lic key crypto system'; -

the essential steps are! -

1- Each user generates a pair of key to be used For Encryption & decryption of message.

2 - Among two keys, one key is public and accessible to others, the other key is called private key which is kept secret.

this public key ↓, secrecy.

* AS shown in the diagram.

→ A wants to send a message (X) to B by encryption using public key system.

→ B generates a pair of keys, public key (PuB) and Private key (PRB).

→ A Encrypt the message by using (PuB) of B. (public key of B).
generate cipher text y.

$y = E_{pub}(X)$.

ince the message can be decrypted only by using private key of B (PRB) this key is keep secret and known only by B and B only can decrypt the message as.

$$X = D_{PRB}(Y).$$

$$= \cancel{D_{PR_B}}(\cancel{E_{PU_B}}(X))$$

$$= X$$

* the crypt analyst will receive the cipher text and trying to learn samples of either plain text $(\hat{x})$ or private key $(\hat{PRB})$

- Different between public key cryptography
and
conventional cryptography.

* conventional Encryption

→ the Same algorithm with the Same key is used for Encryption and decryption.

→ the Sender and receiver must share the algorithm and the key.

→ the key must be kept Secret.

→ knowledge of algorithm plus sample of the cipher text must be insufficient to determine the key.

* Public key Encryption:.

- one algm is used Encryption and Decryption with apair of keys.
one key is used For Encryption and one For decryption.

e Sender and receiver must each have one of the matches pair of keys (not the Same one).

- one of two keys must kept secret.

- knowledge of the algm plus samples of cipher text and one of the keys must be insufficient ~~for~~ to determine the other key.