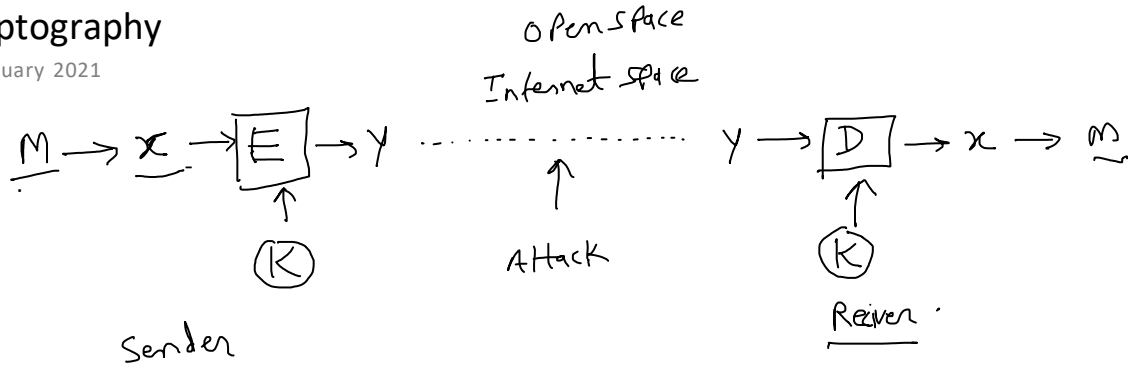
Cryptography

08 January 2021
11:52



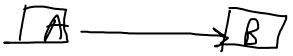
Exa. ① shift cipher.

Cryptography algorithm category:

① on the basis of key:

Ⓐ conventional cryptography (symmetric key cryptography)
single key ← Encryption / Decryption
(require key distribution system)
Exa. ① DES Data Encryption standard
② AES Adv. Encryption standard

Ⓑ public key cryptography (Asymmetric key cryptography)
two key: public key / private key
↓ Receiving ↓ sending



Exa. ① RSA ② Diffie Hellman

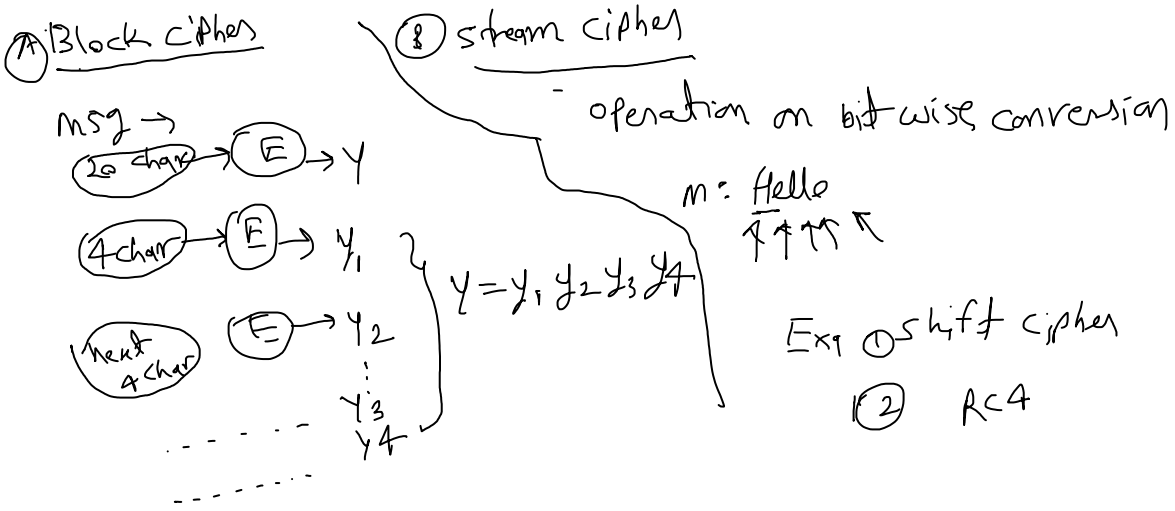
② on the basis of method used to Encrypt / Decrypt:

Ⓐ Substitution Algo
Replacement of alphabet
ACE
↓ ↓ ↓
C E g
Exa shift cipher

Ⓑ Transposition Algo.
Change the position of any alphabet
Hello 1 2 3 4 5
4 1 2 5 4 ← key
lHCOl

x = ACE Key 312
123
y = EAC
Exa. auto key cipher

③ on the basis of process:


(1) Block ciphers
msg →
20 chars
E
Y
4 char
E
Y1
Y = Y1 Y2 Y3 Y4
next 4 char
E
Y2
Y3
Y4
(2) stream cipher
- operation on bit wise conversion
m: Hello
Ex: (1) shift cipher
(2) RC4