خوارزمية تشفير متناظرة بمفتاح ثنائي, باستخدام فيثاغوريّات مولّدة بعدد فردي

الملخص	أسماء الباحثين
يستند هذا البحث إلى بناء ثلاثيّات, رباعيات, خماسيّات, ... فيثاغوريّة, انطلاقاً من عدد فردي λ ولتكن هذه الفيثاغوريّات: $(x_0,x_1,x_2),(x_3,x_4,x_5,x_6),(x_7,x_8,x_9,x_{10},,x_{11}),\dots$ ومن ثمّ تطوير خوارزميّة **Luma and Raufi** للتشفير بالاعتماد على الفيثاغوريّات المنشأة وبمفتاح تشفير ثنائي $\boldsymbol{K(\lambda,m)}$ حيث λ عدد صحيح فردي و m عدد طبيعي لا يساوي الصفر.	نجوى أحمد نجوم ***تاريخ النشر: 2023/11/18*** **الكلمات المفتاحيّة :** ثلاثيّة فيثاغوريّة – رباعيّة فيثاغوريّة . خماسيّة فيثاغوريّة– تشفير – فك التشفير

1. المقدّمة:

في الوقت الذي يعتبر التشفير علماً قائماً بحد ذاته, إلّا أنّه يعتبر فنّاً يظهر روعة الرياضيّات, ولا سيّما نظريّة الأعداد. ربما لم يكن الاهتمام في هذه الأوراق هو التشفير بحد ذاته, وإنّما قضايا في نظريّة الأعداد وإظهار أهميّتها من خلال التشفير.
التّشفير هو تحويل البيانات من شكلها القابل للفهم, إلى شكل آخر لا يمكن إلا لمن يمتلك المفتاح والخوارزميّة بقراءتها من خلال فك التشفير.

يُعد علم التشفير من أقدم العلوم المستخدمة, فقد استخدم منذ 1900 سنة قبل الميلاد تقريباً لفك رموز الحضارة الهيروغليفية في مصر [1] وقد استخدم التشفير بشكل كبير لنقل المعلومات المشفّرة لحماية الرسائل السريّة وخصوصاً حماية الأسرار العسكريّة أثناء الحروب.

في العام 2014 قام كل من Luma and Raufi [1] بإيجاد طريقتين لتوليد ثلاثيّات فيثاغوريّة بوسيطين طبيعيّين p,q بحيث يكون $p>q$ وقاما باستخدام نتائجهما بإيجاد طريقة للتشفير.

استخدم الباحثان (العرنوس – شراباتي 2023) [5] نتائج Luma and Raufi في إيجاد صيغتين جديدتين لتوليد رباعيّات فيثاغوريّة وقاما باستخدام العلاقات في تشفير نص محرفي.
ثم قام الباحث (العرنوس 2023) [6] بتطبيق الخوارزميّة باستخدام خماسيّة فيثاغوريّة مولّدة من ثلاثيّتين فيثاغوريّتين.
عمدنا في هذه الأوراق إلى بناء ثلاثيّات, رباعيات, خماسيّات, ... فيثاغوريّة, انطلاقاً من عدد فردي λ, ومن ثمّ تطوير خوارزميّة Luma and Raufi للتشفير بالاعتماد على الفيثاغوريّات المنشأة وبمفتاح تشفير ثنائي $\boldsymbol{K(\lambda,m)}$حيث λ عدد صحيح فردي و m عدد طبيعي لا يساوي الصفر.

2. هدف البحث:

يهدف البحث إلى بناء ثلاثيّات, رباعيات, خماسيّات, ... فيثاغوريّة, انطلاقاً من عدد فردي λ, واستخدام النتائج في تشفير نص محرفي, من خلال بناء خوارزميّة للتشفير وآليّة لفك التشفير.

3. النتائج والمناقشة:

أوّلاً: بناء فيثاغوريّات انطلاقاً من عدد فردي

تعريف1: [3]

تسمّى ثلاثيّة فيثاغوريّة كل ثلاثيّة مرتّبة (x,y,z) عناصرها من وتحقّق:

$$x^2+y^2=z^2 \qquad (1)$$

وكمثال على ذلك: الثّلاثيّة $(3,4,5)$.

وقد تمّ إيجاد طرائق عدّة لتوليد ثلاثيّات فيثاغوريّة من أهمّها صيغة إقليدس, وهي الصيغة الأساسيّة لثلاثيّات فيثاغوريّة, وتنص على أنّه من أجل زوج اختياري من الأعداد الصحيحة m,n حيث $m>n$ والذي أحدهما زوجي والأخر فردي, فإنّ الثّلاثيّة الآتية تكون فيثاغوريّة:

$$\left(m^2-n^2,\ 2mn,\ m^2+n^2\right) \qquad (2)$$

تمهيديّة: [7]

ليكن $\lambda\in\mathbb{Z}$ وبحيث λ عددٌ فرديّ عندئذٍ تكون الثّلاثيّة الآتية فيثاغوريّة:

$$\left(\lambda,\ \frac{\lambda^2-1}{2},\ \frac{\lambda^2+1}{2}\right) \qquad (3)$$

تعريف 2:

نسمّي رباعيّة فيثاغوريّة كل رباعيّة مرتّبة (x,y,z,w) عناصرها من $\mathbb{Z}$ وتحقّق:

$$x^2+y^2+z^2=w^2 \qquad (4)$$

تعريف 3:

نسمّي خماسيّة فيثاغوريّة كل خماسيّة مرتّبة (x,y,z,w,t) عناصرها من $\mathbb{Z}$ وتحقّق:

$$x^2+y^2+z^2+w^2=t^2 \qquad (5)$$

تمهيدية 2:

ليكن $\lambda\in\mathbb{Z}$ عدداً فرديّاً, والثّلاثيّة المولّدة بالتمهيديّة 1 هي:

$$\left(\lambda,\ \frac{\lambda^2-1}{2},\ \frac{\lambda^2+1}{2}\right)$$

عندئذٍ فإنّ الثالث الفيثاغوري هو فردي.

الإثبات:

بما أنّ λ فرديّ, عندئذٍ يوجد $n\in\mathbb{Z}$ بحيث: $\lambda=2n+1$, وبالتالي يكون:

$$\frac{\lambda^2+1}{2}=\frac{(2n+1)^2+1}{2}=\frac{4n^2+4n+2}{2}=2n^2+2n+1$$

واضح إنّ: $\frac{\lambda^2+1}{2}$ فرديّ.

مبرهنة 1 :

ليكن $\lambda\in\mathbb{Z}$ عدداً فرديّاً, عندئذٍ الرّباعيّة الآتية هي رباعيّة فيثاغوريّة:

$$\left(\lambda,\ \frac{\lambda^2-1}{2},\ \frac{\lambda^4+2\lambda^2-3}{8},\frac{\lambda^4+2\lambda^2+5}{8}\right)$$

والرّابع الفيثاغوريّ, هو عددٌ فرديّ.

الإثبات:

ليكن $\lambda\in\mathbb{Z}$ عدداً فرديّاً, عندئذٍ الثّلاثيّة الآتية فيثاغوريّة:

$$\left(\lambda,\ \frac{\lambda^2-1}{2},\ \frac{\lambda^2+1}{2}\right)$$

أي:

$$(\lambda)^2+\left(\frac{\lambda^2-1}{2}\right)^2=\left(\frac{\lambda^2+1}{2}\right)^2 \qquad (6)$$

ولأنّ: $\frac{\lambda^2+1}{2}$ فرديّ, فإنّ الثّلاثيّة الآتية فيثاغوريّة:

$$\left(\frac{\lambda^2+1}{2},\ \frac{\left(\frac{\lambda^2+1}{2}\right)^2-1}{2},\ \frac{\left(\frac{\lambda^2+1}{2}\right)^2+1}{2} \right)$$

أي:

$$\left(\frac{\lambda^2+1}{2},\ \frac{\lambda^4+2\lambda^2-3}{8},\ \frac{\lambda^4+2\lambda^2+5}{8} \right)$$

وبالتالي:

$$\left(\frac{\lambda^2+1}{2} \right)^2+\left(\frac{\lambda^4+2\lambda^2-3}{8} \right)^2=\left(\frac{\lambda^4+2\lambda^2+5}{8} \right)^2$$

ومنه:

$$\left(\frac{\lambda^2+1}{2} \right)^2=\left(\frac{\lambda^4+2\lambda^2+5}{8} \right)^2-\left(\frac{\lambda^4+2\lambda^2-3}{8} \right)^2$$

بالتعويض في (6) نجد:

$$(\lambda)^2+\left(\frac{\lambda^2-1}{2} \right)^2=\left(\frac{\lambda^4+2\lambda^2+5}{8} \right)^2-\left(\frac{\lambda^4+2\lambda^2-3}{8} \right)^2$$

وبالتالي:

$$(\lambda)^2+\left(\frac{\lambda^2-1}{2} \right)^2+\left(\frac{\lambda^4+2\lambda^2-3}{8} \right)^2=\left(\frac{\lambda^4+2\lambda^2+5}{8} \right)^2$$

وبهذا يتم المطلوب.

الآن, وحيث إنّ λ فردي, فيوجد $n\in\mathbb{Z}$ بحيث: $\lambda=2n+1$, وبالتالي:

$$\frac{(2n+1)^4+2(2n+1)^2+5}{8}=\frac{16n^4+32n^3+32n^2+16n+8}{8}=$$

$$=2n^4+4n^3+4n^2+2n+1$$

واضح انّ هذا العدد فردي.

مبرهنة 2 :

ليكن $\lambda\in\mathbb{Z}$ عدداً فرديّاً, عندئذٍ الخماسيّة (x,y,z,t,w) هي خماسيّة فيثاغوريّة, حيث:

$$x=\lambda,$$

$$y=\frac{\lambda^2-1}{2},$$

$$z=\frac{\lambda^4+2\lambda^2-3}{8},$$

$$t=\frac{\lambda^8+4\lambda^6+14\lambda^4+20\lambda^2-39}{128},$$

$$w=\frac{\lambda^8+4\lambda^6+14\lambda^4+20\lambda^2+89}{128}$$

و w عددٌ فرديّ.

الإثبات:

يتم بنفس طريقة إثبات المبرهنة 1.

نتيجة 1:

من أجل $\lambda \in \square$, و λ عدد فردي, تم بناء ثلاثية فيثاغوريّة, ورباعيّة فيثاغوريّة, وخماسية فيثاغوريّة, نرمز لها بالرمز:

$$(x_0, x_1, x_2) = \left(\lambda,\ \tfrac{\lambda^2-1}{2},\ \tfrac{\lambda^2+1}{2}\right)$$

$$(x_3, x_4, x_5, x_6) = \left(\lambda,\ \tfrac{\lambda^2-1}{2},\ \tfrac{\lambda^4+2\lambda^2-3}{8},\ \tfrac{\lambda^4+2\lambda^2+5}{8}\right)$$

$$(x_7, x_8, x_9, x_{10}, x_{11}) = \left(\lambda,\ \tfrac{\lambda^2-1}{2},\ \tfrac{\lambda^4+2\lambda^2-3}{8}, x_{10}, x_{11}\right)$$

حيث:

$$x_{10} = \frac{\lambda^8 + 4\lambda^6 + 14\lambda^4 + 20\lambda^2 - 39}{128},$$

$$x_{11} = \frac{\lambda^8 + 4\lambda^6 + 14\lambda^4 + 20\lambda^2 + 89}{128}$$

ويمكن بالطريقة ذاتها إيجاد سداسية فيثاغوريّة, سباعية فيثاغوريّة, ...

مثال 1:

من أجل $\lambda = 3$ نجد:

الثلاثيّة الفيثاغوريّة: $(3,4,5)$

الرّباعيّة الفيثاغوريّة: $(3,4,12,13)$

الخماسيّة الفيثاغوريّة: $(3,4,12,84,85)$

السداسيّة الفيثاغوريّة: $(3,4,12,84,3612,3613)$

السباعيّة الفيثاغوريّة: $(3,4,12,84,3612,6526884,6526885)$

ويمكن توضيح طريقة البناء من خلال:

الثّلاثيّة	λ	$\frac{\lambda^2-1}{2}$	$\frac{\lambda^2+1}{2}$
$(3,4,5)$	3	4	5
	5	12	13
	13	84	85
	85	3612	3613
	3613	6526884	6526885

الرّباعيّة	λ	$\frac{\lambda^2-1}{2}$	$\frac{\lambda^2+1}{2}$
$(3,4,12,13)$	3	4	5
	5	12	13
	13	84	85
	85	3612	3613
	3613	6526884	6526885

الخماسيّة	λ	$\frac{\lambda^2-1}{2}$	$\frac{\lambda^2+1}{2}$
$(3,4,12,84,85)$	3	4	5
	5	12	13
	13	84	85
	85	3612	3613
	3613	6526884	6526885

السداسيّة	λ	$\frac{\lambda^2-1}{2}$	$\frac{\lambda^2+1}{2}$
$(3,4,12,84,3612,3613)$	3	4	5
	5	12	13
	13	84	85
	85	3612	3613
	3613	6526884	6526885

السباعية	λ	$\frac{\lambda^2-1}{2}$	$\frac{\lambda^2+1}{2}$
$(3,4,12,84,3612,6526884,6526885)$	3	4	5
	5	12	13
	13	84	85
	85	3612	3613
	3613	6526884	6526885

وهكذا ..

ثانياً: تشفير نص بمفتاح ثنائي $K(\lambda,m)$.

تعريف 3: (مفتاح التشفير)

ليكن $\lambda \in \mathbb{N}$ و λ فرديّ, وليكن m عدد طبيعي لا يساوي الصفر, بحيث:

$m=1$ عندما نبني ثلاثيّة, بحسب النتيجة 1.

$m=2$ عندما نبني ثلاثيّة ورباعيّة, بحسب النتيجة 1.

$m=3$ عندما نبني ثلاثيّة ورباعيّة وخماسيّة, بحسب النتيجة 1.

وهكذا ...

نسمّي الثّنائيّة المرتّبة (λ,m) مفتاح تشفير باستخدام فيثاغوريّات مولّدة بعدد فردي.

وكمثال على ذلك:

المفتاح $(3,2)$ يعني أنّ سيتم بناء ثلاثيّة فيثاغوريّة ورباعيّة فيثاغوريّة مولّدة بالعدد الفردي 3.

تعريف 4:

ليكن $\lambda \in \mathbb{N}$ و λ فرديّ, وليكن m عدد طبيعي لا يساوي الصفر, و x_i معرّفة وفق النتيجة 1, لنعرّف المجموعة التي χ_m على النحو:

- من أجل $m=1$ فإنّ: $\chi_1=\{x_0,x_1,x_2\}$ وعدد عناصرها 3.
- من أجل $m=2$ فإنّ: $\chi_2=\{x_0,x_1,x_2,x_3,x_4,x_5,x_6\}$ وعدد عناصرها $3+4=7$.
- من أجل $m=3$ فإنّ: $\chi_3=\{x_0,x_1,\dots,x_{11}\}$ وعدد عناصرها $3+4+5=12$.

نتيجة 2:

ليكن $\lambda \in \mathbb{N}$ و λ فرديّ, وليكن m عدد طبيعي لا يساوي الصفر, عدد عناصر المجموعة χ_m يساوي:

$$3+4+5+\dots+(m+2)=\frac{m}{2}(3+m+2)=\frac{m}{2}(m+5)$$

تعريف 5: (متتالية مفتاح التشفير)

ليكن $\lambda \in \mathbb{N}$ و λ فرديّ, وليكن m عدد طبيعي لا يساوي الصفر, عندئذٍ نعرّف المتتالية $\{k_i\}$ على النّحو الآتي:

$$\begin{aligned} k_i &= x_i \pmod{256} \quad ; \quad i \in \left\{0,1,\dots,\tfrac{m}{2}(m+5)-1\right\} \\ k_i &= k_{i \left(\bmod \frac{m}{2}(m+5)\right)} \quad ; \quad i \in \left\{\tfrac{m}{2}(m+5),\tfrac{m}{2}(m+5)+1,\dots\right\} \end{aligned} \tag{7}$$

حيث x_i معرّفة وفق النتيجة 1.

مثال 2 :

من أجل مفتاح التشفير $(3,2)$ تكون العناصر x_i:

$$x_0=3, x_1=4, x_2=5, x_3=3, x_4=4, x_5=12, x_6=13$$

وتكون متتالية مفتاح التشفير:

$$\{k_i\}=\{\boxed{3,4,5,3,4,12,13},3,4,5,3,4,12,13,...\}$$

تعريف 6: (متتالية النص الواضح) [5]

ليكن M النص الواضح المراد تشفيره, نشكّل المتتالية $\{m_i\}$ التي تنتج عن النص الواضح باستبدال كل محرف بمقابله في جدول ASCII, بحيث يكون m_0 هو المقابل العددي للمحرف الأوّل من النص الواضح في جدول ASCII, و m_1 هو المقابل العددي للمحرف الثاني من النص الواضح, وهكذا ...

تعريف 7: (متتالية النص المشفّر) [5]

ليكن C النص المشفّر المراد توضيحه, نشكّل المتتالية $\{c_i\}$ التي تنتج عن النص المشفّر باستبدال كل محرف بمقابله في جدول ASCII, بحيث يكون c_0 هو المقابل العددي للمحرف الأوّل من النص المشفّر في جدول ASCII, و c_1 هو المقابل العددي للمحرف الثاني من النص الواضح, وهكذا ...

خوارزميّة التشفير باستخدام المفتاح $K(\lambda,m)$

ليكن M النص الواضح المراد تشفيره باستخدام مفتاح التشفير $K(\lambda,m)$ حيث λ عدد صحيح فردي, و m عدد طبيعي لا يساوي الصفر. وليكن n عدد محارفه.

لتشفير النص M نتّبع الخطوات الآتية:

أوّلاً: نوجد عناصر متتالية النص الواضح $\{m_i\}_{i=0}^{n-1}$.

ثانياً: نوجد عناصر متتالية مفتاح التشفير $\{k_i\}_{i=0}^{n-1}$.

ثالثاً: نحسب عناصر متتالية النص المشفّر $\{c_i\}_{i=0}^{n-1}$ وفق العلاقة الآتية:

$$c_i = m_i + k_i \pmod{256} \;;\; i \in \{0,1,...,n-1\} \qquad (8)$$

رابعاً: نوجد المحارف التي تقابل متتالية النص المشفّر من جدول ASCII, فنحصل على النص المشفّر C.

<u>وبالعكس</u> لفك تشفير النص C والذي عدد محارفه n, نتّبع الخطوات الآتية:

أوّلاً: نوجد عناصر متتالية النص المشفّر $\{c_i\}_{i=0}^{n-1}$.

ثانياً: نوجد عناصر متتالية مفتاح التشفير $\{k_i\}_{i=0}^{n-1}$.

ثالثاً: نحسب عناصر متتالية النص الواضح $\{m_i\}_{i=0}^{n-1}$ وفق العلاقة الآتية:

$$m_i = c_i - k_i \pmod{256} \;;\; i \in \{0,1,...,n-1\} \qquad (9)$$

رابعاً: نوجد المحارف التي تقابل متتالية النص الواضح من جدول ASCII, فنحصل على النص الواضح M.

مبرهنة 3:

إنّ تشفير كل نص واضح M طوله n محرفاً, باستخدام فيثاغوريّات مولّدة بعدد فردي, باستخدام المفتاح $K(\lambda,m)$ يتم بشكلٍ وحيد.

الإثبات :

بطريقة مشابهة لما ورد في [6].

مبرهنة 4:

إنّ فك تشفير نص مشفّر C طوله n محرفاً, باستخدام فيثاغوريّات مولّدة بعدد فردي, باستخدام المفتاح $K(\lambda,m)$ يتم بشكلٍ وحيد.

(الإثبات بنفس طريقة إثبات المبرهنة 3)

مثال 3 :

نهدف في هذا المثال إلى تشفير كلمة mathematics-is-life باستخدام فيثاغوريّات مولّدة بعدد فردي, والمفتاح $K(3,3)$.

باستخدام المفتاح $K(3,3)$ واستناداً إلى النتيجة 1 فإنّ:

(x_0,x_1,x_2)	(x_3,x_4,x_5,x_6)	$(x_7,x_8,x_9,x_{10},x_{11})$
$(3,4,5)$	$(3,4,12,13)$	$(3,4,12,84,85)$

وحيث إنّ طول النص الواضح هو 19 فبحسب العلاقة (7) تكون متتالية مفتاح التشفير هي:

$$\{k_i\}_{i=0}^{18} = \{\boxed{3,4,5,3,4,12,13,3,4,12,84,85},3,4,5,3,4,12,13\}$$

وتكون عمليّة التشفير موضّحة من خلال الجدول الآتي:

M	m_i	k_i	$m_i + k_i$	c_i	C
m	109	3	112	112	p
a	97	4	101	101	e
t	116	5	121	121	y
h	104	3	107	107	k
e	101	4	105	105	i
m	109	12	121	121	y
a	97	13	110	110	n
t	116	3	119	119	w
i	105	4	109	109	m
c	99	12	111	111	o
s	115	84	199	199	ا
¯	175	85	260	4	¬
i	105	3	108	108	l
s	115	4	119	119	w
¯	175	5	180	180	´
l	108	3	111	111	o
i	105	4	109	109	m
f	102	12	114	114	r

ويكون النص المشفّر هو:

peykiynwmoا¬lw´omr

مثال 4 :

إنّ فك تشفير الجملة:

Lvftm»Zdxt¹ĩdxnow»`rgu¹ã|

باستخدام فيثاغوريّات مولّدة بعدد فردي, والمفتاح $K(3,3)$, يُعطي النص الواضح:

Iraqi_Mathematics_Sosiety

4. الاستنتاجات والتوصيات:

من خلال هذا البحث تمّ إيجاد طريقة لتوليد فيثاغوريّات من عدد فردي, ثلاثيّة فيثاغوريّة, رباعيّة فيثاغوريّة, وخماسيّة فيثاغوريّة, ومن ثمّ تمّ بناء متتالية من الأعداد الصحيحة مكوّنة من ثلاثيّة فرباعيّة فخماسيّة ... فيثاغوريّة, واستخدمنا ذلك في بناء متتالية مفتاح التشفير.

بيّنا أنّ التشفير باستخدام فيثاغوريّات مولّدة بعدد فردي يتم بشكل وحيد, وكذلك فك التشفير.

من توصيات البحث بناء كود برمجي يقوم وبشكل آلي بعمليّة التشفير لمجرد إدخال النص ومفتاح التشفير, وكذلك لعمليّة فك التشفير.

المصادر

[1] History of Cryptography, 2013- AN Easy to understand History of Cryptography

[2] Luma A, RAUFI B., 2014- Data Encryption and Decryption Using New Pythagorean Triple Algorithm. *Proceedings of the World Congress on Engineering,* Vol I, London, U.K.

[3] SPARKS J., 2008- The Pythagorean Theorem Crown Jewel of Mathematics. Author House, USA, 176P

[4] صطيف أحمد, الخطيب عبد الباسط, شمّه محمد نور, 2017, دراسة تحليلية معمّقة في التشفير الكلاسيكي والحديث. كليّة العلوم, جامعة البعث, 109 صفحة.

[5] العرنوس باسل, شراباتي محمد, 2023, تشفير نص بواسطة خوارزميّة الرّباعيّات الفيثاغوريّة. مؤتمر الرياضيّات وتطبيقاتها بجامعة الفرات, 18 صفحة.

[6] العرنوس باسل, 2023, توليد خماسيّة فيثاغوريّة بوسيطين طبيعيّين واستخدامها في التشفير. المؤتمر الحادي عشر لجمعيّة الرياضيّات العراقيّة, 14 صفحة.