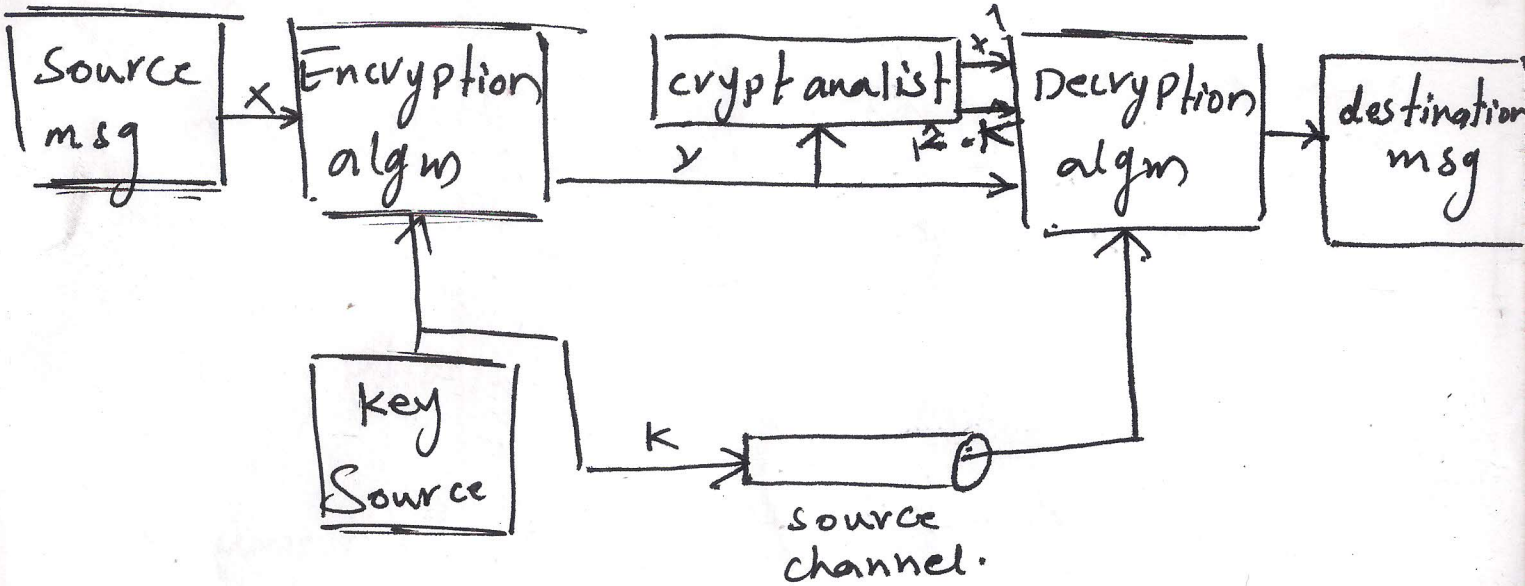
(Conventional cryptography technique)

الطريقة التقليدية



this model contains various blocks as.

1- Message Source :- which generates the plain text (origional message) to be transmitted.

2- Encryption algorithm :- it perform various transformations on the plain text.

3- Secret key :- it is input to the algorithm provide Secrecy to the message.

4- cypher text :- it is scrambled msg produced from Encryption algorithm.

decryption algorithm; it is inverse of Encryption algorithm and produce original plain text..

→ in conventional cryptography same key is used for both Encryption and Decryption.

→ Assume that the plain text is x, secret key is k and cipher text is y. is generated as.

$$Y = E_k(x).$$

at the destination the Decryption is processed by using same secret key and obtain the original plain text.

$$X = D_k(y).$$

Conventional cryptography the source channel is required to transmit secret key only to destination.

the crypt analyst will access the cypher text y and try to obtain either plain text sample ($\hat{x}$) or secret key sample ($\hat{k}$).

* Play Fair cipher

Substitution technique.

* Example

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

(5 x 5)

let key is MONARCHY.

the rules for Encryption of plain text:

step1: consider pair of plain text letter

replace the letter that lies in its own row and the column occupied by another plain text letter.

ex: BP becomes HS.

FA becomes I/J M

tep2;

plain text BALLOON

BA LL OO N.

BA LX LO ON

Repeating plain text letter in the same pair must be seperated with a filler letter such as X.

ex:- BALLOON can be treated as

~~BALXLO~~ BA LX LO ON . . حرفين حرفين

Step 3 ; two plain text letter fall in same column each replace by the letter of down.

ex:- Mu becom CM.

نأخذ الرقم الاسفل منا كل حرف ونحاول تشفيره

Step 4; the two plain text letter fall in same row each letter is replaced by letter to the right.

ex:- A R ~~becam~~ becomes R M