Cryptography And Cryptanalysis

Ph. D. Course/ 2019-2020

Introduced By

Dr. Faez Hassan Ali

Lecture Three-1

Stream Cipher and Shift Register

Modern Cryptosystems

Public Key Cryptosystems

Key space K: a set of strings (keys) over some alphabet, which includes the encryption key e_k and the decryption key d_k.

Encryption process (algorithm) E: E_{ek} (M) = C.

Decryption process (algorithm) D: D_{dk}(C) = M.

The algorithms E and D have the property that:

$Dd_k(C) = Dd_k(Ee_k(M)) = M$.

It's also called **asymmetric cryptosystems**. In a public key (**non-secret key**) cryptosystem, the encryption key e_k and decryption key d_k are different, that is $e_k \neq d_k$.

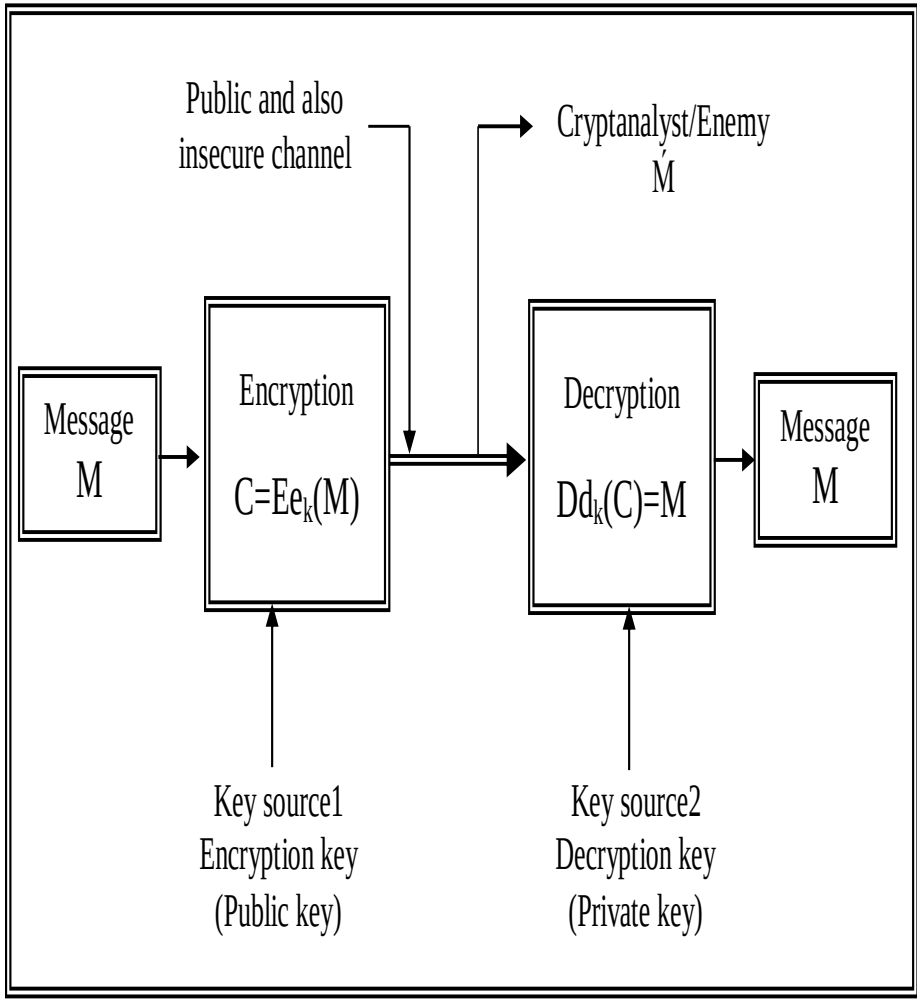


Figure (1) Modern Public-key Cryptosystem $e_k \neq d_k$.

Modern Cryptosystems

Secret Key Cryptosystems

It's also called **symmetric cryptosystems**. In a conventional secret-key cryptosystem the same key ($e_k=d_k=k\in K$), called **secret key**, used in both encryption and decryption; we are interest in this type of cryptosystems.

The sender uses an invertible transformation f defined by: $f : M \xrightarrow{k} C$

So produce the ciphertext:

$C = (E_k(m))$, $m\in M$ and $c\in C$.

and transmits it over the public insecure channel to the receiver. The key k should also be transmitted to the legitimate receiver for decryption but via a secure channel since the legitimate receiver knows the key k, he can decrypt c by transformation f^{-1}defined by: $f^{-1}: C \xrightarrow{k} M$

and obtain:

$D_k(c) = D_k(E_k(m)) = m$, $c\in C$ and $m\in M$,

and it's the original plaintext message.

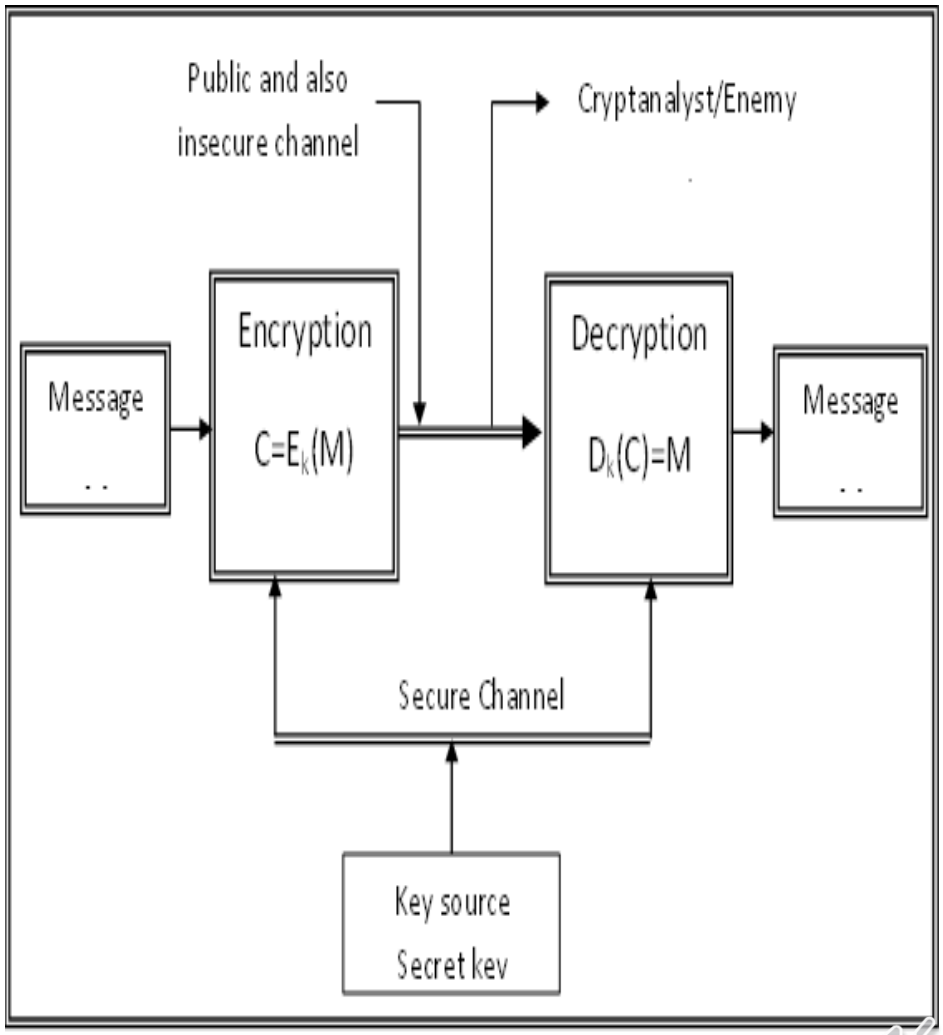


Figure (2) Conventional Secret-key Cryptosystems $e_k=d_k$.

Stream Cipher systems

In **stream ciphers**, the message units are bits, and the key is usual produced by a **random bit generator**. The plaintext is encrypted on a bit-by-bit basis.

The key is fed into random bit generator to create a long sequence of binary signals. This “key-stream” k is then mixed with plaintext m, usually by a bit wise XOR to produce the ciphertext stream, using the same random bit generator and seed.

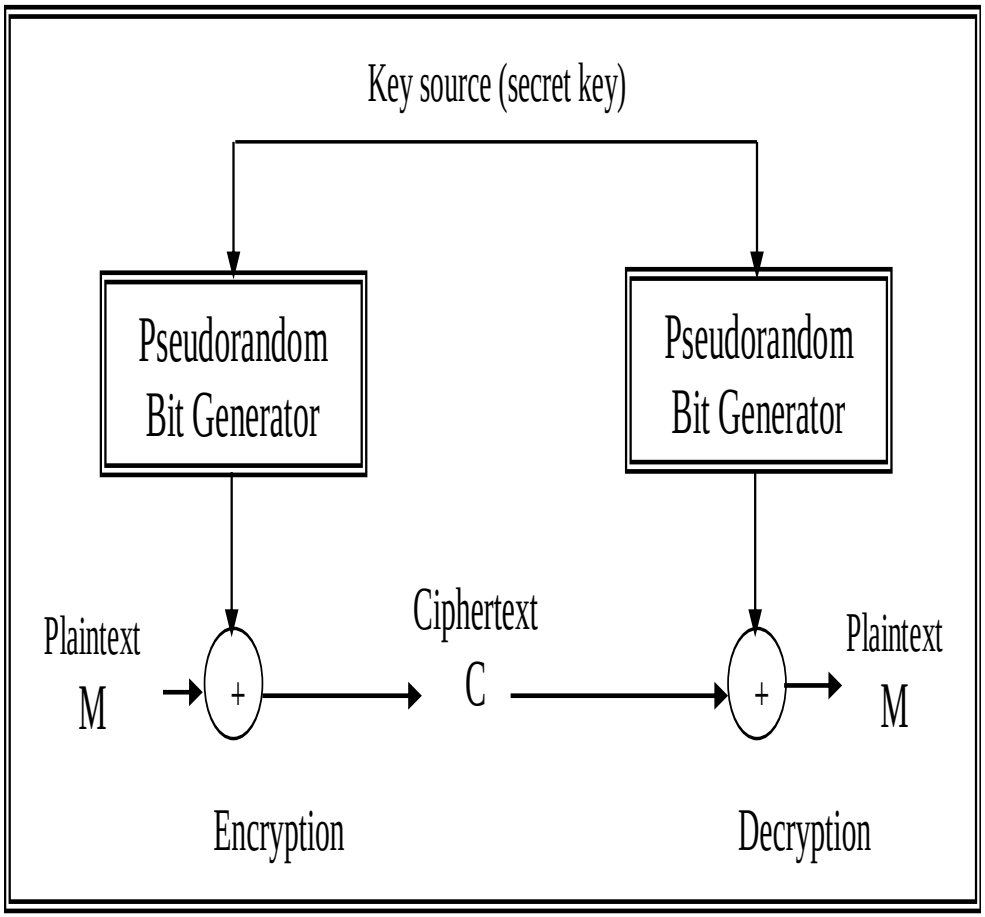


Figure (3) Stream Cipher System.

Advantages of Stream Cipher

- Stream ciphers are generally faster than block ciphers in hardware, and have less complex hardware circuitry.
- They are also more appropriate, and in some cases mandatory (e.g., in some telecommunications applications), when buffering is limited or when characters must be individually processed as they are received.
- Because they have limited or no error propagation, stream ciphers may also be advantageous in situations where transmission errors are highly probable.
- The security of stream cipher is thus always measured relative to the complexity of exhaustive searching for the correct key. If the complexity of an attack is less than that of the exhaustive search, the cipher is said to be **broken**.

Shift Registers Importance

- The Shift Register (SR) used and still be used in many fields, like computers, communications (radar, satellite equipment's,…), information theory, coding theory, protocols …etc.
- It’s an important part of many scientific devices design since its light, cheep, and has small size.
- The importance of SR raised when it's inter many modern and complex fields like communication and data security, so its inter in hardware or software of encryption devices specially the stream cipher system.
- These small devices are combined with each other and some Boolean functions to design an encryption algorithm to generate long binary sequences.
- These sequences have good randomness properties work as encryption key combined with plaintext binary digits to be encrypted before send to the receiver to be safe from intruders and attackers.
- The construction of the encryption algorithm must be designed with much careful. The designer must has good mathematical background before he designs the encryption algorithm to guarantee that the sequence not be estimated or calculated analytically even if the cryptanalyst has some information about the encryption algorithm or part of the encryption key.

Algebraic Concept of Linear Shift Register

Linear Shift Register Components

Linear Shift Register (LSR) is Linear Machine (LM) on finite filed F, combined from three kinds of devices:

- **Adder**: this device has $s \in Z^+$, inputs s.t. $x_1, x_2, \ldots, x_s \in F$, and has one output represent the (+) operation defined of F as in fig (a).
- **Multiplier**: multiply by constant $\alpha \in F$ s.t. has one input $x \in F$ and one output $\alpha x \in F$ as in fig (b).
- **Delay**: this device has memory, the time on it divided into equal and short intervals as in fig (c).

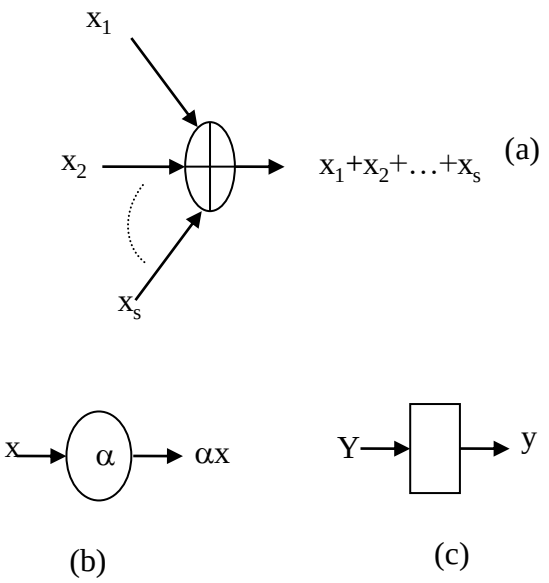
The response of adder and multiplier are in time.

The output of delay in time t is the input to it in time t-1, if we denote the input in time t by Y(t) and the output by y(t) then:

$y(t) = Y(t-1)$ …(1)

The LM contains k of delays which can denote the states of the machine in time t by:

$$\begin{bmatrix} y_1(t) \\ y_2(t) \\ \vdots \\ y_k(t) \end{bmatrix} \in F_k$$ As a special case, the initial state is: $$\begin{bmatrix} y_1(0) \\ y_2(0) \\ \vdots \\ y_k(0) \end{bmatrix} \in F_k$$



(a). Adder, (b). Multiplier (c). Delay

Algebraic Concept of Linear Shift Register

Linear Feedback SR

The linear feedback SR is the most important of one output terminal LM.

Then the LM=[F_k,F_m,α,β] and α: $F_k \rightarrow F_k$, s.t. $\alpha(x_i)=x_j$, i,j=1,…,k and β: $F_k \rightarrow F_m$ s.t. $\beta(x_i)=z_j$, i=1,…,k and j=1,…,m.

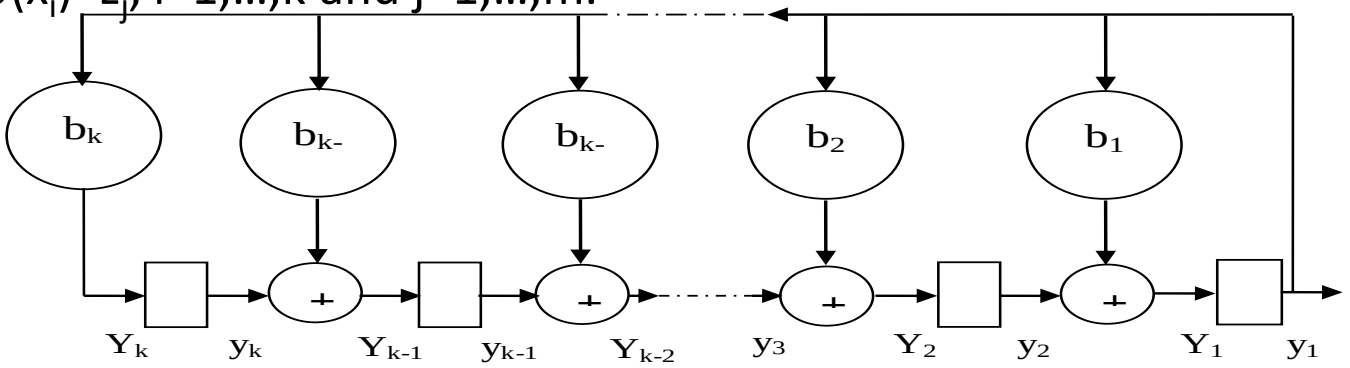


Figure (5) Linear Feedback SR

Example (1):

Let F=GF(2), k=2, m=1, F_1={0,1}, F_2={σ_1,σ_2,σ_3}, and let σ_1 represents the initial state s.t. $\alpha(\sigma_1)=\sigma_2$, $\alpha(\sigma_2)=\sigma_3$, $\alpha(\sigma_3)=\sigma_1$.

$\beta(\sigma_1)=1$, $\beta(\sigma_2)=1$, $\beta(\sigma_3)=0$.

The next state and outputs can be explained in table.

Next state	σ_1	σ_2	σ_3	σ_1
output	-	1	1	0

Algebraic Concept of Linear Shift Register

If we defined the delay operator (D), which is represents the difference in time, depending on equation (1) by:

$y_i(t)=DY_i(t)$, for $t\geq 1$ …(2)

if the difference is k then the operator will be D^k.

From previous figure we notice that:

$Y_k=b_kz$, $Y_i=y_{i+1}+b_iz$, $i=1,\ldots,k-1$, $z=y_1$ …(3)

by using equation (2) in (3) we obtain (H.W: prove):

$z=(b_1D+b_2D^2+\ldots+b_kD^k)z$ …(4)

this equation can be rewritten as follows:

$(1+b_1D+b_2D^2+\ldots+b_kD^k)z = R(D)z = 0$

R(D) is the Recursive polynomial (Connection polynomial), from eq(4):

$Z(t) = b_1z(t-1)+b_2z(t-2)+\ldots+b_kz(t-k)$ (a), when $k<t$

$Z(t) = b_1z(t-1)+b_2z(t-2)+\ldots+b_tz(0)+y_{t+1}(0)$ (b), when $k\geq t$ …(5)

Form equation (5) we can find the current output depending on previous output.

Algebraic Concept of Linear Shift Register

Example (2):

In GF(2^3), when F=GF(2) and let $\alpha^3=\alpha+1$, $(b_3\alpha^0+b_2\alpha^1+b_1\alpha^2+b_0\alpha^3)$ we have LFSR consists from three delays as in figure.

$b_3=1$, $b_2=1$, $b_1=0$, $b_0=1$.

When t=1 then

$\alpha(c_0\oplus c_1\alpha\oplus c_2\alpha^2)=c_2\oplus(c_0\oplus c_2)\alpha\oplus c_1\alpha^2$

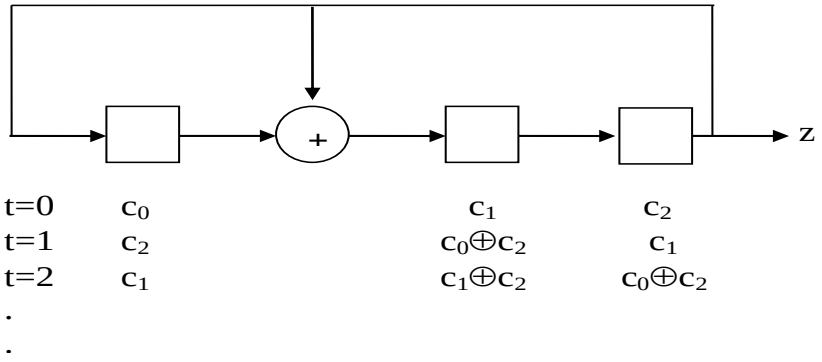


Figure (6) Linear Feedback SR with 3 delays.

And t=2 then

$\alpha(c_2\oplus(c_0\oplus c_2)\alpha\oplus c_1\alpha^2)=c_1\oplus(c_1\oplus c_2)\alpha\oplus(c_0\oplus c_2)\alpha^2$

By applying relation (5-b) to specify the output when t<3:

$z(0)=c_2$, $z(1)=c_1$, $z(2)= c_0\oplus c_2$

and so on by applying relation (5-a) to specify the output when $t\geq 3$:

$z(3)=c_1\oplus c_2$, $z(4)=c_0\oplus c_1\oplus c_2$, …

The binary sequences S =z(0), z(1), z(2),… (or $S=s_0,s_1,s_2,\ldots$, where $s_i=z(i)$, i=0,1,2,…). If the initial state of linear Feedback SR all zero's then $s_i=0$, $\forall i$.