VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering

Winter Semester 2023-24

Continuous Assessment Test – II

Course Name & code: Cryptography and Network Security & BCSE309L

Class Number: Common to all batches **Slot: E1 + TE1**

Exam Duration: 90 mins **Maximum Marks: 50**

Answer all the Questions.

Q.No.	Questions	Max Marks	CO	BL
1.	Alice and Bob want to exchange the key using the Diffie Hellman approach. They both agree on the prime number p = 17 and the generator g = 7. Alice and Bob choose their private key as Xa = 5 and X_b = 4. Meanwhile, an attacker named Darth intercepts their communication with the private keys X_{DA} = 4 and X_{DB} = 8 to break the communication between Alice and Bob. Calculate and analyze the procedure by which the attacker generates the identical key to gather the information from Alice and Bob.	10	CO2	BL4
2.	Consider that two communicating parties, UserA and B, agreed to use the Elgamal cryptosystem to secure their conversation. The values used are as follows: A prime number q = 17 and the generator value α = 11. Suppose that User A chose his private key X_A as 6, and User B chose the random integer k as 5. Show the steps involved in key generation, encryption, and decryption for the message M=7.	10	CO2	BL6
3.	Apply the ECC algorithm to secure the communication for the plain text point P_m= (9, 7). The global public elements used by the user are as follows: Elliptic curve E_{23}(1,1), G= (3,10), and the private key n_A =2, and the secret integer k = 2. Compute the ciphers C1 and C2. (Show the complete calculation.)	10	CO2	BL3
4.	a. Determine the number of padding bits, total length and number of blocks used in HMAC for the hash functions SHA 512 and MD5 if the input message to be sent is M= 1011011100011110 and the key K = 10111011. (5 Marks) b. Evaluate the value of Ch (e, f, g), Maj (a, b, c), of SHA512 algorithm for the buffers ‘a’, ‘b’, ‘c’, ‘e’, ‘f’, and ‘g’ that contain the hexa-decimal values as follows: 1111777700001111, FFFF222222221111, BBBB999911112222, CCCC222222220000, 1111DDDD22221111, and 33331111AAAAFFFF, respectively. (5 Marks)	10	CO3	BL4
5.	Person A wants to send a message to Person B. Both agreed to use SHA1 for obtaining the message digest. Let the generated message digest for the message be 4. Both agree on the public key components {p, q, h} as {23, 11, 7}. Person A selects his private key as 3. Let the pseudorandom integer k be 5. Demonstrate the step-by-step calculation for the following: • Generate the digital signature using DSS. • Signature Verification	10	CO3	BL3

CAT-II key :

1. Man in the Middle Attack

prime number $p = 17$, Generator $g = 7$

Private key $X_a = 5$ $X_b = 4$

Alice

$Y_a = g^{X_a} \bmod p$

$= 7^5 \bmod 17$

$= 11$

Bob

$Y_b = g^{X_b} \bmod p$

$= 7^4 \bmod 17$

$= 4$

Darth $X_{DA} = 4$ $X_{DB} = 8$

$Y_{DA} = 7^4 \bmod 17$

$= 4$

$Y_{DB} = 7^8 \bmod 17$

$= 16$

$\cancel{K_{DA} = 7^{14} \bmod 17}$

$\cancel{= 14}$

$\cancel{K_{DB} = 7^{4} \bmod 17}$

$\cancel{= 4}$

$K_A = Y_{DA}^{X_a} \bmod p$

$= 4^5 \bmod 17$

$= 4$

$K_B = Y_{DB}^{X_b} \bmod p$

$= 16^4 \bmod 17$

$= 1$

$K_{DA} = Y_a^{X_{DA}} \bmod p$

$= 11^4 \bmod 17$

$= 4$ //

$K_{DB} = Y_b^{X_{DB}} \bmod p$

$= 4^8 \bmod 17$

$= 1$ //

② Elgamal Cryptosystem.

prime number $q = 17$

Generator value $\alpha = 11$

User A private key $\boxed{X_A = 6}$

Message $= 7$

public key of user B $= Y_A = \alpha^{X_A} \bmod q$

$= 11^6 \bmod 17$

$\boxed{Y_A = 8}$

$\therefore$ public key $\{q, \alpha, Y_A\} = \{17, 11, 8\}$

Encryption by ~~Bob~~ User B with User A public key.

Calculate $K = (Y_A)^k \bmod q$

$= 8^5 \bmod 17$

$\boxed{K = 9}$

Calculate $C_1 = \alpha^k \bmod q$

$= 11^5 \bmod 17$

$C_1 = 10$

Calculate $C_2 = KM \bmod q$

$= 9 * 7 \bmod 17$

$C_2 = 12$

Ciphertext $(C_1, C_2) = (10, 12\}$

Decryption by User A with Private key :

Calculate $K = (C_1)^{X_A} \bmod q$

$= 10^6 \bmod 17$

$= 9.$

plain Text $M = (C_2 K^{-1}) \bmod q$

$= 12 \times 9^{-1} \bmod 17$

$= (12 \times 2) \bmod 17$

$= 24 \bmod 17$

$\boxed{M = 7}$

3. ECC - Encryption.

Plaintext $P_m = (9,7)$

Elliptic curve $E_{23}(1,1)$

$G = (3,10)$

private key $n_A = 2$

Secret integer $k=2$.

soln

$n_A = 2$ $\quad G = (3,10)$ $\quad 2G = G + G$

$(3,10) + (3,10) = P$

$$\lambda = \frac{3x^2+a}{2y} \bmod p$$

$$= \frac{3 \times 3^2 + 1}{2 \times 10} \bmod 23$$

$$= \frac{\overset{7\ 14}{\cancel{28}}}{\underset{\cancel{10}\ 5}{\cancel{20}}} \bmod 23 \quad = \frac{7}{5} \bmod 23$$

$$= (7 \times 14) \bmod 23$$

$$= 6$$

$x_3 = \lambda^2 - x - x \mod p$

$= 6^2 - 3 - 3 \mod 23$

$= 36 - 6 \mod 23$

$= 30 \mod 23$

$= 7$ //

$y_3 = \lambda(x - x_3) - y \mod p$

$= 6(3-7) - 10 \mod 23$

$= 6(-4) - 10 \mod 23$

$= -24 - 10 \mod 23$

$= -34 \mod 23$

$= 23 - (34 \mod 23)$

$= 23 - 11 \quad = 12$ //

$(x_3, y_3) = (7, 12)$

Encrypt the message (9,7) using the public key.

Secret integer $k = 2$.

Ciphertext $C = [(kG), (M + kP_u)]$

$= [C_1, C_2]$

$P_m = M$

P_u - public key

$C_1 = kG$

$= 2(3, 10)$

$C_2 = M + k P_u$

$= (9,7) + 2(7,12)$

$C = [2(3,10), (9,7) + 2(7,12)]$

$= [(7,12), (9,7) + 2(7,12)]$

$$2(7,12) \Rightarrow (7,12) + (7,12)$$

$$\lambda = \frac{3x^2+a}{2y} \bmod p = \frac{3\times 7^2+1}{2\times 12} \bmod 23$$

$$= \frac{\overset{\overset{37}{\cancel{74}}}{\cancel{148}}}{\cancel{2}\times \underset{6}{\cancel{12}}} \bmod 23$$

$$= (37 \times 6^{-1}) \bmod 23$$

$$= (37 \times 4) \bmod 23$$

$$\boxed{\lambda = 10}$$

$$x_3 = \lambda^2 - x - x \bmod p$$

$$= 10^2 - 7 - 7 \bmod 23$$

$$= 86 \bmod 23$$

$$= 17$$

$$y_3 = \lambda(x - x_3) - y \bmod p$$

$$= 10(7 - 17) - 12 \bmod 23$$

$$= 10(-10) - 12 \bmod 23$$

$$= -100 - 12 \bmod 23$$

$$= 23 - (112 \bmod 23)$$

$$= 23 - 20$$

$$= 3$$

$$\boxed{(x_3, y_3) = (17, 3)}$$

Now compute

$$(9,7) + (17,3)$$

$$\lambda = \left[\frac{y_2 - y_1}{x_2 - x_1}\right] \bmod p = \left[\frac{3-7}{17-9}\right] \bmod p$$

$$= \frac{-4}{8} \bmod 23$$

$= \frac{-1}{2} \bmod 23$

$= -1 * 2^{-1} \bmod 23$

$= -12 \bmod 23$

$= 23 - 12$

$\boxed{\lambda = 11}$

$x_3 = \lambda^2 - x_1 - x_2 \bmod p$

$= 11^2 - 9 - 17 \bmod 23$

$= 121 - 26 \bmod 23$

$= 95 \bmod 23$

$= 3$//

$y_3 = \lambda(x_1 - x_3) - y_1 \bmod p$

$= [11(9-3)-7] \bmod 23$

~~$= 11 * 6 \bmod 23$~~

~~$= 66 \bmod 23$~~

$= 66 - 7 \bmod 23$

$= 59 \bmod 23$

$= 13$//

Cipher Text $= [C_1, C_2]$

$= [(7,12);(3,13)]$ //

4a SHA512

Key is padded to 1024 bits, ~~by addin~~

Original message Length 16

∴ 1024+16 = 1040 ⇒ Total message length.

For SHA512

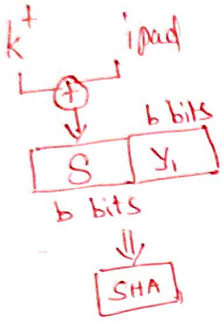
$mL \equiv 896 \bmod 1024$

$1040 \equiv 896 \bmod 1024$.

$16 \not\equiv 896$

∴ 880 bits shd be padded.

No. of blocks needed = 2



MD5

Key is padded to 512 bits.

Original message length. 16

∴ 512+16 = 528 ⇒ Total message length.

For MD5

$ml \equiv 448 \bmod 512$.

$528 \equiv 448 \bmod 512$

$16 \not\equiv 448$

432 bits shd be padded.

No. of blocks needed = 2

1(b) Maj(a,b,c) = (a and b) $\oplus$ (a and c) $\oplus$ (b and c)

```
a       = 0001000100010001 0111011101110111 0000000000000000 0001000100010001
b       = 1111111111111111 0010001000100010 0010001000100010 0001000100010001
c       = 1011101110111011 1001100110011001 0001000100010001 0010001000100010

a and b = 0001000100010001 0010001000100010 0000000000000000 0001000100010001
a and c = 0001000100010001 0001000100010001 0000000000000000 0000000000000000
⊕       = 0000000000000000 0011001100110011 0000000000000000 0001000100010001
          1011101110111011 0000000000000000 0000000000000000
b and c = 1011101110111011 0000000000000000 0000000000000000 0000000000000000
⊕       = 1011101110111011 0011001100110011 0000000000000000 0001000100010001
```

BBBB33330000 1111

Ch(e,f,g) = (e and f) $\oplus$ (Not e and g)

```
(e and f)          = 0000  0000  2222  0000
not e              = 3333  DDDD  DDDD  FFFF
(not e and g)      = 3333  1111  8888  FFFF
(e and f)⊕(not e and g) = 3333  1111  AAAA  FFFF
```

hash value $H(M) = 4$

public components $= \{p, q, h\} = \{23, 11, 7\}$

pseudorandom integer $k = 5$.

private key $x = 3$

Soln

1) Key Generation

Calculate $g = h^{(p-1)/q} \bmod p$

$= 7^{(23-1)/11} \bmod 23$

$= 7^2 \bmod 23$

$= 3$ //

Calculate $y = g^x \bmod p$

$= 3^3 \bmod 23$

$= 27 \bmod 23$

$= 4$ //

2) Signature Generation.

$k = 5$

$r = (g^k \bmod p) \bmod q$

$= (3^5 \bmod 23) \bmod 11$

$= (243 \bmod 23) \bmod 11$

$= 13 \bmod 11$

$= 2$ //

$s = [k^{-1}(H(M) + xr)] \bmod q$

$= 5^{-1}(4 + 3 \times 2)] \bmod 11$

$= [5^{-1} * 10] \bmod 11$

$= (9 * 10) \bmod 11$

$= 90 \bmod 11 = 2$

$(r, s) = (2, 2)$ //

3) Signature Verification

$w = s^{-1} \bmod q$

$= 2^{-1} \bmod 11$

$= 6$ //

$u_1 = [H(m')\, w] \bmod q$

$= [4 \times 6] \bmod q$

$= 24 \bmod 11$

$= 2$ //

$u_2 = (r')\, w \bmod q$

$= (2 * 6) \bmod 11$

$= 12 \bmod 11$

$= 1$ //

$V = [(g^{u_1} . y^{u_2}) \bmod p] \bmod q$

$= [(3^2 \times 4^1) \bmod 23] \bmod 11$

$= [(9 \times 4) \bmod 23] \bmod 11$

$= 13 \bmod 11$

$= 2$ //

$\boxed{V = r}$