🡪Red pochne h umama ,aimen wagera se

1. A stream cipher can be viewed as a generalization of a one-time pad.

Recall that the one-time pad is provably secure. Why can't we prove

that a stream cipher is secure using the same argument that was used

for the one-time pad?

--Yeh random nh hoti basically –wahan key har bar diff or random thi

Ans.About the one-time pad, the key is still large and the same size of the plaintext, so one-time padis more secure than a stream cipher

3. Suppose that Alice uses a stream cipher to encrypt plaintext *P,* obtaining ciphertext C, and Alice then sends *C* to Bob. Suppose that Trudy happens to know the plaintext *P,* but Trudy does not know the key *K* that was used in the stream cipher.

a. Show that Trudy can easily determine the keystream that was used

to encrypt *P*

Alice XOR each bit of the plaintext(P) with the keystream(S).

To encrypt,

C0 = P0 XOR S0,

C1 = P1 XOR S1,

C2 = P2 XOR S2, ..., Cn = Pn XOR Sn

And to decrypt

,P0 = C0 XOR S0,

P1 = C1 XOR S1,

P2 = C2 XOR S2,

…, Pn = Cn XOR Sn

Trudy can do,

S0 = P0 XOR C0,

S1 = P1 XOR C1,

S2 = P2 XOR C2, …,

Sn = Pn XOR Cn*.*

b. Show that Trudy can, in effect, replace *P* with plaintext of her

choosing, say, *P'.* That is, show that Trudy can create a ciphertext

message C" so that when Bob decrypts *C'* he will obtain *P'.*

C’ = S XOR P’ and then, S = C XOR P,We can replace the second to the first such that C’ = C XOR P XOR P’

4. This problem deals with the A5/1 cipher. For each part, justify your answer.

a. On average, how often does the X register step?

3/4 because 2 register at least at 1 clock cycle

b. On average, how often does the Y register step?3/4

c. On average, how often does the Z register step?3/4

d. On average, how often do all three registers step?5/6

e. On average, how often do exactly two registers step? ½

f. On average, how often does exactly one register step?0

g. On average, how often does no register step?0

5. Implement the A5/1 algorithm. Suppose that, after a particular step,

the values in the registers are

*X = (x0,*xi,..., xis) = (1010101010101010101)

*Y* = (i/o, 2/1, \_··, 2/21 ) = (1100110011001100110011)

*Z = {z0,* z i , . . . , *z22)* = (11100001111000011110000)

List the next 32 keystream bits and give the contents of *X, Y,* and *Z*

after these 32 bits have been generated.

---nahi smjh araaa stream kse banrrhe h

6. For bits *x, y,* and *z,* the function maj(x, *y, z)* is defined to be the majority

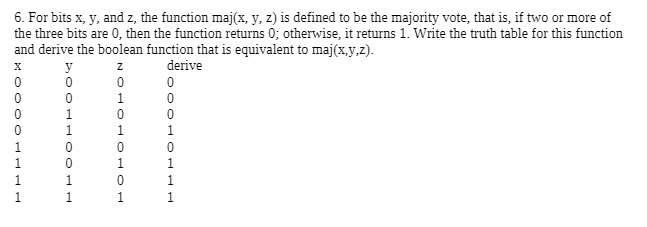
vote, that is, if two or more of the three bits are 0, then the function

returns 0; otherwise, it returns 1. Write the truth table for this function

and derive the boolean function that is equivalent to maj(a;,j/,z).



Xor ka function banrha h



7. The RC4 cipher consists of a lookup table *S,* which contains 256 byte values, and two indices, *i* and *j .*

a. The lookup table *S* is initialized to contain the identity permutation 0,1,2,..., 255 and at each step of the algorithm, *S* contains a permutation. How is this achieved? That is, why does *S* always contain a permutation?

Initialize the permutation using the key, then we can generate the keystream.

-S[] holds the permutation (0-255 bytes)-

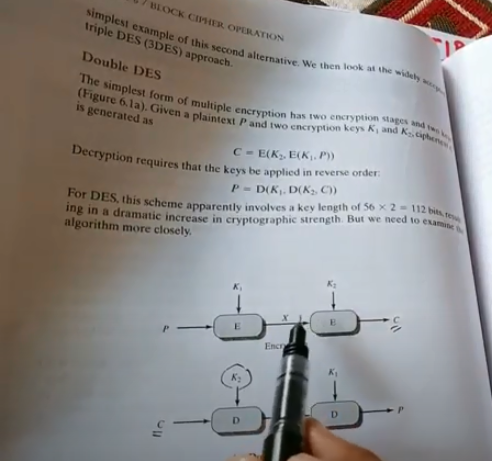
K[] holds the key, the key can be in any length (0-256 bytes)

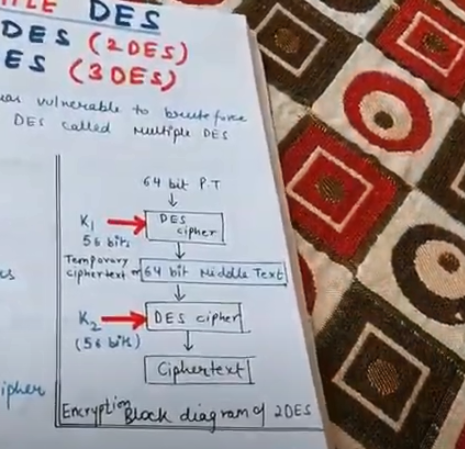
-The key does not always be 256 bytes, K[i] = key[i (mod N)]. Just take how many bytesthe key has, and repeated until we get 256 bytes

-Use the key to scramble the permutation, swap(S[i], S[j]): swap the two guys in thepermutation, still get the permutation; by swapping, the properties is maintaine

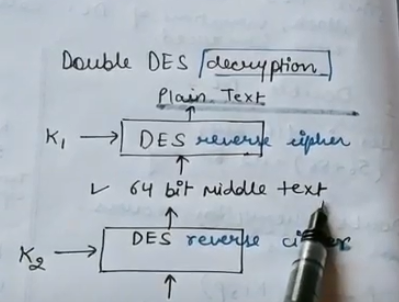
b. Where is RC4 used in the real world?

SSL,WEP,internet explorer





Kuch ciper or kuch plain text hota h or use key generate hosktey h..ek end se encryption dosree end se descruption phir job anta h wo meet in the middle attack hota h



It is advantage of Double DES