مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (١٠) العدد (٦) ٢٠٢٦

Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (10) No. (6) 2026

خوارزمية Hill Cipher المحسنة المعتمدة على الترميز base 64

(تاريخ الإيداع ٢٠٢٦/١/٢٩ . قُبِل للنشر في ٢٠٢٦/٣/٣٠)

□ ملخّص □

د. بشرى معلا *

الملخص

مع تطور الشبكات الحاسوبية وتطبيقاتها، ازدادت الحاجة إلى تأمين البيانات المرسلة ضمنها، وخاصة مع ظهور تطبيقات انترنت الأشياء IoT واتساعها. عادة ما تستخدم تقنيات التشفير من أجل ضمان سرية البيانات. تقدم هذه الورقة البحثية تحسيناً أمنياً لخوارزمية Hill Cipher التقليدية من خلال دمجها مع ترميز Base64 قبل عملية التشفير. تهدف هذه الإضافة إلى تعزيز مقاومة الخوارزمية للهجمات الإحصائية وهجمات القوة الغاشمة، وذلك عبر توسيع مجموعة الأحرف المستخدمة، مما يزيد من تعقيد النص المشفر ويخفي الأنماط الإحصائية للغة الأصلية.

نُمذجت الخوارزمية المعدلة باستخدام برنامج CrypTool، وقُيم أداؤها مقارنةً بالخوارزمية التقليدية باستخدام عدة مقاييس أمنية، مثل الانتروبيا، ومؤشر الصدفة(IC) ، والترابط الذاتي، واختبار التردد، واختبار kassiki. أظهرت النتائج تفوق الخوارزمية المعدلة في زيادة العشوائية وتشتيت الأنماط، مما يجعلها أكثر مقاومة للهجمات التحليلية، وأكثر مناسبة للتطبيقات الأمنية العملية من الخوارزمية التقليدية.

كلمات مفتاحية: شيفرة هيل، التشفير، هجوم، التحليل الإحصائي، ترميز base64، خوارزمية.

* أستاذ مساعد في قسم هندسة الاتصالات والالكترونيات -كلية الهندسة الميكانيكية والكهربائية-جامعة اللاذقية-اللاذقية -سوريا
boushra.maala@latakia-univ.edu.sy

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (١٠) العدد (٦) ٢٠٢٦

Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (10) No. (6) 2026

Base64-Enhanced Hill Cipher Algorithm

Dr. Boushra MAALA*

(Received 29/1/2026 . Accepted 30/3/2026)

□ **ABSTRACT** □

With the development of computer networks and their applications, the need to secure data transmitted within them has increased, especially with the emergence and expansion of Internet of Things (IoT) applications. Encryption techniques are commonly used to ensure data confidentiality.

This paper presents a security enhancement for the traditional **Hill Cipher** algorithm by integrating it with **Base64** encoding prior to encryption. This modification aims to strengthen the algorithm's resistance against statistical and brute-force attacks by expanding the character set, thereby increasing ciphertext complexity and obscuring the statistical patterns of the original language.

The modified algorithm was modeled using **CrypTool**, and its performance was evaluated against the traditional version using several security metrics, including entropy, Index of Coincidence, autocorrelation, frequency tests, and the Kassiki'test.

Results demonstrated the enhanced algorithm's superiority in increasing randomness and dispersing patterns, making it more resistant to analytical attacks.

The paper recommends adopting the modified algorithm in practical applications requiring a higher level of security.

Key words: Hill cipher, encryption, statistical attack, base64 encoding, algorithm

*Assistant professor - Department of Telecommunications and Electronics Engineering- College of Mechanical and Electrical Engineering-Latakia University-Latakia-Syria

boushra.maala@latakia-univ.edu.sy

مقدمة:

يُمثل التشفير (Encryption) حجر الزاوية في أمن المعلومات الرقمية، حيث يشمل مجموعة من التقنيات الرياضية والخوارزميات المصممة لحماية البيانات من الوصول غير المصرح به، وتحويلها من شكلها المقروء (النص الواضح) إلى شكل مشفر غير مفهوم. ينقسم التشفير بشكل أساسي إلى نوعين رئيسيين :التشفير المتناظر (Symmetric Encryption)والتشفير غير المتناظر(Asymmetric Encryption) في النوع المتناظر، يُستخدم مفتاح سري واحد مشترك بين المرسل والمستقبل لكل من التشفير وفك التشفير، مما يمنحه سرعة وكفاءة عالية في معالجة كميات كبيرة من البيانات. بينما يعتمد النوع غير المتناظر على زوج من المفاتيح: مفتاح عام للتشفير ومفتاح خاص لفك التشفير، مما يحل مشكلة توزيع المفاتيح الآمنة ويُستخدم بشكل أساسي للمصادقة وتبادل المفاتيح (KATZ and INDELL, 2025).

يكتسب التشفير المتناظر أهمية من كونه العمود الفقري لتأمين البيانات أثناء تخزينها وانتقالها بسرعة، نظراً لأن عملياته الحسابية أقل تعقيداً مقارنة بالتشفير غير المتناظر، فهو الأنسب لحماية البيانات الساكنة (Data at Rest) مثل تشفير الأقراص الصلبة وقواعد البيانات، والبيانات المتنقلة (Data in Transit) مثل جلسات الاتصال الآمنة. من أبرز تطبيقاته العملية: اتصالات الإنترنت الآمنة TLS/SSL وتشفير الملفات وأنظمة الملفات وحماية الشبكات الخاصة الافتراضية (VPN) لتشفير جميع البيانات المارة بين جهازك والشبكة البعيدة وتأمين الاتصالات اللاسلكية في معايير مثل WPA2وWPA3 للشبكات للاسلكية وكذلك تشفير البيانات في تطبيقات المراسلة حيث تُستخدم الخوارزميات المتناظرة لتأمين المحتوى بعد إنشاء قناة آمنة (STALLINGS, 2023).

وبفضل توازنه بين القوة الأمنية والكفاءة الأدائية، يظل التشفير المتناظر تقنية حيوية لا غنى عنها في مشهد الأمن السيبراني المعاصر، متكاملاً مع التشفير غير المتناظر لبناء أنظمة حماية متكاملة ومرنة، وتندرج خوارزمية شيفرة هيل التقليدية (Hill Cipher)HC ضمن خوارزميات التشفير المتناظر.

رغم القيمة العلمية والتاريخية لخوارزمية HC لكنها تعاني من عدة نقاط ضعف أمنية من أبرزها الخطية المفرطة التي تجعلها عرضة لعدة هجمات وعدم إخفاء أنماط البيانات بشكل كامل.

الدراسات المرجعية:

تعتمد خوارزمية شيفرة هيل التقليدية(NEHA and SACHIN, 2014) في آلية عملها على الجبر الخطي، حيث تبدأ بتحويل النص الأصلي إلى أرقام عادةً A=0 حتى Z=25 ، من ثم تقسيمه إلى كتل طول كل منها n، وهو بعد المصفوفة المربعة التي تمثل المفتاح. وتكون عملية التشفير الأساسية كالآتي: (1) $\mathbf{C = (K \times P) \bmod 26}$

حيثP الكتلة النصية، حيث K هي مصفوفة المفتاح ويجب أن تكون قابلة للعكس26 modulo بعد ذلك، تُحول الأرقام الناتجة مرة أخرى إلى أحرف.

لفك التشفير، يُستخدم معكوس المصفوفةK^{-1} بالنسبة لـ 26 modulo ، حيث تُطبق العملية العكسية :

$$\mathbf{P = (K^{-1} \times C) \bmod 26} \quad (2)$$

الشرط الأساسي لضمان عمل الخوارزمية هو أن يكون محدد المصفوفة غير صفرٍ ولا يشترك مع العدد 26 بأي قاسم لضمان وجود معكوس في الحساب المعياري.

ظهرت عدة تعديلات لهذه الخوارزمية بعضها تناول تعديل مصفوفة المفتاح الخوارزمية أكثر مرونة من حيث اختيار مصفوفة المفتاح وبعضها الآخر عدل على خطوات العمل. نذكر منها:

في (SABA,et al., 2024) قدم الباحثون تحسيناً لخوارزمية Hill Cipher التقليدية لتعزيز أمن البيانات الحساسة في القطاع المصرفي، وذلك من خلال دمج الأعداد الصحيحة الغاوسية في عملية التشفير. اختبرت الطريقة على نصوص مختلفة وأظهرت دقة في التشفير وفك التشفير. تجعل زيادة التعقيد بدمج الأعداد الغاوسية الخوارزمية المقترحة أكثر مقاومة للهجمات مقارنة بـ Hill Cipher التقليدية. الناتج النصي المشفر يظهر كقيم ASCIIغير قابلة للطباعة، مما يزيد من التمويه. في (NARENDRA, 2015) عمل الباحثون على حل مشكلة الحاجة إلى وجود معكوس لمصفوفة المفتاح واستهدف تشفير الصور بشكل أساسي. إذ يقترح المقال استخدام مصفوفات ذاتية المعكوس (Involutory) لتجنب حساب المعكوس في أثناء فك التشفير. وكما يستخدم مصفوفات مُبدلة (Permuted) ومتكررة (Reiterative) لتوليد مفاتيح مختلفة لكل كتلة بيانات، مما يزيد مستوى أمن الخوارزمية لكن ذلك أضاف تكلفة حسابية مقارنة مع الخوارزمية التقليدية. بينما تؤكد الدراسة (VIJAYARAGHAVAN, et al., 2018) على أهمية التشفير في عالم الاتصالات الرقمية لحماية سرية وسلامة البيانات .إذ تشير إلى أن الشيفرات البسيطة مثل شيفرة قيصر (Caesar Cipher) كانت عرضة للكسر بالتحليل الإحصائي لترددات الأحرف. فتقدم Hill Cipher كحل لهذه المشكلة باستخدام التحويل الخطي عبر المصفوفات، مما يدمر أنماط التردد في النص الأصل. بينما نجد أن (BIBHUDENDRA, et al., 2009) تقترح تعديلاً تجنب الخوارزمية مشكلة عدم وجود معكوس لمصفوفة المفتاح، وتقلل التكلفة الحسابية، وتوفر تشفيراً قوياً يناسب تطبيقات الصور بمختلف أنواعها. كما نجد أن المقال (GUPTA, 2022) يعالج نفس مشكلة معكوس مصفوفة المفتاح من أجل ضمان عملية فك التشفير باستخدام مصفوفات عكسها نفسها. من الدراسات المرجعية نلاحظ أن العمل على تطوير هذه الخوارزمية ما يزال قائماً وبقوة، ويتناول عدة جوانب فيها.

أهمية البحث وأهدافه:

تكمن أهمية هذا الموضوع في أن خوارزمية شيفرة هيل ما تزال تعاني من محدودية في التطبيق العملي لما تعانيه من ضعف تجاه هجوم القوة الغاشمة (Brute Force) وبسبب الخطية التي تجعل كسرها ممكن.

يهدف هذا البحث إلى تعديل خوارزمية HC التقليدية بحيث يكون من الصعب على المهاجم كسر هذه الخوارزمية في حال حصل على النص المشفر، ويكون ذلك بإضافة خطوة إلى النص المراد تشفير بترميزه باستخدام BASE64 وكذلك إضافة فك ترميز BASE64 في جهة الاستقبال.

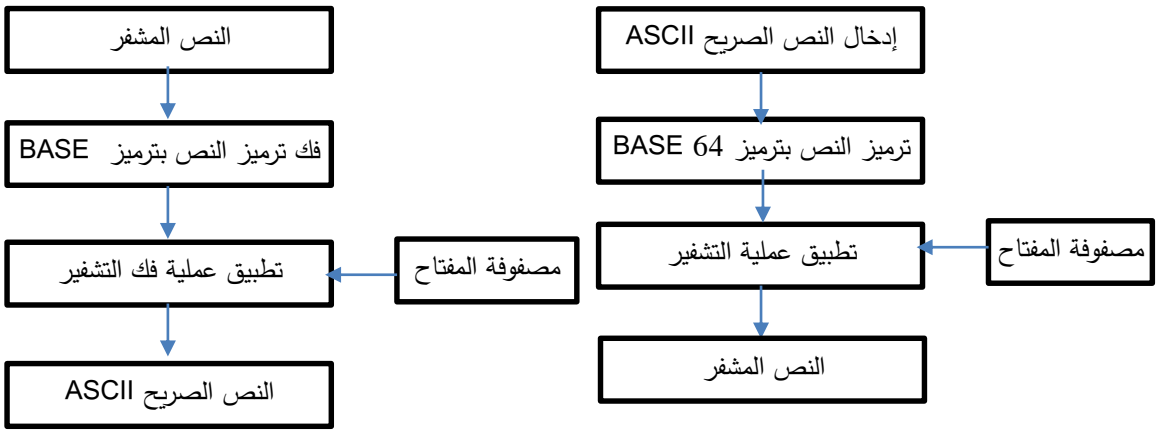
طرائق البحث ومواده:

اعتمدنا في هذا البحث بداية على وضع مخطط دقيق لآلية عمل خوارزمية **HC** المعدلة، ومن ثم نمذجة هذا المخطط باستخدام برنامج CRYPTOOL (cryptool,2026). إنه برنامج مفتوح المصدر مصمم خصيصاً لغرض واحد رئيسي هو تبسيط وتعليم مفاهيم التعمية من خلال التجربة العملية والتفاعلية. وكأنه "مختبر افتراضي" شامل يضع بين أيدينا أدوات التشفير في بيئة تعليمية آمنة وسهلة الاستيعاب. وهذا ما يفتح المجال أمامنا لتنفيذ التعديل ومقارنة أداء الخوارزمية قبل وبعد التعديل باستخدام عدة مقاييس: الانتروبيا ومؤشر الصدفة والترابط الذاتي وتردد التكرار واختبار kassiki وكلها تعطي أدلة على قدرة المهاجم على كسر النص المشفر، أي تعطينا تقييماً لقدرة الخوارزمية على مقاومة هجوم القوة الغاشمة.

1 . مخطط الخوارزمية المعدلة:

يتكون المخطط من جزأين، يمثل الجزء الأول عملية التشفير والجزء الثاني عملية فك التشفير، كما يظهر الشكل (1)، حيث تنفذ عملية التشفير بشكل مماثل لخوارزمية HC التقليدية لكن بدخل هو ترميز BASE64 للنص الصريح، وتنفذ عملية فك التشفير باستخدام نفس مراحل عملية فك التشفير في الخوارزمية التقليدية ومن ثم يطبق فك الترميز BASE64 للحصول على النص الصريح الأصلي.

كما نلاحظ أن إضافة خطوة الترميز قبل التشفير يزيد عدد الرموز المستخدمة التي يمكن أن تظهر في النص المشفر من 26 محرف تشمل الأحرف الأبجدية فقط إلى 64 محرف بما تتضمنه من أحرف كبيرة وأحرف صغيرة وكل من الرمزين + و / .هذا يعطي للمهاجم مجالاً أوسع للتخمين وبالنتيجة يزيد من صعوبة الكسر، ويزيد من قوة الخوارزمية ضد هجوم القوة الغاشمة Brute Force. في عملية فك التشفير نلاحظ أنه بعد تطبيق فك التشفير يجب تطبيق فك الترميز. مما يجعل المهاجم حتى في حال حصوله على النص المشفر وكسر هذا النص غير قادر بسهولة الحصول على النص الأصلي من النص المشفر، فناتج عملية الكسر سيكون النص المرمز وليس النص الصريح الممثل للدخل.



(a) خطوات التشفير

(b) خطوات فك التشفير

(الشكل ١ : مخطط الخوارزمية المعدلة)

1-1 الترميز BASE64 :

إنه ترميز مصمم لمنع حدوث مشاكل في الاتصالات أثناء نقل المعلومات الثنائية (JOSEFSSON, 2006). يحقق ذلك من خلال تحويل البيانات الثنائية في النهاية إلى تدفق من أحرف ASCII، والتي يمكن بعد ذلك إرسالها وفك ترميزها. يكون حجم البيانات المرمزة بـBase64 دائماً أكبر من الأصلية، يظهر الجدول (1) الجدول القياسي المستخدم لترميز الأحرف وفك ترميزها.

(الجدول ١ : جدول ترميز BASE64)

Index	Binary	Char	Index	Binary	Char	Index	Binary	Char	Index	Binary	Char
0	000000	A	16	010000	Q	32	100000	g	48	110000	w
1	000001	B	17	010001	R	33	100001	h	49	110001	x
2	000010	C	18	010010	S	34	100010	i	50	110010	y
3	000011	D	19	010011	T	35	100011	j	51	110011	z
4	000100	E	20	010100	U	36	100100	k	52	110100	0
5	000101	F	21	010101	V	37	100101	l	53	110101	1
6	000110	G	22	010110	W	38	100110	m	54	110110	2
7	000111	H	23	010111	X	39	100111	n	55	110111	3
8	001000	I	24	011000	Y	40	101000	o	56	111000	4
9	001001	J	25	011001	Z	41	101001	p	57	111001	5
10	001010	K	26	011010	a	42	101010	q	58	111010	6
11	001011	L	27	011011	b	43	101011	r	59	111011	7
12	001100	M	28	011100	c	44	101100	s	60	111100	8
13	001101	N	29	011101	d	45	101101	t	61	111101	9
14	001110	O	30	011110	e	46	101110	u	62	111110	+
15	001111	P	31	011111	f	47	101111	v	63	111111	/

1-1-2 خطوات الترميز وفك الترميز:

يتضمن الخطوات الآتية على البيانات الثنائية:

١. تجمع 3 بايتات (24 بتاً) من البيانات الثنائية ككتلة واحدة.

٢. يقسم الـ 24 بت إلى أربعة أجزاء من 6 بتات.

٣. يربط كل جزء من 6 بتات بحرف في أبجدية Base64 .

٤. إذا لم تكن البيانات الأصلية من مضاعفات لـ 3 بايتات، يستخدم الحشو padding وتدل عليه علامة التساوي (=).

تتبع عملية فك تشفير سلاسل Base64 عملية مشابهة، ولكنها معكوسة. فيما يأتي نستعرض مثالاً عن الترميز BASE64 . ذلك بفرض أن النص المراد ترميزه هو: Hello. لتنفيذ ذلك نتبع الخطوات الآتية:

١. تحويل النص إلى قيم(ASCII)عشري:

المحرف ASCII	H	E	L	l	O
القيمة بالعشري	72	101	108	108	111

المحرف ASCII	H	E	L	L	o
القيمة بالثنائي	01001000	01100101	01101100	01101100	01101111

٢. تحويل إلى ثنائي (8 بت لكل حرف):

٣. إضافة Padding لجعل العدد مضاعف 24 بت:

نحتاج إلى 24×2 = 48 بت، لدينا 40 بت، نضيف 8 بت صفر (بايت واحد)

01001000 01100101 01101100 01101100 01101111 00000000

٤. **تقسيم إلى مجموعات 6 بتات:**

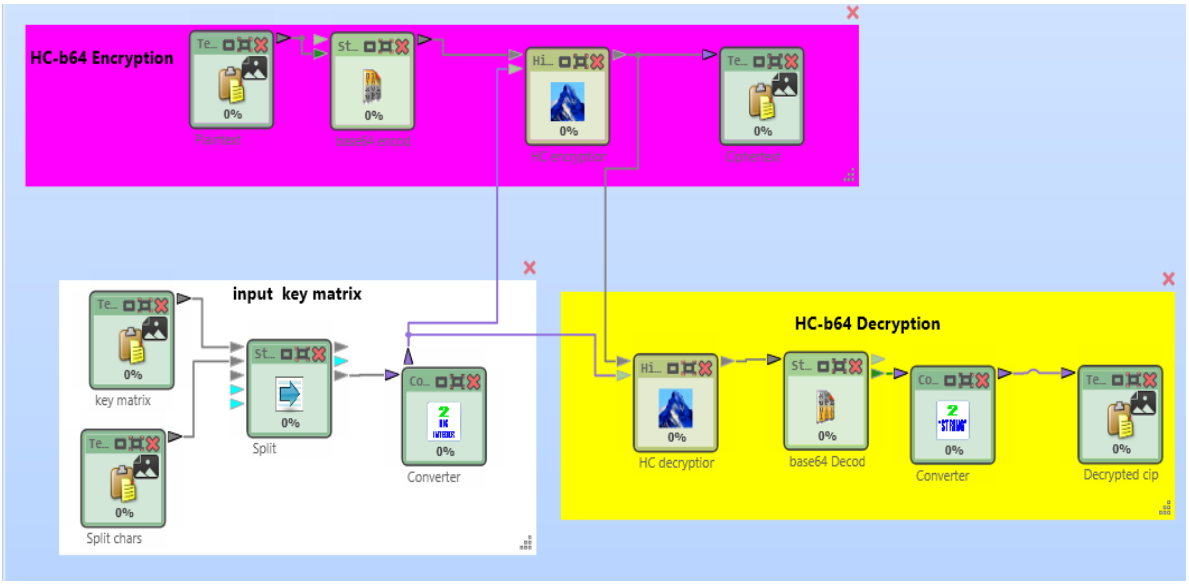
010010	000110	010101	101100	011011	000110	111000	00000
18	6	21	44	27	6	60	Padding

٥. من جدول base64 يكون: SGVsbG8=

بينما تنفذ عملية فك الترميز بطريقة معاكسة تماماً العملية الترميز. وفي مثال كمثالنا هذا ستكون أول خطوة هي خطوة إزالة الحشو (padding) فتكون: SGVsbG8 ومن ثم متابعة الخطوات بالعكس.

2. نمذجة الخوارزمية المعدلة:

كما يظهر في الشكل (2) تتكون الخوارزمية من مجموعة من الصناديق التي ربطت مع بعضها البعض وأعدت بارامتراتها بما يتناسب مع ما هو مطلوب تنفيذه.

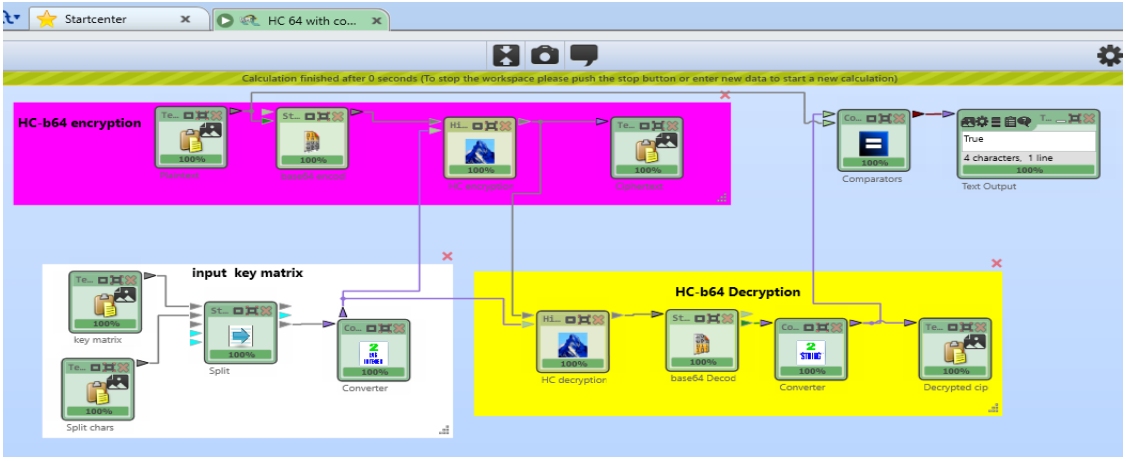


(الشكل ٢ : تنفيذ خوارزمية HC المعدلة)

بداية عدلنا على صندوق الخوارزمية التقليدية بحيث أصبحت قادرة على التعامل مع الـ 64 رمز المستخدم ضمن الترميز BASE64 بدلاً من الـ 26 محرف فقط كما في التقليدية. ومن ثم أضفنا الصندوق string encoding وربطناه ما بين صندوق Text input ودخل صندوق الخوارزمية المهيئة لتنفيذ عملية التشفير، وضُبطت إعداداته بحيث ينفذ الترميز base64 لذا يظهر بالشكل باسم base64 encoding .

في الجانب الآخر من الخوارزمية في مرحلة فك التشفير، أعددنا الخوارزمية لتنفذ فك التشفير مع تغيير الرموز التقليدية فيها لتكون قادرة على التعامل مع نص مرمز بترميز base64، ومن ثم ربطنا خرجها إلى صندوق string decoding والذي ضبطنا بارامتراته حتى ينفذ فك ترميز base64 ، يظهر في الشكل باسم base64 decoding . ومن ثم استخدمنا محول يحول للحصول على الخرج على شكل محارف ASCII بحيث تتطابق مع النص الصريح في الدخل. للتحقق من دقة النمذجة يجب عند تنفيذ الخوارزمية أن نحصل على النص الصريح الناتج عن عملية فك الترميز متطابق تماماً النص الصريح الأصلي. في الشكل (3) نفذنا عملية المطابقة بين النصين باستخدام المقارن الذي يعطي على خرجه نتيجة المقارنة، نلاحظ أنه في المثال المستخدم أعطت

true أي تطابق بينها. علماً أن عملية المتطابقة نفذت مع عدة نصوص مختلفة ولعدة مرات للتحقق منها وليس لمرة واحدة فقط.



(الشكل ٣: مقارنة النص الصريح الأصلي مع النص الناتج عن فك التشفير في الخوارزمية المعدلة)

3. مقارنة خوارزمية HC المعدلة مع خوارزمية HC التقليدية:

سيقدم التعديل الذي أجريناه على الخوارزمية عدة نقاط إيجابية وهي كالآتي:

١.تشتيت إحصائي أفضل: يحول الترميز Base64 النص إلى تمثيل أكثر عشوائية ظاهرياً.

٢. توسيع مجموعة الأحرف: من 26 حرفاً (A–Z) إلى 64 حرفاً (A–Z, a–z, 0–9، +، /)

٣. إخفاء أنماط اللغة الطبيعية: يحجب التوزيع الإحصائي المميز للغة الأصلية.

ولتأكيد هذه النقاط اختبرت الخوارزمية المعدلة وتمت مقرنتها بالخوارزمية التقليدية. من خلال مجموعة من القيم التي ستستعرضها تالياً.

3-1بارامترات المقارنة المستخدمة:

فيما يأتي نستعرض البارامترات التي اعتمدت في عملية المقارنة:

١. الانتروبيا (entropy): وهي بارامتر مهم جداً، إذ أنه قادر على تقييم العشوائية ضمن خرج الخوارزمية (FERGUSON, 2015) . وتعطى بالعلاقة: (3) $H(X) = \sum_{i=1}^{n} p_i . log_2 \left(\frac{1}{p_i}\right)$

حيث: p_i: احتمال ورود المحرف ضمن النص.

ومنه كلما كانت قيمة الانتروبيا أكبر كلما كان النص المشفر أكثر عشوائية وأكثر مقاومة للكسر.

٢. مؤشر الصدفة IC(Index of Coincidence) : هو مقياس إحصائي مهم في تحليل التشفير، يُستخدم لقياس مدى تشابه توزيع الأحرف في نص معين مع التوزيع العشوائي أو مع لغة طبيعية. يعبر عن احتمال أن يكون حرفان مُختاران عشوائياً من نص ما متطابقين. ويعطى بالعلاقة: $IC = \frac{\sum_{i=A}^{Z} n_i(n_i-1)}{N(N-1)}$ (4)

حيث: n_i = تكرار الحرف i في النص، N = إجمالي عدد الأحرف في النص، المجموع $\sum$ يُحسَب لجميع الأحرف في الأبجدية. وتختلف قيمته باختلاف التطبيق الذي نتج عنه النص المدروس. كلما كانت قيمة هذا المؤشر منخفضة كلما كان التشفير أقوى، لكن قيمته تختلف من لغة إلى أخرى، في حال كانت قيمته في اللغة الإنكليزية ضمن المجال IC ≈ 0.015-0.020 تدل على نص مشفر قوي (STALLINGS, 2023) .

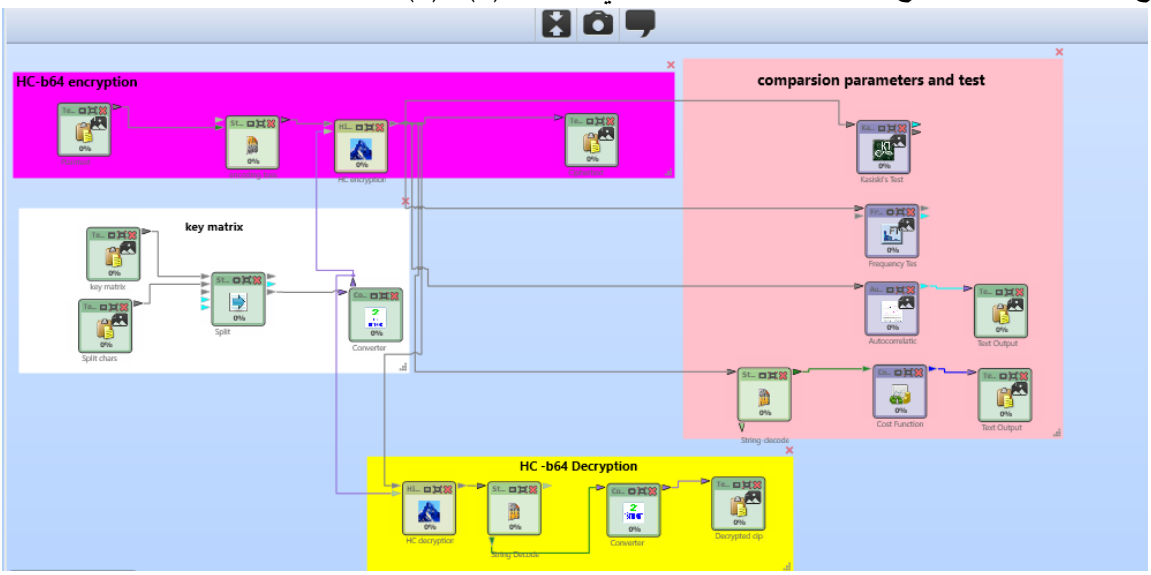
٣. الترابط الذاتي Autocorrelation: هو مقياس إحصائي يساعد على تحديد الأنماط المتكررة داخل البيانات. إنه يقيس العلاقة بين نقاط بيانات تنتمي للمتغير نفسه ولكن عند أوقات مختلفة (STALLINGS, 2023) ، فكلما كان الترابط الذاتي ضعيف كلما كان هناك صعوبة في تحديد النمط الذي بنيت عليه مجموع من البيانات، وكلما صعب كسره من قبل المهاجم.

٤. تردد التكرارات Frequency Test: هو أسلوب إحصائي أساسي يستخدم لتقييم مدى عشوائية أو انتظام مجموعة من البيانات. الهدف الأسمى لاختبار التكرار هو تحديد مدى توافق توزيع البيانات الملحوظ مع فرضية العدم التي تفترض أن البيانات أُنشئت بواسطة عملية عشوائية نزيهة. وهذه العشوائية تساهم في الحماية من كسر المهاجمين للنص المشفر (STALLINGS, 2023).

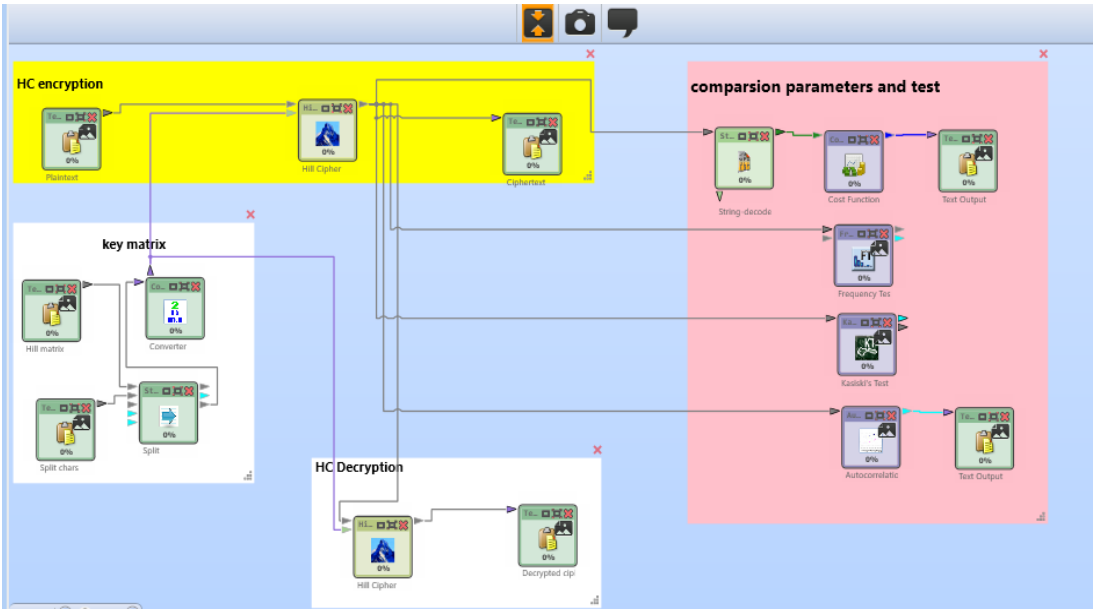
٥. اختبار كاسيكي kassiki's test :

يُبنى هذا الاختبار على فكرة أن التكرار في التشفير يخلق نقاط ضعف قابلة للاستغلال من قبل المهاجمين. يعتمد في فكرته على أنه عندما يشفر جزء من النص الصريح بنفس جزء المفتاح، سينتج نفس النص المشفر. تكرار هذه التسلسلات في النص المشفر يدل على طول المفتاح المحتمل (STALLINGS, 2023).

بهدف اختبار كل من الانتروبيا ومؤشر الصدفة تم استخدام الصندوق cost function وتمت تهيئته للقيام بذلك. ومن أجل تقييم تردد التكرار تم استخدام الصندوق frequency test، وكذلك استُخدم الصندوق autocorrelation لاختبار الترابط الذاتي، إضافة إلى إجراء اختبار كاسيكي kassiki's test. تم ربك جميع صناديق هذه القيم والاختبارات مع الخوارزمية المعدلة ومع الخوارزمية التقليدية يظهر في الشكلين (4) و(5):



(الشكل٤: نمذجة مقاييس التقييم في الخوارزمية المعدلة)



(الشكل 5: نمذجة مقاييس التقييم في الخوارزمية التقليدية)

3-3 قيم المقارنة المستخدمة:

عند المقارنة بين أية خوارزميتين يجب أن تُستخدم قيم الدخل ذاتها. سواء من نص صريح أو مفتاح لتكون نتائج المقارنة حقيقية ودقيقة. في الحالة المدروسة يفضل أن يكون النص بطول يزيد عن 200 محرف. لتكون النتائج الإحصائية دقيقة. لذا تم اعتماد على نصاً صريحاً بطول 324 محرف. وتم استخدام مصفوفة مفتاح 4x4 .

3-4 نتائج المقارنة:

بتطبيق الخوارزميتين ودراسة البارامترات المذكورة سابقاً نحصل على النتائج الآتية:

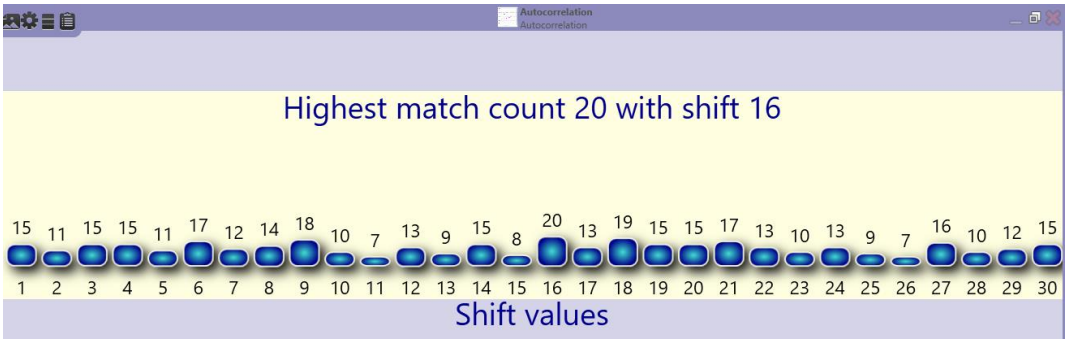
١. عند اختبار الانتروبيا ومؤشر الصدفة IC تم الحصول على القيم في الجدول الآتي:

(الجدول ٢ :قيم الانتروبيا ومؤشر الصدفة للخوارزميتين)

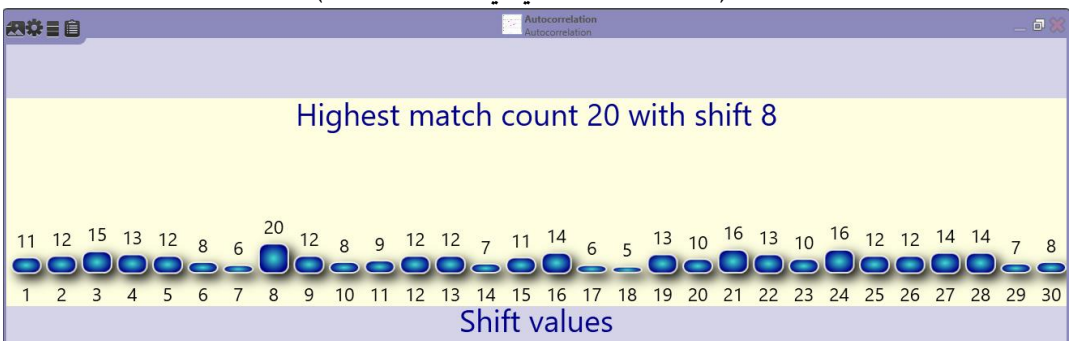
الخوارزمية	الخوارزمية المعدلة HC-B64	الخوارزمية التقليدية HC
قيمة الانتروبيا	5.79984760284424	4.64595890045166
مؤشر الصدفة IC	0.0159007352941176	0.0375919117647059

يبين الجدول أن قيمة الانتروبيا في الخوارزمية المعدلة أعلى من قيمة الانتروبيا في الخوارزمية الأصلية وهذا يدل أن الخوارزمية المعدلة تعطي نصاً مشفراً بعشوائية تتفوق على الخوارزمية التقليدية. كما أن مؤشر الصدفة في الخوارزمية المعدلة يقع ضمن مجال النص المشفر القوي، وهو أفضل من الخوارزمية التقليدية.

٢. عند تفعيل الترابط الذاتي نحصل على المخططين في الشكلين الآتيين (6) و(7):



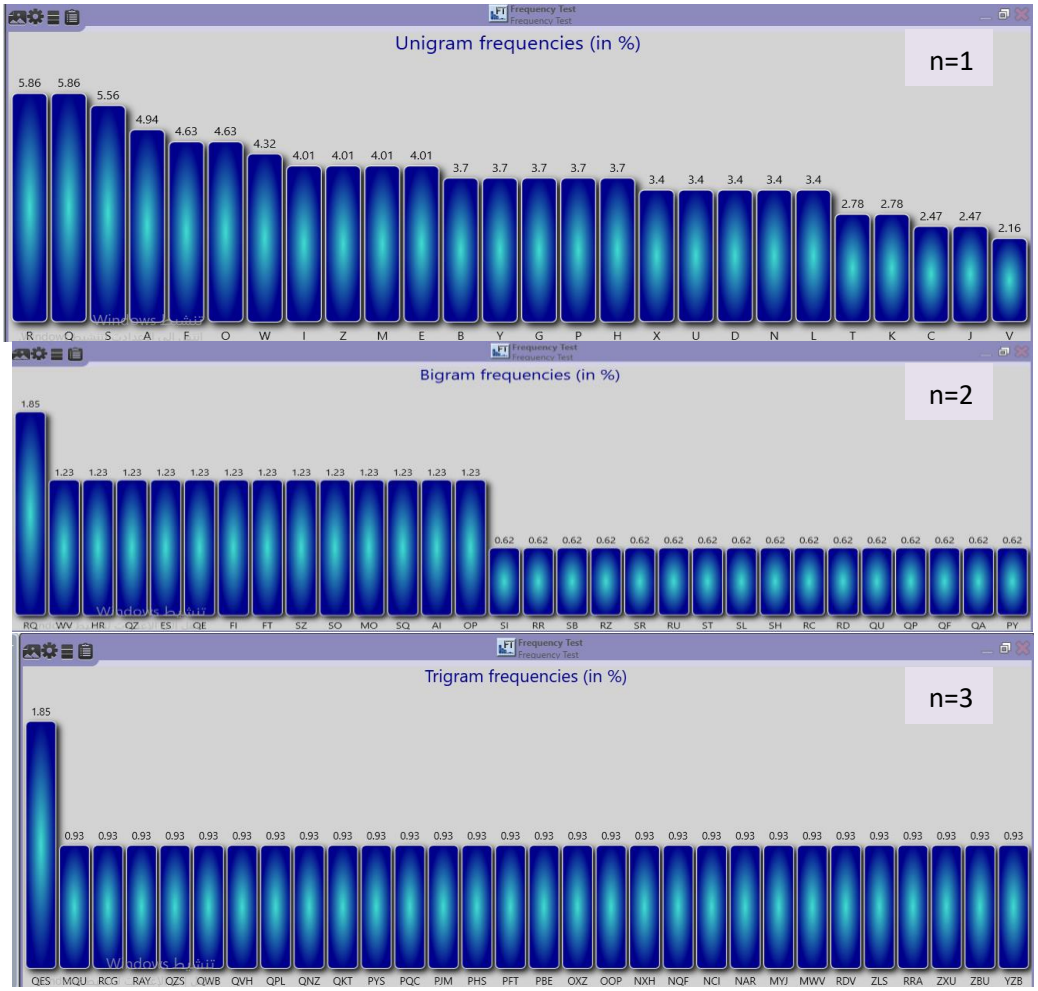
(الشكل ٦: الترابط الذاتي في الخوارزمية المعدلة)



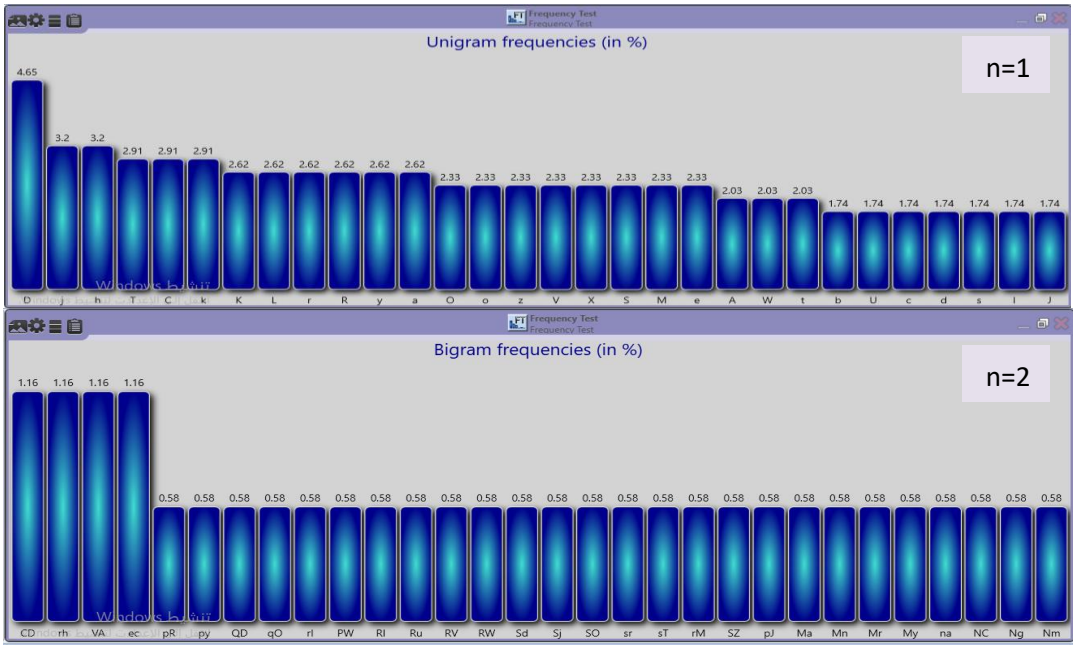
(الشكل ٧ :الترابط الذاتي في الخوارزمية التقليدية)

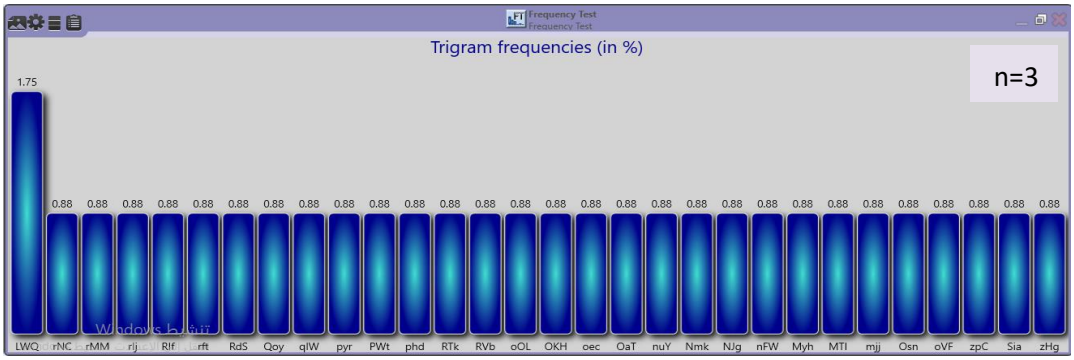
يمكن الملاحظة أعلى قيمة هي ذاتها في كلا الخوارزميتين وتساوي20 لكن عند إزاحة 8 في التقليدية و16 في المعدلة. أي لهما قيمة الترابط الذاتي نفسها كمياً لكن مع اختلاف بالإزاحة، فهي أعلى في الخوارزمية المعدلة، هذا يعطي دلالة أنها أكثر مقاومة لهجوم التحليل الإحصائي من الخوارزمية التقليدية.

٣. كما دُرس تردد التكرار في كلا الخوارزميتين. حيث تم أخذ قيم مختلفة لطول الكتل المختبرة (n) التي سيقسم إليها النص والتي يختبر تكرارها: n=1,2,3 ، فتم الحصول على النتائج في الشكلين (8) و(9). يُظهر الشكلان أن التوزيع في الخوارزمية التقليدية غير متجانس مع قمم واضحة مع نطاق محدود من الرموز الممثلة للأحرف وتظهر فيها بعض الأحرف بتكرارات عالية جداً مقارنة بأخرى أي التشتت فيها محدود مع تركيز في نطاق محدد من الترددات. بينما في الخوارزمية المعدلة يكون التوزيع أكثر تجانساً والنطاق أوسع يشمل حروف وموز خاصة والتشتت أفضل. يمكن الملاحظة أن الانحراف المعياري للترددات بالتقليدية مرتفع يتراوح بين 20–40 % بينما يكون منخفضا في المعدلة إذ يتراوح بين 5–15% أي توزع متجانس للحروف مما يجعل من الصعب تخمين الحرف من قبل المهاجم. إن ما سبق يعطي من الناحية الأمنية دلالة أن الخوارزمية المعدلة أكثر مقاومة للهجمات الإحصائية المعتمدة على تحليل التردد.



(الشكل ٨: تردد التكرار من أجل قيم n=1,2,3 في الخوارزمية التقليدية)

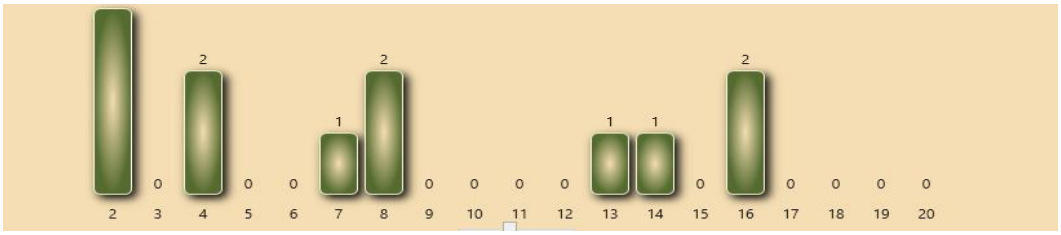




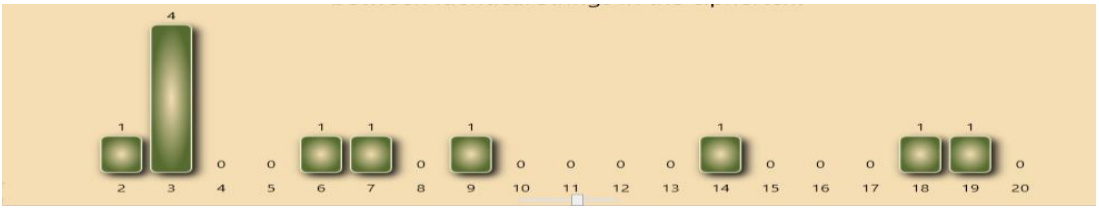
(الشكل ٩ : تردد التكرار من أجل قيم n=1,2,3 في الخوارزمية المعدلة)

4 . اختبار كاسيكي:

بتطبيق هذا الاختبار على الخوارزميتين التقليدية والمعدلة، نتج الشكلان الآتيان:



(الشكل ١٠: نتائج تطبيق اختبار kassiki على الخوارزمية التقليدية)



(الشكل ١١: نتائج تطبيق اختبار kassiki على الخوارزمية المعدلة)

يمكن ملاحظة أنه في الخوارزمية التقليدية يوجد تكرارات واضحة على مسافات ثابتة وقمم بارزة عند مضاعفات حجم مصفوفة المفتاح فمثلاً تظهر قمم عند إزاحات 4,8,16 وهي من مضاعفات العدد 4 هذا يدل أن المفتاح مصفوفة ذات بعد 4x4 وهي فعلاً أبعاد المفتاح المستخدم في هذا السيناريو، بينما في الخوارزمية المعدلة تكون التكرارات أقل وضوحاً والقمم غير منتظمة والمسافات متغيرة بين التكرارات، ولا يوجد أي قمم تدل على طول مفتاح متوقع. هذا يُشير إلى أنه من الممكن بسهولة في الخوارزمية التقليدية كشف طول المفتاح بينما يكون أكثر صعوبة في الخوارزمية المعدلة، ويعود السبب في ذلك إلى أن عملية الترميز المستخدمة في المعدلة تشتت التكرارات الأصلية.

4. تحديات الخوارزمية المعدلة:

رغم التفوق الأمني الذي حققته هذه الخوارزمية نجد أن اهم تحدي لها هي زيادة حجم البيانات على خرج هذه الخوارزمية مقارنة مع الخوارزمية التقليدية. مثلاً في التجربة المطبقة كان نص الدخل مكون من 324محرف. بالنسبة للخوارزمية التقليدية نتج نص مشفر بنفس الحجم بمعدل زيادة 0%، بينما في الخوارزمية المعدلة كان حجم النص المشفر الناتج كان مكوناً من 432 حرفاً، باعتبار أن كل حجم كل محرف هو 1byte، هذا يدل على أن هناك زيادة تصل تقريباً إلى 33%. إن هذه الزيادة تكون غير مقبولة في الأنظمة المحدودة الذاكرة،

ولكنها تكون مقبولة في الأنظمة ذات السعات التخزينية الجيدة، وفي تطبيقات الأمن العالية عندما تكون الحماية أهم من الحجم، وعندما تكون النصوص متوسطة الطول تكون الزيادة محدودة.

الاستنتاجات والتوصيات:

مما خلال دراسة للبارامترات السابقة على الخوارزمية المعدلة ومقارنتها بالخوارزمية التقليدية، يمكن الوصول إلى عدة استنتاجات وهي:

- إن الخوارزمية المعدلة تتفوق على الخوارزمية التقليدية من حيث المقاومة لهجوم التحليل الإحصائي، ولهجمات التحليل التكراري وكذلك هجوم القوة الغاشمة الأمر الذي يعطيها المجال لتكون هدفاً يستخدم في التطبيقات العملية.
- كما أنها تعطي تنوعاً كبيراً في قيم الخرج المشفر.
- إن التعديل الذي أُجري على الخوارزمية أدى إلى زيادة في حجم النص المشفر، بسبب زيادة عدد الرموز المستخدمة في ترميز base64 إضافة إلى الحشو، لكن هذه الزيادة تعد مقبولة في التطبيقات الأمنية، وهي ثمن بسيط مقارنة مع التحسينات الأمنية التي طرأت على الخوارزمية وخاصة أن هذا التعديل أدى إلى إخفاء تام لأنماط اللغة الأصلية.

لذا نوصي باستبدال الخوارزمية التقليدية بالخوارزمية المعدلة المذكورة ضمن هذه الورقة الحثية ضمن التطبيقات العملية. وسنعمل مستقبلاً على إضافة تقنية ضغط على الخرج تساعد في التخلص من زيادة حجم البيانات الحاصلة على خرج الخوارزمية المعدلة.

المراجع:

BIBHUDENDRA, A.; SAROJ, K. P.; SARAT, K. P.; GANAPATI, P. 2009, *Image Encryption Using Advanced Hill Cipher Algorithm*. International Journal of Recent Trends in Engineering, U.S.A. Vol. 1, No. 1, 663-667.

FERGUSON, N.; SCHNEIER, B.; KOHNO, T. 2015, *Cryptography Engineering: Design Principles and Practical Applications*. WILEY, U.S.A. 353.

GUPTA, A. 2022, *The Hill Cipher Algorithm for Data Encryption and Decryption*. International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), India. Vol. 2, Iss. 5, 220-225**.**

JOSEFSSON, S. 2006, *RFC 4648: The Base16, Base32, and Base64 Data Encodings*. Internet Engineering Task Force (IETF).

KATZ, J.; LINDELL, Y. 2025, *Introduction to Modern Cryptography*. 4th ed., CRC Press, U.S.A. 648.

NARENDRA, B. P. 2015, *Hill Cipher Modifications: A Detailed Review*. International Journal of Innovative Research in Computer and Communication Engineering, India. Vol. 3, Iss. 3, 1467-1474.

NEHA, S.; SACHIN, C. 2014, *A Novel Approach to Hill Cipher*. International Journal of Computer Applications, U.S.A. Vol. 108, No. 11, 34-37.

SABA, A. S.; YASMIN, M. M.; ABBAS, A.; NADIA, M. H. 2024, *A Novel Method for Hill Cipher Encryption and Decryption Using Gaussian Integers Implemented in Banking Systems.* Iraqi Journal for Computer Science and Mathematics, Iraq. Vol. 5, Iss. 1, 155-163**.**

STALLINGS, W. 2023, *Cryptography and Network Security: Principles and Practice*. 8th ed., Global ed., Pearson, U.K. 864

VIJAYARAGHAVAN, N.; NARASIMHAN, S.; BASKAR, M. 2018, *A Study on the Analysis of Hill's Cipher in Cryptography*. International Journal of Mathematics Trends and Technology, India. Vol. 54, Iss. 7, 519-522.

CRYPTOOL,2026.https://www.cryptool.org/en/ct2/downloads/