توليد مفتاح لتشفير النص باستخدام نظرية الرسم البياني

key generation for text encryption using graph theory

م.م.اسيل شاكر ناجي Aseel Shakir Naji
ثانوية المغرب للمتميزات
asulaso33@gmail.com

تاريخ تقديم البحث: 2023/06/06
تاريخ قبول النشر: 2023/06/17

المستخلص

مع زيادة استخدام الإنترنت والاتصالات واعتماد المجتمع الحالي بشكل كبير على التكنولوجيا الرقمية في العديد من التطبيقات مثل الخدمات المصرفية، التجارة الإلكترونية وكلمات مرور الكمبيوتر. أصبح التشفير مجالًا رئيسيًا للبحث والتحسين من أجل نقل البيانات وحماية المعلومات عند تخزينها ومشاركتها.

علم التشفير هو دراسة الكتابة السرية التي تطبق قواعد الرياضيات المعقدة لتحويل الرسالة الأصلية إلى صيغة غير مفهومة باستخدام خوارزميات التشفير. يتطلب استحداث خوارزميات تشفير جديدة لمنع الخوارزميات التقليدية فرصة من اختراق البيانات والوصول الغير مصرح. الخوارزمية المقترحة في هذا البحث، خوارزمية تشفير جديدة تعمل على تشفير البيانات وفك تشفيرها بشكل آمن وبالاستفادة من خصائص نظرية الرسم البياني الجديد، حيث تستخدم خوارزمية التشفير المتماثل بالاعتماد على مفاهيم الرسم البياني الحلقي, بالإضافة الى تحديد الحد الأدنى شجرة المولدة الموسعة (Complete graph) (الرسم البياني المتكامل (Cycle graph

لإنشاء نص مشفر معقد باستخدام مفتاح مشترك. (EMST)

الكلمات المفتاحية: نظرية المخطط البياني ، التشفير، فك التشفير.

Abstract

With the increase of using Internet and other new telecommunications technology in several different applications such as banking services, e-commerce, transactions, computer passwords. The encryption has become a key area of research and improvement in order to transfer data securely and safely without leakage. Cryptography is the science of transforming the secret data into coded information using encryption algorithms. it is required to develop new encryption algorithms to prevent any traditional algorithm from data breaches and unauthorized access.

In this paper ،the proposed algorithm represents a new encryption algorithm that securely encrypts and decrypts data with the advantages of the graph theory properties, the new symmetric encryption algorithm uses the concepts of cycle graph, complete graph and the extended minimum spanning tree (EMST) to generate a complex ciphertext using a shared key.

Key words: graph theory, encryption, decoding.

المبحث الاول

1-المقدمة:-

اصبح استخدام الإنترنت والهواتف المحمولة وتكنولوجيا الكمبيوتر على نطاق واسع في كل مجالات الحياة تقريبًا، ويوماً بعد يوم تزداد الحاجة إلى الحفاظ على المعلومات المهمة بشكل امن وسري.

علم التشفير هو علم تحويل البيانات السرية إلى معلومات مشفرة بهدف الوصول إلى نهايتها بأمان دون تسرب. تم استخدامه أساسًا لوضع خططاً لوقت الحرب. يعود علم التشفير الكلاسيكي إلى أكثر من ألفي عام. أسس شانون علم التشفير الحديث في عام 1949 [1]. بعد تطوير الاتصالات الرقمية، ظهرت أشكال جديدة من التشفير. تعالج مشاكل السرية والخصوصية والمصادقة وكلمات المرور والتوقيعات الرقمية وتحديد الهوية والنقود الرقمية. وهو الآن جزء لا يتجزأ من المجتمع الحديث.

تسمى عملية تحويل الرسالة الأصلية إلى نص مشفر بالتشفير، وتعرف العملية العكسية بفك التشفير [4،3،2]. في أي نظام تشفير ، يتم تشفير المعلومات المشار إليها بالنص العادي أو تشفيرها لإنشاء نص مشفر بمساعدة مفتاح محدد. ثم يتم تحويل هذا النص المشفر إلى رسالة قابلة للقراءة من خلال فك التشفير. المفتاح هو جزء من المعلومات يتم استخدامه لوضع البيانات الأصلية في شكل نص ثم فك تشفيرها للحصول على نص حقيقي. من خلال المفتاح المتوفر، يمكن للمستلم المعتمد فتح الرسالة المخفية بسهولة تامة. تصنف خوارزميات التشفير بشكل أساسي إلى نوعين رئيسيين: تشفير المفتاح المتماثل وتشفير المفتاح العام (غير المتماثل) [7،6،5].

يستخدم تشفير المفتاح المتماثل مفتاحًا واحدًا لكل من (المرسل والمستلم) في عمليتي التشفير وفك التشفير ، بينما يستخدم تشفير المفتاح العام ((غير المتماثل) مفتاحاً للتشفير ومفتاحًا آخر(المفتاح الخاص) لفك التشفير . يمكن أن يكون المفتاح العام موزع مجانا للجميع ، بينما يجب أن يبقى مفتاحها الخاص المقترن سريًا [10،9،8].

من خلال البحث ، سنعتمد المخطط البياني الغير موجه (undirected graph) ويرمز له G(V,E) حيث ان V يمثل مجموعة من الرؤوس (Vertices) ,E يمثل الاضلاع (Edges) والتي تربط الرؤوس مع بعضها البعض في المخطط البياني.

المسار (Path) يمثل السير من نقطة (Vertex) الى أي نقطة أخرى بحيث تظهر مرة واحدة فقط من دون تكرار. ومن الممكن ان تشكل (Cycle) حول النقطة اذا بدأ المسار وانتهى بنفس النقطة.

ويمكن ان نطلق على الرسم البياني الحلقي اذا تكونت حلقة (Cycle) على جميع الرؤوس (Vertices) داخل الرسم البياني.

ويسمى الرسم البياني المتكامل(Complete graph) عندما يكون هناك ضلع مرتبط بين أي راسين فيالرسم البياني .

طريقتين رئيسيتين لتمثيل الرسوم البيانية (graph), القائمة المجاورة (adjacency list) و المصفوفة المتجاورة (adjacency matrix) .تتكون القائمة المجاورة (adjacency list) من مصفوفة لقوائم الرؤوس (Vertices), حيث ترتبط كل نقطة (Vertex) مع الاخرى داخل الرؤوس, وبذلك يمكن معرفة جميع الرؤوس المتجاورة عن طريق الاضلاع المرتبطة بها .

اما المصفوفة المتجاورة (adjacency matrix) فيجب ان تكون مربعة الشكل ويمكن تمثيلها

|V|* |V| للمصفوفة Aij كما في المثال التالي:-

للمخطط البياني الغير موزون

$$Aij = \begin{cases} 1 & \text{اذا كان } i, j \in E \\ 0 & \text{والا} \end{cases}$$

Or

$$A_{ij} = \begin{cases} w_{ij} & \text{اذا كان } i, j \in E \\ \text{Nil value} & \text{(مجموعة خالية)} \end{cases}$$

للمخطط البياني الموزون

يمثل البيان الموزون (weighted graph) للمخطط البياني, بان كل ضلع E او راس V او كليهما مرفق بدالة وزن حقيقية موجبة تعبر عن طول المسافة (بين الراسين) او الزمن اللازم لرحلة ما او تكلفة معينة [11] .

يمكن ان يسمى الرسم البياني الفرعي (الشجرة) بالشجرة الموسعة (spanning tree) عندما يوجد رسم بياني فرعي متصل ويحتوي على جميع الرؤوس وبالحد الأدنى لوزن الأضلاع المطلوب، عندئذ يسمى بالحد الأدنى للشجرة المولدة (الموسعة) (minimum spanning tree) ، وهناك العديد من الخوارزمية لحل مشكلة الحد الادنى للشجرة المولدة الموسعة (MST) .

مثل خوارزمية Kruskal وخوارزمية Prime [12].

2- الدراسات السابقة:-

Yamuna et. Al. [13] ، قدموا آلية التشفير باستخدام خصائص مسار هاميلتون (المسار الذي يمر بجميع الرؤوس في الرسم البياني) ، وعملوا على تشفير البيانات مرتين ، الاولى باستخدام مسار هاميلتون، والثانية باستخدام الرسم البياني الكامل بهدف الحصول على طريقة أكثر أمانًا.

اما Kilma and Sigmon [14] ، اظهرا كيفية تحليل شفرات الرسم البياني باستخدام شفرات Vigenere (يتم تحليل الشفرات عن طريق تحليل المعلومات المشفرة والحصول على نص عادي دون معرفة مفاتيح التشفير).

استخدم Ustimenko [15] ، تقنية الحسابات الرمزية بإنشاء مفتاح عام يعتمد على الرسوم البيانية الجبرية و خوارزمية تشفير متماثل التي يمكن تنفيذها بشكل آمن و سريع.

Steve et al [16] ، استخدام الرسم البياني العشوائي وذلك بجعل جميع الرؤوس في الصور "عامة" وجميع الاضلاع داخل الصور " سرية" وباستخدام هذه التقنية، ثم ضبط التباين لتتناسب مع عدد الصور في دراسة اخرى اجريت بواسطة Perera and Wijesiri [17] ,استخدما خوارزمية التشفير المتماثلة ،تم تحويل مصفوفة النص الاصلي الى عدة رسوم بيانية من خلال المفتاح السري المستخدم, وبذلك اصبح حجم النصوص المشفرة اكبر من النص الاصلي.

و في [18] ،عملوا على نوعين من مبادئ الامنية هما تشفير البيانات واخفاء المعلومات باستخدام نظرية البيانات ، حيث تم تشفير و تحويل كلمة السر الى مخطط بياني واستخدامه كمفتاح مشفر للنص الاصلي ، و بطريقة البت الاقل اهمية (LSB) تم اخفاء الرسالة في صورة ملونة لحمايتها من الدخلاء.

3- الخوارزمية المقترحة:-

تتلخص الخوارزمية بتمثيل البيانات (احرف النص الاصلي) بشكل رؤوس (Vertices) متجاورة ، ونستمر في إضافة الاضلاع (Edges) الى ان نشكل رسمًا بيانيًا حلقياً (Cycle graph). لكل ضلع (Edge) في الرسم البياني له وزنه الخاص والذي يمثل المسافة بين الحرفين ، ويتم تمثيل جميع الأحرف الأبجدية بواسطة شفرة محددة لكل حرف ضمن جدول خاص. سيتم ربط كل النقاط (Vertexes) في الرسم البياني مع الاضلاع (Edges) لجعله رسمًا بيانيًا كاملاً ، وكل ضلع جديد لديه وزن تسلسلي يبدأ من الفهرس الأخير في جدول التشفير.

بعد إنشاء المصفوفة المتجاورة adjacency–matrix للرسم البياني المتكامل. يمكن حساب الحد الأدنى للشجرة المولدة الموسعة (EMST) من الرسم البياني المتكامل ويتم تمثيلها كمصفوفة مجاورة تحافظ على البيانات ويكون ترتيب الأحرف قطريًا . يتم اجراء عملية الضرب اولاً (لمصفوفة التجاور للرسم البياني المتكامل مع مصفوفة متجاورة من (EMST)) . وثانياً (المصفوفة الناتجة مع مصفوفة المفتاح المشترك) . وبذلك تكون المصفوفة النهائية هي بيانات التشفير التي سيتم إرسالها إلى المستلم. خوارزمية (1) و(2) توضح خطوات العمل المقترحة.

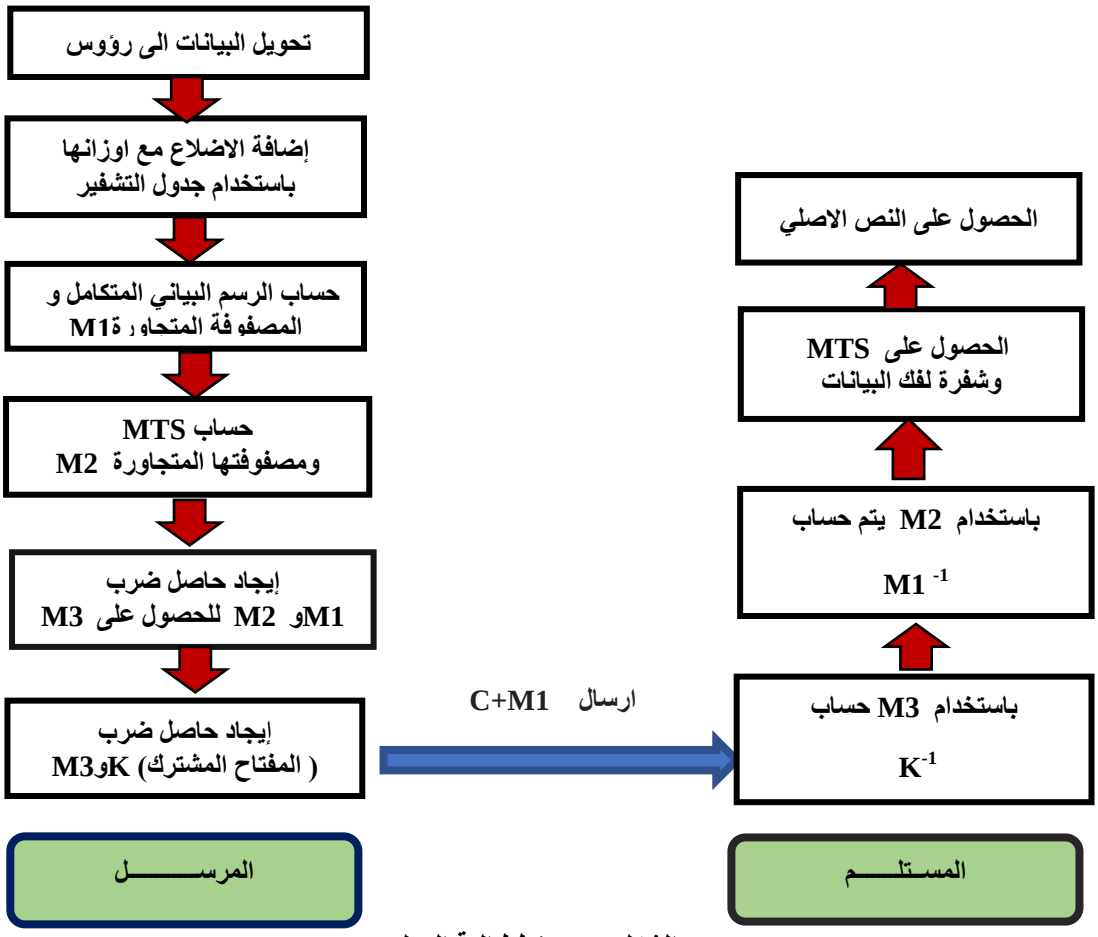
الشكل (1) يوضح اليه عمل خوارزميات المقترحة (التشفير و فك التشفير)

خوارزمية 1 : مرحلة التشفير.

- أضافة حرفًا خاصًا لتحديد حرف البداية مثلاً حرف (A).
- أضافة نقطة (Vertex) لكل حرف في النص الاصلي إلى الرسم البياني.
- ربط الرؤوس ببعضها البعض عن طريق إضافة ضلع بين كل حرف متسلسل في النص الاصلي الى ان يتشكل رسم بياني حلقي.
- يوزن كل ضلع باستخدام جدول التشفير. كل ضلع موزون يمثل المسافة بين الرأسين المتصلين من جدول التشفير.
- إضافة المزيد من الاضلاع لتشكيل الرسم البياني الكامل M1 ، كل ضلع جديد له وزن متسلسل يبدأ من الوزن الأقصى في جدول التشفير.
- بعدها نبحث عن الحد الأدنى للشجرة المولدة (الموسعة) M2.
- ثم نعمل على خزن ترتيب الرؤوس في مصفوفة M2 في الأماكن المائلة بشكل (القطري).
- و نضرب المصفوفات M1 في M2 لنحصل على M3.
- واخيراً نقوم بضرب M3 في المفتاح المشترك K المحدد مسبقًا لتشكيل C (النص المشفر).
- عندئذ نحصل على نص التشفير المتكون من Matrix C و Matrix M1 بتنسيق خطي.

خوارزمية 2: مرحلة فك التشفير.

- المستلم يحسب M3 باستخدام معكوس المفتاح المشترك K^{-1}.
- بعدها يحسب M2 باستخدام معكوس لـ M1.
- ثم يحسب النص الأصلي عن طريق فك تشفير M1 باستخدام خوارزمية التشفير.

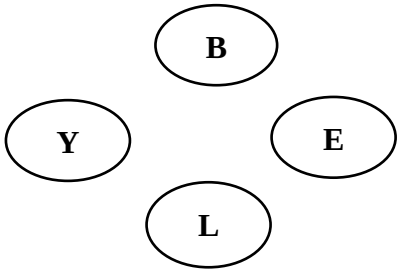


الشكل (1) مخطط الية العمل

4- النتائج:-

نفترض لدينا رسالة مشفرة (BELY) تم ارسالها الى الطرف الاخر وهو المستلم . حيث سيكون لدينا مجموعة من خطوات العمل وهي:

الخطوة الأولى : تحويل الرسالة الى مخطط بياني ، عند طريق وضع راس Vertices لكل حرف كما هو موضح بالشكل (2).



الشكل (2) تحويل كل حرف الى راس

يتم ربط كل حرفين متسلسلتين سويةً مكوناً بذلك الرسم البياني الحلقي. ويمكن معرفة وزن كل ضلع من خلال جدول التشفير التالي:-

جدول (1) جدول التشفير

A	B	C	D	E	...	L	...	W	X	Y	Z
1	2	3	4	5		12		23	24	25	26

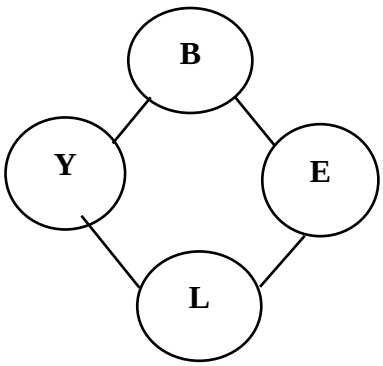
لكل ضلع وزن (المسافة) يربط بين أي رأسين في جدول التشفير ، يمكن حساب المسافة بين الحرفين B, E كما يأتي:-

المسافة = رمز E - رمز B

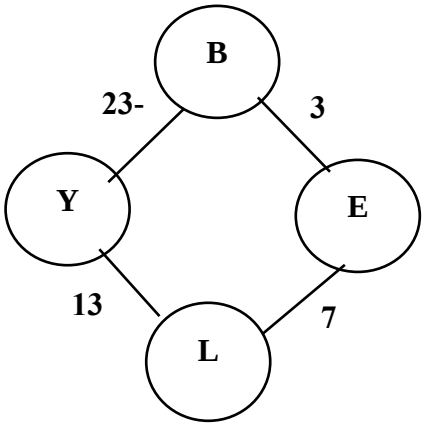
= 5 - 2

= 3

وبنفس الطريقة أعلاه، يتم حساب المسافة بين احرف النص الأصلي داخل الرسم البياني. كما موضح في الشكل (3) وكذلك في الشكل (4).

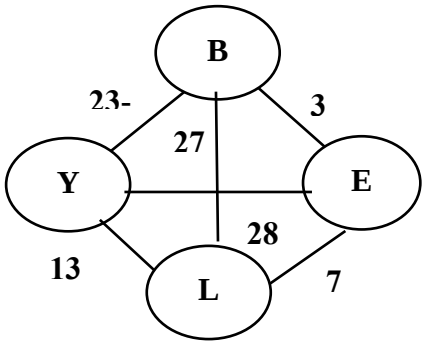


الشكل (3) الرسم البياني لأحرف النص الأصلي



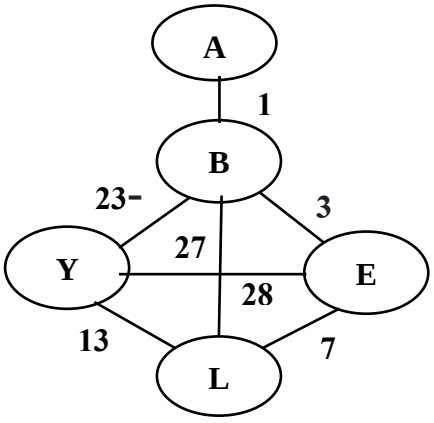
الشكل (4) الرسم البياني الموزون لأحرف النص الاصلي

نستمر في إضافة الاضلاع لتشكيل الرسم البياني المتكامل، لكل ضلع مضاف له وزن متسلسل يبدأ من الوزن الأقصى لجدول التشفير، (26 +1=27) كما موضح بالشكل (5).



الشكل (5) الرسم البياني المتكامل للنص الأصلي

نضيف حرفاً جديداً كمؤشر بداية للرسم البياني ويوضع قبل اول حرف من النص الأصلي، افترضنا الحرف (A) مؤشراً للبداية كما موضح في الشكل (6).

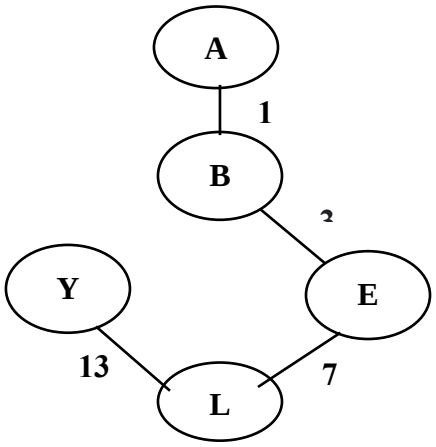


الشكل (6) الرسم البياني المتكامل للنص الأصلي مع المؤشر

تمثيل النص البياني المتكامل في الشكل (5) كمصفوفة .

$$M1=\begin{bmatrix}0 & 1 & 0 & 0 & 0\\ 1 & 0 & 3 & 27 & -23\\ 0 & 3 & 0 & 7 & 28\\ 0 & 27 & 7 & 0 & 13\\ 0 & -23 & 28 & 13 & 0\end{bmatrix}$$

نجد الحد الأدنى للشجرة المولدة الموسعة (EMST)



الشكل (7) الحد الأدنى للشجرة المولدة الموسعة (EMST)

$$M2=\begin{bmatrix}0 & 1 & 0 & 0 & 0\\ 1 & 0 & 3 & 0 & 0\\ 0 & 3 & 0 & 7 & 0\\ 0 & 0 & 7 & 0 & 13\\ 0 & 0 & 0 & 13 & 0\end{bmatrix}$$

يمكن خزن الاحرف المرتبة قطرياً بالترتيب (0، 1، 2، 3، 4) بدلاً من الاصفار. بحسب الجدول ادناه:

الاحرف	A	B	E	L	Y
الترتيب	0	1	2	3	4

لتصبح المصفوفة بعد التعديل.

$$M2=\begin{bmatrix}0 & 1 & 0 & 0 & 0\\ 1 & 1 & 3 & 0 & 0\\ 0 & 3 & 2 & 7 & 0\\ 0 & 0 & 7 & 3 & 13\\ 0 & 0 & 0 & 13 & 4\end{bmatrix}$$

يتم اجراء عملية ضرب بين مصفوفة M1 ومصفوفة M2 لنحصل على M3

$$M3= M1M2=\begin{bmatrix} 1 & 0 & 3 & 0 & 0 \\ 1 & 10 & 192 & -278 & 315 \\ 3 & 6 & 58 & 378 & 91 \\ 27 & 21 & 102 & 218 & 39 \\ -23 & 84 & 22 & 196 & 169 \end{bmatrix}$$

يستخدم المفتاح المشترك K لتشفير المصفوفة M3

$$K=\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

الحصول على النص المشفر C

$$C=\begin{bmatrix} 1 & 1 & 4 & 4 & 4 \\ 1 & 11 & 203 & -75 & 276 \\ 3 & 9 & 67 & 445 & 536 \\ 27 & 48 & 150 & 368 & 405 \\ -23 & 61 & 83 & 279 & 448 \end{bmatrix}$$

وبالخطوات أعلاه أصبحت البيانات مشفرة، يتم ارسال (النص المشفر C + مصفوفة M1)

بعد الاستلام ، يتم عملية فك الشفرة للحصول على النص الأصلي ، من خلال إيجاد المصفوفة M3 وذلك بضرب النص المشفر المستلم C مع معكوس المفتاح المشترك K^{-1} .

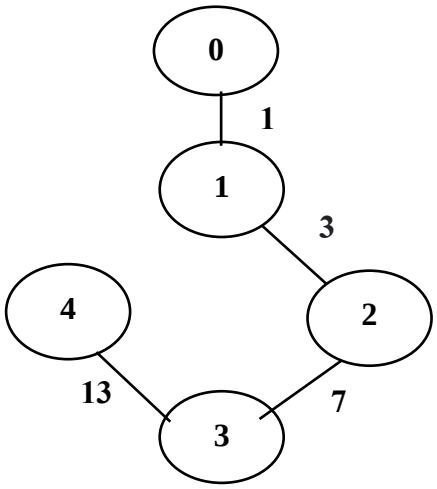
$$M3=CK^{-1}=\begin{bmatrix} 1 & 1 & 4 & 4 & 4 \\ 1 & 11 & 203 & -75 & 276 \\ 3 & 9 & 67 & 445 & 536 \\ 27 & 48 & 150 & 368 & 405 \\ -23 & 61 & 83 & 279 & 448 \end{bmatrix} * \begin{bmatrix} 1 & -1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$=\begin{bmatrix} 1 & 0 & 3 & 0 & 0 \\ 1 & 10 & 192 & -278 & 315 \\ 3 & 6 & 58 & 378 & 91 \\ 27 & 21 & 102 & 218 & 39 \\ -23 & 84 & 22 & 196 & 169 \end{bmatrix}$$

بعد ذلك يتم حساب M2 عن طريق ضرب M3 بـ $M1^{-1}$

$$M2=M3M1^{-1}=\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 3 & 0 & 0 \\ 0 & 3 & 2 & 7 & 0 \\ 0 & 0 & 7 & 3 & 13 \\ 0 & 0 & 0 & 13 & 4 \end{bmatrix}$$

يمثل الشكل (8) الرسم البياني النهائي ، حيث يمكن استرداد النص الأصلي.



الشكل (8) الرسم البياني النهائي

افترضنا ان الراس (0) هو الحرف (A)، عن طريق جدول التشفير يمكن معرفة النص الاصلي ، الراس(1)=رمز (A) + 1= 2 والذي يمثل الحرف (B) .

و الراس (2) = رمز (B) + 3 = 5 والذي يمثل الحرف (E) وهكذا الى ان نحصل على النص الأصلي الكامل (**BELY**) .

الأستنتاجات :

من خلال الخوارزمية المستخدمة تم الحصول على النتائج التالية:-

1-الخوارزمية توفر قوة الحماية في حالة عدم الكشف عن النص المشفر حتى إذا كان المهاجم لديه كل المعلومات الخاصة بالخوارزمية. بسبب صعوبة تخمين المفتاح السري و النص الاصلي حتى وان حصل المهاجم على النص المشفر بأكمله .

2- مهما كان طول المفتاح العام متغير ومختلف يمكن تطبيق الخوارزمية عليه وذلك بتكراره وتوسيعه للطول المطلوب.

3- الطريقة المقترحة تولد نصًا مشفرًا حيث يكون حجمه أكبر من حجم النص الاصلي ، لذلك فان الخوارزمية تكون أكثر فاعلية عندما تكون رسالة النص الاصلي صغيرة.

4- يزداد الوقت المطلوب لتشفير النص أيضًا بسبب مضاعفة عمليات الضرب للمصفوفات.

5- وجود المفتاح السري، يجعل من الصعب تخمين السر مفتاح. يتم الحصول على النصوص المشفرة عن طريق عملية ضرب المصفوفة ومن ثم فك التشفير باستخدام المعكوس للمفتاح والمصفوفة . وهذا يضيف المزيد من الأمان إلى النص الاصلي ويجعل الخوارزمية قوية ضد تحليل التشفير.

في هذا البحث ، نقدم خوارزمية تشفير جديدة حيث يمكن تنفيذها بلغات برمجية مختلفة مثل : (C++,JAVA,MATLAB) تستخدم هذه الخوارزمية للتشفير، حيث يتم ارسال البيانات باستخدام جدول الترميز وخصائص نظرية الرسم البياني كالرسم البياني المتكامل (Complete graph) والحد الأدنى من الشجرة المولدة الموسعة (EMST). ويمكن ان تستخدم خوارزمية التشفير

المتماثل مفهوم المفتاح المشترك الذي يجب تحديده مسبقًا ومشاركته بين المرسل والمستقبل. ولمزيد من التعقيد والأمان يستخدم المفتاح العام والذي يحتوي على مفتاحين أحدهما للتشفير والآخر لفك التشفير.

الاعمال المستقبلية

يمكن إجراء العديد من التحسينات في المستقبل المتعلقة بتقليل المصفوفات المطلوبة من تشفير وفك تشفير الرسائل ، ولتقليل حجم النص المشفر مثل: تقسيم الرسالة الى رسالة إلى مجاميع صغيرة من الرسائل وتشفر كل مجموعة على حدة ثم تسلسل النصوص مشفرة لتشكل نص تشفير الرسالة بالكامل.

المصادر

[1] C. E. Shannon, "Communication theory of secrecy systems∗ ," Bell System Technical Journal, vol. 28, no. 4, pp. 656–715, 1949.

[2] K. H. Rosen, Elementary Number -eory and its Applications, Addison-Wesley, Boston, MA, USA, 5th edition, 2005.

[3] D. B. West, Introduction to Graph -eory, Pearson, London, UK, 2nd edition, 2001.

[4] Keijo Ruohonen, Graph Theory (2013).

[5] G. A. Selim, "How to encrypt a graph," International Journal of Parallel, Emergent and Distributed Systems,vol. 35, no. 6, pp. 668–681, 2020.

[6]Berrak, O., Belmeguenai, A., Ouchtati, S Secure Transfer of Color Images Using Horizontal and Vertical Scan. Traitement du Signal, Vol. 36, No. 1, pp. 45-51. (2019).

[7] P. L. K. Priyadarsini, "A survey on some applications of graph theory in cryptography," Journal of Discrete Mathematical Sciences and Cryptography, vol. 18, no. 3, pp. 209–217, 2015.

[8] Monrose, F., Reiter, M. K., Li, Q., & Wetzel, S. Cryptographic key generation from voice. (pp. 202- 213). IEEE.2001.

[9] Keijo Ruohonen, Graph Theory (2013).

[10] Safaa Hraiz and Wael Etaiwi. Symmetric encryption algorithm using graph representation. In 2017 8th International Conference on Information Technology (ICIT), pages 501-506. IEEE, 2017**.**

[11] Paszkiewicz A, et al. Proposals of graph based ciphers, theory and implementations. Research Gate; 2001.

[12] Corman TH, Leiserson CE, Rivest RL, Stein C. Introduction to algorithms 2 nd edition, McGraw-Hill.2001.

[13] Yamuna M, Meenal Gogia, Ashish Sikka, Md. Jazib Hayat Khan. Encryption using graph theory and linear algebra. International Journal of Computer Application. ISSN:2250-1797; 2012.

[14] Rick Kilma and Neil Sigmon. Cryptology: Classical and Modern (Chapman & Hall/CRC Cryptography and Network Security Series) 2nd Edition.first issue.2022.

[15] Ustimenko VA. On graph-based cryptography and symbolic computations, Serdica. Journal of Computing.131-156,2007.

[16] Steve Lu, Rafail Ostrovsky. Daniel Manchala. Visual Cryptography on Graphs, CiteSeerx, COCOON.225-234;2008.

[17] P.A.S.D.Perera, G.S.Wijesiri. Encryption and Decryption Algorithms in Symmetric Key Cryptography Using Graph Theory, ISSN: 00333077: 2021.

[18] Samaher Adnan Abdul-Ghani , Renna D.Abdul-Wahhab , Enas Wahab Abood, Securing Text Messages Using Graph Theory and Steganography, E-ISSN: 2411-7986: 2022.