أوليةٍ $m_1 = 11, m_2 = 13, m_3 = 17, m_4 = 19$

ولإتمامِ عمليةِ التشفير نستخدمُ مبرهنةَ البواقي الصينية لإيجاد العددِ الصحيحِ الموجبِ C الذي يحقق:

$$C \equiv 7(mod\ 11)$$

$$C \equiv 9(mod\ 13)$$

$$C \equiv 12(mod\ 17)$$

$$C \equiv 15(mod\ 19)$$

وهذه القيمةُ يجب أن تكونَ أصغرَ من $M = m_1.m_2.m_3.m_4 = 46189$ ومن ثم نجدُ

$$M = 11 \times 13 \times 17 \times 19$$

$$M_1 = 13 \times 17 \times 19 = 4199$$

$$M_2 = 11 \times 17 \times 19 = 3553 \quad M_3 = 2717\,, \quad M_4 = 2131$$

وأيضاً نقومُ بإيجادِ معكوس $M_j$ بالمقاس $m_j$ والذي يحققُ $y_i M_j \equiv 1(mod\ m_j)$ فنجد:

$$y_1 = 7\,, \quad y_2 = 10\,, \quad y_3 = 11\,, \quad y_4 = 18$$

لذلك ستكونُ المفاتيحُ الجزئيةُ

$$e_1 = 4199 \times 7 = 29393, e_2 = 3553 \times 10 = 35530$$

$$e_3 = 2717 \times 11 = 29887, e_4 = 2431 \times 18 = 43758$$

ولبناءِ النصِّ المشفر

$$C \equiv e_1F_1 + e_2F_2 + e_3F_3 + e_4F_4$$

$$C \equiv 29393 \times 7 + 35530 \times 9 + 29887 \times 12 + 43758 \times 18$$

$$C \equiv 1540535 \equiv 16298(mod\ 46189)$$

لذلك سيكونُ $C \equiv 16298$

عمليةُ فك التشفير: لقراءةِ المفاتيحِ الجزئيةِ ولاستعادة الملفات $F_j$ من الكتلة المشفرة C

علينا إيجادُ أصغر باقٍ موجبٍ لــ C بالمقاسات $m_j$ على سبيلِ المثال لإيجاد الملفِ الأول $F_1$ كما يلي:

$$F_1 \equiv 16298 \equiv 7\ (mod\ 11)$$

وهكذا بالنسبة لــ $F_2, F_3, F_4$ سنحصل على $F_2 = 9\ ,\ F_3 = 12\ ,\ F_4 = 15$

## (3-2) الكسور المستمرة

استخدمت الكسورُ المستمرةُ في الهجمات من قبل المتطفلين للحصول على المفتاحِ الخاص من المفتاح العام بحالتين (القيمةُ الأسيةُ الصغيرةُ و هجماتُ وينر )

### (3-2-1) القيمة الأسية الصغيرة: [2]

القيمةُ الأسيةُ الصغيرةُ يمكنُ أن تُشغل عندما تكون نفسُ الرسالة تُرسلُ إلى عدة أشخاص ، ولتوضيح هجماتِ المتطفلين لنفرض أنَّ الرسالةَ $m$ تُرسلُ إلى ثلاثة أشخاص ، والتي القيم الأسية لهم $e_1 = e_2 = e_3 = 3$ والقياس لهم $n_1, n_2, n_3$ والرسالةُ المشفرة تكون $m^3\ (modn_1)\ , m^3(\ modn_2)\ , m^3\ (modn_3)$ باستخدامِ نظريةِ البواقي الصينية أحدهُم يمكنُ أن يجدَ $m^3\ mod\ n_1.n_2.n_3$ ولكن $m^3 < n_1.n_2.n_3$ لأنَّ لذلك $m < n_1.n_2.n_3$

$m^3$ لا تتأثرُ بتقليلِ المقاسِ $n_1.n_2.n_3$ والرسالةُ يمكنُ أن تُعاد للاختراقِ مَّرةً أخرى بأخذِ الجذر التكعيبي لـــ $m^3$ وسوفَ نشرحُ الهجماتِ على الأسِّيةِ السريِّةِ وهذه الهجماتُ هي التي تعتمدُ على الكسورِ المستمرة.

$$\frac{A}{B} = \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\ddots \frac{1}{q_{n-1} + \frac{1}{q_n}}}}}$$

$$= a_1/(q_1 + a_2/(q_2 + a_3/ \ldots./q_{m-1} + a_m/a_n \ldots))) \qquad (1)$$

ونحنُ نهتمُ بالكسور المستمرةِ التي يكونُ فيها $a_i = 1$ وبالتالي

$$< q_0, q_1, \ldots, q_n > \; = \; q_0 + 1(q_1 + 1/\ldots /q_{n-1} + 1/q_n \ldots)) \qquad (2)$$

مثال **3** :

$$< 0,2,1,3 >= 0 + \frac{1}{2 + \frac{1}{1+\frac{1}{3}}} = \frac{4}{11}$$

ندعو $< 0,2,1,3 >$ امتدادَ الكسورِ المستمرة $\frac{4}{11}$ "continued fraction expansion"

ونحصل على هذا الامتداد المنطقي $f$ بطريقة طرحِ الجزء الصحيح من $f$ وقلب الباقي (عكس) وتكرار هذه العمليةِ حتى نصلَ إلى باقٍ معدوم ( صفر).

ليكن $q_i$ الجزءَ الصحيحَ من خارج القسمة ، $r_i$ هي الباقي في الخطوةِ (i) وليكن m العددَ للمعكوس في خطواتِ المعكوس $q_0 = \lfloor f \rfloor, r_0 = f - q_0$

$$q_i = \left\lfloor \frac{1}{r_{i-1}} \right\rfloor \; ; \; r_i = \frac{1}{r_{i-1}} - q_i \quad for \;\; i = 1,2, \ldots, m \;\ldots\ldots\ldots (3)$$

ولأنَّ $r_m = 0$ نحصلُ على $f =< q_0, q_1, \ldots, q_m >$

**ملاحظة:**

أ- $q_m \geq 2$ لأنَّ لو كان $q_m = 1 \Longleftarrow r_{m-1} = 1$ وهذا شيءٌ مستحيل

ب- لأجل $q > 0$ نميز حالتين:

$$\begin{cases} \frac{A}{B} < < q_0, q_1, \dots, q_{m-1}, q_{m+n} > & if\ m\ is\ even \\ \frac{A}{B} > < q_0, q_1, \dots, q_{m-1}, q_{m+n} > & if\ m\ is\ odd \end{cases} \quad (4)$$

ضروريٌ أن نكونَ قادرينَ على استعادة الكسر من $n_i, d_i, q_0$ (سلسلة البسوط والمقامات) كالتالي:

$$\frac{n_i}{d_i} =< q_0, q_1, \dots, q_i > ; gcd(n_i, d_i) = 1 \ \ for\ i = 0,1, \dots, m \quad (5)$$

يمكن أن نُظهر أن:

$$\begin{aligned} i = 0 &\Longrightarrow n_0 = q_0 \ \ ; \ d_0 = 1 \\ i = 1 &\Longrightarrow n_1 = q_0 q_1 + 1 \ \ ; \ d_0 = q_1 \\ i \geq 2 &\Longrightarrow n_i = q_i n_{i-1} + n_{i-2} \ \ ; \ d_i = q_i d_{i-1} + d_{i-2} \end{aligned} \quad (6)$$

في هذه الطريقة سيكون $f = \frac{n_m}{d_m}$ يمكن استعادته.

ملاحظة: العلاقةُ بين البسوطِ والمقاماتِ كالآتي $n_i d_{i-1} - n_{i-1} d_i = -(-1)^i$ لأجل $i = 1,2, \dots, m$.

## بنية خوارزمية الكسور المستمرة:

لنعرف $f`$ بالشكل $f` = f(1 - s) \ \dots \dots \dots \ (7)$ لأجل $s \geq 0$

ليكن $q`_i, r`_i, q_i, r_i$ البواقي ونواتج القسمة لـــ $f`, f$ على الترتيب

إذا كانت $s$ صغيرةً بقدرٍ كافٍ فإنَّ البسطَ والمقامَ لـــ $f$ يمكنُ أن يُوجد باستخدامِ الخوارزمية التالية:

- توليدٌ ناتجٌ القسمةِ $(q`_i)$ لتمديد الكسر المستمر
- حسبِ العلاقة (6) الكسرُ يكون زوجياً إذا كان $< q`_0, q`_1, \dots, q`_{i+1} >$

  فردياً إذا كان $< q`_0, q`_1, \dots, q`_i >$
- نختبرُ فيما إذا كانَ الكسرُ يساوي $f$ أم لا.

وأن $ff`$ كما أن الاختبارُ يجبُ أن يكونَ موجوداً لتحديد فيما إذا كان التخمينُ لـــ $f$ صحاً أم لا.

خوارزمية الكسور المستمرة سوف تنجح إذا كان:

$$\begin{cases} < q_0, \dots, q_{m-1}, q_m - 1 > \ < \ f` \leq < q_0, \dots, q_m > if\ m\ is\ \ even \\ < q_0, \dots, q_{m-1}, q_m + 1 > \ < \ f` \leq < q_0, \dots, q_m > if\ m\ is\ odd \end{cases} \quad (8)$$

سوفَ نعتبرُ في حالة العلاقة (7) أن $s$ يكون:

$$s = 1 - \frac{f`}{f} \quad (9)$$

لنميزَ الحالات التالية $m = 0, m = 1$ , $m$ عددٌ زوجي $m \geq 2$, عددٌ فردي $m \geq 3$

1)- حالة $m = 0$ باستخدامِ العلاقة (8) وباستبدال $f`$ في (9) يقود إلى:

$$s < 1 - \frac{f`}{f} \Longrightarrow s < 1 - < q_0 - 1 > / < q_0 > \quad (10)$$

باستخدام العلاقةِ رقم (2) $[n_0 = q_0$ وأن $d_0 = 1]$ لذلك يكونُ:

$$s < 1 - \frac{f`}{f} = 1 - \frac{n_0 - 1}{n_0} = \frac{n_0 - n_0 + 1}{n_0} = \frac{1}{n_0} \Longrightarrow s < \frac{1}{n_0 d_0} \quad (11)$$

2)- $m = 1$ باستخدامِ العلاقة (8) وباستبدال $f`$ في (9) يقود إلى:

$$s \ < \ 1 - < q_0, q_1 + 1 > / < q_0, q_1 > \quad (12)$$

حسب العلاقة (2)

$$s < \frac{1}{(q_0 q_1 + 1)(q_1 + 1)} \quad (13)$$

وحسب العلاقة (6)

$$q_1 + 1 \leq \frac{3}{2} q_1$$

$$q_1 + 1 \leq \frac{3}{2} d_1$$

$$\Longrightarrow s < \frac{1}{\frac{3}{2} n_1 d_1}$$

وهذا كافٍ لتحقيقِ خوارزميةِ الكسورِ المستمرةِ في هذه الحالة.

3)- حالةُ $m \geq 2$ وأن $m$ زوجيٌّ سيكونُ: $s < \frac{1}{n_m d_m}$

4)- حالةُ $m \rangle 2$ وأن $m$ فرديٌّ سيكونُ: $s < \frac{1}{\frac{3}{2} n_m d_m}$

وبالتالي ستكونُ النتيجةُ التي وصلنا إليها في الحالات الأربع:

$$s < \frac{1}{\frac{3}{2}n_m d_m} \quad (14)$$

وهذا الضمانُ كافٍ لنجاحِ خوارزميةِ الكسورِ المستمرة ونذكرُ أن $n_m$ هو بسط $f$ و $d_m$ هو المقام

## (3-2-2) تطبيق خوارزمية الكسور المستمرة على RSA :

إن القيمةَ السرِّيةَ الخاصةَ هي معكوسُ القيمةِ الأسِّية العامةِ (مرجع [10])

$$e.d \equiv 1(mod\ M) \quad (15)$$

حيثُ $M = lcm(p-1, q-1)$ ، ومن هذه العلاقةِ يتبينُ أنه يجب أن يوجد عدد صحيح $k$ بحيث يكونُ:

$$e.d \equiv K\ lcm(p-1, q-1) + 1$$

فإذا وضعنا أن $G = gcd(p-1, q-1)$ واستخدمنا $lcm(p-1, q-1) = \frac{(p-1)(q-1)}{G}$ سوف نحصل على:

$$ed = \frac{K}{G}(p-1)(q-1) + 1 \quad (16)$$

ويمكن لـــ $G, K$ أن يملكا عناصرَ مشتركةً ولْنعرف:

$$g = \frac{G}{gcd(K,G)}\ , k = \frac{K}{gcd(K,G)}$$

لذلك سيكون $\frac{k}{g} = \frac{K}{G}$ وأن $gcd(k,g) = 1$ وبالتالي يكونُ لدينا

$$ed = \frac{k}{g}(p-1)(q-1) + 1$$

وبقسمة الطرفين على المقدار $dpq$ سنحصلُ على العلاقة:

$$\frac{e}{pq} = \frac{k}{dg}(1-s) \quad ; \quad s = \frac{p+q-1-\frac{g}{k}}{pq} \quad (17)$$

نلاحظُ أنَّ $\frac{e}{pq}$ تعتبرُ معلوماتٍ عامةٍ وللتقريب أكثر لـــ $\frac{k}{dg}$ استناداً لخوارزميةِ الكسور المستمرة وباستخدامِ التعبير عن $s$ في العلاقة (17) والعلاقة التي تدل على شرط نجاح الكسور المستمرة (العلاقة رقم (14) أعلاه ) يمكنُ أن يظهرَ أن:

$$kdg < \frac{pq}{\frac{3}{2}(p+q)} \qquad (18)$$

وهذا كافٍ لإيجاد $dg$ وَ $K$.

ويمكنُ إعادةُ كتابةِ العلاقة رقم (16) لتصبحَ بالشكل

$$edg = k(p-1)(q-1) + g \qquad (19)$$

ونرى إذا قمنا بقسمةِ الطرفين على $k$ سنحصل على $(p-1)(q-1)$ والباقي لـــ $g$ طالما أن $k > g$ وهذا يزوِّدُنا بالتخمين عن $(p-1)(q-1)$ وعن $g$ فإذا كان التخمينُ عن $(p-1)(q-1)$ معدوماً (صفراً) عندئذٍ تكون $K, dg$ خطأ والتخمين $(p-1)(q-1)$ يمكن أن يستخدمَ ليعالج $(\frac{p+q}{2})$ من خلال العلاقة:

$$\frac{pq-(p-1)(q-1)+1}{2} = \frac{p+q}{2} \qquad (20)$$

فإذا كان التخمين $(\frac{p+q}{2})$ ليس عدداً صحيحاً فإن $k$ و $dg$ خطأٌ وهذا أيضاً يقودنا إلى تَخْمِينِ $(\frac{p-q}{2})^2$ مربعٍ كاملٍ من خلال العلاقة:

$$(\frac{p+q}{2})^2 - pq = (\frac{p-q}{2})^2 \qquad (21)$$

فإذا كان التخمينُ $(\frac{p-q}{2})^2$ مربعاً كاملاً كان التخمينُ الأساسُّي لـــ $k$ و $dg$ صحيحاً.

والقيمةُ السرية $d$ يمكن أن نحصلَ عليها بتقسيم $dg$ على $g$ كما نذكرُ بأنَّ $g$ هي الباقي عندما قمنا بقسمة $edg$ على المقدار $k$

أيضاً يمكنُ إعادةُ تعيين (استنتاج) قيم $p, q$ من علاقتي $(\frac{p-q}{2}), \left(\frac{p+q}{2}\right)$

ولازالت الدراساتُ مجالَ مكافحةِ هجماتِ المتطفلينَ باستخدام الكسورِ المستمرةِ على تشفير RSA.

**مثال 3 :** لنأخذ $n = p.q = 8927$ , $e = 2621$ وبالتالي الكسرُ المستمرُ سيكون

$$\frac{e}{pq} = \frac{2621}{8927}$$

$$\frac{e}{pq} = 0 + \frac{2621}{8927} = 0 + \frac{1}{3 + \frac{1064}{2621}} = 0 + \frac{1}{3 + \frac{1}{2 + \frac{493}{1064}}}$$

$$= 0 + \frac{1}{3 + \frac{1}{2 + \frac{1}{2 + \frac{28}{493}}}}$$

$q_0 = 0\,,\quad q_1 = 3\,,\quad q_2 = 2\,,\quad q_3 = 2$

$r_0 = 0\,,\quad r_1 = \frac{1064}{2621}\,,\quad r_2 = \frac{493}{1064}\,,\quad r_3 = \frac{78}{493}$

| حساب المقادير | كيفية الوصول إليها | i=0 | i=1 | i=2 |
|---|---|---|---|---|
| $q`_i$ | العلاقة رقم (3) | 0 | 3 | 2 |
| $r`_i$ | العلاقة رقم (3) | $\frac{2621}{8927}$ | $\frac{1064}{2621}$ | $\frac{493}{1064}$ |
| $\frac{n`_i}{d`_i}$ | العلاقة رقم (6) | $\frac{0}{1}$ | $\frac{1}{3}$ | $\frac{2}{7}$ |
| $< q`_0, \dots, q`_i >$ | $< 0,3,2,2 >$ | | | |
| $\frac{k}{dg}$ تخمين | $< q`_0, \dots, q`_{i+1} >$ $< q`_0, \dots, q`_i >$ | $\frac{1}{1}$ | $\frac{1}{3}$ | $\frac{3}{10}$ |
| $edg$ تخمين | $e.dg$ | 2621 | 7863 | 26210 |
| $(p-1)(q-1)$ توقع | $\left\lfloor \frac{edg}{k} \right\rfloor$ | 2621 | 7863 | 26210 |
| $g$ تخمين | $edg\ mod k$ | 0 | 0 | 2 |
| $\frac{p+q}{2}$ تخمين | العلاقة رقم (31) | 3153.5 | 532.5 | 96 |
| $\left(\frac{p-q}{2}\right)^2$ تخمين | العلاقة رقم (32) | | | $289 = 17^2$ |
| $d$ | $\frac{dg}{g}$ | | | 5 |

وبالتالي هجماتُ الكسور المستمرةِ لهذا المثال أعطتنا:

$$d = 5\,, \quad p = 113\,, \quad q = 79\,, \quad k = 3\,, \quad g = 2$$

وهو الأسُّ السرِّي (المفتاح الخاص).

كما أثبت Winer تطبيقٌ آخرُ للكسورِ المستمرة وهو استخدامٌ للكسورِ المستمرةِ في الهجمات للوصول للمفتاح الخاص من المفتاح العام ، وذلك عن طريقِ عدد من المبرهنات التالية :

**(3-2-3) مبرهنة : [2]**

إذا كانَ لدينا الكسرُ المستمرُ المنتهي $< a_1, a_2, \dots, a_n >$ ووضعنا

$$p_1 = a_1\ ,\ p_2 = a_1a_2 + 1\,,\ \ p_3 = a_3p_2 + p_1\,, \dots\ ,\ p_i = a_ip_{i-1} + p_{i-2}$$
$$q_1 = 1\ ,\ q_2 = a_2\ ,\ q_3 = a_3q_2 + q_1\ , \dots\ ,\ q_i = a_iq_{i-1} + q_{i-2}$$

فإن التقريبَ من المرتبة $n$ أي $c_n$ للكسر يساوي $c_n = \frac{p_n}{q_n}$ وعندما $n \geq 1$

تذكرةٌ: بنظامِ تشفير RSA: في البداية نجد $N$ عدداً صحيحاً كبيراً حيث $N = p.q$ وهما عددان أوليان مختلفان ، ومن ثم حساب $\emptyset(N) = (p-1)(q-1)$

وبعدها نختار عددين $1 < e, d < \emptyset(N)$ بحيث يكون $ed \equiv 1(\ mod \emptyset\ (N))$

ويكون المفتاحُ الخاص هو الثنائية $(p, q, d)$

أما المفتاحُ العام هو $(N, e)$ ولتشفير أيِّ رسالة $N > m$ والتي نرسلُها في كتلٍ نستخدم دالةَ التشفيرِ $E(m) \equiv (m^e)^d \equiv m^{ed}(\ mod\ N)$ حيث $m^{ed} \equiv m(\ mod\ N)$

والآن سوفَ ندرسُ هجماتِ (Winer) على هذا النظامِ والذي استخدمِ فيها الكسورِ المستمرةِ ولأجل ذلك سنبدأ بالنظريات والتمهيديات الآتية:

ليكن $N = p.q$ حيث $p, q$ أوليان فرديان ولتحديد قيمة $a$ صغيرة $a \in N$ بحيث $p < q < ap$

لأن $ed \equiv 1(\ mod\ \emptyset(N))$ ويمكن إعادة كتابتها:

$$\emptyset(N) = \frac{ed-1}{k}\ \ ;\ \ (n \in N) \qquad (22)$$

والفكرةُ الأساسيةُ لهجمات Winer هي إظهار $d$ من تقريبِ الكسر $\frac{k}{d}$ تقريب لـــ $\frac{e}{N}$ وسنبدأُ بالتمهيديةِ التالية:

**(3-2-4) تمهيدية: [2]** ليكن $p,q$ أوليين فرديين مختلفين بحيث $p < q < ap$ لأجل $a \in N$ عندئذٍ يكون

$$N - (a+1)\sqrt{N} < \emptyset(N) < N \qquad (23)$$

الإثبات: أولاً أن $\emptyset(N) < N$ واضح أنّ $(p-1)(q-1) < pq$

ومن ثم لنثبتَ $N - (a+1)\sqrt{N} < \emptyset(N)$ كما يلي:

$$\sqrt{N} > p > p - \frac{1}{a+1}$$

و بضربٍ بالمقام $(a+1)$ وأخذِ أولِذ حدين نجد:

$$(a+1)\sqrt{N} > (a+1).p - 1$$

$$\Rightarrow \quad (a+1)\sqrt{N} > ap + p - 1$$

ولأن $ap < q$ (نستبدلُ $ap$ بـــ $q$) نجدُ

$$(a+1)\sqrt{N} > (p+q) - 1$$

وأخيراً سيكون:

$$N - (a+1)\sqrt{N} < N - (p+q) + 1 = \emptyset(N)$$

ونحن نبحثُ عن الشرط ليقاربَ الكسر $\frac{k}{d}$ ليقترب من الكسر $\frac{e}{N}$ في التمهيدية الآتية:

**(3-2-5) تمهيدية :[2]** ليكن $(N,e)$ المفتاحَ العام و $N = pq$ بحيث $p < q < ap$ لأجل $a \in$ $N$ وليكن $x \in N$ .عندئذٍ:

$$\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{(a+1)k}{d\sqrt{N}} \qquad (24)$$

الإثبات: حسبِ التمهيديةِ السابقةِ $\frac{ed-1}{k} = \emptyset(N) < N - (a+1)\sqrt{N}$

ومنه نضربُ بـــ $k$

$$\Rightarrow k(N - (a+1)\sqrt{N}) < ed - 1$$

نقسِّمُ على dN

$$\frac{k}{d}-\frac{e}{N}<\frac{(a+1)k}{d\sqrt{N}}-\frac{1}{dN} \qquad (25)$$

من العلاقة $\emptyset(N)=\frac{ed-1}{k}$ ونكتبُ $ed=k\,\emptyset(n)+1$ وبالتالي

$$ed+1=k\,\emptyset(N)+2<kN+(a+1)k\sqrt{N}$$

$$-\left(\frac{(a+1)k}{d\sqrt{N}}-\frac{1}{dN}\right)<\frac{k}{d}-\frac{e}{N} \qquad (26)$$

وحسبِ خواصِ القيمةِ المطلقة نجد

$$\left|\frac{e}{n}-\frac{k}{d}\right|<\frac{(a+1)k}{d\sqrt{N}}-\frac{1}{dN}<\frac{(a+1)k}{d\sqrt{N}}$$

$$\left|\frac{e}{N}-\frac{k}{d}\right|<\frac{(a+1)k}{d\sqrt{N}}$$

وحتى يكون $\frac{k}{d}$ هو تقريبٌ لـــ $\frac{e}{N}$ نضعُ على $d$ شرطاً موضَّحاً في التمهيدية التالية :

**(3−2−6) تمهيدية:[2]** ليكن $k,d$ المعرفان في العلاقات السابقة عندئذٍ يكون $k<d$

الإثبات: لدينا $\emptyset(N)=\frac{ed-1}{k}\Leftarrow\emptyset(N)=\frac{ed}{k}-\frac{1}{k}$

$$\Rightarrow \emptyset(N)+\frac{1}{k}=\frac{ed}{k} \quad\Rightarrow\quad \frac{k\,\emptyset(N)+1}{k}=\frac{ed}{k} \quad\Rightarrow\quad \frac{k\,\emptyset(N)+1}{ek}=\frac{d}{k}$$

$$\Rightarrow\quad \frac{d}{k}=\frac{k\,\emptyset(N)+1}{ek}>1$$

وهذا يعني أنَّ $\frac{d}{k}>1$ وبذلك $d>k$ تم المطلوب .

والآن لنثبتِ الهدفِ الرئيسي من اختيار Winer وهو أنَّ الكسر $\frac{k}{d}$ هو تقاربٌ لـــ $\frac{e}{N}$ لأجلِ بعضِ قيمِ $d$ محددةٌ ، ولْنفعل ذلك نطبقُ التمهيديةَ (3−2−4) عندما يكونُ

$$\left|\frac{e}{N}-\frac{k}{d}\right|<\frac{1}{2d^2} \qquad (27)$$

**(3-2-7) مبرهنة: [2]** اذا كان $\frac{k}{d}$ هو تقاربُ (تقريب) لــ $\frac{e}{N}$ فإنّ :

$$d \leq \frac{\sqrt[4]{N}}{\sqrt{2(a+1)}} \qquad (28)$$

الإثبات: حسبَ المبرهنةِ (3-2-3) والتمهيديةِ (3-2-5) يكونُ $\frac{k}{d}$ تقريباً لــ $\frac{e}{N}$ إذا كان

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{(a+1)k}{d\sqrt{N}} < \frac{1}{2d^2}$$

ومنه $2d(a+1)k < \sqrt{N}$

وبما أنَّ $k < d$ يكونُ

$$2(a+1)kd < 2(a+1)d^2 < \sqrt{N}$$

ومنه نجدُ أكبرَ قِيَمٍ لــ $d$

$$2(a+1)d^2 \leq \sqrt{N}$$

$$\Rightarrow d^2 \leq \frac{\sqrt{N}}{2(a+1)}$$

وبالجذر $d \leq \frac{\sqrt[4]{N}}{\sqrt{2(a+1)}}$ وهو المطلوب.

ومن هذه المبرهنةِ نلاحظُ أنَّ قيمَ $\emptyset$ تعتمدُ على $a$ وكلما ازدادت قيمةُ $a$ فإن قيمة $d$ والتي تتضمن تقاربَ $\frac{k}{d}$ من $\frac{e}{N}$ تنقصُ وسوفَ نحددُ التقريبَ $\frac{k}{d}$ بطريقةٍ أسهلَ للكسر $N$ ، لنفرضَ أننا يمكن أن نعبَّرَ عن $N$ كما يلي:

$$N = x^2 - y^2 = (x-y)(x+y)\ ; x, y \in N \qquad (29)$$

وطالما أنَّ $N = p.q$ فإنه لدينا إما $p = x - y\ , q = x + y$

أو $1 = x - y\ , N = x + y$ وحلٌّ لأجلِ $x, y$ في الحالتين التاليتين :

ففي الحالةِ الأولى: $x = \frac{p+q}{2}\ , y = \frac{q-p}{2}$

وفي الحالةِ الثانيةِ: $x = \frac{N+1}{2}\ , y = \frac{N-1}{2}$

وهذه الطريقةُ من الكسورِ تُدعى (خوارزميةَ عواملِ فيرما) ولمعلوماتٍ أكثرَ [2]

الآن نرى كيف يمكنُ أن نستخدمَ النتائج السابقة في هجمات (Winer) لتحديد المفتاح الخاص $(p,q,d)$ ، بفرض $N=x^2-y^2$ وأنَّ العلاقة $d \leq \frac{\sqrt[4]{N}}{\sqrt{2(a+1)}}$ محققةٌ حيثُ نختبرُ كلَّ تقريبٍ بالتتابعِ وليكن$\frac{k`}{d`}$ تقريباً لــ $\frac{e}{N}$ الذي اختبرناه ولأجلِ هذا التقريب ليكن $\frac{k`}{d`}$ المعرف كالآتي: $\emptyset`(N)$

$$\emptyset`(N)=\frac{ed`-1}{x`} \qquad (30)$$

والمبرهنةُ التاليةُ هامةٌ جداً والمعروفةُ باسم (اختبار Winer) والتي تقومُ باختبارنا بالمفتاح الخاص $(p,q,d)$ وإنطلاقاً من $x`,y`$ .

**(3-2-8) مبرهنة : اختبار وينر Winer test: [2]**

ليكن $\frac{k`}{d`}$ تقريباً لــ $\frac{e}{N}$ إذا كانَ $x`,y` \in N$ المعرفتان $y`=\sqrt{(x`)^2-N}$ ,$x`=\frac{N-\emptyset`(N)+1}{2}$

فإن المفتاحَ الخاصَ هو : $(p,q,d)=(x`-y`,x`+y`,d)$

الإثبات:

لتكن $x`,y` \in N$ وحسْبَ العلاقةِ (32) لدينا:

$$N=x`^2-y`^2=(x`-y`)(x`+y`)$$

لنفرض أنَّ $x`=\frac{N+1}{2}$ ومنه $2x`=N+1$ وحسْبَ العلاقةِ (24) يكون:

$$N+1=2x`=N-\emptyset`(N)+1$$

وحسْب (30) لدينا $\emptyset`(N)=\frac{ed`-1}{x`}$ ومنه $N+1=N-\emptyset`(N)+1$

والتي $N+1=N-\frac{ed`-1}{x`}+1$ وهي محققةٌ إذا كان $e=1$ أما إذا كان $e>1$ نجدُ

$$y`=\frac{q-p}{2} \quad ,x`=\frac{p+q}{2} \quad \text{ومنه} \quad 2x`=p+q$$

وبالتالي يكونُ $N+1=N-(p+q)+1$

وطالما$\emptyset`(N)=\emptyset(N)$ سيكونُ الآتي:

$$d` \equiv d \ (mod \ \emptyset(N)$$

وبما أنَّ $1<d<\emptyset(N)$ وبالتالي سيكون $d`=d$.

**ملاحظة:** إن أهميةَ اختبارِ (Winer) تكمنُ بإعطاء المفتاح الخاص $d$ والذي من خلاله يتمُ فكُّ التشفيرِ ، والتي تعتبرُ اختراقاً وكسراً للخوارزمية RSA.

**مثال4** : ليكنْ $N = 826513 , e = 589063$ استخدمْ اختبارَ Winer لإظهارِ أنَّ

$$(p, q, d) = (829,997,7)$$

الحل: نحسبُ الكسرَ $\frac{e}{N}$ فنجدُ $\frac{e}{N} = [0,1,2,2,12,1,1,19,1,2,5,2,6]$

أولَ ثلاثِ تقريباتٍ تكون $\frac{0}{1}, \frac{1}{1}, \frac{2}{3}$ وفيها كلُّها يفشلُ اختبارُ Winer ، وبتطبيقِ الاختبارِ على التقريب التالي (الرابع) وهو $\frac{5}{7}$ سيكون $\emptyset`(N) = \frac{7e-1}{5} = 824688$

والذي يعطينا $x` = 913 , y` = 84$ طالما أن $x, y \in N$

وحسْبَ المبرهنةِ السابقة (3−2−8) سيكون $\frac{5}{7}$ هو التقريب الصحيح ، لذلك سيكون

$$(p, q, d) = (829,997,7)$$

ملاحظة: لتوضيحِ قيمةِ هذه النقطةِ حيث تعطي حدودَ $d$ والذي يعطي $d \leq \frac{\sqrt[4]{N}}{\sqrt{6}}$ وهذا الشرط يتحققُ ، ولكنه ليسَ ضرورياً لنجاحِ اختبارِ Winer.

**مثال 5:** ليكن $N = 826513 , e = 697813$ استخدمْ اختبارَ Winer لإظهار أن

$$(p, q, d) = (829,997,13)$$

الحل: حسْبَ المبرهنةِ السابقةِ أكبرُ قيمةٍ لحدودِ $d$ هي 12 ولأنَّ لدينا الكسرَ

$$\frac{e}{N} = \frac{697813}{826513} = [0,1,5,2,1,2,2,1,1,13,1,1,1,3,3,2]$$

وبالتالي التقريبات الثلاثةُ الأولى $\frac{0}{1}, \frac{1}{1}, \frac{5}{6}$ عندها يفشلُ اختبارُ Winer والتقريب التالي هو $\frac{11}{13}$ ولكون $12 < 13$ لذلك لا يوجد ضمانٌ للعمل ، ولكن اختبار Winer يخبرنا أن $\emptyset`(N) = \frac{13e-1}{11}$ ومنه $\emptyset`(N) = 824688$

ولأننا استخدمنا $\emptyset`(N), N$ تعتمدُ على $\emptyset(N)$ في المثال السابق لذلك نكون قد اختبرنا التقريبَ الصحيحَ وبالتالي سيكون $(p, q, d) = (829,997,13)$

وهذا المثالُ يوضحُ لنا نجاحَ الاختبارِ ، وأنَّ الملاحظةَ ليست صحيحةً دوماً.

**مثال6 :** ليكن $N = 826513 , e = 697813$ استخدمْ هجماتِ (Winer) ، لإثبات أن

$$(p, q, d) = (829,997,13)$$

حسْبَ العلاقةِ $[d \leq \frac{\sqrt[4]{N}}{\sqrt{6}}]$ نجدُ أنَّ حدودَ $d$ هي 12

$$\frac{e}{N} = [0,1,5,2,2,1,2,2,1,1,13,1,1,1,3,3,2]$$

التقريبُ لأجلِ $d \leq 12$ تكون $\frac{0}{1}, \frac{1}{1}, \frac{5}{6}$ وكلٌّ هذه التقريباتِ تفشلُ عندها اختبارُ Winer والتقريب التالي هو $\frac{11}{13}$ طالما $13 > 12$ ، فإنَّ الهجماتِ ليست مضمونِّة العمل ، وحسب اختبار Winer فإن $\emptyset`(N) = \frac{13e-1}{11} = 824688$

وبما أننا استخدمنا $N$ في المثال السابق ، وكانت $\emptyset`(N)$ مطابقةً لـــ $\emptyset(N)$ في المثال السابق فإننا نكون قد اخترنا التقريبَ الصحيحَ ومنه نجدُ أنَّ $d$ هو المقامُ أي $d = 13$ ، وبالتالي

$$(p, q, d) = (829,997,1)$$

# تطبيقات معادلة ديوفانتس الخطية

في هذا الفصلِ درسنا أنظمةَ التشفير التي تعتمد على حلول معادلةِ ديوفانتـــس الخطيَّةِ ، $a_1x_1 + a_2x_2 + \cdots + a_nx_n = S$ وذلك باســـتخدام نظامِ العدِّ الثنائـــيِّ ، بحيثُ تأخـــذُ المتحولاتُ القيمَ $x_i \in \{0,1\}$ ، ثم قمنا بتعريفِ المتجه مضاعفِ التعامدِ لمعاملات معادلة ديوفانتس الخطية ، بالإضافة لوضْعِ خوارزميةٍ تحلُّ جميعَ معادلاتِ ديوفانتـــس التـــي تحقق شروطَ المتجهِ مضاعفِ التعامد بالنظام الثلاثي$\{0,1,2\}$ $x_i \in$ ، وأخيراً قُمنا ببناء نظام التشفير بالمفتاح العام SY الذي أعتمد علـــى الخوارزمية الســـابقة و المتجه مضاعف التعامد ، مع تقديم مثال تطبيقي عن هذا النظام .

## (4-1-1) تعريف: [3]

ان حل معادلة ديوفانتس الخطية $a_1x_1 + a_2x_2 + \cdots + a_nx_n = S$ بنظام العد الثنائي $x_i \in \{0,1\}$ لأجل $a_1, a_2, \dots, a_n$ أعداداً طبيعيةً ، وبفرض $S$ مجموعٌ جزئيٌ لعدد من هذه الأعداد $a_i$ , $i = 1,2,..,n$ يدعى بمسألة حقيبة السارق (حقيبة الظهر ) أو مسألة Knapsack ، حيث تُمثل $S$ سعةَ حقيبةِ السارق ، كما تمثل الأعداد $a_1, a_2, \dots, a_n$ الأشياء المسروقة (المختارة).

فمسألة Knapsack تسألُ أيَّ من هذه الأعداد تُجمع إلى بعضها البعض لتعطينا المجموع $S$ ؟

ويعبَّر عن $S$ بـــ $a_1x_1 + a_2x_2 + \cdots + a_nx_n = S$

حيث المتحولات $x_1, x_2, \dots, x_n$ تأخذُ القيمَ 1 , 0 وأنَّ $S$ ، $a_i$ معلومةٌ ، فإذا أخذ المتحولُ $x_i$ القيمةَ 1 ، فهذا يعني أنَّ الشيءَ $a_i$ من الأشياءِ المختارةِ ، وهو موجودٌ ضمن الحقيبةِ ، أما إذا كانت القيمةُ 0 ، فهذا يعني أنَّ السارقَ لم يأخذْ الشيء $a_i$ ، وندعو $a = (a_1, a_2, \dots, a_n)$ بمتجهِ حقيبةِ السارق (حقيبة الظهر ) ، وسوفَ نأخذُ مثالاً لتوضيحِ مسألةِ حقيبةِ السارقِ (حقيبة الظهر) .

**مثال 1** : لتكنْ $(a_1, a_2, a_3, a_4, a_5) = (2,7,8,11,12)$ ، وبالبحثِ نجدُ أنَّ هناك مجموعتين جزئيتين من هذه الاعداد ، لو جمعناهما الى بعض (كلا على حده ) لوجدنا المجموع 21 وهمّا 2+8+11=2+7+12=21

وبالمقابل ، يوجدُ بالضبط حلان للمعادلة:

$2x_1 + 7x_2 + 8x_3 + 11x_4 + 12x_5 = 21$ بوضع $x_i = 0$ أو 1

حيث $i = 1,2, \dots ,5$

أحدُهما $x_1 = x_2 = x_5 = 1,\ x_3 = x_4 = 0$

والأخرُ $x_1 = x_3 = x_4 = 1\ , x_2 = x_5 = 0$

للتحققِ من حلولِ المعادلة السابقة ، يتطلبُ منا إجراءَ n عملية جمعٍ على الأكثر

من جهة ثانيةٍ فإنَّ البحثَ في تجزئةِ حلول المعادلة قد يتطلب $2^n$ أمكانية لأجل $x_1, x_2, \dots, x_n$ وأفضلُ طريقةٍ لإيجاد حلول مسألة Knapsack ، تتطلب $O(2^{n}/_{2})$ عملية بتيةً ، والتي تعطينا الحلَّ الحاسوبيَّ ، وبشكل عام فإنَّ مسألةَ Knapsack غيرُ ممكنةٍ لأجل n=100

يمكنُ أن نجدَ طريقةً سهلةً لمسألة السارقِ Knapsack ، باختيار متجهَ أعدادٍ صحيحةٍ متزايدَ.

**(4−1−2) تعريف : [10]** نقول عن متتالية $a_1, a_2, \dots, a_n$ من الأعداد الطبيعية إنها متتاليةٌ متزايدة (sequence–increasing) إذا كان $\sum_{i=1}^{j-1} a_i < a_j$ لأجل كل $j = 1,2, \dots$.

وسنرى أنَّ مسألةَ السارق Knapsack والتي تعتمدُ على متتاليةٍ متزايدةٍ تكونُ أسهلَ .

**مثال 2** : لنأخذْ المتتاليةَ المتزايدةَ $(a_1, a_2, a_3, a_4, a_5) = (2,3,7,14,27)$

ولنأخذْ المجموعَ لـــ 37 ، نلاحظ أنَّ كلَّ حدٍّ هو أكبرُ من مجموعِ سابقاتهِ

$$2x_1 + 3x_2 + 7x_3 + 14x_4 + 27x_5 = 37$$

لدينا $2 + 3 + 7 + 14 < 27$ أي أن $a_5 = 27 < 37 = S$

وبالتالي سيكونُ $x_5 = 1$

ومن ثم يكونُ $2x_1 + 3x_2 + 7x_3 + 14x_4 = 10$

( توضيح 10هي $S - \sum_{i=j+1}^{n} a_i \Leftrightarrow 37 - 27$ )

وطالما أنَّ $10 < 14$ ( مجموعَ المعاملات التي أكبرُ من $a_4$ والتي أمثالُها واحد $S < a_4$)

ومنه يكون $x_4 = 0$

ومنه أصبح لدينا $2x_1 + 3x_2 + 7x_3 = 10$ و $7 < 10$ لذلك $x_3 = 1$ وأن $2 + 3 < 7$

لذلك يكون $2x_1 + 3x_2 = 3$ وضوحاً يكون $x_2 = 1$ و يكون $x_1 = 0$ وبالتالي الحلُّ يكون

3+7+27=37

لحل مسألةِ Knapsack نستخدمُ الخوارزمية التالية :

لتكن لدينا المعادلةُ $a_1x_1 + a_2x_2 + \cdots + a_nx_n = S$ حيث $a_1, a_2, \dots, a_n$ متتاليةً متزايدةً من الأعدادِ الصحيحةِ الموجبةِ ، والمطلوب إيجادُ قيمِ $x_1, x_2, \dots, x_n$ والّتي تأخذُ القيمَ 0 أو 1

فمن أجل $S$ عدد مُعطى ، يمكننا إيجادُ قيمةِ $x_n$ من خلال العلاقة

$$x_n = \begin{cases} 1 & if \quad S \geq a_n \\ 0 & if \quad S < a_n \end{cases}$$

ومن ثم نقومُ بإيجادِ $x_{n-1}, x_{n-2}, x_{n-3}, \dots, x_1$ باستخدامِ العلاقةِ

$$x_j = \begin{cases} 1 & if \quad S - \sum_{i=j+1}^{n} x_i a_i \geq a_n \\ 0 & if \quad S - \sum_{i=j+1}^{n} x_i a_i < a_n \end{cases}$$

لأجل $j = n-1, n-2, \dots, 1$

## (4−1−6) نظام التشفير باستخدام متتالية متزايدة: [16]

قدَّمَ Helman-Merkle ( 1978) أشهرَ أنظمةِ التشفيرِ التي اعتمدت على مسألةِ حقيبة السارق (الظهر) ، بمتجهِ معاملاتٍ متزايدٍ $a = (a_1, a_2, \dots, a_n)$ وبنظامِ العدِّ الثنائي $\{0,1\}$ ، ويتلخصُ هذا النظامُ وِفْقَ الآتي :

كلُّ مستخدمٍ يقومُ باختيارِ متتاليةٍ متزايدةٍ من الأعداد الصحيحة الموجبة ، بطولٍ محددٍ وليكن هذا الطولُ N أي $a_1, a_2, \dots, a_N$ ، ولنأخذ m كمقاسٍ يحقق $m > 2a_N$ ونضربُ $a_i$ بـــ $w$ حيث $(w, m) = 1$ لنحصلَ على المتتالية $b_1, b_2, \dots, b_N$ أي :

$$b_i \equiv wa_i (mod\ m) \qquad \text{حيث} \qquad 0 < b_j < m \tag{1}$$

وعندما يريدُ شخصٌ ما أن يرسلَ رسالة $P$ إلى اشخص آخر ، أولاً تتحولُ الرسالةُ إلى سلسلةٍ من الأرقام 1,0 (النظامَ الثنائي) المكافئ للحروف في الجدول التالي :

| الحرف | النظام الثنائي | الحرف | النظام الثنائي | الحرف | النظام الثنائي |
|---|---|---|---|---|---|
| A | 00000 | J | 01001 | S | 10010 |
| B | 00001 | K | 01010 | T | 10011 |
| C | 00010 | L | 01011 | U | 10100 |
| D | 00011 | M | 01100 | V | 10101 |
| E | 00100 | N | 01101 | W | 10110 |
| F | 00101 | O | 01110 | X | 10111 |
| G | 00110 | P | 01111 | Y | 11000 |
| H | 00111 | Q | 10000 | Z | 11001 |
| I | 01000 | R | 10001 | | |

وهذه السلسلةُ من الأصفارِ و الواحداتِ تقسم إلى مجموعةِ مرتبات من الطول N

ومن ثم نحسبُ المجموعَ لكلِّ كتلةٍ باستخدام المتتاليةِ $b_1, b_2, \dots, b_N$ على سبيل المثال الكتلةُ

$S = b_1x_1 + b_2x_2 + \cdots + b_Nx_N$ تعطي $x_1, x_2, \dots, x_N$

وأخيراً المجموعُ يتولدُ من كلِّ كتلةٍ من الرسالةِ المشفرة.

إن عمليةَ فكِّ التشفيرِ لنظام تشفيرِ Knapsack تكونُ مسألةً صعبةً دون معرفة $w, m$ فقط يتطلبُ منا تجزئةً لمسألة Knapsack ، عندما تكون $w, m$ معرفةً فإنَّ مسألةَ Knapsack تتحولُ إلى مسألةٍ قابلةٍ للحلِ بسهولةٍ فإذا كان :

$$S = b_1x_1 + b_2x_2 + \cdots + b_Nx_N$$

نوجد المعكوسَ $\overline{w}$ ومن ثم

$$\overline{w}S \equiv (\overline{w}b_1x_1 + \overline{w}b_2x_2 + \cdots + \overline{w}b_Nx_N)(mod\ m)$$

$$\equiv (a_1x_1 + a_2x_2 + \cdots + a_Nx_N)(mod\ m)$$

حيثُ $\overline{w}b_i \equiv a_i(mod\ m)$ وأنَّ معكوسَ $w$ بالمقاسِ m لذلك يكونُ

$$S_0 = a_1x_1 + a_2x_2 + \cdots + a_Nx_N$$

حيثُ $S_0$ أصغرُ باقٍ موجبٍ لـــ $\overline{w}S$ بالمقاس m .

فإذا كانت لدينا $a_1, a_2, \dots, a_n$ متتاليةً متزايدةً عندئذٍ لإيجادِ حلولِ حقيبةِ السارقِ S معلومةً علينا معرفةُ قيمةِ $x_n$ من العلاقة :

$$x_n = \begin{cases} 1 & if \quad a_n \le S \\ 0 & otherwise \end{cases}$$

ومن ثم نجدُ المتحولاتِ $x_1, x_2, \dots, x_{n-1}$ من العلاقة :

$$x_j = \begin{cases} 1 & if \quad a_j < S - \sum_{k=j+1}^{n} a_kx_k \\ 0 & otherwise \end{cases}$$

**مثال3 :** لتكنْ المتتاليةُ المتزايدةُ $(a_1, a_2, a_3, a_4, a_5) = (3,5,9,20,44)$

والتي تتحولُ إلى المتتاليةِ $(b_1, b_2, b_3, b_4, b_5) = (23,68,69,5,11)$ باستخدامِ العلاقةِ

رقم (1) وبفرض أنَّ $m = 89$ وأنَّ $w = 67$ سيكونُ

$b_j \equiv 67a_j (mod\ 89)$ حيث $j = 1,2,3,4,5$ ، ولحلِ مسألة Knapsack

$$23x_1 + 68x_2 + 69x_3 + 5x_4 + 11x_5 = 89 \qquad (2)$$

نبحثُ عن معكوسِ العدد 67 بالمقاس 87 فنجدُ أنه يساوي 4 ، ومن ثم نضربُ العلاقةَ رقم (2) به

ثم بأخذ المقاسِ للطرفين 89 نحصلُ على التطابق

$$3x_1 + 5x_2 + 9x_3 + 20x_4 + 44x_5 \equiv 336 \equiv 69\ (mod\ 89)$$

بما أنَّ $3 + 5 + 9 + 20 + 44 < 89$ يمكنُ استنتاجُ أنَّ للمعادلة

$$23x_1 + 68x_2 + 69x_3 + 5x_4 + 11x_5 = 84$$

حلُّ هذه المسألة هو $x_2 = x_4 = x_5 = 1$ وأن $x_1 = x_3 = 0$ لذلكَ يكونُ حلُّ مسألةِ

Knapsack الأصليةِ هو $68 + 5 + 11 = 84$

وسوفَ نوضِّحَ عمليةِ التشفير وفكهِ من خلالِ المثالِ الآتي:

**مثال4 :** باستخدام نظامِ التشفيرِ الذي يعتمد على متجه حقيبة السارق (Knapsack ) ، والذي

معاملاتهُ متتاليةُ الأعدادِ المتزايدةِ التالية :

لتكن المتتاليةُ المتزايدةُ

$a = (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10})$

$= (2,11,14,29,58,119,241,480,959,1917)$

شفَّر الرسالةَ (الردُّ فوراً REPLY IMMEDIATELY) ثم فكَّ التشفيرَ .

الحل: نضعُ m=3837 كمقاسٍ للتشفير بحيث يحققُ : $m > 2a_{10}$

ونأخذُ w=1001 بحيثُ (w , m)=1 ، فتتحولُ المتتاليةُ المتزايدةُ باستخدام التطابق (1) إلى المتتاليةِ التالية

(2002,3337,2503,2170,503,172,3347,855,709,417) (3)

ولنشفيرِ الرسالةِ

(الردُّ فوراً REPLY IMMEDIATELY)

أولاً نحوِّلُ حروفَ الرسالةِ في نظامٍ ثنائيٍّ من خمسةِ منازلَ ، حسْبَ الجدولِ أعلاه ، ومن ثم تجميعُ الكلماتِ في كتلٍ ، كلُّ كتلةٍ طولُها 10 (بحسْبِ طولِ المتتالية)

1000100100 0111101011 1100001000 0110001100

0010000011 0100000000 1001100100 0101111000

نوجدُ مجموعَ كلِّ الكتلِ بإضافةِ الحدودِ المناسبةِ من المتتالية (3) (أَيْ نجمعُ كلَّ رقمٍ مقابلٍ للعدد 1) وهذا يعطينا المجاميعَ التاليةَ:

3360 12986 8686 10042 3629 3337 5530 9729

على سبيل المثال المجموعُ الأول 3360 حصلنا عليه بإضافة 855+503+2002 ، وهي الأرقامُ المقابلةُ للواحداتِ في الكتلة الأولى.

لفكِّ التشفيرِ نوجدُ أصغرَ باقٍ موجبٍ بالمقاس 3837 وهو 23 لكلِّ مجموعٍ ، وذلك لأنَّ 23 معكوسُ 1001 بالمقاس 3837 ومن ثم نحلُّ مسألةَ Knapsack المقابلةِ للمتتاليةِ المتزايدةِ الأصلية (2,11,14,29,58,119,241,480,959,1917)

على سبيلِ المثال لفكِّ التشفيرِ لأولِّ كتلةٍ فإننا نجد :

$$3360 \times 23 \equiv 540 (mod\ 3837)$$

ومن ثم نلاحظُ أنَّ 2+58+480=540 وهذا يدلُّ بأنَّ الكتلةَ الأولى من النص المشفَّرِ هي 1000100100

لتوضيح الكتلة الثانية أيضاً

$$12986 \times 23 \equiv 3229(mod\ 3837)$$

3229=1917+959+241+58+29+14+11 وهي تكافئُ 0111101011

والمتتاليةُ المتزايدةُ في متجهِ حقيبة السارق ليستِ الطريقَ الوحيد البسيط لحلِّها ، فيمكنُ حلُّ مسألةِ حقيبةِ السارق بالاعتمادِ على المتجه المتعامد

**(3-1-4) تعريف : [4]** نقولُ عن متجهِ حقيبةِ السارقِ $a = (a_1, a_2, \dots, a_n)$ إنَّه متجهٌ متعامدٌ إذا وجدت أعدادَ $m_1, m_2, \dots, m_n$ أوليةً مثنى مثنى تحقق :

(a $a_i \equiv 0\ (mod\ m_j)$ من أجل كلِّ $i \neq j$

(b $a_i \not\equiv 0\ (mod\ m_i)$ من أجل كلِّ $i$ حيث $i = 1,2, \dots, n$

مثال5 : لدينا المتجهُ $a = (a_1, a_2, a_3, a_4, a_5) = (210,330,462,770,1155)$

نلاحظ أنه يحققُ شروطَ التعريفِ السابقِ وبالتالي فهو متجه متعامد .

ولبناء أيِّ متجهٍ متعامدٍ يتمُّ ذلك باختيارِ $m_1, m_2, \dots, m_n$ أعداداً أوليةً مثنى مثنى ولنضع

$$m = m_1 . m_2 . \dots . m_n$$

ثم نشكِّلُ الأعدادَ $a_i = \frac{m}{m_i}$ لأجل كل $i = 1, .., n$ عندئذٍ نحصلُ على المتجه

$a = (a_1, a_2, \dots, a_n)$ وهو متجهٌ متعامدٌ ويحققُ الشرطين $a$ ,$b$ من التعريف السابق

**(4-1-4) مبرهنة [3]:** ليكن $a = (a_1, a_2, \dots, a_n)$ متجهاً متعامداً ،عندئذٍ مسألةُ حقيبةِ السارق بالنسبة للمتجه $a$ تُحلُ في النظام الثنائي ، و بالارتباط مع الوقت .

للبرهان انظر المرجع [3]

### (4–1–5) نظام التشفير باستخدام المتجه المتعامد:[4]

الأنظمةَ التي اعتمدت على مسألة حقيبة السارق باستخدام متجه معاملات متعامد ومتحولات تأخذ قيمها من المجموعة $x_i \in \{0,1\}$ (النظام الثنائي ) ، تشابهٌ لحدٍّ كبيرٍ لنظامِ Helman-Merkle ، إنما اختلافٌ في عملية فكِّ التشفير ، والتي تعتمدُ على حل مسألةِ حقيبةِ السارق من أجل متجهِ متعامدٍ ، وباستخدام الصيغة :

$$\text{لأجل } i = 1,2,\dots,n \quad x_n = \begin{cases} 0 & S \equiv 0\ (mod\ m_i) \\ 1 & S \not\equiv 0\ (mod\ m_i) \end{cases}$$

**(4–1–6) تعريف: [3]** لتكن $a_1, a_2, \dots, a_n$ أعداداً طبيعيةً ، يُعرف $p = a_1^{x_1} a_2^{x_2} \dots a_n^{x_n}$ بحقيبةِ السارقِ الضربيةِ حيث $x_i \in \{0\ ,1\}$ ومن أجل المجموعةِ $a_1, a_2, \dots, a_n$ أو مجموعاتٍ جزئيةٍ منها .

**وبعد ان قمنا بالدراسة المرجعية لمسألة حقيبة السارق سنورد النتائج التي حصلنا عليها :**

### (4–2) نظام التشفير SY :

إنَّ حلَّ معادلةِ ديوفانتس الخطية $a_1x_1 + a_2x_2 + \dots + a_nx_n = S$ حيث $a_i\ ,S$ أعدادٌ صحيحةٌ صعبةٌ نوعاً ما بشكلها العام ، لذلك وضَع الرياضيون بعض الشروط الخاصةِ لتُحل بطرقٍ أسهلَ كما رأينا سابقاً ، وسنقومُ بوضع شروطٍ جديدةٍ على معاملات هذه المعادلة الخطية ، وسنجمعْ هذه الشروطَ ضمن تعريفٍ ندعوه تعريفَ المتجهِ المتعامدِ المضاعفِ ، ومن ثم حلُّ معادلة ديوفانتس الخطيةِ باستخدام هذا المتجه بواسطةِ الصيغِ والعلاقاتِ التي سنوردها من خلال الخوارزمية (4–2–2) ، ومن ثم بناءُ نظامِ التشفير $SY$ جديدٍ ، يعتمدُ على المتجهِ المتعامدِ المضاعف ، وباستخدامِ نظامِ العدِّ الثلاثيِّ .

**(4-2-1 ) تعريف:**

لتكن $m_1, m_2, \dots, m_n$ أعداداً اوليةً ، ولنضع $m = m_1 m_2 \dots m_n$ ولتكن الأعداد $a_i = \frac{m}{mi}$

عندئذٍ ندعو المتجهَ $a = (a_1, a_2, \dots, a_n)$ الذي يحققُ الشروط:

(a $a_i \equiv 0 \ (mod\ m_j)$ من أجل كل $i \neq j$

(b $a_i \not\equiv 0 \ (mod\ m_i)$

(c $a_j > 2 \sum_{i=1}^{j-1} a_i$

بالمتجه **المتعامد المضاعف** وذلك لأجل كل $i, j = 1,2, \dots, n$

**(4-2-2 ) خوارزمية حلِّ معادلة ديوفانتس الخطية بمعاملات المتجه المتعامد المضاعف وبنظام العد الثلاثي :**

تَهدفُ هذه الخوارزميةُ إلى حساب قيمِ المتحولات$( x_1, x_2, \dots, x_n)$ ، وبالتالي حلُّ كلِّ معادلةِ ديوفانتس خطيةٌ $\sum_{i=1}^{n} a_i x_i = S$ بمعاملاتِ متجهٍ متعامدٍ مضاعفٍ، الموضح بالتعريف (4-2-1) وذلك ضمن نظام العد الثلاثي أي للمتحولاتِ $(x_1, x_2, \dots, x_n)$ حلول ضمن المجموعةِ

$x_i \in \{0,1,2\}$

**<u>بنيةُ الخوارزميةِ :</u>** من أجلِ $a = (a_1, a_2, \dots, a_n)$ متجهٌ متعامدٌ مضاعفٌ يحقق التعريف (4-2-1) وبالتالي يوجد $m_1, m_2, \dots, m_n$ من الأعداد الاولية المختلفةِ لحل المعادلة

$\sum_{i=1}^{n} a_i x_i = S$

نبدأُ بحسابِ المتغير $x_n$ من الصيغة :

$$x_n = \begin{cases} 0 & S \equiv 0 \ (mod\ m_i) \quad and \quad S < 2a_n \\ 1 & S \not\equiv 0 \ (mod\ m_i) \quad and \quad S < 2a_n \\ 2 & \qquad\qquad\qquad\quad S \geq 2a_n \end{cases}$$

وبعد الحصولِ على قيمة $x_n$ نقومُ بحساب المجموع $F = S - \sum_{i=j+1}^{n} a_i \, x_i$

ثم لنحسب بعدها المتحولاتِ $x_1, x_2, \dots, x_{n-1}$ من الصيغة :

$$x_j = \begin{cases} 0 & S \equiv 0(mod\ m_i) \quad and \quad F < 2a_n \\ 1 & S \not\equiv 0(mod\ m_i) \quad and \quad F < 2a_n \\ 2 & F \geq 2a_n \end{cases}$$

حيث $j = 1,2, \dots n-1$ و $i = 1,2, \dots n$ وبذلك نكونُ قد أوجدنا حلَّ معادلةِ ديوفانتس الخطيةِ $(x_1, x_2, \dots, x_n)$ وفْقَ هذه الخوارزميةِ ، ولأجلِ كلِّ متجهٍ متعامدٍ مضاعف.

## بنية النظام *SY*:

من الواضحِ أنه كلما زادت صعوبةُ العلاقاتِ الرياضيةِ وتعقدت ، كان نظامُ التشفير أكثرَ أمناً وسيعتمدُ هذا النظامُ على المتجه المتعامد المضاعفِ باستخدام نظام العد الثلاثي وسنقومُ بشرحهِ وفق النقاط التالية:

## تشفير النص:

1. على المُرْسِلِ كتابةُ حروفِ رسالتِه بما يكافئها من نظام العد الثلاثي ، ثم نختارُ $n$ عدداً أولياً $m_1, m_2, \dots, m_n$ ، عليها نقومُ ببناء المتجهِ المتعامدِ المضاعفِ المحقق لشروط التعريف .
2. كذلك نختار قيمة $M$ ، والتي يجبُ أن تحقق $M > 2\sum_{i=1}^{n} a_i$ ومن ثم نختارُ عدداً مثل $W$ يحقق $GCD(M, W) = 1$ ونحسب $W^{-1}$ (النظير الضربي لـ $W$).
3. نقومُ بتجميعِ الرسالةِ التي هي عبارةٌ عن أرقامٍ من المجموعة $\{0, 1, 2\}$ في مرتباتٍ من الطول $n$ ولتكن إحداها $(x_1, x_2, \dots, x_n)$ .

4. نحسب $b_1 = wa_1(mod\ M)$

$b_2 = wa_2\ (mod\ M)$

$b_3 = wa_3\ (mod\ M)$

حتى نحصلَ على المتجه B والذي يعتبرُ المفتاحَ العام وهو :

$$B = (b_1, b_2, \dots, b_n) = wa_i(mod\ M)$$

5. وبالتالي نقومُ بتشفيرِ كلِّ مرتبهٍ من خلال العملية $C = \sum_{i=1}^{n} b_i x_i$

وبذلك نحصلُ على كتل النصِّ المشفر $C$.

**<u>فكُّ النصِّ المشفَّرِ :</u>**

1. للرجوع للنص الاصلي وفكِّ تشفيرهِ نقومُ بحساب $S = W^{-1}C(\ mod\ M)$ ، لنحصلَ على المتجه $S = (S_1, S_2, \dots, S_n)$ ويعتَبَرْ الطرفُ الثاني في معادلة ديوفانتس ولحساب متحولاتها $x_i$ نبدأُ أولاً بحسابِ المتحول $x_n$ من الصيغة :

$$x_n = \begin{cases} 0 & S \equiv 0\ (mod\ m_i) \quad and \quad S < 2a_n \\ 1 & S \not\equiv 0\ (mod\ m_i) \quad and \quad S < 2a_n \\ 2 & \qquad\qquad\qquad\quad S \geq 2a_n \end{cases}$$

وبعدَ الحصولِ على قيمةِ $x_n$ نقومُ بحساب المجموع $F = S - \sum_{i=j+1}^{n} a_i\, x_i$

ثم نحسبُ بعدها المتحولاتِ $x_1, x_2, \dots, x_{n-1}$ من الصيغة :

$$x_j = \begin{cases} 0 & S \equiv 0\ (mod\ m_i) \quad and \quad F < 2a_j \\ 1 & S \not\equiv 0 (mod\ m_i) \quad and \quad F < 2a_j \\ 2 & \qquad\qquad\qquad\quad F \geq 2a_j \end{cases}$$

$$i = 1,2, \dots n \quad , \quad j = 1,2, \dots n-1$$

2. أخيراً ننوه إلى أنَّ القيَم $M, W, W^{-1}$ والمتجهَ المتعامدَ المضاعفَ تعتبرُ مفتاحاً خاصاً يجبُ الحفاظُ على سريَّتهِ وإعلانُ المتجه $B$ (المفتاحُ العام ) ، وسنوضح بالمثال التالي.

**مثال تطبيقي :**

سنقومُ بشرحِ النظام $SY$ من خلال تشفيرِ عبارة (HELLO MOM) ، سنكتب الرسالةَ بحروفٍ متقطعةٍ ونضعُ مقابلَ كلِّ حرفٍ ترتيبه باللغة الانكليزية ، ومن ثمَّ ما يقابلُ كلَّ حرف بالنظام الثلاثي

| حرف النص الصريح | H | E | L | L | O | M | O | M |
|---|---|---|---|---|---|---|---|---|
| ترتيبه الحرف | 7 | 4 | 11 | 11 | 14 | 12 | 14 | 12 |
| ما يقابله بالنظام الثلاثي | 0021 | 0011 | 0102 | 0102 | 0112 | 0110 | 0112 | 0110 |

نختار أربعةً من الأعدادِ الأولية المختلفةِ ولتكن

$$m_1 = 47\ , m_2 = 23\ , m_3 = 7\ , m_4 = 2$$

وعليها نبني المتجهَ المتعامدَ المضاعفَ والذي يحققُ شروطَ التعريفِ فينتجُ :

$$a = (a_1, a_2, a_3\ , a_4) = (322,658,2162,7567)$$

$$\sum_{i=1}^{4} a_i = 10709 \quad \text{لكون}$$

$$2\sum_{i=1}^{4} a_i = 21418 \quad \text{وأن}$$

نختارُ عدداً طبيعياً $2\sum_{i=1}^{4} a_i > M = 25025$

ونختارُ عدداً طبيعياً آخرَ $W = 12513$ يحقق $gcd(12513\ ,25025) = 1$

ونحسبُ $w^{-1} = 2$ ، فنجدُ المفتاح العام من التطابق $b_i = Wa_i\ (mod M)$

$$b_1 = 12513 * 322\ (mod\ 25025) = 161$$

$$b_2 = 12513 * 658(\ mod\ 25025) = 329$$

$$b_3 = 12513 * 2162\ (mod\ 25025) = 1081$$

$$b_4 = 12513 * 7567\ (mod\ 25025) = 16296$$

فنحصلُ على المتجهِ $B = (161, 329, 1081, 16296)$

وبعد أن كُتبتْ حروفُ الرســـالةِ وفق النظام الثلاثي ، نقومُ بتجميعها بمرتباتِ من الطول $n = 4$ لنحصلَ على :

$$X_1 = (0,0,2,1)$$
$$X_2 = (0,0,1,1)$$
$$X_3 = (0,1,0,2)$$
$$X_4 = (0,1,0,2)$$
$$X_5 = (0,1,1,2)$$
$$X_6 = (0,1,1,0)$$
$$X_7 = (0,1,1,2)$$
$$X_8 = (0,1,1,0)$$

وعليه تكونُ الرسالةُ المشفرةُ:

$$C = \begin{bmatrix} 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 1 & 0 & 2 \\ 0 & 1 & 1 & 2 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 \\ 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 161 \\ 329 \\ 1081 \\ 16296 \end{bmatrix}$$

$$C = [18458 \quad 17377 \quad 32921 \quad 32921 \quad 34002 \quad 1410 \quad 34002 \quad 17377]$$

أمّا عمليةُ فكِّ التشفيرِ علينا حساب $S \equiv W^{-1}.C(\ mod\ M)$ أي :

$$S \equiv \begin{bmatrix} 18458 \times 2 \\ 17377 \times 2 \\ 32921 \times 2 \\ 32921 \times 2 \\ 34002 \times 2 \\ 1410 \times 2 \\ 34002 \times 2 \\ 17377 \times 2 \end{bmatrix} (mod\ 25025) \equiv \begin{bmatrix} 11891 \\ 9729 \\ 15792 \\ 15792 \\ 17954 \\ 2820 \\ 17954 \\ 9729 \end{bmatrix}$$

وبالتالي أصبحَ لدينا $S = (S_1, S_2, S_3\ , S_4, S_5, S_6, S_7, S_8)$

وهي الطرفُ الثاني لمعادلة ديوفانتس بالمتجهِ المتعامدِ المضاعفِ ، ولْنَقُمْ بحسابِ

$$X_1, X_2, X_3\ , X_4, X_5, X_6, X_7, X_8$$

ولنبدأ بإيجادِ مركبات $X_1$ ، ومن أجلِ ذلك علينا حلُّ المعادلةِ:

$$322x_1 + 658x_2 + 2162x_3 + 7567x_4 = 11891 = S_1$$

$$S_1 = 11891 < 2a_4 = 15134 \quad and \quad 11891 \not\equiv 0(\ mod\ 2)$$

$$\Longrightarrow\ x_{14}\ = 1$$

$$F_1 = 11891 - 7567 = 4324 = 2a_3$$

$$\Longrightarrow\ x_{13}\ = 2$$

$$F_1 = 11891 - (7567 + 4324) = 0 < 2a_3 = 1316$$

$$and \quad 11891 \equiv 0(\ mod\ 23)$$

$$\Longrightarrow\ x_{12}\ = 0$$

$$0 < 2a_1 = 644 \qquad and \qquad 11891 \equiv 0\ (mod\ 47)$$

$$\Longrightarrow\ x_{11}\ = 0$$

وعليه يكونُ المتجهُ $X_1 = (0, 0, 2\ , 1)$

لإيجادِ مركباتِ $X_2$ ، ومن أجلِ ذلك علينا حلُّ المعادلةِ:

$$322x_1 + 658x_2 + 2162x_3 + 7567x_4 = 9729 = S_2$$

$$S_2 = 9729 < 2a_4 = 15134 \quad and \quad 9279 \not\equiv\ 0\ \ (\ mod\ 2)$$

$$\Longrightarrow\ x_{24}\ = 1$$

$$9729 - 7567 = 2162 < 2a_3 = 4324 \ \ and \ \ 9279 \not\equiv 0(mod\ 23)$$

$$\Longrightarrow \ x_{23} = 1$$

$$2162 - 2162 = 0 < 2a_2 = 1316 \ \ and \ \ 9279 \equiv 0(\ mod\ 7)$$

$$\Longrightarrow \ x_{22} = 0$$

$$2162 - 2162 = 0 < 2a_1 = 644 \ \ and \ \ 9279 \equiv 0\ (\ mod\ 47)$$

$$\Longrightarrow \ x_{21} = 0$$

وعليه يكونُ المتجهُ $X_2 = (0, 0, 1\ , 1)$

و لإيجادِ مركباتِ $X_3$ ، ومن أجل ذلك علينا حلُّ المعادلة:

$$322x_1 + 658x_2 + 2162x_3 + 7567x_4 = 15792 = S_3$$

$$S_3 > 2a_4 \ \Longrightarrow \ \ x_{34} = 2$$

$$15792 - 15134 = 658 < 2a_3 = 4324$$

$$and \ \ 15792 \ \equiv 0(mod\ 7)$$

$$\Longrightarrow x_{33} = 0$$

$$658 < 2a_2 and \ \ 15792 \not\equiv 0 \ \ (mod\ 23)$$

$$\Longrightarrow \ \ x_{32} = 1$$

$$658 - 658 = 0 < 2a_1 and \ \ 15792 \equiv 0(\ mod\ 47)$$

$$\Longrightarrow \ \ x_{31} = 0$$

وعليه يكونُ المتجهُ $X_3 = (0, 1, 0\ , 2)$

لإيجاد مركباتِ $X_4$ ، نلاحظ أنَّ $S_3 = S_4$ ، وعليه يكونُ $X_3 = (0, 1, 0\ , 2) = X_4$

لإيجادِ مركباتِ $X_5$ ، ومن أجلِ ذلك علينا حلُّ المعادلةِ:

$$322x_1 + 658x_2 + 2162x_3 + 7567x_4 = 17954 = S_5$$

$$S_5 > 2a_4 \quad \Longrightarrow \quad x_{54} = 2$$

$$17954 - 15134 = 2820 < 2a_3 = 4324$$

$$and \ \ 17954 \not\equiv 0 \ (mod\ 7)$$

$$\Longrightarrow \ x_{53} = 1$$

$$2820 - 2162 = 658 < 2a_2 and \ \ 17954 \not\equiv 0 \ \ (mod\ 23)$$

$$\Longrightarrow \ x_{52} = 1$$

$$658 - 658 = 0 < 2a_1 and \ \ 17954 \equiv 0 \ (mod\ 47)$$

$$\Longrightarrow \ x_{51} = 0$$

وعليه يكونُ المتجهُ $X_5 = (0, 1, 1, 2)$

و لإيجادِ مركباتِ $X_6$ ، ومن أجلِ ذلك علينا حلُّ المعادلةِ:

$$322x_1 + 658x_2 + 2162x_3 + 7567x_4 = 2820 = S_6$$

$$S_6 = 2820 < 2a_4 = 15134 \quad and \quad 2820 \equiv 0 \ (mod\ 2)$$

$$\Longrightarrow \ x_{64} = 0$$

$$S_6 = 2820 < 2a_3 and\ 2820 \not\equiv 0 (mod\ 7\ )$$

$$\Longrightarrow \ x_{63} = 1$$

$$2820 - 2162 = 658 < 2a_3 and \ \ 2820 \ \not\equiv 0 (mod\ 23)$$

$$\Longrightarrow \ x_{62} = 1$$

$$658 - 658 = 0 < 2a_1 and \ \ 2820 \equiv 0 \ \ (mod\ 47)$$

$$\Longrightarrow \quad x_{61} = 0$$

وعليه يكونُ المتجهُ $X_6 = (0, 1, 1, 0)$

و لإيجاد مركباتِ $X_7$ ، نلاحظ أنَّ $S_5 = S_7$ وعليه يكونُ

$$X_5 = (0, 1, 1, 2) = X_7$$

و لإيجاد مركباتِ $X_8$ ، نلاحظ أنَّ $S_2 = S_8$ وعليه يكونُ

$$X_2 = (0, 0, 1, 1) = X_8$$

و بذلك نكونُ قد أوجْدنا المتجهاتِ $X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8$ ، وهي التي تعبرُ عن النصِ الصريح (HELLO MOM).

**<u>النتائج التي حصلنا عليها :</u>**

1. تعريفُ متجهٍ جديدٍ لمعادلة ديوفانتس الخطية ، وهو المتجهُ المتعامدُ المضاعفُ ، و يضمُّ ثلاثةَ شروطٍ تضمن التعامد والتزايد بالضعف .
2. وضْعُ خوارزميةٍ تحلُّ كلَّ معادلة ديوفانتس الخطية ،وبمعاملات المتجهِ المتعامدِ المضاعفِ.
3. بناءُ نظامِ التشفيرِ ***SY*** ، والذي يستخدمُ كلاً من الخوارزميةِ ، والمتجهِ المتعامدِ المضاعفِ باستخدام نظامِ العد الثلاثي ، ومن ثمَ طرْحُ مثالٍ تطبيقيٍّ عن هذا النظام .
4. تم نشرُ بحث علمي بالنتائجِ السابقة .

## المراجع العلمية :


**[1].** AJAEB.E.F,(2014)- **Cryptography by Mean of Liner Algebra and Number theory.** Gazimagusa**,** North Cyprus.

**[2].** AARON.H.K,(2009)-**Applications of Continued Fraction in Cryptography and Diophantine Equations.** School of Mathematical Sciences.

**[3].** BARAKAT.M,HANK.T,(2012)- **Cryptography Lecture notes version .**April ,Kaiserslautern, Germany.

**[4].** CADING.D,PEI.A.S (1996 )**Chinas Remainder theorem Application in Computing, Coding, Cryptography ,**World Scientific.

**[5].** COHEN.H,(2006)- **Number theory tools and Diophantine Equations.**

**[6].** CRANDALL.R,POMERANCE.C,(2001)- **Prime number A computational Perspective .** spring.

**[7].** HARRY.Y,(2011)- **The Key Exchange Cryptosystems used with Higher order Diophantine Equation.** Journal of network security vol.3.

**[8].** HELLMAN.M.E,(1979)-**the mathematics of public–Key Cryptography .**scientific American.

**[9].** HOFFSTEN.J and PIPHER.J,(2008)- **An Introduction to Mathematical Cryptography.** spring.

**[10].** KOBLITZ.N,(1987)- **A coarse in Number theory and Cryptography.** Spring, Verlag.

**[11].** KOBLITZ.N,(2007)- **the uneasy relationship between mathematics and Cryptography.** Notices Amer.

**[12].** LAGARIA.S.J.C,(1984)- **Knapsack Public Key Cryptosystems and Diophantine Approximation.** Spring, Verlag.

**[13].** MAYMIN.A,(2008)- **the application of prime number to RSA encryption.** Boston university, summer.

**[14].** MICHAEL.J.W,(1990)- **Cryptanalysis of short RSA Secret Exponents** IEEE Trans Canada pp 552-559**.**

**[15].** Richard .A,(2002)- **RSA and Public Key Cryptography**. Chapman and Hall ,CRC Press.

**[16].** ROSEN.H,( 1983)-**Elementary number theory and it is applications .** ADDISON-WESLEY, pp 450-485.

**[17].** SILVERMAN.J.H,FRINDLY.A ,(2006)- **Introduction to number theory.** prentice Hall,3rd edition.

**[18].** TALBOT.J and WELSH.P , (2006)- **Complexity and Cryptography : An Introduction .**Cambridge University press.

**[19].** Various the Prime Page ,www.utm.edu/researen/primes/selecte information about primes.

**[20].** WASHINTON.L.C,(2003)- **Number theory and Cryptography**.CRC press ,Boca Raton.

[21] د. دعد الحسيني ، د. بشير قابيل (2006 ) –نظرية الأعداد ، منشورات جامعة دمشق .

[22] د. حمزة حاكمي ، (2009) – بنى جبرية 1 ، منشورات جامعة دمشق .

[23] د. يحيى قطيش ،مروان الرفاعي (2016) تطبيقات البواقي التكعيبية ، منشورات جامعة البعث.

**التوصيات والمقترحات:**

1. دراسةُ معادلةِ ديوفانتس الخطية بالنسبة لإساسٍ أوليٍّ آخر عدا الرقم 3 ومحاولةُ التعميم.
2. محاولةُ استخدامِ معادلةِ درجةٍ ثانيةٍ ، أو أيَّ معادلة غير خطيَّةٍ كمفتاحٍ عامٍّ للتشفير ، بدلاً من المعادلةِ الخطية .
3. برمجةُ النظامِ SY ، ومحاولةُ تطبيقهِ .

# سرد بعض المصطلحات

| انكليزي | عربي |
|---|---|
| Addition Modulo n | مجموع بالمقاس n |
| Alpha pets | أبجدية |
| Algorithm | خوارزمية |
| Block ciphers | تشفير بالكتل |
| Cryptography | تشفير |
| Cipher text | نص المشفر |
| Continued fraction | كسور المستمرة |
| Cryptosystem | نظام تشفير |
| CRT | نظرية البواقي الصينية |
| Data base | قاعدة البيانات |
| Deciphering transformation | تحويل فك التشفير |
| Discrete log | لوغاريتم المميز |
| Diophantine equations | معادلة ديوفانتس |
| Enciphering transformation | تحويل التشفير |
| Exponentiation ciphers | تشفير الآسي |
| Knapsack | حقيبة السارق(الظهر) |
| Modular arithmetic | حساب القياسي |
| One way function | تابع الاتجاه الواحد |
| Orthogonal vector | متجه متعامد |
| Public key | مفتاح العام |
| Plain text | نص الصريح |
| Signature | توقيع |
| Squaring modulo n | تربيع بالمقاسn |
| Secret sharing | مشاركة السرية |
| Short secret Exponents | قيمة الأسية الصغيرة |
| Sequence increasing | متتالية متزايدة |
| Threshold schem | مخطط العتبة |