تقسم شفرات الإحلال Substitution Cipher إلى أربعه أقسام رئيسيه :

النوع الأول : Monoalphabetic Substitution Cipher
النوع الثاني : Polyalphabetic Substitution Cipher
النوع الثالث : PolyGram Substitution Cipher
النوع الرابع : Homophonic Substitution Cipher

وسوف نتطرق لكل من هذه الطرق بالتفصيل ، أحب أن أنوه إلى أن هناك بعض الترجمات السيئة لهذه الأنواع ، لكني سأتحفظ عنها هنا ، وسنذكر المصطلح كما هو باللغة الأنجليزيه .

شفرات Monoalphabetic Substitution Cipher :

هذا النوع يعتبر من أقدم أنواع التشفير استخداما ، حيث نقوم في هذا النوع بإحلال Substitution حرف من النص الأصلي بحرف أخر جديد . وهو بالاضافه إلى قدمه يعتبر من أضعف أنواع التشفير ويسهل كسره باستخدام طريقه تسمى التحليل الإحصائي frequency analysis ، وهذه الطريقة من اكتشاف العالم العربي المسلم **أبو يعقوب الكندي** وهو أول من وضع أساسيات كسر الشفرات Cryptanalysis، حيث لاحظ وجود حروف تتكرر في القران الكريم أكثر من غيرها.

من أشهر شفرات هذا النوع Monoalphabetic Substitution :

Caesar Cipher
Affine Cipher
ROT13 Cipher
Abash Cipher

شفره قيصر Caesar Cipher :

من أحد أشهر أنواع التشفير الكلاسيكي ، حيث تتميز ببساطتها ويعيبها سهوله كسر الشفرة الناتجة ببساطه ،

وطريقه التشفير بأن نأخذ الحرف الأول من النص الأصلي ثم نقوم بجمع مفتاح (وهو دائما يكون 3 في شفره قيصر) مع النص الأصلي ، ويكون هو الحرف الأول في النص المشفر . وهكذا بالنسبة لباقي الحروف.

وفي حال كان الحرف هو الحرف الأخير في الأبجدية نقوم بالرجوع إلي بداية الحروف (تكون على شكل دائرة) .

انظر الصوره المقابلة :

Plaintext letter	A	B	C	D	.....	W	X	Y	Z
Ciphertext letter	D	E	F	G	.....	Z	A	B	C