

ولأن كتاب الرموز حجمه كبير للغاية (لأنه يحتوي على جميع الكلمات التي يتوقع استخدامها في عملية الإرسال ، وبعض الأحيان جميع الكلمات المعروفة تكون فيه) ، يكون مرتب بالترتيب الهجائي ، (مثلا) الحرف A يقابله في CodeNumber مثلا الرقم 20 ، الحرف B يقابله 21 ، الحرف C يقابله 22 ، سوف نلاحظ أنه يمكن لكاسر الشفرة كسر هذه الرموز لأنه يعرف أن الحرف A دائما أقل من الحرف Z وبقليل من المحاولة يتم كسرها ، لذلك تم اللجوء إلى **Two-Part-Code** وهنا يوجد كتاب للتشفير ، وكتاب آخر مرتب بطريقة أخرى لفك التشفير ، وهكذا لن يمكن تخمين ما ينتجه الكتاب الأول .

و على الرغم من سريه هذه الطريقة ، إلا إنها غير مجديه تماما ، نظرا لصعوبة الاحتفاظ بهذا الكتاب عند الطرفين ، وفي حال استخدمنا Two-Part-Code سنحتاج إلى كتابين عند كل طرف حتى يستطيعوا إرسال واستقبال الرسائل فيما بينهم ، ناهيك عن صعوبة إرسال الكتاب إلى الطرف الآخر والتأكد من أنه العدو لا يملك نسخه منه ، بالإضافة إلى صيانتها (أضافه كلمات أخرى ) وإرسالها مره أخرى للطرف الآخر .

### التشفير بالطرق الكلاسيكية *Classical Method* :

الطرق الكلاسيكية هي الطرق القديمة التي استخدمت فيما مضى من قبل اختراع الحواسيب ، وبقيت الأساس لكثير من الخوارزميات الحديثة التي تستخدم اليوم ، حيث كانت تعتمد على أحلال أو أبدال حرف مكان آخر ، والخوارزميات الجيدة كانت تقوم بالاثنين ، لكن جميع هذه الخوارزميات تعمل على الحروف فقط **Character-Based** أي على مدى 26 حرف ، بعكس الطرق الحديثة التي تعتمد على التعامل مع الBit (0 أو 1) ، وتقسم الطرق الكلاسيكية إلى قسمين رئيسيين :

#### شفرات الإحلال **Substitution Cipher** :

في هذا النوع من الشفرات ، التشفير يكون عن طريق إحلال حرف من النص الأصلي Plaintext بحرف آخر ليكون هو الحرف المشفر cipher char ، عملية الإحلال هذه تكون طريق جمع مفتاح ما إلى الحرف من النص الأصلي .

#### شفرات الإبدال **Transposition** :

في هذا النوع التشفير يكون عن تغيير أماكن حروف النص الأصلي ، أي مجرد تبديل في المواقع . (بعض الكتب تطلق على هذا النوع اسم **Permutation** تقليب ) .

#### شفرات **XOR** :

هناك بعض الكتب تصنف طريقه التشفير هذه مع الطرق الكلاسيكية ، وبالرغم من ضعف هذه الطريقة ، إلا أن أغلب الشفرات الحديثة تعتمد على هذه العملية الرياضية في علميات أخرى (وقد تحدثنا عنها في الفصل الأول) .

نبدأ بالنوع الأول ، شفرات الإحلال :