المحاضرة الثانية

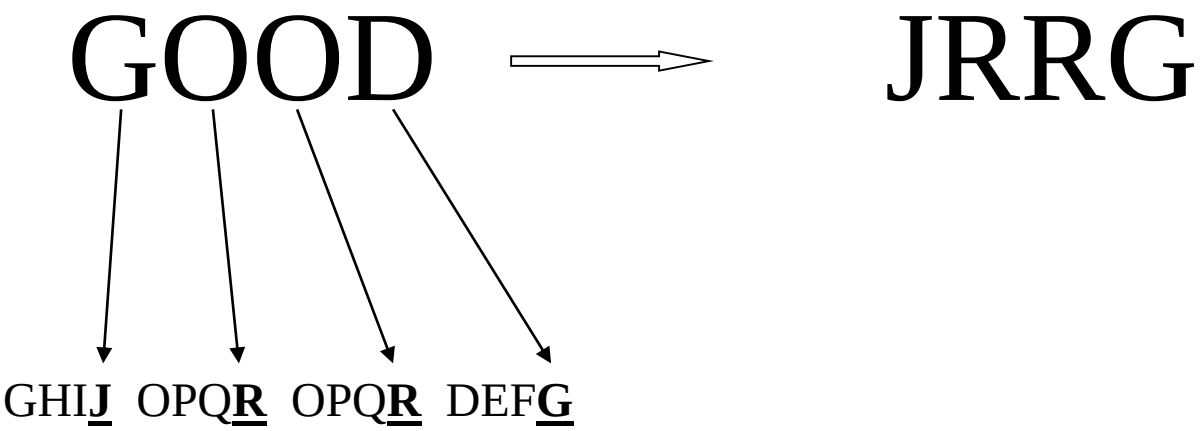
ملاحظة:

1- تعتمد سرعة طرائق التشفير على المفتاح والخوارزمية المصممة.
2- هناك عدة طرائق للتشفير منها تقليدي (قديم) ومنها حديث.

إذ قام العالم ستانون باستخدام احدى حقول الرياضيات وهو (Number theory) بمعنى انه يمكننا التعبير عن النص بعبارات رياضية.

في علم التشفير او ما يسمى علم التعمية ظهرت شفرة أو خوارزمية قيصر وهي واحدة من ابسط واكثر تقنيات التشفير انتشارا وتمثل نوع من شفرة الاستبدال.

مثال: قم بتشفير كلمة Good باستخدام شفرة قيصر؟



ملاحظة:

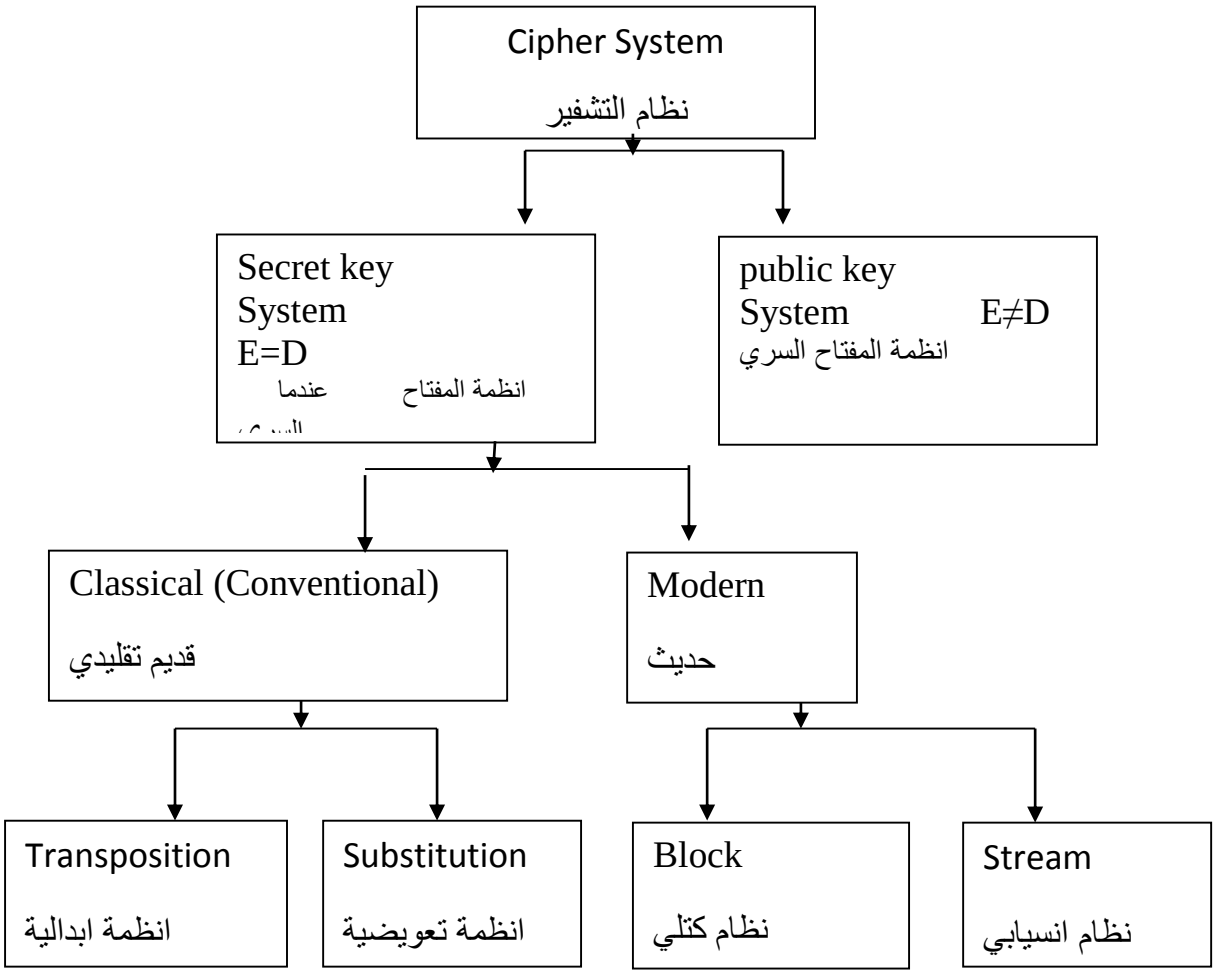
1. نلاحظ في المثال اعلاه شفرة قيصر تعمل على اراحة الحرف لثلاث مواقع لنحصل على النص المشفر.
2. في المثال السابق ممكن ان تكون الإزاحة 2 فنحصل على كلمة اخرى أو تكون الإزاحة 4 وهكذا اي باستخدام مفاتيح مختلفة (أي إزاحات مختلفة) نحصل على نصوص مختلفة مشفرة لنص صريح واحد.

ماهو الفرق بين الترميز والتشفير؟

الترميز Coding تحول البيانات من صيغة الى اخرى لكنها تبقى واضحة ومفهومة. اما التشفير Encryption تحول البيانات من صيغة واضحة الى صيغة غير واضحة (صيغة مبهمة unobvious)

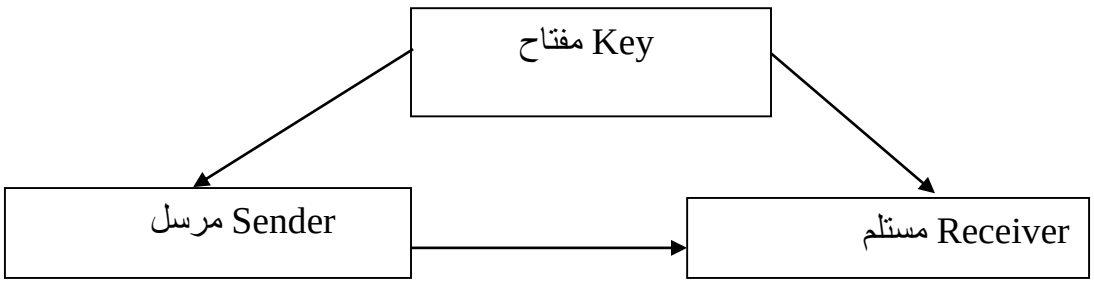
Types of Encryption system:

تقسم خوارزميات التشفير الى عدة انواع حسب حجم البيانات المشفرة وأسلوب تبادل المفاتيح، كما في المخطط الآتي الذي يمثل خوارزميات التشفير.



أنظمة التشفير ذات المفتاح السري Secret Key System

هي الأنظمة التي تستخدم مفتاح واحد لعملية التشفير فك الشفرة، اذن هذه الأنظمة تعتمد على المبدأ الآتي:



ملاحظة:

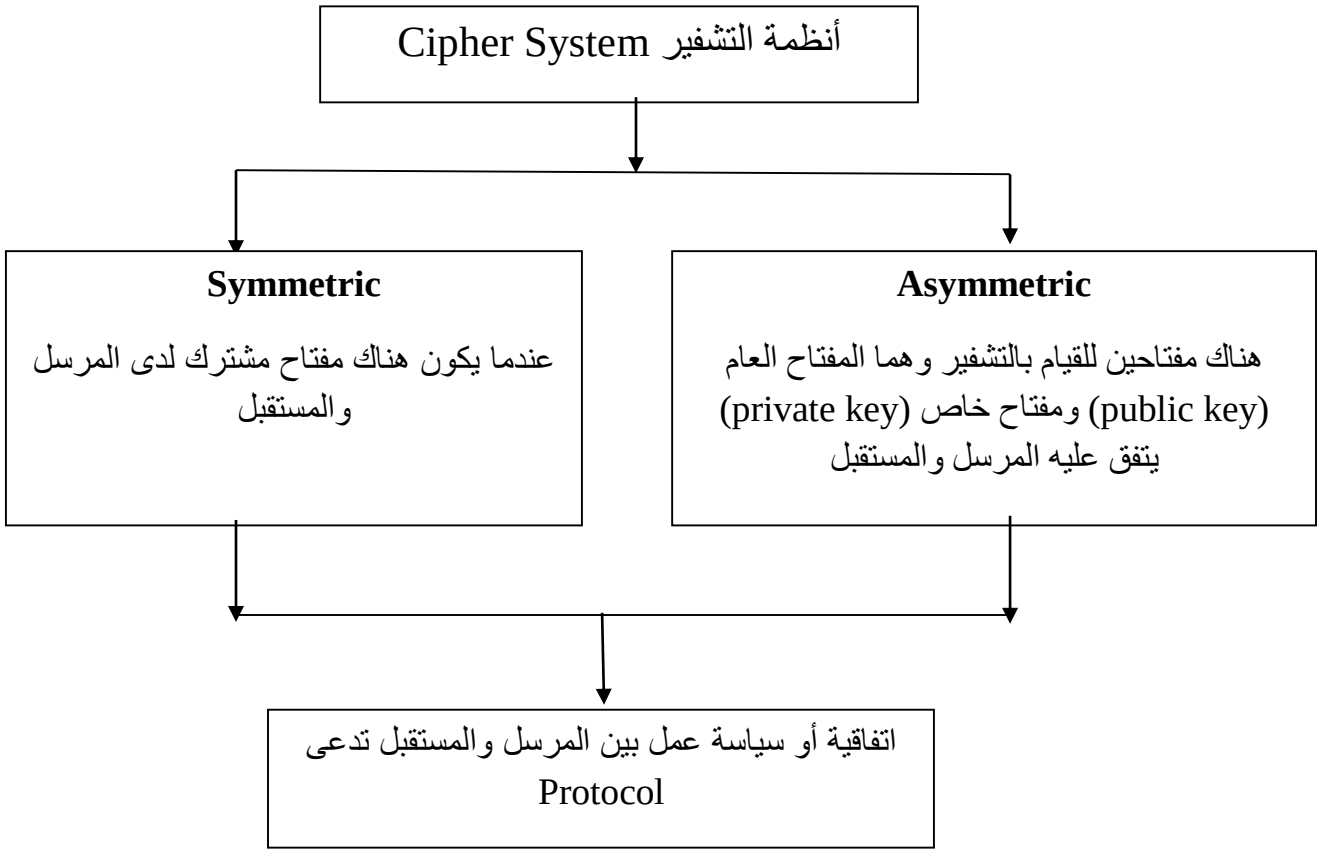
نلاحظ من الشكل اعلاه لدينا نفس المفتاح للتشفير وفك الشفرة.

Then any cipher system or algorithm depend on:

1-Strength of an algorithm

2-Security of the key

3-Protocoles that works.



الأنظمة التقليدية Classical (Conventional) Systems:

تعتبر بمثابة ولادة لعلم التشفير وهنا اعتمدت الخوارزميات بشكل اساسي على إحلال أو إبدال حرف مكان آخر (الجيد من هذه الخوارزمية كانت تقوم بالإثنين معا)

وتقسم خوارزميات هذه الأنظمة الى قسمين:

First: Transposition إبدال

Second: Substitution تعويض

First (Transposition): A rearrange or reorder the characters of plain text to get cipher text.

الإبدال: يمثل اعادة ترتيب أحرف أو رموز النص الصريح للحصول على نص مشفر.

أنواع خوارزميات الإبدال: Types of Transposition Algorithms

1) Simple as: البسيطة
   - *(a) Message Reversal Algorithm: قلب الرسالة*
   - *(b) Route Transposition Algorithm: خوارزمية ابدال المسار*
   - *(c) Column Transposition Algorithm: خوارزمية ابدال العمود*
2) Double Transposition Algorithm: خوارزمية الابدال المزدوجة
3) Polyliteral Transposition Algorithm: خوارزمية الابدال متعدد الحروف

نبدأ مع أول خوارزمية من خوارزميات Simple والتي تنتمي للتشفير الكلاسيكي الابدالي.

Example: By using message reversal algorithm encrypt the following message?

(Plain text) P: send help soon.

(Cipher text) C: noos pleh dnes.

عكس أو قلب الرسالة هنا تمت (كتابة الرسالة من اليمين).