

**جامعة حلب**

**كلية الهندسة الكهربائية والإلكترونية**

**قسم هندسة الاتصالات**

***إخفاء البيانات الرقمية المشفرة في الصور الرقمية الملونة باستخدام AES, RSA***

مشروع أُعدَّ لنيل درجة الإجازة في هندسة الاتصالات

|  |
| --- |
| **بإشراف الدكتور المهندس عبد المنعم العبدالله**  **أستاذ في قسم هندسة الاتصالات**  **كلية الهندسة الكهربائية والإلكترونية جامعة حلب** |

**إعداد الطالبتان جودي ديري و راما شاهين**

2022 م

**الملخص**

مع تطور التكنولوجيا أصبح لدى كل شخص بيانات هامة خاصة به وتعتبر سرية للغاية، كالمستندات والملفات والصور وكلمات السر و رقم الحساب الشخصي وغيرها من البيانات الهامة. لذا تطور علمي التشفير و الإخفاء بشكل كبير لتحقيق سرية وأمان هذه البيانات, حيث يعمل التشفير على خلط المعلومات السرية بطريقة يعلم المستقبل فقط كيفية استرجاعها, أما الإخفاء فهو دمج المعلومات السرية مع ملف آخر ( نص, صورة, صوت, فيديو) بحيث لا يثير شبهة لأي طرف يحاول الحصول على البيانات السرية بوجودها اصلاً.

إن الإخفاء المعتمد على الصور الرقمية هو النظام الذي يساعد على نقل المعلومات السرية داخل الصور الرقمية.

في هذا العمل قمنا ببناء ومحاكاة نظام لإخفاء نص سري مشفر باستخدام AES و RSA ضمن ملفات الصور الرقمية الملونة باستخدام بيئة الماتلاب, حيث تم تنفيذ الآليات التالية:

1. **تطبيق RSA لتشفير النص السري و LSB لإخفاء هذا النص ضمن صورة ملونة و AES لتشفير الصورة.**
2. **تطبيق AES لتشفير النص السري و LSB لإخفاء هذا النص ضمن صورة ملونة و RSA لتشفير الصورة.**

بينت نتائج المحاكاة تفوق الطريقة الثانية من حيث السرعة على الطريقة الأولى نظراً لسرعة تنفيذ خوارزمية RSA بالمقارنة مع AES.

**الفصل الأول**

**الإخفاء في الصور الرقمية**

**1-1- مقدمة:**

يقدم هذا الفصل نظرة على أساسيات الإخفاء الرقمي كطريقة للاتصالات المخفية, حيث تم تعريف الإخفاء وتقديم نظرة عن تاريخ الإخفاء, وتوصيف الاختلاف بين أنواع الملفات الممكن استخدامها كملف غطاء, كما تم شرح كيفية ارسال رسالة سرية باستخدام الإخفاء, ونظراً لذلك من الممكن مراقبة الاتصال بين كلا طرفي الارسال من قبل المهاجمين, لذلك تم شرح أنواع المهاجمين المختلفة والتي تتعرض للإخفاء الرقمي. ثم تم تقديم تصنيفات طرق الإخفاء الأساسية وتقنياتها, حيث توضح تقنيات الإخفاء كيفية ادخال الرسالة السرية ضمن ملف الغطاء, أما تقنيات الإخفاء في الشبكة فتوضح كيفية إخفاء المعلومات السرية على الشبكة.

ومن أجل قياس فعالية تقنية الإخفاء, يتم قياس بعض الخصائص الأساسية لتقنية الإخفاء. وأخيراً تم تعريف وشرح تقنيات التحليل المستخدمة لإفشال الإخفاء.

**1-2- تعريف الإخفاء:**

يعرف الإخفاء بأنه الكتابة السرية حيث يتكون من كلمتين اغريقيتين Steganos والتي تعني السرية, graphy والتي تعني الكتابة.

يعرف الإخفاء عملياً بأنه إدخال المعلومات السرية في حوامل زائفة تبدو بريئة (رسائل غطاء) بطريقة لا يمكن من خلالها رؤية أو اكتشاف وجود المعلومات المخفية بالوسائل الإدراكية أو الإحصائية. تكون عادة البيانات السرية إما كنص صريح أو ملف مشفر أو أي نوع من البيانات والتي يمكن إخفاؤها في الوسائط الرقمية, ثم تتم ترجمة هذه البيانات السرية إلى الصيغة الثنائية.

يعتبر الإخفاء الرقمي علم متعدد الاختصاصات حيث أنه يتألف من طرق ضغط البيانات والإشارة الرقمية, نظرية المعلومات, نظرية تشفير الإشارة الرقمية, نظرية الاتصالات الرقمية, معالجة الإشارة الرقمية, نظرية ادراك الرؤية البشرية, وجميعها مستخدمة للاحتياجات الأمنية للمعلومات.

**1-3- نظرة تاريخية:**

بدأت استخدامات هذا العلم في عهد الإغريق في حدود 700سنة قبل الميلاد, وذلك بكتابة الرسائل السرية على الأحجار أو الجلود وإخفاؤها في بطون الحيوانات, ومن ثم ارسالها بعد اتفاق مسبق بين الطرفين.

وكان بعض الملوك يكتب الرسالة على الخشب ثم يضع فوقها الشمع فتظهر كأنها ألواح خشبية مشمعة وهذه الألواح كانت تستعمل للكتابة في العصر الروماني. كذلك استخدم قدماء الصينيين, وفراعنة مصر والعرب علم الإخفاء بطرق مختلفة, وفي سنة 440 قبل الميلاد قام أحد القادة بحلق رأس أحد خدامه الموثوق بهم ووشم على رأسه رسالة اختفت بعد أن نمى شعره عليها.

في القرن التاسع عشر الميلادي أصبح لدى معظم الدول الأوربية خدمات سرية وظهر آنذاك ما عرف باسم الغرف السوداء, ومهمتها تفحص الرسائل الخاصة بالغرباء والمشبوهين.

ظهرت طرق كثيرة لعملية إخفاء البيانات منها:

* **الحبر السري:** يتم كتابة الرسالة المراد إخفائها بهذا الحبر بحيث لا يمكن رؤية الرسالة إلا بطرق معينة كتعريضها للضوء وفق زاوية معينة أو استخدام مادة كيميائية معينة, وكمثال عنها في عام 1940 اكتشف الإنكليز رسالة مكتوبة بالحبر السري كتبها جاسوس ألماني من مدينة هافانا بكوبا يصف مكان سفن الحلفاء وعددها.
* **طريقة Null Cipher:** وهي تقوم بإخفاء الرسالة الأصلية في كمية كبيرة من النصوص.
* **طريقة التعمية:** كأن نتفق على أن كلمة الفريق تعني العلم والعربي تعني نور, فعندما نقول الفريق العربي فنقصد العلم نور.

وعند ظهور نهضة الحاسبات الالكترونية والتكنولوجية دخل فن الإخفاء إلى عصر جديد يطلق عليه بالعصر الرقمي حيث أول مرة تم استخدم هذا المصطلح في الأوساط العلمية يعود إلى عام 1994 من قبل  [Johannes Trithemius](http://en.wikipedia.org/wiki/Johannes_Trithemius)في أطروحته Steganographia التي تحدث فيها عن علم التعمية وعلم التشفير.

**1-4- ملفات الغطاء المستخدمة في الإخفاء:**

تمثل ملفات الغطاء الصندوق (الوسيط) الحامل للبيانات المخفية, وذلك يؤدي إلى تعديل بعض الخصائص لهذه الملفات الحاملة [5]. يجب أن تبقى هذه التعديلات غير محسوسة أي يجب أن يبقى مظهر ملف الغطاء سليماً بعد إجراء الإخفاء للبيانات السرية, وكنتيجة لذلك لا يمكن أن تستخدم كل أنواع الملفات كملف غطاء, أي يتم اعتماد ملفات غطاء حاوية على مناطق فائضة تكون كافية لاستبدالها بالرسالة السرية. هناك تنوع لملفات الغطاء المستخدمة في الإخفاء مثل ملفات HTML, وملفات XML, وعناوين TCP, كما يوجد عدة أنواع للوسائط الرقمية (ملف صورة, صوت, فيديو, نص) مستخدمة أيضاً في الإخفاء.

تعتمد كمية المعلومات المخفية ضمن ملف الغطاء (الوسيط) على حجم هذا الملف, ولذلك يعتبر ملف الغطاء كمكون أساسي لأنظمة الإخفاء.

**1-5- مكونات أنظمة الإخفاء:**

إن مكونات أي نظام أخفاء هي (وهي موضحة بالشكل (1-1)):

1. ملف الغطاء
2. المعلومات السرية
3. خوارزمية الإخفاء



**الشكل(1-1): مكونات نظام الإخفاء**

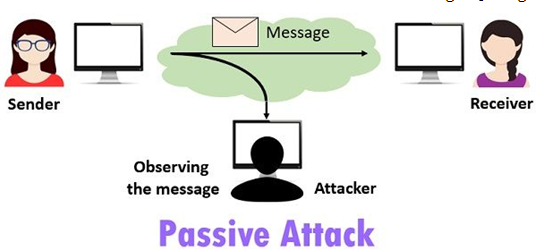
**1-6- أنواع قرصنة أنظمة الإخفاء:**

يعترض مهاجم الإخفاء الملفات المخفية في قنوات الاتصال لكشف الرسائل المخفية داخل هذه الملفات, حيث تصنف هجمات الإخفاء إلى ثلاثة أنواع, ولذلك يوجد ثلاث سيناريوهات لمواجهتها, حيث تعالج التقنية الأولى حماية نظام الإخفاء ضد كشف الرسالة في الهجوم السلبي, أما التقنية الثانية فتحمي الرسالة ضد الكشف و التعديل من الهجوم الفعال, بينما تهدف التقنية الثالثة لحماية نظام الإخفاء ضد التزوير من قبل الهجوم الخبيث [7].

**1-6-1- الهجوم السلبي:**

يراقب المهاجم السلبي الاتصالات فقط بدون أي تدخل, بمعنى آخر إذا تم تقييد المهاجم من تعديل محتوى الرسالة في الملف المخفي خلال إجراء الاتصال عندها يسمى مهاجم سلبي.

يستطيع المهاجم السلبي أن يستلم الرسالة فقط, لذلك سيتم قطع الاتصال السري إذا شك المهاجم بحدوث مثل هذا الاتصال.



**الشكل(2-1): الهجوم السلبي**

**1-6-2- الهجوم الفعال:**

هو الهجوم الذي يتمكن فيه المهاجم من تعديل محتوى الملف المعمى خلال عملية الاتصال. بمعنى آخر يقوم الهجوم الفعال بتعديل وتشويه الملف المعمى خلال الاتصالات السرية بهدف منعها حتى وإن لم يشك المهاجم الفعال بوجود اتصالات سرية, فمن الممكن أن يعدل ويشوه الملف المخفي بهدف تشويه الرسالة السرية المنقولة إن وجدت.

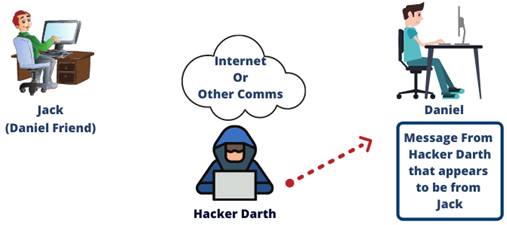


**الشكل(2-1): الهجوم الفعال**

تعرف أنظمة الإخفاء المقاومة لهذا النوع من الهجوم والمحافظة على البيانات السرية المنقولة من إمكانية القراءة بأنها أنظمة إخفاء متينة. يستخدم هذا النوع من الأنظمة في تطبيقات التوثيق والعلامة المائية أكثر من استخدامه كطريقة اتصالات سرية.

**1-6-3- الهجوم الخبيث:**

هو الهجوم الذي يتظاهر فيه المهاجم بأنه أحد طرفي الاتصال خلال عملية الاتصال السري. لذلك في هذا النوع من الهجوم بإمكان المهاجم تمرير رسالته إلى الطرف الآخر باعتباره طرف اتصال محدد.



**الشكل(3-1): الهجوم الخبيث (التنكر)**

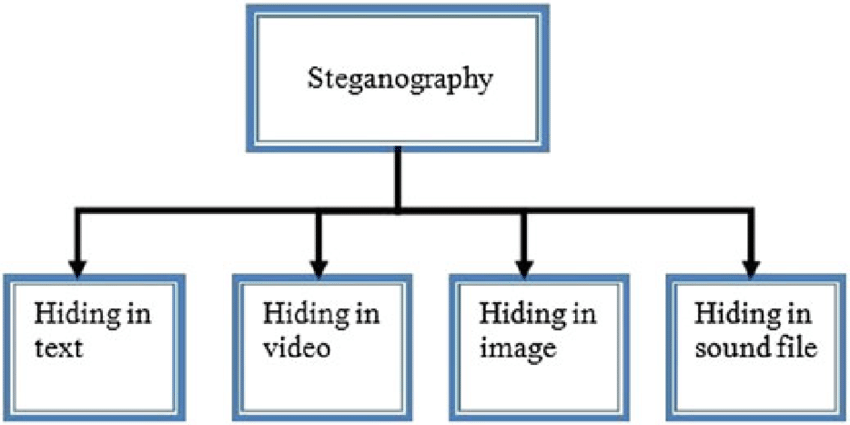
هذا النوع من الهجوم صعب ونادر الحدوث من بين الأنواع الثلاثة للهجمات كونه يحتاج إلى معرفة مفتاح الإخفاء المشترك بين أطراف الاتصال, بالإضافة لمعرفة مفتاح التشفير الخاص بالمرسل.

**1-7- طرق تصنيف إخفاء المعلومات:**

يتم تصنيف طرق إخفاء المعلومات إلى طريقتين, حيث تعتمد الطريقة الأولى على نوع الغلاف الغطاء, بينما الثانية فتعتمد على طريقة الإخفاء [7].

**1-7-1- التصنيف حسب نوع الملف الغطاء:**

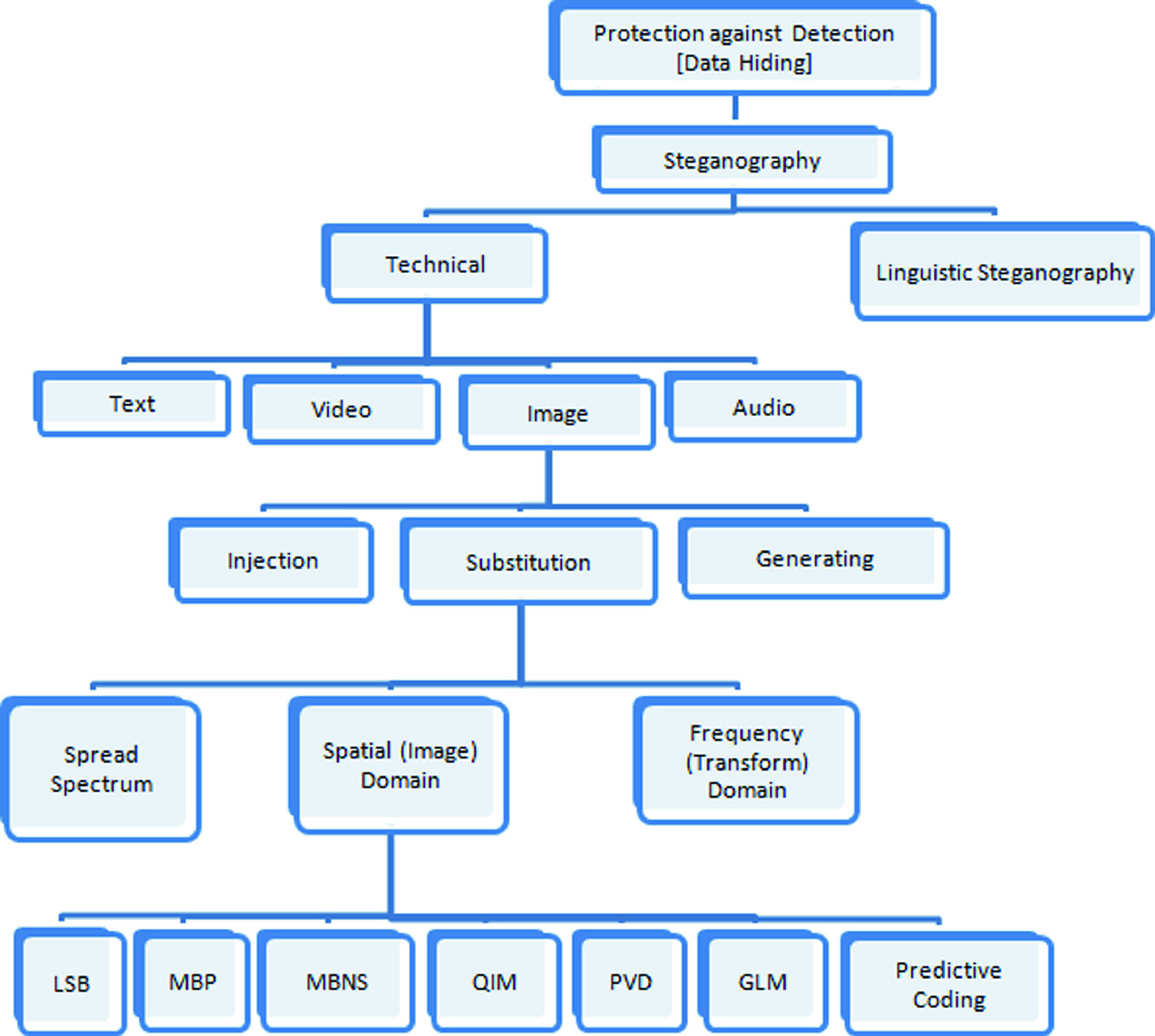
يوجد العديد من الوسائط الرقمية المستخدمة كملف غطاء, وتختلف خصائص ملفات الغطاء عن بعضها, والتي تتحكم بدورها بكيفية إخفاء البيانات السرية ضمنها. من الممكن استخدام ملفات (صورة, صوت, نص, فيديو,.....) كملفات لإجراء عملية الإخفاء.



**الشكل(4-1): تصنيف طرق الاخفاء وفقاً لنوع ملف الغطاء**

**1-7-2- التصنيف حسب طريقة الإخفاء:**

يمكن تصنيف أنظمة الإخفاء تبعاً لطريقة إخفاء البيانات السرية بغض النظر عن نوع ملف الغطاء, ومن هذه التقنيات:



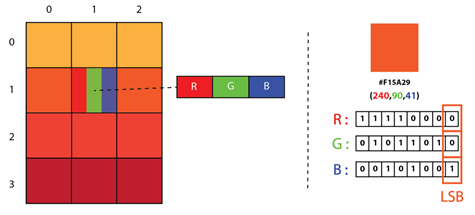
**الشكل(5-1): تصنيف طرق الاخفاء وفقاً للطريقة**

**1-7-2- تقنيات الاستبدال:**

**1-7-2-1- في المجال الحيزي:**

ومن أشهرها الاخفاء في البت الأفل أهمية حيث يتم فيها استبدال المعلومات الإضافية أو غير الهامة في الملف الغطاء بالمعلومات السرية دون أن يؤثر ذلك على جودة الملف أو إضافة ضجيج إضافي. تمتلك الملفات الرقمية عدد كبير من البتات غير الهامة (البتات الأقل أهمية Least Significant Bits- LSB).

تعتبر تقنية (LSB) تقنية مجال فراغي كون البتات تدخل مباشرة ضمن ملف الغطاء, كما أنها تقنية سريعة وسهلة الاستخدام, وهي من التقنيات الأكثر شيوعاً في الإخفاء الرقمي وخاصة مع الصور الرقمية مثل (bmp, Gif, jpg).

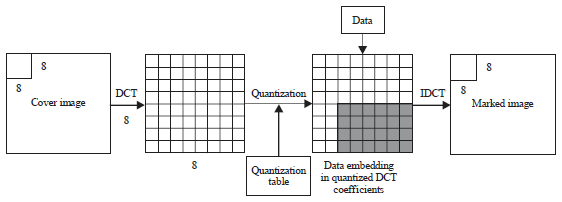


**الشكل(6-1): الاخفاء في البت الأقل أهمية**

**1-7-2-2- تقنيات مجال التحويل:**

تخفي تقنيات مجال التحويل البتات السرية في أماكن هامة من الملف الغطاء, ولذلك تعتبر أكثر متانة للهجمات من تقنيات المجال الفراغي. يوجد عدة أنواع للتحويل إلى المجال الترددي, منها تحويل تجيب المتقطع (DCT), تحويل الموجي المتقطع (DWT), وتحويل فورييه المتقطع (DFT), والتي تستخدم لإدخال الرسائل السرية في الصور الرقمية.

تنتشر الرسالة السرية على كامل الصورة ولا تكون مركزة في منطقة محددة والذي يؤدي بدوره إلى تغيير كامل الصورة.



**الشكل(7-1): الاخفاء في معاملات الـ DCT**

**1-7-2-3- تقنيات الطيف المنتشر:**

تم تعريف اتصالات الطيف المنتشر من قبل (Marvel) بأنه عملية انتشار الإشارة ذات عرض الحزمة الضيقة عبر ترددات الحزمة العريضة. يعتبر المجال الترددي في إخفاء الطيف المنتشر للملف الغطاء كقناة اتصال بينما تعتبر الرسالة السرية كإشارة يتم ارسالها عبر هذه القناة. هذه التقنية منيعة نسبياً ضد تعديل الملف المخفي أو إزالة الرسالة السرية.

**1-7-3- التقنيات الإحصائية:**

تعتمد هذه التقنية على إدخال بت واحد فقط من البيانات السرية في الملف الغطاء. فلإخفاء (1) نقوم بتغيير بعض الخصائص الإحصائية للملف الغطاء (على سبيل المثال الانتروبية), بينما يترك ملف الغطاء سليماً لإخفاء (0). لذلك تعتمد هذه التقنية على مقدرة المستقبل على التمييز بين التغيرات من عدمها على الملف الغطاء.

**1-7-4- تقنيات التشويه:**

يحتاج المستقبل في هذه التقنية إلى الملف الغطاء الأصلي ليستخلص الرسالة الأصلية من الملف المعمى, حيث أن الرسالة الأصلية تمثل الفرق بين الملف الغطاء المعمى والملف الغطاء الأصلي.

**1-7-5- تقنيات توليد الغطاء:**

لاتحتاج هذه التقنية إلى ملفات غطاء بل تقوم بتوليد الملف المعمى اعتماداً على المعلومات السرية.

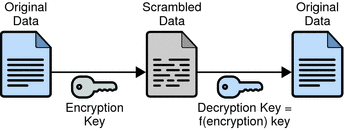
**الفصل الثاني**

**أنظمة التشفير**

**2-1- مقدمة:**

يعد التشفير وحدة البناء الأساسية لأمن البيانات. وهو أبسط الطرق وأهمها لضمان عدم سرقة معلومات نظام الحاسوب أو قراءتها من جانب شخص يريد استخدامها لأغراض ضارة.

يعرف التشفير بأنه " تحويل نص مفهوم مكتوب باستخدام أبجدية لغوية (أو عدة أبجديات) إلى شكل آخر غير مفهوم ".الشكل (2-1).



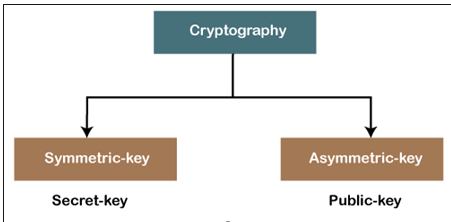
**الشكل(2-1) المبدأ العام للتشفير**

يُستخدم تشفير البيانات لتأمينها على نطاق واسع من قبل المستخدمين الأفراد والشركات الكبيرة بغرض حماية معلومات. قد تشمل تلك المعلومات أي شيء من بيانات الدفع إلى المعلومات الشخصية. ويتم استخدام برنامج تشفير البيانات، المعروف أيضًا باسم "خوارزمية التشفير" أو "التشفير" فحسب، لتطوير مخطط تشفير لا يمكن اختراقه نظريًا إلا بقوة حوسبية هائلة.

**2-2- تصنيف خوارزميات التشفير:**

تصنف خوارزميات التشفير بشكل أساسي إلى نوعين:

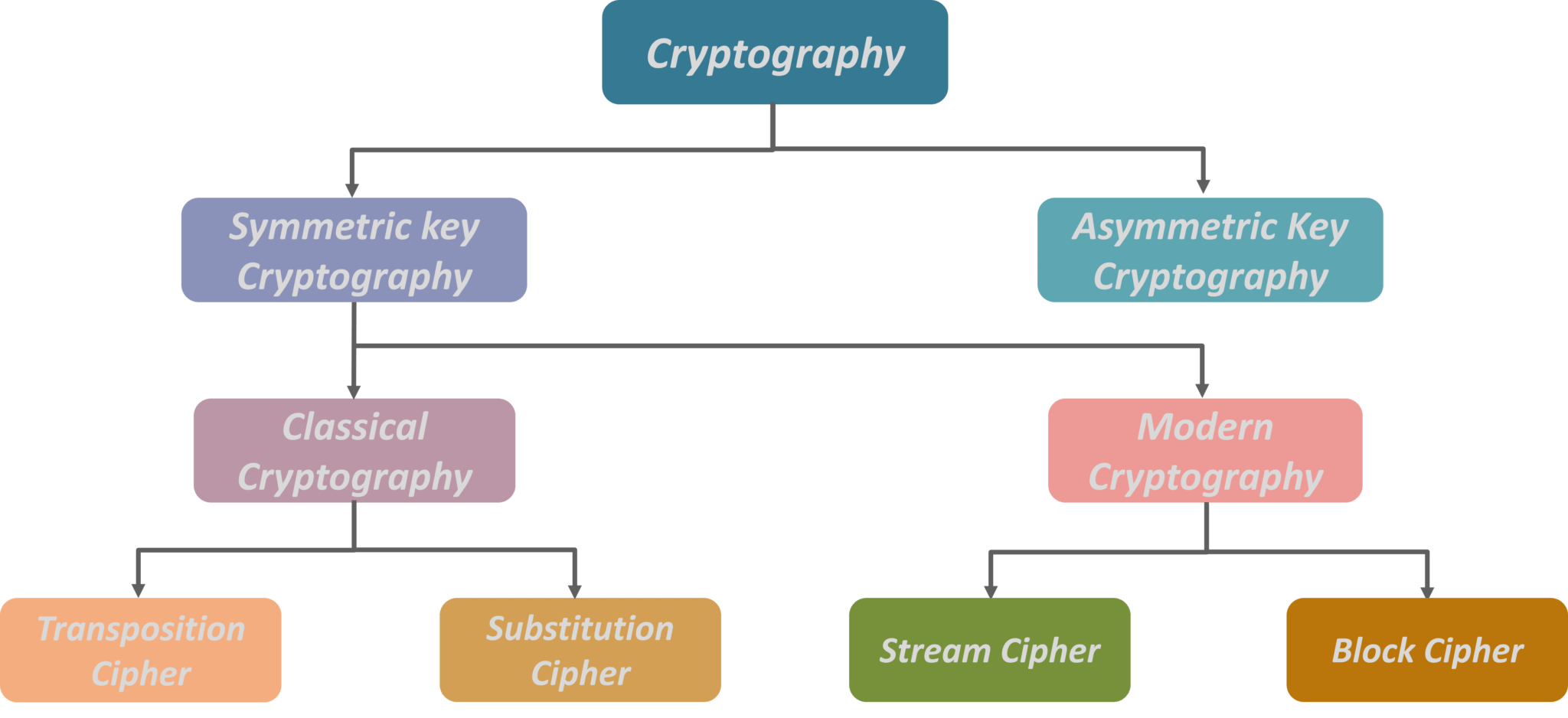
1. متناظرة وتسمى خوارزميات التشفير بالمفتاح السري.
2. غير متناظرة وتسمى خوارزميات التشفير بالمفتاح العام.



**الشكل(2-2) تصنيف خوارزميات التشفير**

كما تصنف خوارزميات التشفير المتناظر إلى:

1. خوارزميات تقليدية (النقل و الاستبدال)
2. خوارزميات حديثة



**الشكل(2-3) التصنيفات الأساسية لخوارزميات التشفير المتناظر**

**2-3- تصنيف أنظمة التشفير الحديثة حسب طريقة معالجة البيانات:**

بعض الأنظمة تناسب طبيعة بنيتها المعالجة الكتلية بحجم محدد, والأنظمة الأخرى يناسبها تطبيق البيانات على شكل سيل مستمر, و ذلك بحسب التطبيقات التي وجدت لأجلها.

1. **نمط** **التشفير المستمر :**

يتم معالجة الرسالة على شكل سيل مستمر من البتات, و تتم المعالجة هنا على مستوى البت. و تعتبر أنظمة التشفير المستمرة من أكثر الأنظمة استخداماً, وذلك لما تتميز به من خواص مهمة منها عدم تضاعف الأخطاء في حال حدوثها، ولذلك تستخدم في تشفير الصوت, والصورة, والفيديو إضافة لتشفير النصوص والبيانات. تشترك معظم أنظمة التشفير المستمرة باستخدامها مجموعة مسجلات الإزاحة ذات تغذية عكسية خطية, ومجموعة دوال ربط خطية, ولا خطية مختلفة لتوليد تتابعات شبه عشوائية لضمان عدم انتقال الخواص الإحصائية للنص الصريح إلى النص المشفر، حيث يتم هنا التشفير بت بعد بت بدالة متغيرة زمنية.

1. **نمط التشفير الكتلي** :

يتطلب نمط التشفير الكتلي تقطيع الرسالة إلى كتل من المعطيات بحجم ثابت (64 بت ,128 بت,......) , و يتم تشفير كل كتلة من هذه الكتل على حدى.

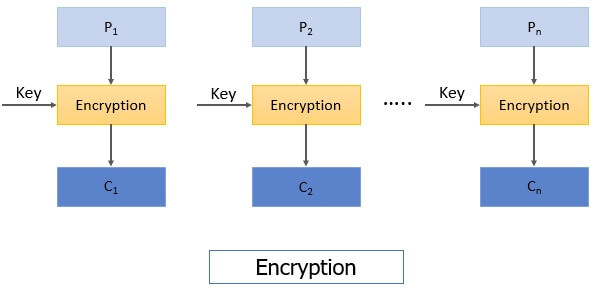
من المفيد ذكره أن التشفير الكتلي له مجالات تطبيق أوسع من التشفير المستمر, حيث أنه يناسب التطبيقات المبنية على شبكات الحواسيب. هناك أربعة أنماط معالجة أساسية:

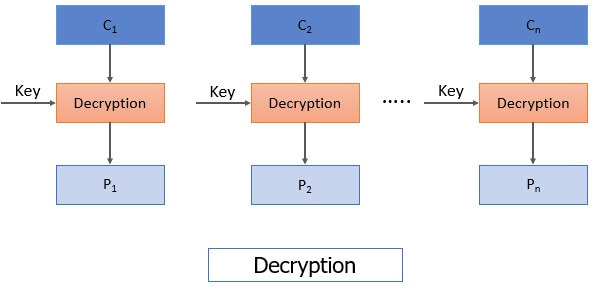
1. **نمط ECB Electronic Code Book)):**

خصائص هذا النمط:

1. في حالة استعمال مفتاح واحد لجميع الكتل, فإن تشفير كتل الرسالة المتماثلة يؤدي إلى كتل تشفير متماثلة.
2. يتم تشفير الرسالة على شكل كتل مستقلة (كتلة-كتلة).
3. عند حدوث خطأ (بت أو أكثر) ضمن كتلة مشفرة , فهو لا يؤثر على تفكيك الكتلة.

لتحسين هذا النمط لا بد من حشو الكتل ببتات إضافية و خلافه.

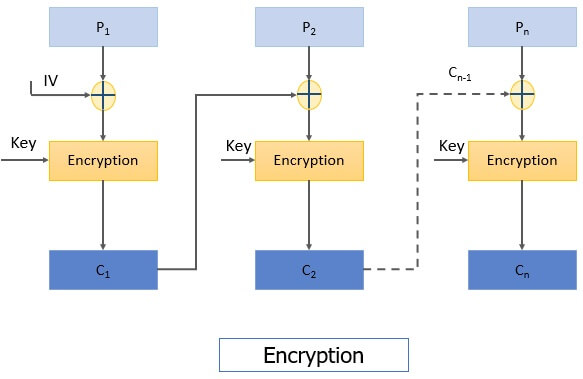


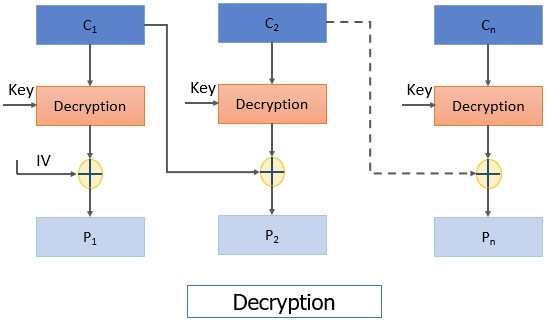


**الشكل (2-4) المخطط العام لنمط ECB**

1. **نمط (Cipher Block Chaining) : CBC**

يتم إنجاز تكافؤ شعاع الإقلاع باستخدام بوابة XOR , أي تقسم الرسالة إلى كتل وكل منها بحجم nبت , ويتم تطبيق الكتلة على بوابة XOR (عدم التكافؤ) مع شعاع الإقلاع (iv) , كما هو مبين في الشكل (2-5).





**الشكل (2-5) المخطط العام لنمط CBC**

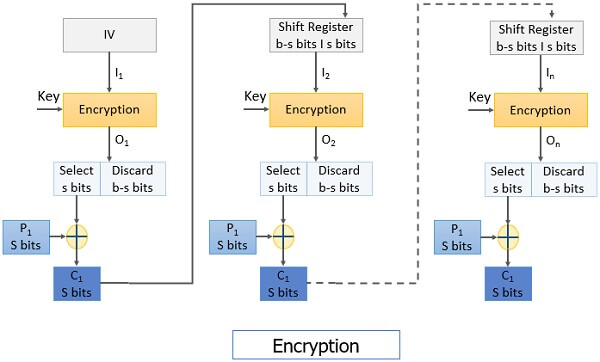
كل الكلمات المشفرة تعتمد على شعاع أولي iv, و عادة يتم توليده عشوائياً.

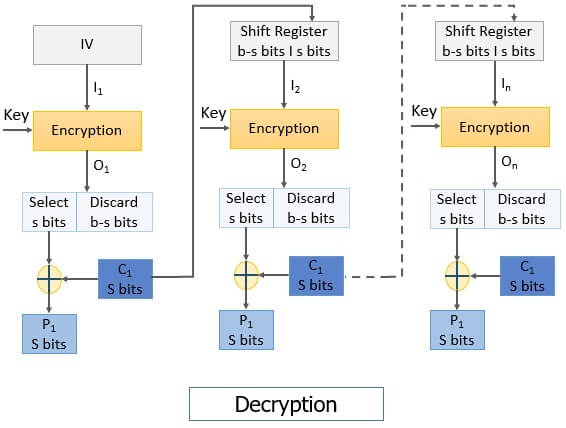
خصائص النمط CBC:

* 1. يمكن الحصول على كتل تشفير متماثلة في حال تطبيق نفس المفتاح k و شعاع الإقلاع (كلمة السر) (iv), ولكن تغيير المفتاح k أو تغيير كلمة السر iv سوف يؤدي إلى كتل تشفير مختلفة.
  2. كل كتلة تعتمد على الكتل السابقة ,كتلة التشفير ci تعتمد على جميع كتل الرسالة السابقة, ولهذا السبب فإن إعادة ترتيب كتل التشفير يؤثر على عملية التفكيك.
  3. إذا حصل خطأ في الكتلة ci عندئذ تفكك الكتلة ci و ci +1 بشكل خاطئ, بينما تفكك الكتلة ci+2 بشكل صحيح (السبب دارة XOR).

1. **نمط (Cipher Feedback Book): CFB**

يعتمد هذا النمط على مسجلات إزاحة بحجم 64bit. مسجل الإزاحة يجب أن يكون أطول من كتلة الرسالة, يناسب هذا النمط تشفير وإرسال وحدات من الرسالة s بت عادة تكون 8 بت, وهو حل يسمح بتحويل التشفير الكتلي إلى تشفير مستمر.

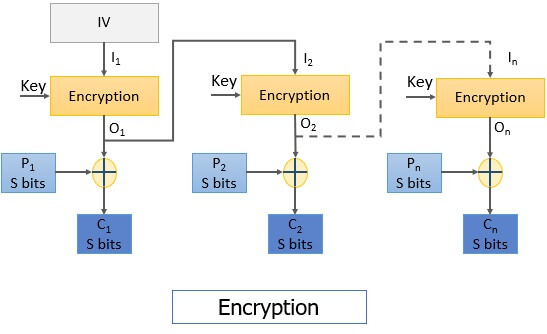


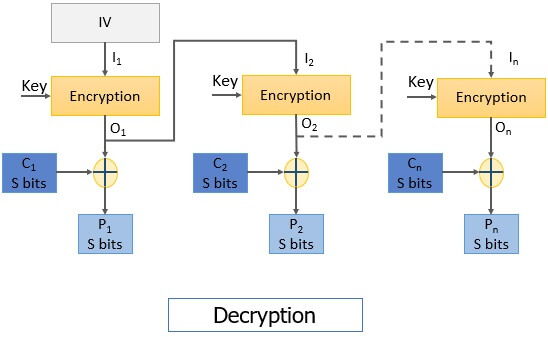


**الشكل (2-6) المخطط العام لنمط CFB**

1. **نمط (Output Feedback Book) OFB**

هذا النمط هو تعديل للنمط السابق عن طريق التغذية الخلفية لمسجل الإزاحة, حيث يتم تبديل شعاع الإقلاع, مما يؤدي إلى عدة كتل تشفير مختلفة لنفس الرسالة, وقد تخلص هذا النمط من تأثير انتشار الخطأ ضمن الكتل المتتالية، إذ أن حدوث خطأ في كتلة التشفير ci سوف يؤثر على تفكيك تلك الكتلة فقط , و الشكل (2-7) يبين مخطط هذا النمط , وبذلك يلائم هذا النمط التطبيقات التي ترغب في تجنب انتشار الأخطاء كاملة.

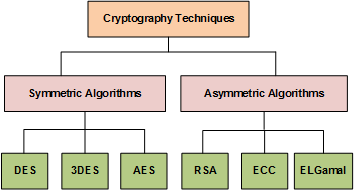




**الشكل (2-7) المخطط العام لنمط التشغيل OFB**

**2-4- تصنيف أنظمة التشفير الحديثة تبعاً لنوع المفتاح المستخدم:**

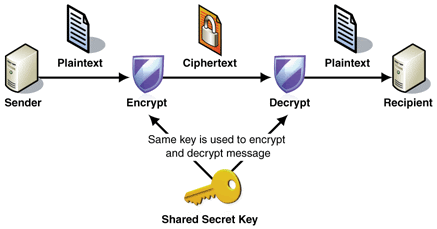
يعتمد هذا التصنيف على نوعية المفاتيح المستعملة في جهتي التشفير و فك التشفير, و يمكننا تقسيم الأنظمة إلى قسمين أساسيين, كما هو مبين بالشكل (2-8) , تشفير متناظر, و تشفير بالمفتاح العام.



**الشكل (2-8) أنظمة التشفير الحديثة**

**2-4-1- أنظمة التشفير المتناظر:**

تعتمد هذه الأنظمة على مفتاح واحد, وعادة ما يسمى بالمفتاح السري secret key , من أجل عملية التشفير, و فك التشفير.



**الشكل (2-9) مخطط التشفير المتناظر**

و حسب الشكل (2-8) هناك العديد من الخوارزميات التي تعمل بهذا الأسلوب سنذكر منها مايلي.

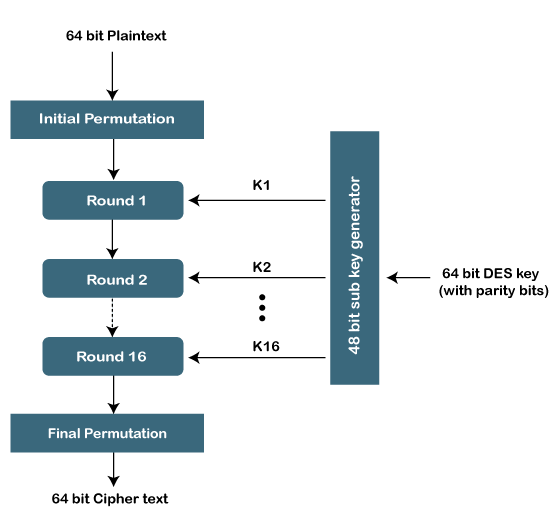
1. **خوارزمية التشفير DES (Data Encryption Standard)**:

إن خوارزمية DES تستخدم التشفير الكتلي، حيث تشفر كتل طولها bit 64, أي دخلها كتلة من النص الصريح بطول 64 bit, و خرجها كتلة من النص مشفر بطول 64bit.

تعتبر خوارزمية DES تطوير لنظام Luciefer المعمول به في شركة IBM عام 1973. و أصبحت DES معيارية عام 1977 .

تعتمد خوارزمية DES على مجموعة من الخصائص:

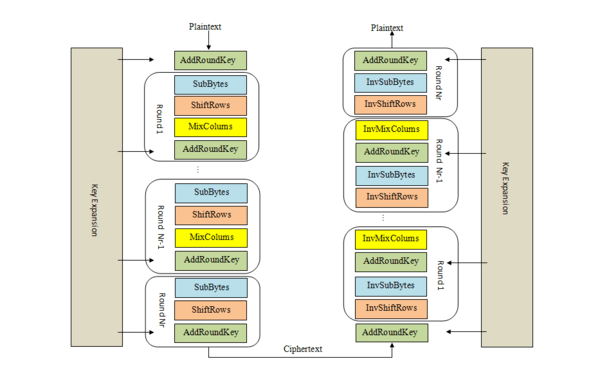
* حجم كتلة المعطيات 64 بت.
* حجم (طول) المفتاح 56 بتاً.
* تعتمد على مخطط مؤلف من 16 دورة كما هو مبين في الشكل (3-11), و لها بنية شبكة فيستل Feistel Network.
* تعتمد على مجموعة من المصفوفات لتحقيق التبادلات المطلوبة.



**الشكل(2-10) مراحل خوارزمية DES**

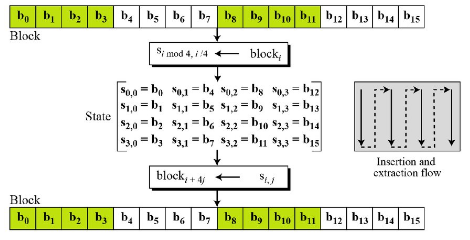
1. **خوارزمية التشفيرAES (Advance Encryption Standard)**:

هي نظام تشفير قياسي يمكن فيه اختيار طول المفتاح من أحد القيمbit 128،192،256 بشكل مستقل .وتوجد إمكانية استخدام الأطوال الثلاثة للمفاتيح مع تحديد طول الكتلة ليكون bit 128 فقط**.**



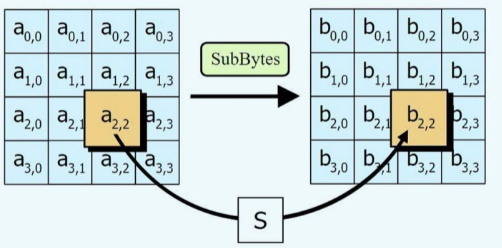
**الشكل(2-11) البنية الداخلية الصندوقية لخوارزمية AES**

حيث تمر عملية التشفير بـ 10 جولات ينفذ في كل جولة 4 عمليات وذلك بعد تشكيل مصفوفة الحالة State من النص الصريح كما في الشكل:



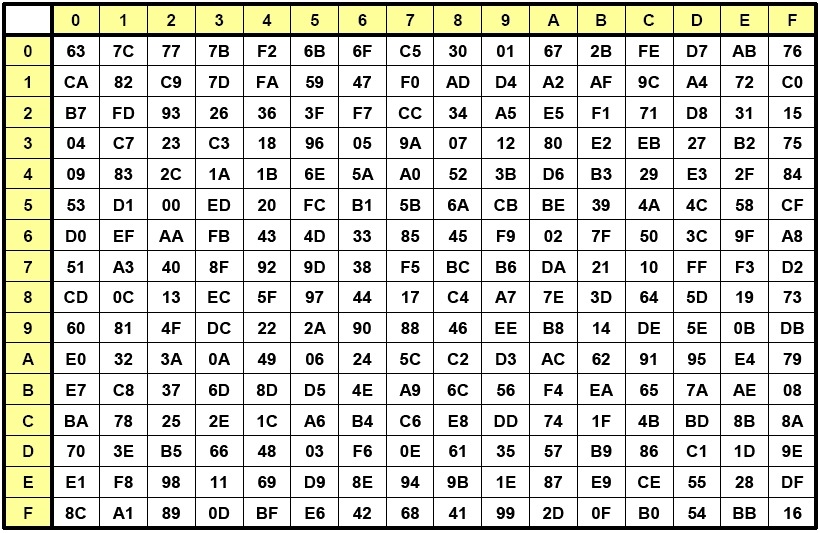
**الشكل(2-12) تحويل البلوك إلى مصفوفة وبالعكس**

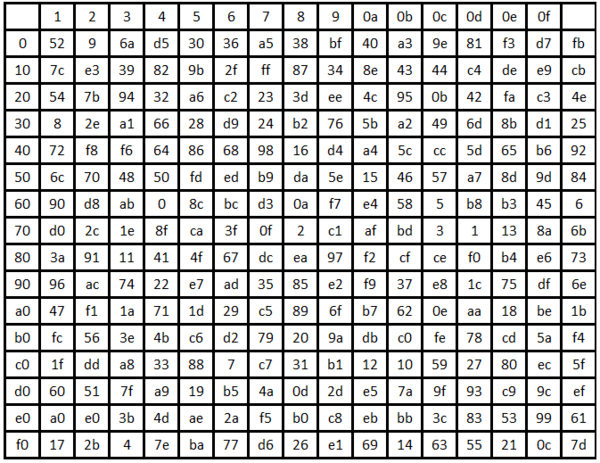
العملية الأولى: استبدال البايتات SubByte



**الشكل(2-13) عملية استبدال البايتات**

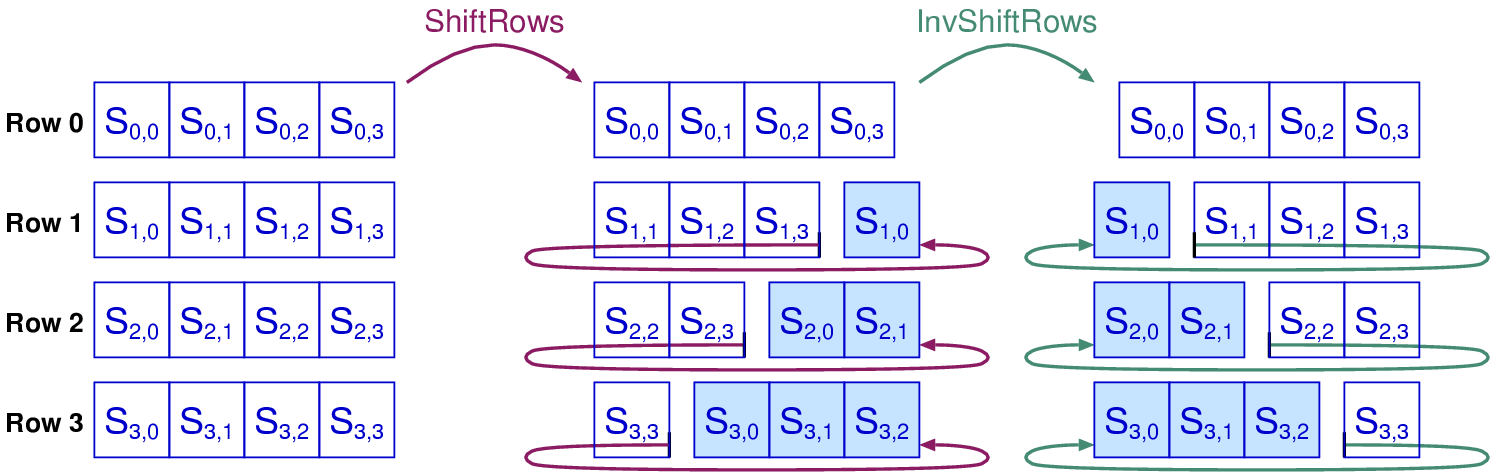
حيث تتم عملية التبديل وفق الجدول الأمامي في التشفير و وفق الجدول العكسي في فك التشفير والموضحين في الشكل التالي.





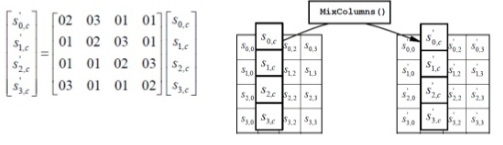
**الشكل(2-14) جدولي SubByte و InvSubByte**

العملية الثانية: إزاحة الأسطر Shift Row



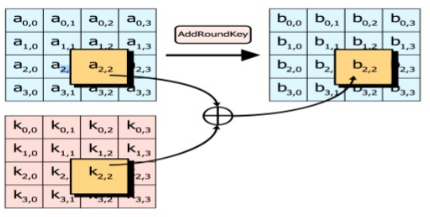
**الشكل(2-15) إزاحة الأسطر**

العملية الثالثة: مزج الأعمدة MixColumns



**الشكل(2-16) مزج الأعمدة**

العملية الرابعة: هي إضافة مفتاح الحلقة وذلك بعمل XOR بن مصفوفة الحالة ومصفوفة المفتاح

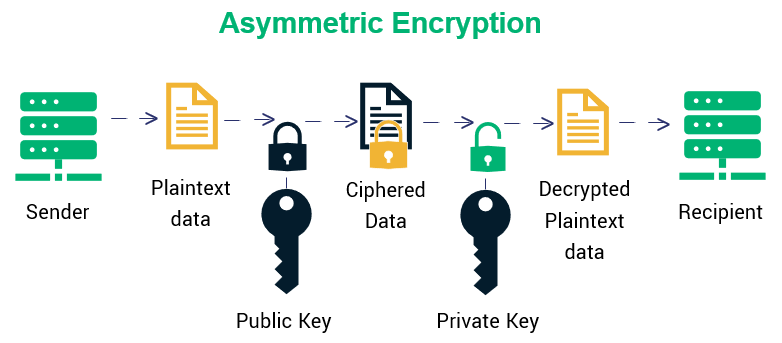


**الشكل(2-17) إضافة مفتاح الدورة**

مع الإشارة إلى أن الجولة الأخيرة لا تحتوي على عملية MixColumn.

**2-4-2- أنظمة التشفير بالمفتاح العام:**

هذه الأنظمة تعتمد على استخدام مفتاحين مختلفين أحدهما يستخدم في التشفير و يدعى المفتاح العام public key و يكون معلناً و غير سري, و الآخر يستخدم في فك التشفير و يدعى المفتاح الخاص private key, لقد حلت هذه الأنظمة مسألة توزيع المفاتيح التي كانت تعد مشكلة في التشفير المتناظر.



**الشكل (2-18) مخطط التشفير غير المتناظر**

هناك العديد من الخوارزميات التي تعمل وفق هذه النوع سنذكر منها ما يلي:

1. **خوارزميةRSA :**

يعود تصميم خوارزمية RSA إلى الفريق المؤلف من Rivest-Shamir-Adlman عام1977, وهي نظام تشفير يعتمد المفتاح العام, و بذلك يتخلص من مشكلة توزيع المفاتيح الموجودة في الأنظمة السابقة ذات التشفير المتناظر. و يمكن استعمالها لتشفير النصوص أو كنظام مصادقة Authentication.



**الشكل (2-19) المبدأ العام لخوارزمية RSA**

**وصف الخوارزمية:**

إن RSA هي نظام تشفير كتلي يشفر النص على شكل كتل, حيث تكون الرسالة و النص المشفر عبارة عن أعداد صحيحة. تأخذ عمليتا التشفير وفك التشفير الشكل التالي, حيث M هي كتلة النص الصريح و C هي كتلة النص المشفر:

يجب أن يعرف كل من المرسل والمستقبل القيمة n, و يجب أن يعلم المرسل القيمة e, في حين أن المستقبل فقط هو الذي يعرف القيمة d. وبالتالي سيكون لدينا خوارزمية تشفير عمومية ذات مفتاح عمومي هو , ومفتاح خصوصي هو .

لكي تكون هذه الخوارزمية مرضية كخوارزمية تشفير بالمفتاح العام, يجب أن تلبي المتطلبات التالية:

1. يجب أن يكون من الممكن إيجاد القيم e و d وn بحيث تحقق من أجل جميع قيم M التي تكون أصغر من .
2. يجب أن يكون من السهل نسبياً حساب و من أجل جميع قيم .
3. يجب أن يكون من غير المجدي تحديد قيمة d انطلاقاً من e و n فقط.

كما يوضح الشكل (2-20) مثالاً على تطبيق هذه الخوارزمية. تم توليد المفتاح في هذا المثال كما يلي:

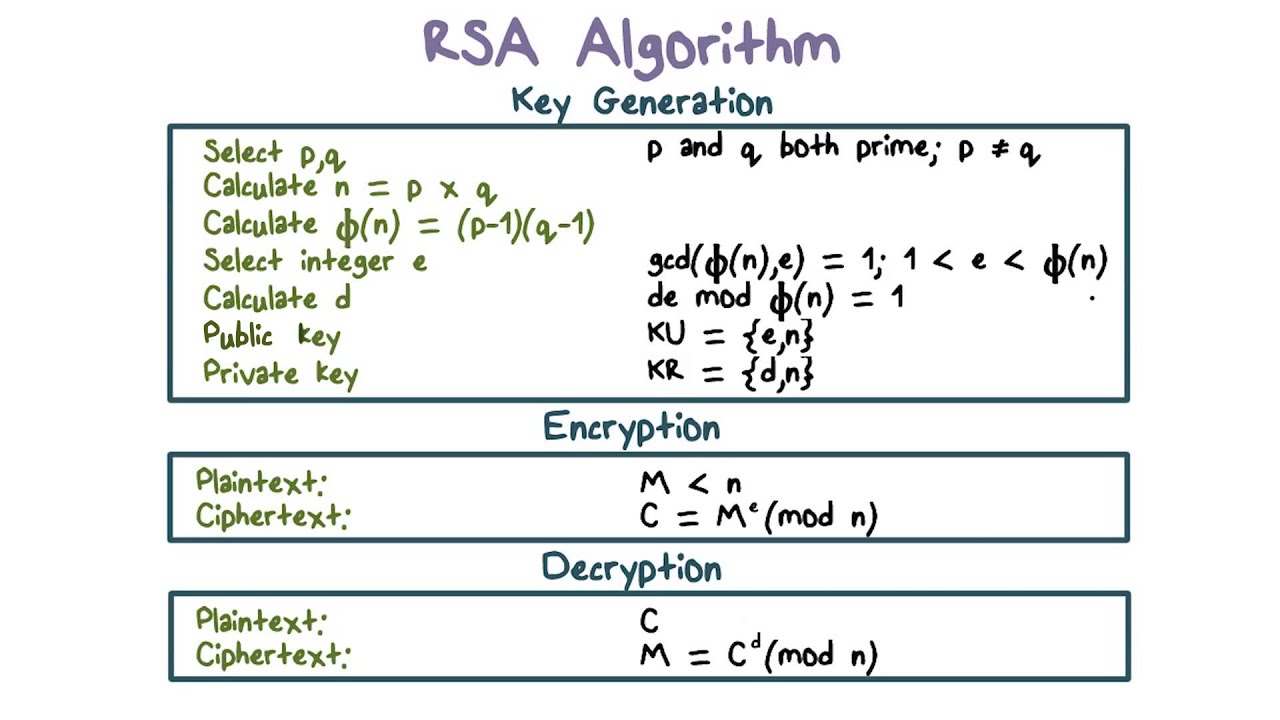
1. نختار عددين أوليين p=17 و q=11

2. نحسب .

3. نحسب .

4. نختار e بحيث يكون أولياً بالنسبة لقيمة وأصغر منها, وفي هذا المثال اخترنا e=7.

5. نحدد قيمة d بحيث يكون de=1 mod 160 وبحيث يكون d< 160. والقيمة الصحيحة ستكون d=23, ذلك لأن , يمكن حساب d باستخدام نظرية إقليدس الموسعة.



**الشكل (2-20) خوارزمية RSA**

**أمن خوارزمية RSA: The** **Security Of RSA algorithm**

هناك عدة طرق لمهاجمة خوارزمية RSA,وهي على التوالي :

🞸 الهجوم الشامل Brute force: ويتضمن تجريب كل المفاتيح المحتملة.

🞸 الهجوم الرياضي Mathematical attack: هناك عدة طرق لتحليل ناتج ضرب عددين أوليين, وكل هذه الطرق تملك التأثير نفسه.

🞸 الهجوم الزمني Timing attack: ويعتمد على زمن تنفيذ خوارزمية فك التشفير.

🞸 الهجوم بنص مشفر مختار Chosen Ciphertext Attack المعتمد على خصائص الخوارزمية.

* فيما يخص الهجوم الشامل : فإن طريقة الدفاع ضده في خوارزمية RSA تشابه طرق الدفاع ضد نفس الهجوم على أية خوارزمية أخرى, وبالتحديد هي باستخدام مفاتيح طويلة قدر الإمكان. وبالتالي كلما كانت قيمة كل من e و d كبيرة, كلما ارتفع مستوى الحماية. إلا أنه نتيجة لتعقيد عمليات الحساب سواء في عملية توليد المفاتيح, أو في عمليتي التشفير/فك التشفير, فإن تكبير المفتاح سوف يؤثر سلباً على سرعة عمل النظام بشكل عام.
* فيما يخص الهجوم الرياضي :يمكن تعريف ثلاث طرق لمهاجمة خوارزمية RSA رياضياً هي:

🞸تحليل n إلى عاملين أوليين. سيساعد هذا الأمر على حساب

والذي يمكننا بدوره من تحديد .

🞸 تحديد مباشرةً, دون تحديد p و q أولاً. تساعد هذه الطريقة مرة أخرى على حساب .

🞸 تحديد d مباشرةً, بدون تحديد أولاً.

تُركِّز معظم النقاشات الخاصة بتحليل تشفير RSA على تحليل n إلى عاملين أوليين. تحديد من خلال معرفة n هو مكافئ لتحليل n إلى عاملين أوليين.

يظهر من الخوارزميات المعروفة حتى الآن لتحديد d بالاعتماد على معرفة e و n, أنها تستهلك زمناً مشابهاً للزمن لإجراء التحليل إلى عوامل أولية. وبالتالي يمكننا استخدام سرعة وأداء عملية التحليل إلى عوامل كتقييم لمدى أمن خوارزمية RSA.

من أجل قيم كبيرة للعدد n, وبالتالي قيم كبيرة للعوامل المؤلفة له, تعتبر عملية التحليل من العمليات الصعبة. إلا أنها ليست صعبة بالقدر الذي يفترض أن تكون عليه. وفيما يلي عرض واضح لذلك. قام مبتكرو خوارزمية RSA عام 1977 بتحدي قراء مجلة Scientific American Readers, وذلك من خلال طرح مسألة في أحد أعمدة المجلة (عمود الألعاب الرياضية), وهي فك ترميز شيفرة طبعت في هذا العمود, وقد طرحوا مكافأة مقدارها 100$ لمن يستطيع استرجاع النص الأصلي لهذه الشيفرة, و قد تم فك المفتاح المكون من 200 رقم عشري (663 بت) في أيار عام 2005 و استغرق ذلك 8 شهور من خلال استعمال منظومة مرتبطة بشبكة الانترنيت.

**الفصل الثالث**

**القسم العملي**

تصميم وتنفيذ منظومة اخفاء البيانات الرقمية المشفرة في الصور الرقمية

**3-1- مقدمة:**

بعد التعرف على تقنيتي التشفير بالمفتاح العام باستخدام خوارزمية RSA والتشفير المتناظر باستخدام خوارزمية AES سنقوم في هذا الفصل باستثمار هذه التقنية في مشروعنا لتنفيذ آلية اخفاء لنص مشفر بواسطة إحدى هاتين الخوارزميتين ضمن صورة رقمية ملونة ومن ثم تشفير الصور باستخدام الخوارزمية الأخرى وذلك من خلال برنامج الماتلاب.



**3-2- منهجية العمل:**

يبين الشكل الآتي (3-1) مخطط صندوقي لتوضيح آلية عمل الطريقة المقترحة:

**الشكل (3-1) مخطط يبين آلية العمل المتبعة**

حيث:

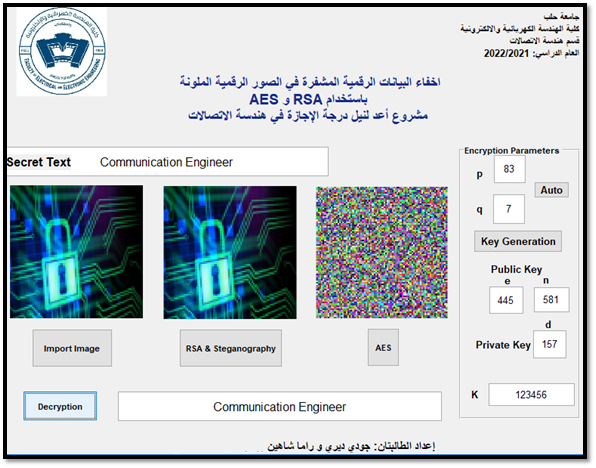
1. يتم ادخال النص السري المراد تشفيره.
2. يشفر النص السري باستخدام خوارزمية RSA أو AES.
3. يتم اخفاء النص المشفر ضمن الصورة باستخدام خوارزمية LSB.
4. تشفير الصورة باستخدام AES أو RSA.

والشكل (3-2) يبين الواجهة الرئيسية للبرنامج المقترح.



**الشكل (3-2) الواجهة الرئيسية للبرنامج**

يبين الشكل التالي تشفير النص "Communication Engineer" باستخدام خوارزمية RSA ثم اخفاء النص المشفر ضمن الصورة ومن ثم تشفير الصورة باستخدام AES.



**الشكل (3-3) تشفير النص RSA والصورة AES**

حيث استغرقت عملية التشفير وفك التشفير والحصول على النص الصريح حوالي 20 ثانية.

والشكل التالي يبين عملية تشفير النص "Communication Engineer" باستخدام خوارزمية AES ثم اخفاء النص المشفر ضمن الصورة ومن ثم تشفير الصورة باستخدام RSA.



**الشكل (3-4) تشفير النص AES والصورة RSA**

وهنا يظهر الفرق الواضح في السرعة بين هذه الحالة والحالة السابقة حيث لم يستغرق زمن التشفير وفك التشفير والحصول على النص الصريح أكثر من 2 ثانية.

يبين الشكل التالي عدم التمكن من الحصول على النص الصريح في حال وجود خطأ في مفاتيح التشفير



**الشكل (3-5) حالة وجود خطأ في المفاتيح**

بينت نتيجة المحاكاة للآليات المقترحة أنه عند تشفير النص AES والصورة RSA فإن زمن فك التشفير والحصول على النص الصريح أسرع بعشر مرات تقريباً من الآلية المعتمدة على تشفير النص RSA والصورة AES كما هو مبين في الجدول (3-1)

|  |  |  |
| --- | --- | --- |
| زمن فك التشفير والحصول على النص الصريح | | |
| حجم النص | **تشفير نص AES وتشفير الصورة RSA** | **تشفير نص RSA وتشفير الصورة AES** |
| 4Byte | 0.263 | 20.72 |
| 8Byte | 0.265 | 21.60 |
| 16Byte | 0.268 | 21.83 |

**بعض الأجزاء البرمجية المستخدمة في المشروع**

**الكود البرمجي المستخدم لتحميل الصورة**

[filename, pathname] = uigetfile({'\*.jpg;\*.png'},'Select a photo');

myimage =imread(filename);

myimage=imresize(myimage,[80 80]);

axes(handles.axes1)

imshow(myimage)

**كود تشفير النص باستخدام AES والاخفاء**

secret\_text=char(get(handles.edit1,'String'));

AA=secret\_text;

[s\_box, inv\_s\_box] = s\_box\_gen;

rcon = rcon\_gen;

[poly\_mat, inv\_poly\_mat] = poly\_mat\_gen;

inputaes=uint8(AA);

keyaes=char(get(handles.edit13,'String'));

b=0;

keybin=[];

for i=1:length(keyaes)

b=unicode2native(keyaes(i));

temp1=dec2bin(b,8);

keybin=horzcat(keybin,temp1);

b=0;

end

keyzero=[];

zeroadd=mod(length(keybin),128);

if length(keyaes)<16

keyzero=zeros(1,128-zeroadd);

keybin=[keybin,keyzero];

end

kstr=num2str(keybin);

keydec=[];

kstart=1;

kstop=8;

for i=1:16

keydec(i)=bin2dec(kstr(kstart:kstop));

kstart=kstop+1;

kstop=kstop+8;

end

w = key\_expansion (keydec, s\_box, rcon, 1);

plaintext =inputaes;

plaintext\_len=length(plaintext);

if(mod(length(plaintext),16)~=0)

for i=1:16-mod(length(plaintext),16)

plaintext(plaintext\_len+i)=0;

end

end

arr\_size=length(plaintext)/16;

start=1;

stop=16;

plaintextarray=[];

for i=1:arr\_size

plaintextarray(i,1:16)=plaintext(start:stop);%16\*n array

start=stop+1;

stop=stop+16;

end

ciphertextarray=[];

for i=1:arr\_size

ciphertext = cipher (plaintextarray(i,:), w, s\_box, poly\_mat, 1);

ciphertextarray(i,:)=ciphertext(1,:);

end

cc=[];

for i=1:arr\_size

cc=[cc ciphertextarray(i,:)];

end

[ stego ] = LSBHide(myimage,cc);

axes(handles.axes3)

imshow(stego)

كود تشفير الصورة باستخدام RSA

n=char(get(handles.edit12,'String'));

n=str2num(n);

e=char(get(handles.edit11,'String'));

e=str2num(e);

C=[];

stego=int32(stego);

for k=1:size(stego,3)

for i=1:size(stego,1)

for j=1:size(stego,2)

C(i,j,k)=modexp(stego(i,j,k),e,n);

end

end

end

axes(handles.axes4)

imshow(uint8(C))

**3-3 - الخلاصة:**

خلال السنوات الماضية أصبح علم أمن المعلومات هو محل اهتمام لكثير من الباحثين التي تحاول جهودهم أن تتوصل إلى حلول وتقنيات و أفكار جديدة تضمن نقل المعلومات بأمان من خلال الشبكة وخاصة شبكة الانترنت دون حدوث أي اختراق وكشف لتلك المعلومات.

ونتيجة لذلك , ظهرت العديد من التقنيات ومن أهمها علم إخفاء المعلومات, الفكرة من وراء هذا العلم أنه طالما أن هناك معلومات سواءً شُفرت أو لم تشفر , فإنها تكون في خطر .

وفي هذا البحث تم اقتراح نظام هجين يمكننا من إرسال معلومات نصية بشكل سري وذلك من خلال تشفير النص ثم اخفاؤه ضمن صورة ثم تشفير الصورة.

اخترنا طريقة خوارزمية الحشر في البت الأقل أهمية لسهولة تطبيق هذه التقنية ، وقد قمنا بتصميم البرنامج باستخدام لغة الماتلاب.

**3-4- أفكار مستقبلية لتطوير المشروع:**

1. استخدام مفتاح للإخفاء وفك الإخفاء لزيادة وثوقية هذه الخوارزمية.
2. اخفاء نصوص عربية (يونيكود)
3. استخدام انواع اخرى من الملفات :نص داخل فيديو – صورة داخل صورة – صورة ضمن فيديو
4. التنفيذ العملي للتطبيق المقترح في بيئة أنظمة تشغيل الأجهزة المحمولة (الأندرويد).
5. الاعتماد على لغة البايثون بدلا من الماتلاب.

**3-5- الصعوبات التي واجهتنا في عمل المشروع:**

1. صعوبة تطبيق خوارزمية AES في الماتلاب والاعتماد على توابع جاهزة لهذه الغاية يمكنها تشفير محارف الأسكي فقط (الأرقام من 0 حتى 255).
2. ندرة المراجع العربية التي تتحدث عن علم وتقنيات الاخفاء في الصور الرقمية.

المراجع العربية

1. د. يحيى بري. 2012 – **أمن المعلومات في نظم الاتصالات.** منشورات جامعة حلب.

المراجع الأجنبية

[1] Shamim Ahmed Laskar,Kattamanchi Hemachandran., **2012 – High Capacity data hiding using LSB Steganography and Encryption**. International Journal of Database Management Systems.Vol.4,No.6, Department of Computer Science Assam University, Silchar, Assam, India.

[2] Kanika Anand, Rekha Sharma., **2014** – **Data Security Using LSB &MSB Image Steganography**. International Journal of Electrical & Electronics Engineering (IJEEE). Vol. 1, Issue 6, Swami Devi Dyal Institute of Engg. & Technology, Barwala, Haryana, India.