وزارة التعليم العالي والبحث العلمي
جامعة ديالى / كلية التربية للعلوم الصرفة
قسم علوم الحاسوب

Adaptive cipher algorithm in bitmap format

خوارزمية التشفير المضاف في تنسيق الصورة النقطية

المشروع مقدم الى كلية التربية للعلوم الصرفة قسم علوم الحاسوب
وهو جزء من متطلبات نيل شهادة البكالوريوس
في تربية علوم الحاسوب

تقديم الطالب:
عامر ياسر ناصر
اشراف:
أ.م.د. سلام عبدالخالق نعمان

١٤٤٠هـ ٢٠١٩م

الفصل الاول

تشفير النص وحفظه بتنسيق صورة ملونة(RGB)

CIPHER TEXT AS RGB COLOR IMAGE

الاطار العام للبحث

تصميم برنامج لتشفير نص وحفظه بتنسيق صورة ملونة (RGB) بلغة سي شارب C#.

١.١ مشكلة البحث :

بسبب استخدام الوسائل الالكترونية وعدم امان عملية نقل البيانات والرسائل الالكترونية بين الاشخاص فواجهتنا العديد من المشاكل المطلوب حلها من خلال نظامنا ومنها:

١. **حماية ضعيفة (Low security):** ففي طبيعة الرسائل الغير مشفرة يكون الحماية ضعيفة وقابلة للاختراق بسهولة بواسطة المتطفلين.

٢. **السرية أو الخصوصية (Confidentiality) :** ففي الوضع الطبيعي تكون ضعيفة جدا حيث يمكن للأشخاص الغير مصرح لهم بالاطلاع على الرسائل..

٣. **إثبات الهوية (Authentication):** من المشاكل المطلوب ان يقوم النظام بحلها .

٤. **تكامل البيانات (Integrity ضافة أو تعديل):** المطلوب حل مشكلة تكامل البيانات حيث لا يمكن لأي شخص التعديل على الرسائل الا الشخص المخول.

١.٢ أهداف البحث:

١. السرية أو الخصوصية (Confidentiality) : هي خدمة تستخدم لحفظ محتوى المعلومات من جميع الأشخاص ما عدا الذي قد صرح لهم الإطلاع عليها.

٢. تكامل البيانات (Integrity) من قبل الأشخاص الغير مصرح لهم بذلك.

٣. إثبات الهوية (Authentication) : وهي خدمة تستخدم لإثبات هوية التعامل مع البيانات (المصرح لهم).

إضافة إلى ذلك فان هدف التشفير هو لجعل الرسالة أو السجل غير قابل للإدراك من قبل الأشخاص غير المخولين.

إذاً الهدف الأساسي من التشفير هو توفير هذه الخدمات للأشخاص ليتم الحفاظ على أمن معلوماتهم.

١.٣ حدود البحث:

بسبب التنوع الهائل في طرق التشفير اقتصر هذا البحث على استخدام طريقة واحدة وهي (خوارزمية قيصر).

١.٤ مقدمة

عُرف علم التشفير أو التعمية منذ القدم، حيث استخدم في المجال الحربي والعسكري. فقد ذكر أن أول من قام بعملية التشفير للتراسل بين قطاعات الجيش هم الفراعنة. وكذلك ذكر أن العرب لهم محاولات قديمة في مجال التشفير. و استخدم الصينيون طرق عديدة في علم التشفير والتعمية لنقل الرسائل أثناء الحروب. فقد كان قصدهم من استخدام التشفير هو إخفاء الشكل الحقيقي للرسائل حتى لو سقطت في يد العدو فإنه تصعب عليه فهمها. وأفضل طريقة استخدمت في القدم هي طريقة القصير جوليوس وهو أحد قياصرة الروم. أما في عصرنا الحالي فقد باتت الحاجة ملحة لاستخدام هذا العلم "التشفير" وذلك لإرتبط العالم ببعضه عبر شبكات مفتوحة. وحيث يتم استخدام هذه الشبكات في نقل المعلومات إلكترونياً سواءً بين الأشخاص العاديين أو بين المنظمات الخاصة والعامة، عسكرية كانت أم مدنية. فلابد من طرق تحفظ سرية المعلومات. فقد بذلت الجهود الكبيرة من جميع أنحاء العالم لإيجاد الطرق المثلى التي يمكن من خلالها تبادل البيانات مع عدم إمكانية كشف هذه البيانات[23].

استخدم التشفير منذ أقدم العصور في المراسلات الحربية وكذلك في الدبلوماسية والتجسس في شكليهما المبكرين. يعتبر العلماء المسلمون والعرب أول من اكتشف طرق استخراج المعمَّى وكتبها وتدوينها .تقدمهم في علم الرياضيات أعطاهم الأدوات المساعدة الأزمة لتقدم علم التعمية، من أشهرهم يعقوب بن إسحاق الكندي صاحب كتاب علم استخراج المعمَّى وابن وَحشِيَّة النبطي صاحب كتاب شوق المستهام في معرفة رموز الأقلام، المؤلف الذي كشف اللثام عن رموز الهيروغليفية قبل عشرة قرون من كشف شامبليون لها وكذلك اشتهر ابن دريهم الذي كان لا يشق له غبار في فك التشفير فكان تعطى له الرسالة معماة فما هي إلا أن يراها حتى يحولها في الحين إلى العربية ويقرئها وله قصيدة طويلة يشرح فيها مختلف الطرق في تعمية النصوص وكان يحسن قراءة الهيروغليفية من أمثلة استخدام التعمية قديما هو ما ينسب إلى يوليوس قيصر من استعمال ما صار يعرف الآن بخوارزمية ROT13 لتعمية الرسائل المكتوبة باللاتينية التي يتبادلها مع قواده العسكريين، وهو أسلوب تعمية يُستبدل فيه كل حرف بالحرف الذي يليه بثلاثة عشر موقعا في ترتيب الأبجدية اللاتينية، مع افتراض أن آخر حرف في الأبجدية يسبق

الأول في حلقة متصلة .ومازال العمل والبحث في مجال علم التشفير مستمراً وذلك بسبب التطور السريع للكمبيوتر والنمو الكبير للشبكات وبخاصة الشبكة العالمية الإنترنت.[23]

١.٥ التشفير [15]

التشفير (بالإنجليزية: Encryption) يتناولها علم المعلومات (التي تكون بشكل نص بسيط عند التخزين على وسائط التخزين المختلفة أو عند نقلها على شبكات نص مجرد (plaintext) بحيث تصبح غير مقروءة لأحد باستثناء من يملك معرفة خاصة أو مفتاح خاص لإعادة تحويل النص المشفر إلى نص مقروء. عملية الفك هذه تتم عن طريق ما يدعى مفتاح التشفير كما موضح في الشكل رقم (١.١) كيف تتم عملية التشفير . نتيجة عملية التشفير تصبح المعلومات مشفرة وغير متاحة لأي أحد لأغراض سرية عسكرية أو سياسية أو أمنية كما نلاحظ في الشكل (١.١) كيف تجري عملية التشفير.

شكل (١.١) كيف تتم عملية التشفير (Encryption)

بمجرد إرسال حزم البيانات من المكالمات الصوتية والدردشة و البريد الإلكتروني أو حتى استخدام بطاقة الائتمان في الإنترنت ربما جميع هذه البيانات قد تتعرض للتنصت أو حتى السرقة، لذا وجب علينا استخدام التشفير أثناء القيام بهكذا عمليات حساسة.

يطلق على التشفير باللغة الإنجليزية بالـ Encryption أو الـ Ciphering, حيث أن الكلمة الأولى مأخوذة Cryptography وهي تعني الكتابة السرية أما الثانية فهي مأخوذة من كلمة Cipher والتي يقال بأنها تعود الى الكلمة العربية "تصفير" أو جعل القيمة مساوية لـ "صفر" أي بلا قيمة أو بلا معنى .

١.٦ مصطلحات ومفاهيم علم التشفير

A. علم التشفير (Cryptography) هي كلمه تعني بالإغريقية كلمتان

Cryptography → krypton + graphy

(اخفاء) + (الكتابة)

علم التشفير هو من العلوم التي تستخدم الحساب للتشفير (encrypt) وفك التشفير (decrypt) بالنسبة للبيانات وبالتالي تتيح تخزين وارسال البيانات بطريقه سريه بحيث لا يستطيع احد قراءتها ماعدا المصرح.

B. التشفير (Encryption):

هي عملية تحويل النص او البيانات الى شكل غير مفهوم بغرض اخفاء هذه البيانات او هو عملية تحويل نص صريح(plain text) الى نص مشفر (cipher text) غير صريح بواسطة مفتاح سري (secret key)

او عملية ارجاع النص المشفر (cipher text) الى نص صريح (plain text) تعرف بعملية فك التشفير (decryption).

C. المفتاح (key):

وهو عباره عن كلمه السر المستخدمة في خوارزمية التشفير او فك التشفير ويعتبر من اهم الاشياء التي يجب اخفائها حيث انه يعتبر من الاشياء السرية التي لا يعرفها الا المخول لهم.

D. الخوارزمية(Algorithm):

هي عباره عن الخطوات اللازمة لحل مسألة ما، وقد تكتب هذه الخوارزمية باللغة العربية او الإنجليزية وقد يعبر عنها برسم اشكال هندسيه معينه.

النص الاصلي قبل عملية التشفير--> plaintext

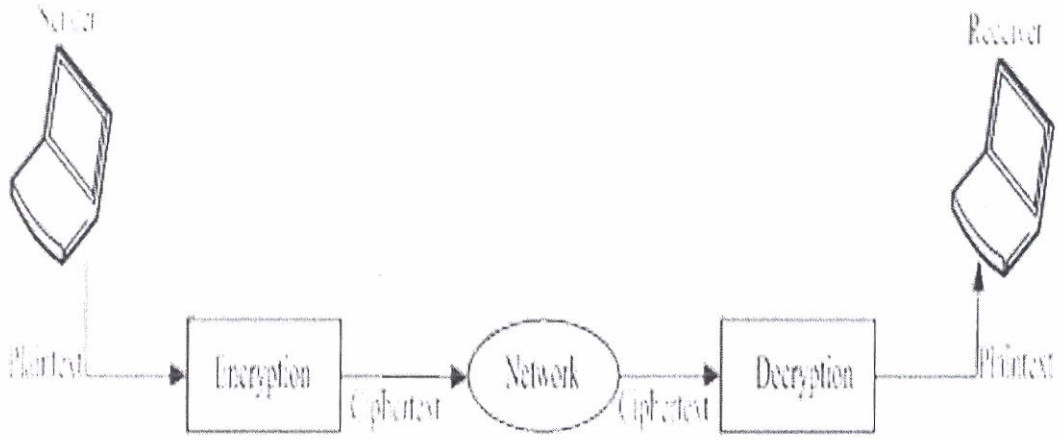
النص المشفر بعد عملية التشفير--> ciphertext

تحويل النص العادي الى نص مشفر --> encryption

فك التشفير أي تحويل النص المشفر الى نص عادي --> decryption

E. مثال بسيط عن الية التشفير (Basic Terminology)

كما نلاحظ العملية في الشكل (١.٢)



شكل (١.٢) عملية التشفير (Encryption) وفك التشفير (Decryption)

F. فن كسر الشفرة (cryptanalysis)

هو العلم الذي يستخدم لكسر الخوارزميات وإيجاد نقط الضعف بها. أي إنه العلم الذي يستطيع تحويل الكتابة المكتوبة بطريقة سرية تستخدم التشفير وتحويل النص المشفر إلى نص غير مشفر، والتشفير وتحليل الشفرات هما جانبان من عملية التشفير. فن كسر الشفرة يقوم باسترجاع النص الصريح(plain text) من النص المشفر (cipher text) بدون معلومية المفتاح key.

(cryptographer) هم الاشخاص الذين يستخدمون علم التشفير.

١.٧ انواع خوارزميات التشفير حسب طريقة ادخال البيانات

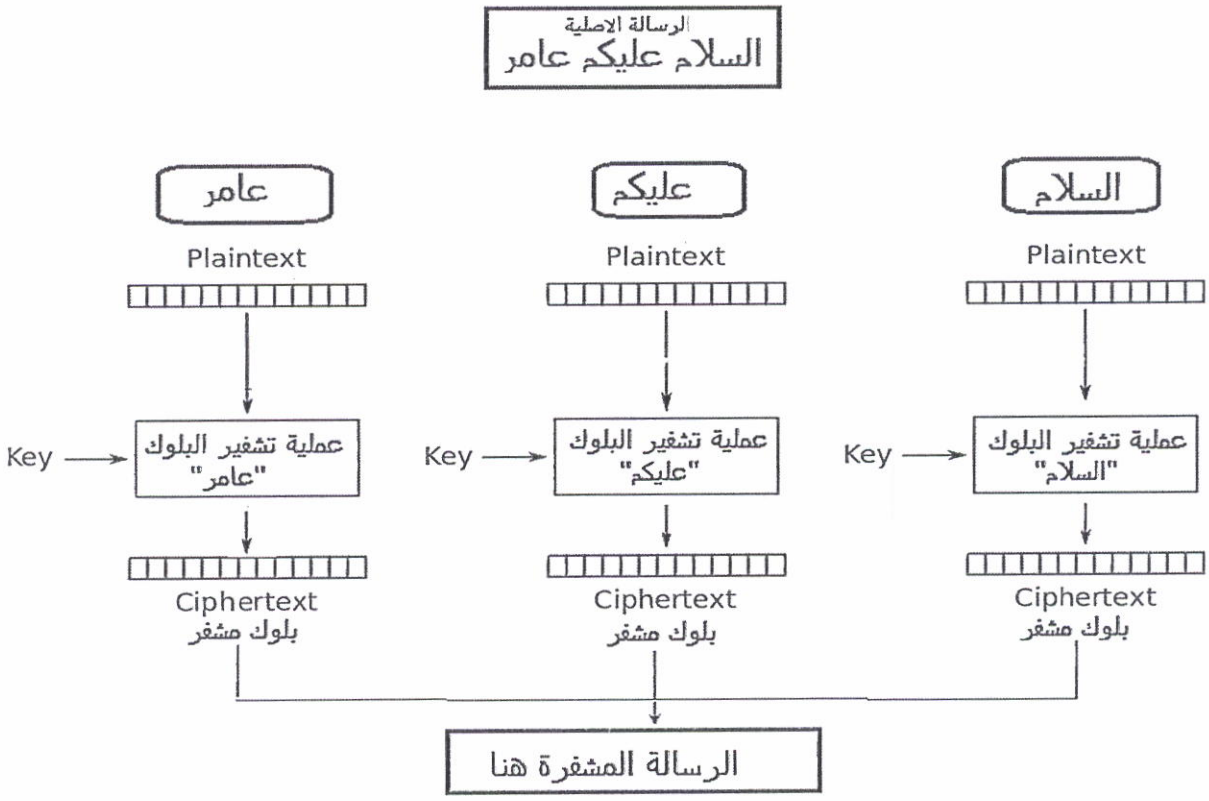
تقسم خوارزميات التشفير حسب طريقة العمل على اجزاء ورموز البيانات إلى نوعين: المقطعي والمتصل.

١.٧.١ التشفير المقطعي (Block Cipher) [15]

يقوم على مبدأ تقسيم المحتوى الاصلي (نصوص أو صور أو أي شيء آخر) إلى مجموعات متساوية الطول من البتات تسمى بلوكات Blocks أو مقاطع ثم تشفير كل مقطع على حدة.

إن أكثر خوارزميات التشفير تعتمد على التشفير المقطعي مثل خوارزميات إيه إي إس، DES، 3DES، خوارزمية آر إس إيه، إم دي٥، TIGER وغيرها ...**وطريقة التشفير في هذا النوع كالتالي :**

يحاول ادخال مجموعة من البتات (Bits) وتشفيرهم ثم ادخال مجموعة أخرى وتشفيرها وهكذا حتى يتم تشفير كامل الملف فمثلا "عامر ياسر" يتم ادخال مجموعة من البتات (Bits) "عامر" ثم تشفيرها ثم الانتقال إلى مجموعة أخرى "ياسر" ثم تشفيرها حتى يتم الانتهاء من كامل الملف ك ما موضح في الشكل (١.٣):



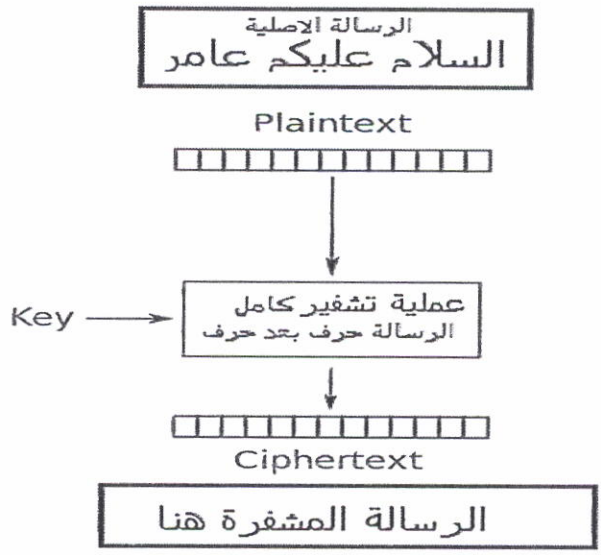
شكل (١.٣) التشفير المقطعي (Block Cipher)

١.٧.٢ التشفير المتصل (Stream Cipher)

ويقوم على مبدء تشفير البيانات المتصل أو جدول البيانات بشكل مستمر. حيث يتم توليد مفتاح مستمر يتم دمجه مع البيانات الأصلية بخوارزمية تشفير ذات مفتاح متماثل وغالبا يتم ذلك بعملية XOR المنطقية وكما موضح في الشكل (١.٤) [15] . بشكل اساسي في بحثنا سوف نعتمد على هذا النوع من التشفير وبشكل خاص سنقوم باستخدام عملية XOR المنطقية في التشفير. ومن خوارزميات التشفير

المتصل على سبيل المثال RC4 التي تعد خوارزمية التشفير المتصل الأوسع انتشارا.[14] وطريقة التشفير (Encryption) في هذا النوع كالتالي:

يحاول تشفير المعلومات كل بت (Bit) على حدة حتى يتم الانتهاء من كامل الملف فمثلا كلمة "مرحبا" يتم تشفير "م" ثم يتم الانتقال إلى "ر" حتى يتم الانتهاء من كامل الملف او النص.



شكل (١.٤) التشفير المتصل (Stream Cipher)

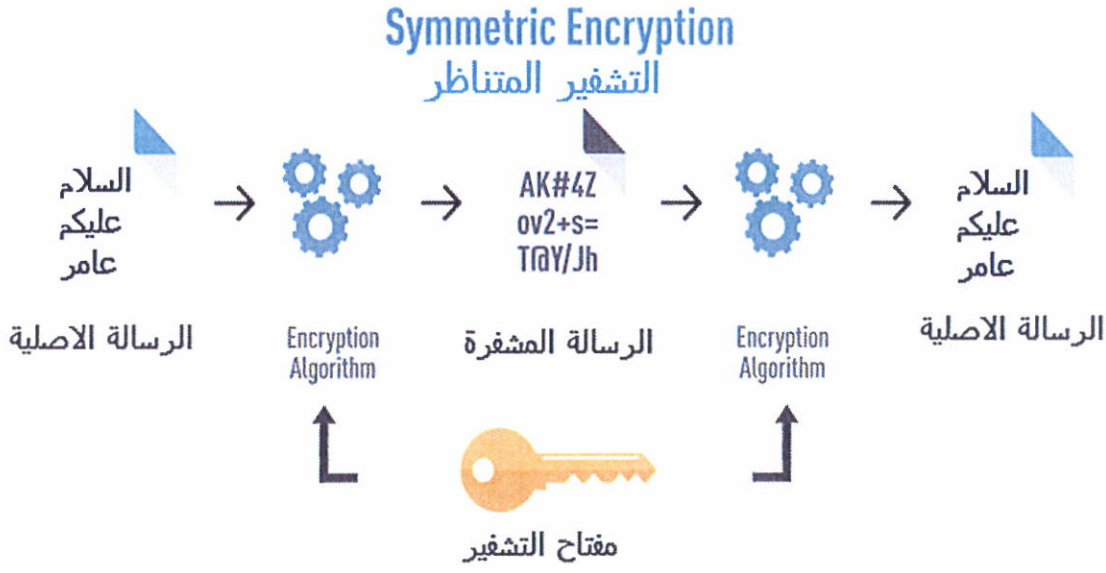
١.٨ انواع خوارزميات التشفير(Encryption)حسب نوع مفتاح التشفير وفك التشفير [12]

تقسم خوارزميات التشفير حسب طريقة نوع مفتاح التشفير وفك التشفير إلى نوعين: المتناظر وغير المتناظر، بالإضافة إلى نوع لايحتاج إلى مفتاح تشفير وهو دالة هاش التشفيرية.

١.٨.١ التشفير المتناظر (Symmetric Encryption)

التشفير بالمفتاح المتناظر

ان خوارزمية التشفير المتناظر إذا استخدم نفس المفتاح في التشفير وفك التشفير يقوم نظام التشفير المتماثل symmetric systems باستخدام نفس المفتاح في التشفير وفك التشفير. من مزايا التشفير المتماثل انه سهل الاستعمال وسريع وكما موضح في الشكل (١.٥).



شكل (١.٥) التشفير المتناظر (Symmetric Encryption)

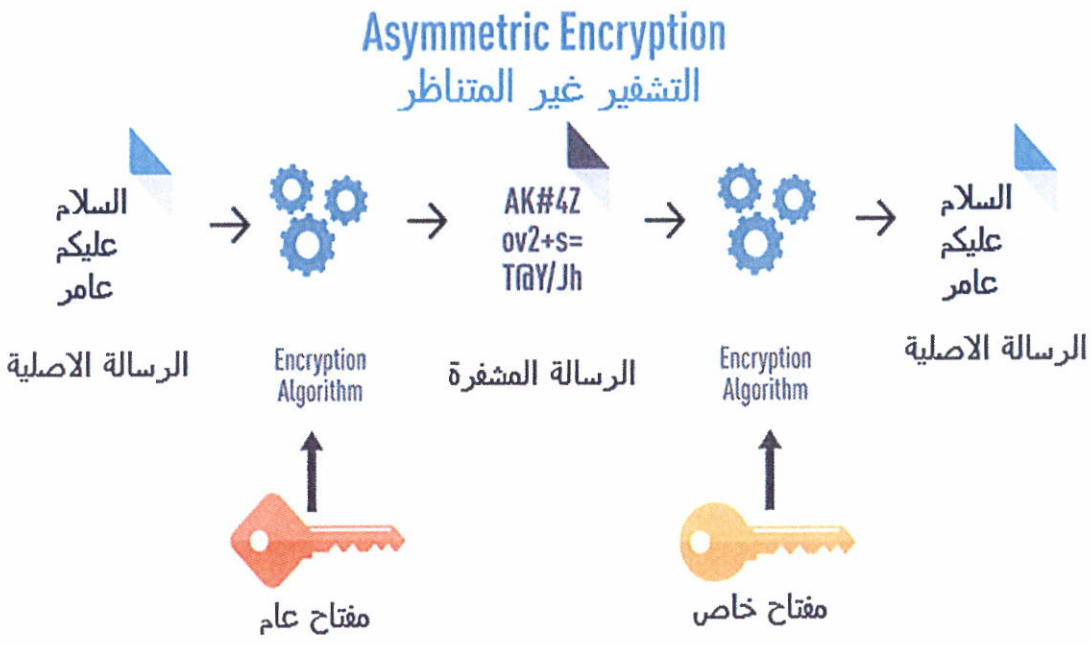
ففي مشروعنا يندرج التشفير الى هذا النوع من التشفير كوننا نستخدم نفس المفتاح للتشفير وفك التشفير.

ومن الامثلة على الخوارزميات التي تستخدم المفتاح المتناظر AES، DES, 3DES، وغيرها.

١.٨.٢ التشفير غير المتناظر(Asymmetric Encryption)

التشفير بالمفتاح غير المتناظر

خوارزمية غير المتناظر أو المفتاح العام إذا استخدم مفتاح للتشفير واخر لفك التشفير asymmetric systems،فهو يقوم بتوليد مفاتيح مختلفة ثم استخدامها في تشفير وفك تشفير زوجين من مفاتيح الحماية. وباستخدام هذين الزوجين من المفاتيح، أحدهما عام public والآخر خاص private، يستطيع مفتاح واحد منهما فقط أن يقوم بفك الشفرة التي ينشئها الآخر وكما موضح في الشكل (١.٦) .



شكل (١.٦) التشفير غير المتناظر(Asymmetric Encryption)

ومن غيرالمرجح أن تؤدي معرفة مفتاح واحد فقط إلى تحديد المفتاح الآخر، ولهذا يتم استخدام نظام التعمية غير المتماثل في إنشاء التوقيعات الرقمية ونقل المفاتيح المتماثلة

من الامثلة على الخوارزميات التي تستخدم المفتاح المتناظر خوارزمية خوارزمية آر إس إيه

لقد كانت معظم أنظمة التعمية في الماضي تستخدم النظام المتماثل فقط، وتكمن مشكلة هذا النظام في الصعوبة التي يتم مواجهتها في توزيع المفاتيح على أشخاص بعينهم، فنظرا لأن التشفير المتماثل يعتمد على استخدام نفس المفتاح في التشفير وفك التشفير، فإن المرء يضطر إلى استخدام أساليب مبتكرة وصعبة معاً لمنع الآخرين من اعتراض المفتاح،

ولكن إذا ما تمكن أحدهم من اعتراض المفتاح، فستكون لديه القدرة على استخدامه في فك شفرة(في حالة التشفير المتماثل فقط) أي شيء قام المفتاح بتشفيره.

1.9الاستعمالات الحديثة للتشفير[13]

في العصر الحديث، تعد آلة إنجما التي استخدمها الجيش الألماني في الحرب العالمية الثانية، أبرز مثال على استخدام التعمية لتحقيق تفوق على العدو في مجال الاتصالات، وكانت الأبحاث التي جرت بشكل منفصل في كل من المؤسستين العسكريتين الأمريكية والبريطانية في سبعينيات القرن العشرين فتحا جديدا فيما صار يعرف الآن بتقنيات التعمية القوية المعتمدة على الحوسبة، وارتبطت التعمية بعلوم الجبر ونظرية الأعداد ونظرية التعقيد ونظرية المعلومات.

توسع نطاق تطبيقات التعمية كثيرا في العصر الحديث بعد تطور الاتصالات وحدوث ثورة الاتصالات بما تتطلبه أحيانا من استيثاق وحاجة إلى ضمان عدم التصنت ومنع التجسس والقرصنة الإلكترونيين وتأمين سبل التجارة الإلكترونية.

الفصل الثاني

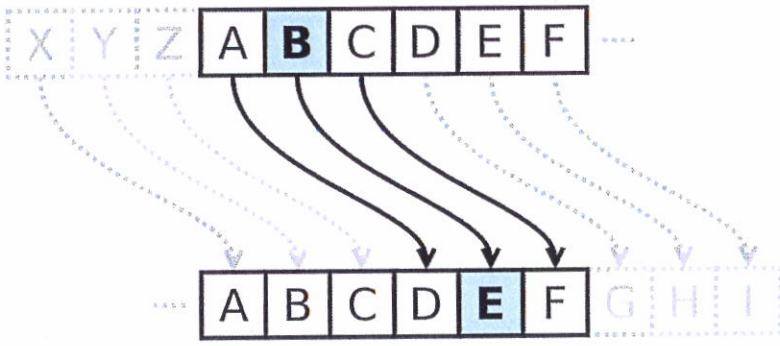
تشفير النص وحفظه بتنسيق صورة ملونة (RGB)

CIPHER TEXT AS RGB COLOR IMAGE

الجانب النظري

٢.1 التمثيل الرياضي لخوارزمية قيصر [8]

يعد تشفير قيصر ، واحدًا من أبسط تقنيات التشفير وأكثرها انتشارًا. إنه نوع من شفرات الاستبدال حيث يتم استبدال كل حرف في النص العادي بعدد ثابت من المواقع (الازاحة). على سبيل المثال ، مع التشفيت ثلاث مرات الى اليسار ، سيتم استبدالA بـ D، B تصبح E ، وهكذا... كما في الشكل (٢.١).



شكل (٢.١) التمثيل الرياضي لخوارزمية قيصر

أولاً ، قم بترجمة جميع الرموز إلى أرقام ، ' a' = 0 ، 'b' = 1 ، 'c' = 2 ، ... ، 'z' = 25. ثم نطبق خوارزمية تشفير قيصر ، e (x) ، حيث x هي الرمز الذي سنقوم بتشفيره ، باستخدام المعادلة (١) :

$$e(x)=(x+k) \pmod{26} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

حيث k هو مفتاح التشفير و x هو الحرف الذي تجري عليه عملية التشفير، (التشفيت او التزحيف) المطبق على كل حرف. بعد تطبيق هذه الدالة ، تكون النتيجة رقماً ، ومن ثم يجب ترجمته مرة أخرى إلى حرف. دالة فك التشفير هي:

$$e(x)=(x-k) \pmod{26} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (2)$$

حيث k هو مفتاح التشفير و x هو الحرف الذي تجري عليه عملية فك التشفير

٢.٢ الخوارزمية المقترحة proposed algorithm :

٢.٢.١ مقدمة: [7]

كما هو معروف جيدًا ، فإن صورة RGB (الأحمر والأخضر والأزرق) عبارة عن ثلاثة مصفوفات الأبعاد يخزن بوضوح قيمة اللون لكل بكسل في الصورة. تتكون هذه المصفوفات من العرض وارتفاع الصورة وثلاث قنوات معلومات ملونة. يتم تخزين الصور الممسوحة ضوئيًا بشكل شائع كصور RGB. تمثل قناة واحدة مقدار اللون الأحمر في الصورة (القناة الحمراء) ، وتمثل قناة واحدة مقدار اللون

الأخضر في الصورة (القناة الخضراء) ، وتمثل قناة واحدة مقدار اللون الأزرق في الصورة (القناة الزرقاء). سيتم تخصيص احدى القنوات اللونية للبيانات النصية المشفرة ، والقناة الأخرى للمفتاح ، وستستخدم القناة الثالثة لاستخراج النص المشفر. يتم إرسال ملف الصورة إلى المستلم ، والذي بدوره يعكس الخطوات المتفق عليها مسبقًا لاستخراج النص المشفر والمفتاح ثم استخراج النص الصريح.

في علم التعمية، شفرة قيصر Caesar cipher، أو خوارزمية قيصر، هي واحدة من أكثر تقنيات التعمية انتشاراً . تعتبر شفرة قيصر من أقدم أنواع التشفير باستخدام تقنيات تبديل الحروف التي يتم فيها استبدال كل حرف في النص الصريح بحرف اخر بالاعتماد على المفتاح. وسميت هذه الشفرة على اسم يوليوس قيصر، الذي استخدمها في مراسلاته الخاصة. وكما هو معروف ، هناك خطوات يتم تنفيذها بواسطة المرسل ، والخطوات الأخرى التي يقوم بها المستلم لغرض الحصول على النص الصريح ، كما يلي:

٢.٢.٢ خوارزمية التشفير (المرسل) :

المدخلات: النص الصريح

الخطوة ١. اختر خوارزمية التشفير بالاتفاق مع المستلم (قيصر في بحثنا هذا) .

الخطوة ٢. مطابقة حروف الرسالة لواحدة من السلسلة المتفق عليها المعروفة مثل Ascii code

الخطوة ٣. تشفير النص الصريح باستخدام خوارزمية التشفير المتفق عليها

الخطوة ٤. إنشاء ثلاثة مصفوفات أحادية البعد R، G، B ، على التوالي

الخطوة ٥. املأ المصفوفة الأولى (R) بأرقام عشوائية مرتبة بترتيب تصاعدي

الخطوة ٦. املأ المصفوفة G بالنص المشفر

الخطوة ٧. رتب المصفوفة R بالترتيب التنازلي بالاقتران مع المصفوفة G

الخطوة ٨. املأ الصف B بعناصر المفتاح

الخطوة ٩. مرة أخرى ، يتم إعادة ترتيب الصفيف R مع مصفوفة G و B

الخطوة ١٠. يتم إرسال الرسالة (المصفوفات الثلاثة) كملف صورة RGB

المخرجات: النص المشفر

٢.٢.٣ خوارزمية فك الشفرة (المستلم) :

يعكس المستلم الخطوات التي اتخذها المرسل للحصول على النص الصريح للرسالة المستلمة:

المدخلات: النص المشفر

الخطوة ١. إعادة ترتيب المصفوفة R تصاعدي بالتزامن مع المصفوفة G و B ، تمثل

المصفوفة G الآن النص المشفر

الخطوة ٢. إعادة ترتيب المصفوفة R تنازليًا بالاقتران مع المصفوفة G و B ، تمثل المصفوفة B الآن المفتاح

الخطوة ٣. استعادة النص الصريح (فك تشفير) باستخدام الخوارزمية المتفق عليها ، والنص المشفر والمفتاح

المخرجات: النص الصريح

مثال:

٢.٢.٤ خطوات المرسل (تشفير الرسالة):

الخطوة ١: استخدام خوارزمية تشفير قيصر مع إزاحة مختلفة (تمثل المفتاح)

الخطوة ٢: مطابقة حروف الرسالة لواحدة من السلسلة المتفق عليها المعروفة مثل Ascii code

Alpha bet	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
Ascii Code	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90

الخطوة ٣: تشفير النص الصريح باستخدام خوارزمية التشفير المتفق عليها الرسالة هي: GO HOME SOON

Caesar encryption algorithm with different displacement	Message	G	O	H	O	M	E	S	O	O	N
	Ascii code	71	79	72	79	77	69	83	79	79	78
	displacement	1	3	5	5	3	1	1	3	5	5
	Encrypted text	H	R	M	T	P	F	T	R	T	S

الخطوة 4: إنشاء ثلاثة مصفوفات أحادية البعد R، G، B ، على التوالي

R										
G										
B										

الخطوة 5: املأ المصفوفة الأولى (R) بأرقام عشوائية مرتبة بترتيب تصاعدي

R	7	11	20	22	23	24	44	50	65	74
G										
B										

الخطوة 6: املأ المصفوفة G بالنص المشفر

R	7	11	20	22	23	24	44	50	65	74
G	H	R	M	T	P	F	T	R	T	S
B										

الخطوة 7: رتب المصفوفة R بالترتيب التنازلي بالاقتران مع المصفوفة G

R	74	65	50	44	24	23	22	20	11	7
G	S	T	R	T	F	P	T	M	R	H
B										

الخطوة 8: املأ الصف B بعناصر المفتاح

R	74	65	50	44	24	23	22	20	11	7
G	S	T	R	T	F	P	T	M	R	H
B	1	3	5	5	3	1	1	3	5	5

الخطوة 9:مرة أخرى ، يتم إعادة ترتيب الصفيف R مع مصفوفة G و B

R	65	44	22	20	7	74	50	24	23	11
G	T	T	T	M	H	S	R	F	P	R
B	3	5	1	3	5	1	5	3	1	5

الخطوة ١٠: يتم إرسال الرسالة (المصفوفات الثلاثة) كملف صورة RGB ، في المثال ، استخدمت الأبجدية بدلاً من كود أسكي لاجل المزيد من التوضيح ، في الواقع سيكون ملف RGB مثل:

R	65	44	22	20	7	74	50	24	23	11
G	84	84	84	77	72	83	82	70	80	82
B	3	5	1	3	5	1	5	3	1	5

٢.٢.٥ خطوات المستلم(استعادة الرسالة):

الخطوة ١: إعادة ترتيب المصفوفة R تصاعدي بالتزامن مع المصفوفة G و B ، تمثل المصفوفة G الآن النص المشفر

R	7	11	20	22	23	24	44	50	65	74
G	H	R	M	T	P	F	T	R	T	S
B	5	5	3	1	1	3	5	5	3	1

النص المشفر هو: HRMTPFTRTS

الخطوة ٢: إعادة ترتيب المصفوفة R تنازليًا بالاقتران مع المصفوفة G و B ، تمثل المصفوفة B الآن المفتاح

R	74	65	50	44	24	23	22	20	11	7
G	S	T	R	T	F	P	T	M	R	H
B	1	3	5	5	3	1	1	3	5	5

المفتاح هو: ١٣٥٥٣١١٣٥٥.

الخطوة ٣: استعادة الرسالة الاصلية (فك تشفير) باستخدام الخوارزمية المتفق عليها ، والنص المشفر والمفتاح :

Encrypted text	H	R	M	T	P	F	T	R	T	S
Ascii code	72	82	77	84	80	70	84	82	84	83
displacement	1	3	5	5	3	1	1	3	5	5
Reversed Caesar algo	71	79	72	79	77	69	83	79	79	78
Explicit text	G	O	H	O	M	E	S	O	O	N

سي شارب C# هي لغة برمجةٍ حديثةٍ موجّهةٍ للكائنات، تم تطويرها في عام ٢٠٠٠ بواسطة أندريس هيجلسبرج Anders Hejlsberg في Microsoft، وهي لغة عامة الغرض مصممة لتطوير التطبيقات على أنظمة التشغيل الأساسية لـ Microsoft وتتطلب .NET framework على Windows للعمل.

يمكن تعلم اللغة ولكن ليس بشكل كلي كونها بحر عميق في البرمجة فهي تصنف على أنها High Level Language مما يعني أنها قريبة من لغة البشر في أكوادها (سطور البرمجية) ويمكن من خلاها المرور عن عقبة الأخطاء التي يمكن أن تحدث أثناء وضع الأكواد. وغالباً ما يُنظر إلى C# على أنها هجين يأخذ الأفضل من C وC++ لإنشاء لغة حديثة؛ فكونها لغةً موجَّهة [1,2,3] .

الفصل الثالث

تشفير النص وحفظه بتنسيق صورة ملونة RGB

CIPHER TEXT AS RGB COLOR IMAGE

الجزء العملي

3.1 مقدمة:

تم كتابة البرنامج في بيئة السي شارب #C لقراءة رسالة وتشفيرها وفك الشفرة باستخدام خوارزمية القيصر ويتكون البرنامج من الواجهات التالية :

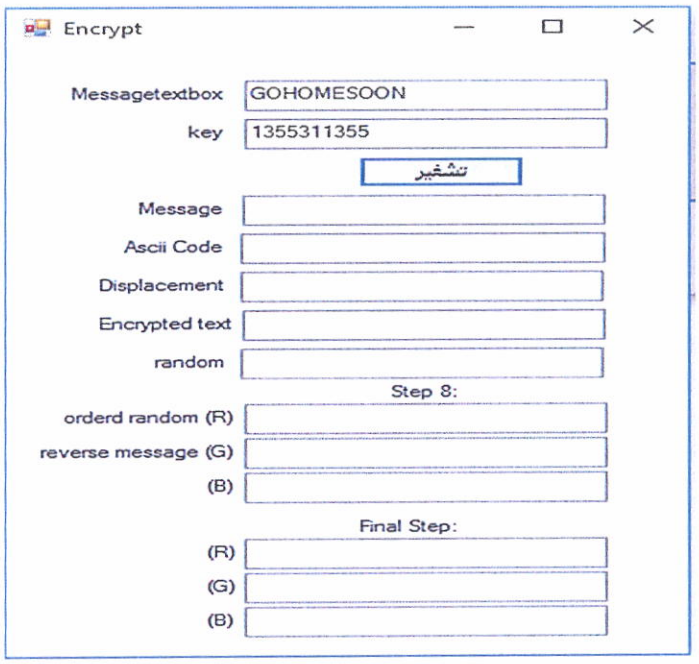
٣.٢ واجهة البرنامج الرئيسية:

الشكل (٣.١) يمثل واجهة البرنامج الرئيسية

هنا الواجهة الرئيسية للبرنامج حيث تتضمن جزئين اساسيين كما يلي:

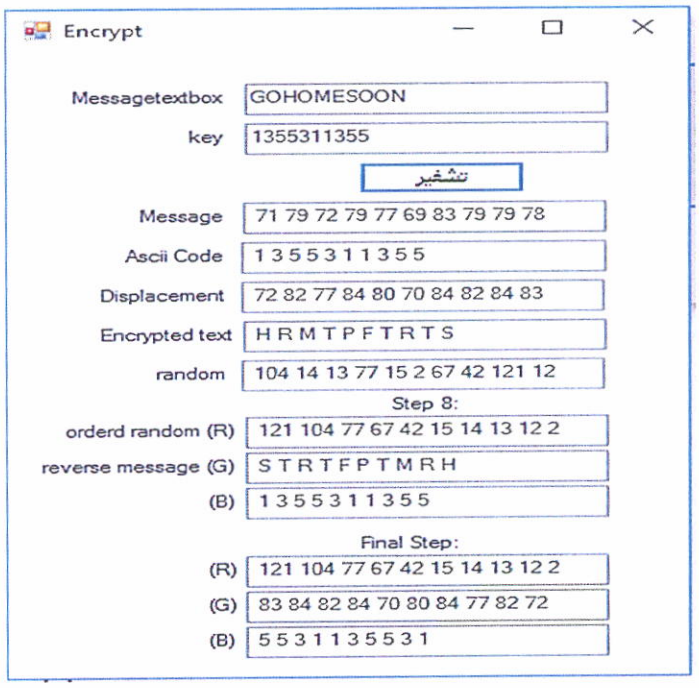
٣.٢.١ التشفير:

في البداية نقوم بادخال الرسالة المطلوب تشفيرها ثم نقوم بادخال مفتاح التشفير كما في الشكل (٣.٢).



الشكل(٣.٢) يمثل واجهة لعملية التشفير

وبعدها نضغط على تشفير ليقوم بالخطوات اللازمة لاجراء عملية التشفير كما في الشكل (٣.٣).



الشكل(٣.٣) واجهة الخطوات اللازمة لإجراء عملية التشفير

وسيقوم بخزن (R) و(G) و(B) في صورة RGB وتكون بصيغة bitmap (bmp) سنجدها مخزونة على الدرايف D كما في الشكل (٣.٤).

testnew	4/27/2019 2:06 PM	BMP File	1 KB

الشكل (٣.٤) الصورة الناتجة عن عملية التشفير بصيغة (BMP)

ان الصورة اعلاه ناتجة من عملية التشفير حيث تم فيها دمج (R) و(G) و(B) بصيغة بايتات وخزنها بصيغة bmp من خلال دالة الرسم الموجودة في السي شارب دالة (System.Drawing) وعند استرجاعها نعيد قراءة البايتات ونحولها الى صيغة ارقام ونستخرج (R) و(G) و(B) منها.

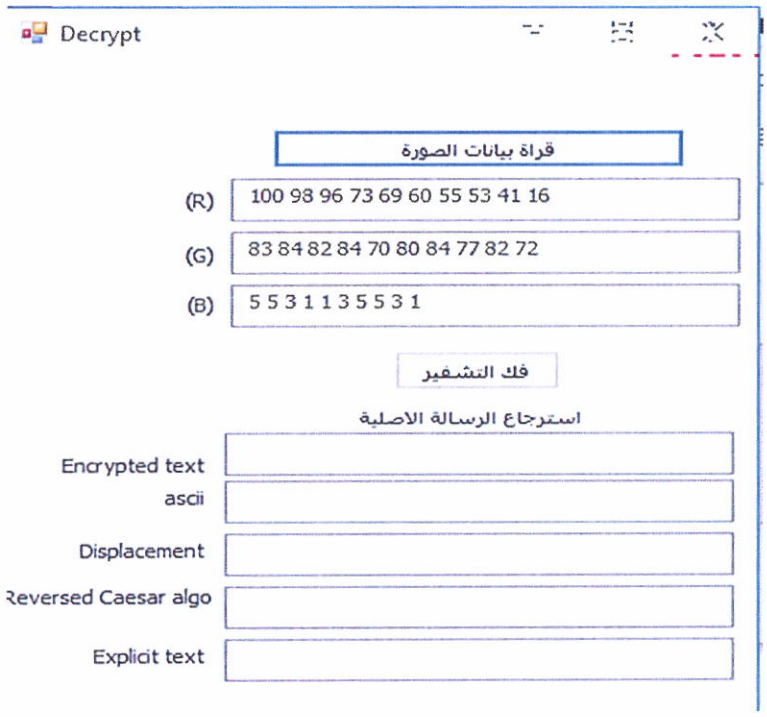
وعند الضغط على خصائصها نلاحظ:

فك التشفير:

الجزء الثاني عملية فك التشفير وتكون الواجهة الخاصة به موضحة كما في الشكل (٣.٥).

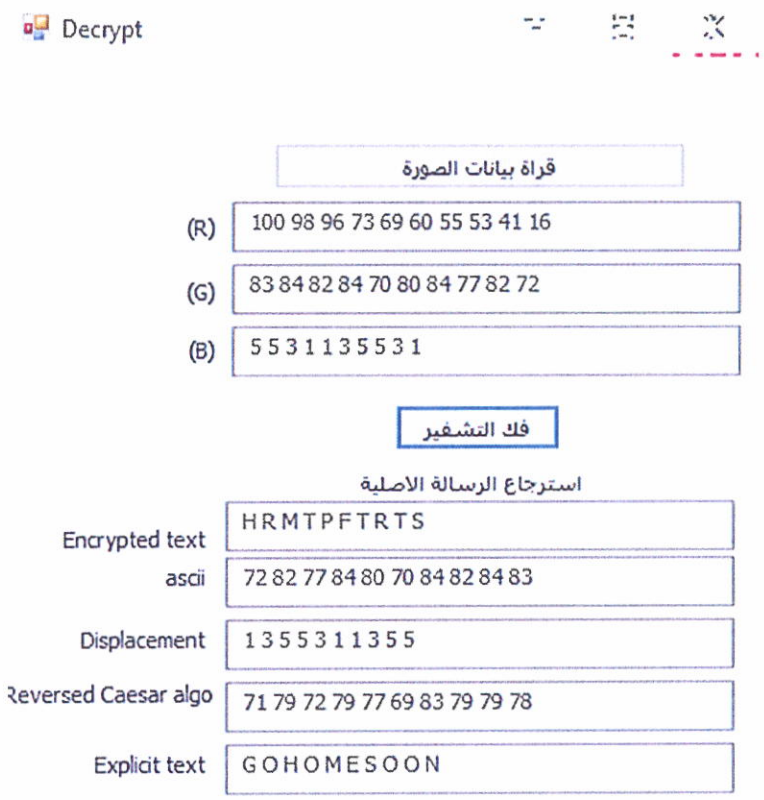
الشكل (٣.٥) واجهة قراءة بيانات الصورة (BMP) من خلال قراءة قيم R,G,B

في البداية نتاكد من ان الصورة الناتجة من عملية التشفير موجودة على القرص D ، بعد ذلك نقوم بقراءة بيانات الصورة من ملف الصورة من خلال قراءة قيم R,G,B كما في الشكل (٣.٦).



الشكل (٣.٦) يمثل واجهة لعملية فك التشفير

بعد ذلك نضغط على فك التشفير وسيقوم البرنامج باجراء عملية فك التشفير لينتج لنا الرسالة الاصلية كما في الشكل (٣.٧).

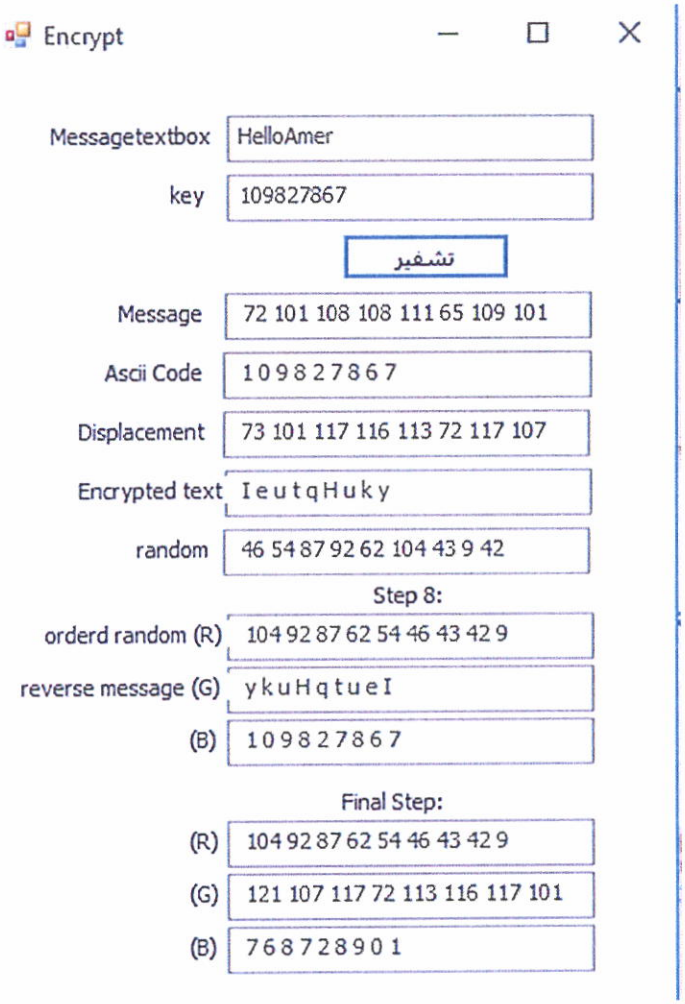


الشكل (٣.٧) يمثل واجهة الخطوات اللازمة لعملية فك التشفير

امثلة اخرى على عملية التشفير وفك التشفير:

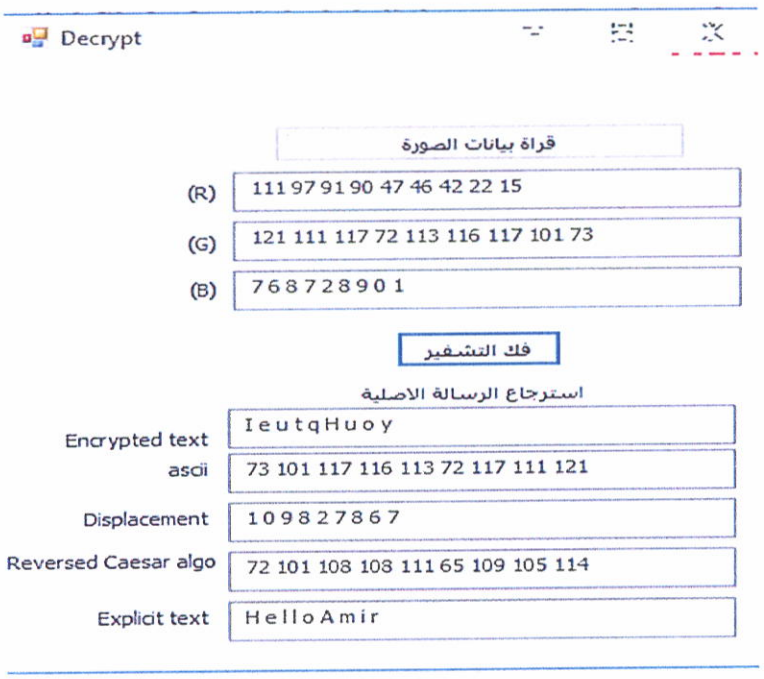
مثال ١:

التشفير:


Encrypt
Messagetextbox
HelloAmer
key
109827867
تشفير
Message
72 101 108 108 111 65 109 101
Ascii Code
1 0 9 8 2 7 8 6 7
Displacement
73 101 117 116 113 72 117 107
Encrypted text
I e u t q H u k y
random
46 54 87 92 62 104 43 9 42
Step 8:
orderd random (R)
104 92 87 62 54 46 43 42 9
reverse message (G)
y k u H q t u e I
(B)
1 0 9 8 2 7 8 6 7
Final Step:
(R)
104 92 87 62 54 46 43 42 9
(G)
121 107 117 72 113 116 117 101
(B)
7 6 8 7 2 8 9 0 1

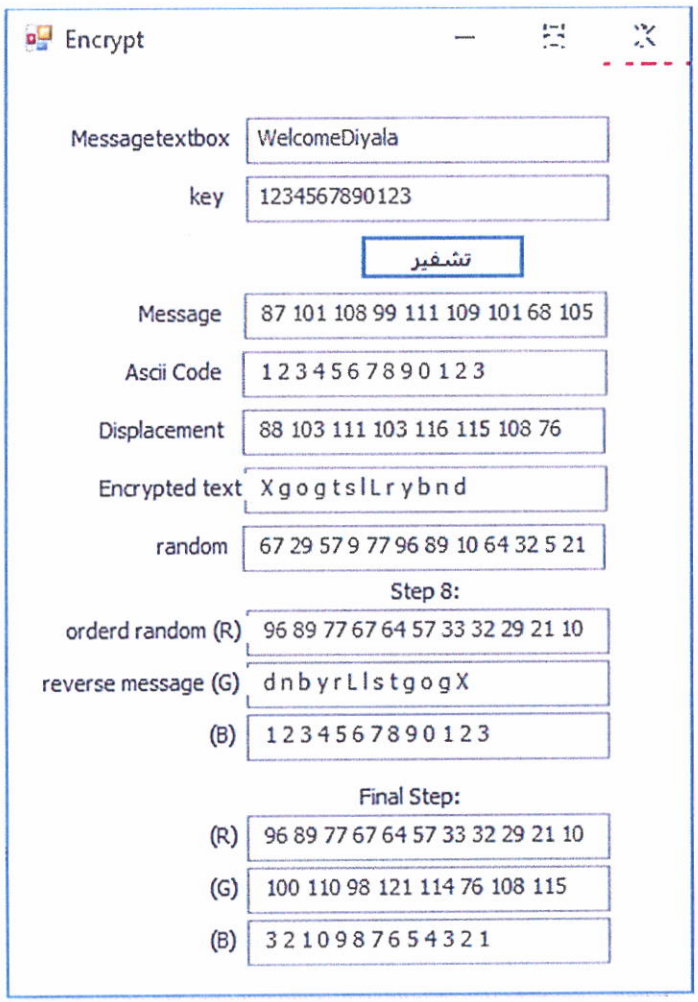
قراءة بيانات الصورة:

فك التشفير:

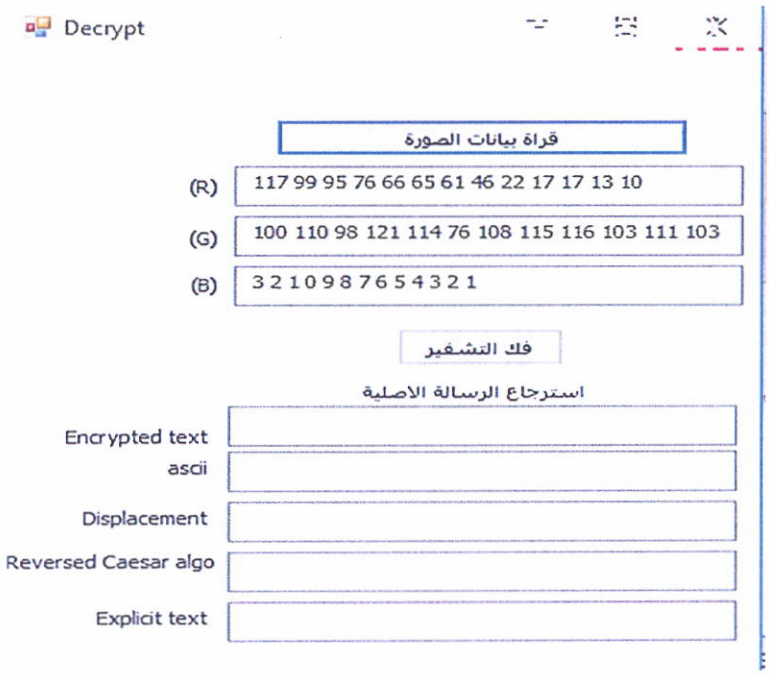
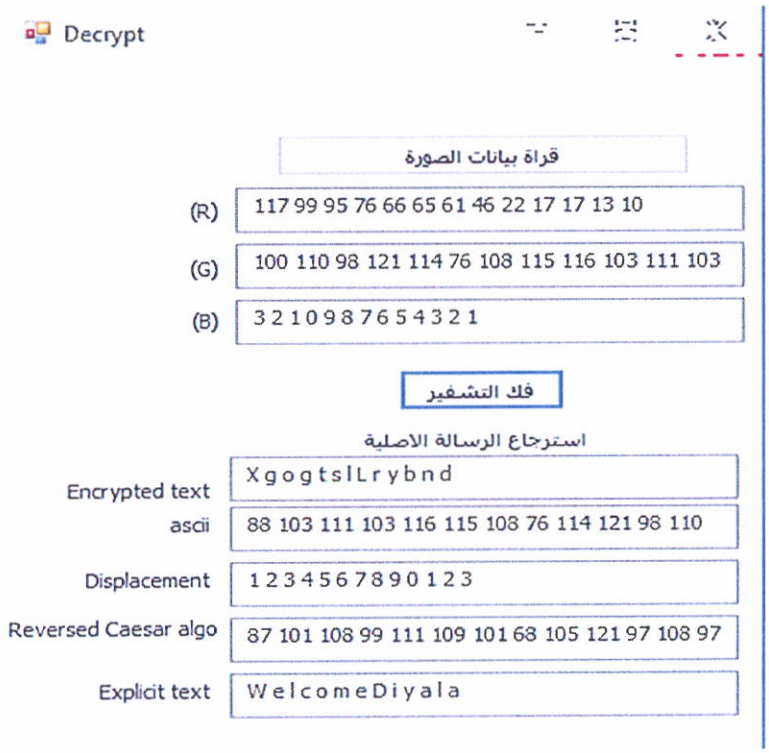


مثال٢:

التشفير:



قراءة بيانات الصورة:



٣.٢.٢ فك التشفير: