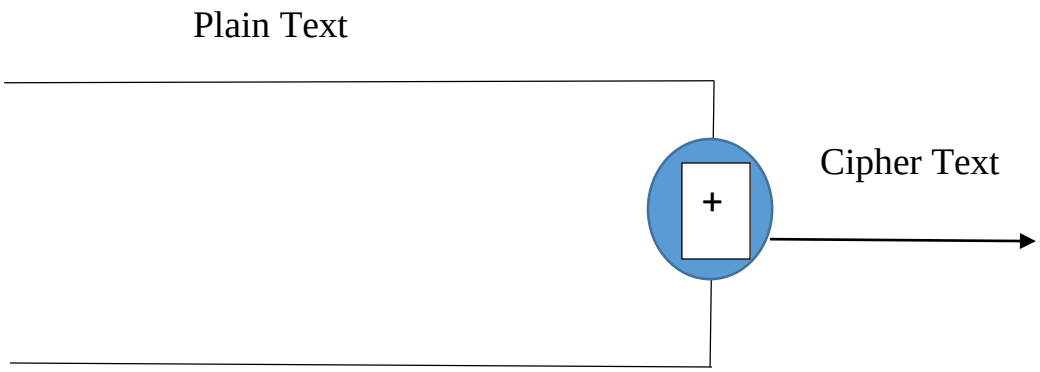
المحاضرة الحادية عشر:

التشفير الانسيابي Stream Cipher

هذا التشفير قائم على فكرة نظام (منصة لمرة واحدة) one –time-pad



ملاحظة: تسمى عملية التشفير الانسيابي ب منصة لمرة واحدة one–time–bit لان المفتاح يستخدم لمرة واحدة فقط.

ان عملية التشفير الانسيابي تجري كالاتي:

1–اعطاء مفتاح ابتدائي من bit أي متكون من سلسلة من الرموز codes (0 و1)

2–يتم تحويل النص الأصلي باستخدام ال Ascii code الى مايقابلها بالثنائي أي تحويل الأرقام العشرية الى ثنائية 0 و1.

3–دمج المفتاح مع النص الأصلي باستخدام XOR operation وبالتالي يتولد النص المشفر والذي نحصل عليه من إعادة الناتج 0و1 الى النظام العشري ومعرفة الحرف المقابل له بنظام ASCII code.

Ex: By using stream cipher. Encrypt the message (DO) if you know the key=0101100100011111

من جدول ASCII لدينا الحرف D=68 والحرف O=79 يتم تحويل كل من الرقمين الى النظام الثنائي

Binary system وذلك بقسمة العدد على 2 واخذ الباقي

$D=(68)_{10}=01000100$

$O=(79)_{10}=01001111$

الآن ندمج عناصر النص الصريح مع المفتاح للحصول على النص المشفر

Plain text	(0 1 0 0 0 1 0 0) (0 1 0 0 1 1 1 1)
Binary key	0 1 0 1 1 0 0 1 0 0 0 1 1 1 1 0
XOR	(0 0 0 1 1 1 0 1) (0 1 0 1 0 0 0 1)

$29=.....+ 2^1x0+2^0x0 =(0\ 1\ 0\ 1\ 0\ 0\ 0\ 1)_2$

$81=(0\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ )2$