Name of the Subject: E-COMMERCE & E-SECURITY Subject Code: IT-718

Seat No: IT076 Student ID: 18ITUBN116 Branch/Sem: IT-VII

Q2 (b)

Deffie- Hellman key exchange algorithm.

- The Deffie- Hellman algorithm is being used to establish a shared Secret that can be used for secret Communication while exchanging data over a public network.

- Public keys avaliable - P, G for both the User.

- Now, Select the Private a for one user & b for second User.

- Key are generated by $X = G^a \bmod P$
  $Y = G^b \bmod P$

- ~~It~~ can be Show
- Exchange of generated keys.

Key receive = y, x.

Secret key = $k_a = y^a \bmod P$
$k_b = x^b \bmod P$

- It can be Show
  $k_a = k_b$.

PTO →

Section – II Date: 06/09/2021 Signature of Student:

Name of the Subject: E-COMMERCE & E-SECURITY Subject Code: IT-718

Seat No: IT076 Student ID: 18ITUBN116 Branch/Sem: IT-VII

Given

$a = 23$ $q = 5$

$X_a = 6$ & $Y_A = 15$

$X_b = ?$ & $Y_B = ?$

∴ ~~[illegible]~~ ~~mad q~~ .

∴

~~[illegible] 23~~

∴ $Y_A = a^{Y_B}$ mad q.

∴ $15 = 23^{Y_B}$ mad 5

$15 = 5^{Y_B}$ mas

∴ ~~[illegible]~~

∴ $Y_B = 17$.

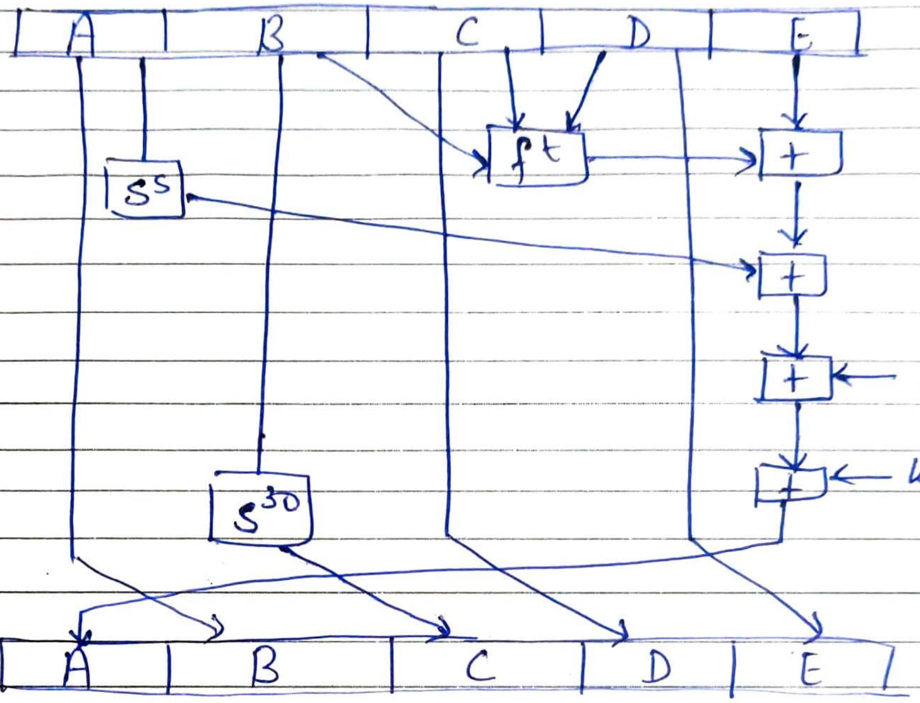
∴ $X_A = a^{X_B}$ maq

∴ $6 = 5^{X_B}$ md 23.

$X_B = 18$.

Secret key $k_{AB} =$

Q2 (C) SHA-1



Single Step

- Each round of ~~q~~ the form.

$A, B, C, D, E \leftarrow (E, f(t, B, C, D) + S^5(A) + W_t + K_t) + A, S^{30}(B), C, D$

$A, B, C, D, E \rightarrow$ 5 words of the buffer.

$t \rightarrow$ Step no $(0 \leq t \leq 79)$

$f(t, B, C, D) =$ Primitive logic function for step t.

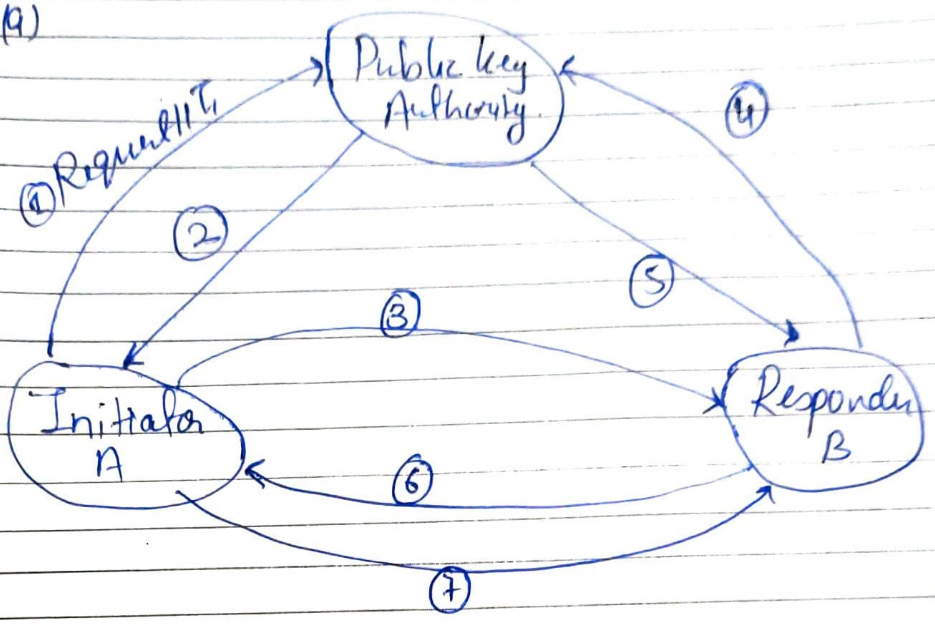
S^k = Circular left shift of 32 bit argument by k bit.

W_t = a word derived from current 512 bit block.

K_t = additive constant

$+$ → modulo 2^{32} addition.

Q3 (a)



Public Key Authority.

① A Sends a timeStamped message to the public key authority for current public key B

② The authority responds with a message that is encrypted using private key. Therefore A is assured that the message oriented with the authority.

- The orignal timestamp given so A can determine that is not old message.

③ A Store B's public key & also uses it to encrypt a message.

(4,5) B retrives A's public key from the authority.

⑥ A returns N2, which is encrypted using B's public key.

Name of the Subject: E-CES Subject Code: IT718

Seat No: IT076 Student ID: 18ITUBN116 Branch/Sem: IT-VII

Q3 (b)

MD5	SHA 1.
① MD5 Can be have 128 bit length of message digest	SHA1 has 160 bit length message digest.
② To make initial message the aggresor would want 2^128 operation.	In SHA1 it will be 2^160 that makes it quite troublesome.
③ MD5 is Simple indigent or poor Security	Provide balanced or tolerable Security.
④ MD5 is Simple than SHA1	SHA1 is Complex
⑤ In MD5 needs to seek out the 2 message having identical message digest 2^{64} operation.	In SHA1 2^80 operation.