



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.

1. Alice and Bob want to exchange public keys 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 $X_a = 5$ 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
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 $\alpha = 11$. 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
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
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) 10
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, FFFF22222221111, BBBB999911112222, CCCC22222220000, 1111DDDD22221111, and 33331111AAAAFFFF, respectively. (5 Marks)
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: 10
 - Generate the digital signature using DSS.
 - Signature Verification

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

$$\begin{aligned} Y_a &= g^{X_a} \mod p \\ &= 7^5 \mod 17 \\ &= 11 \end{aligned}$$

Bob

$$\begin{aligned} Y_b &= g^{X_b} \mod p \\ &= 7^4 \mod 17 \\ &= 4 \end{aligned}$$

Darth $X_{DA} = 4$

$X_{DB} = 8$

$$\begin{aligned} Y_{DA} &= 7^4 \mod 17 \\ &= 4 \end{aligned}$$

$$\begin{aligned} Y_{DB} &= 7^8 \mod 17 \\ &= 16 \end{aligned}$$

~~$$\begin{aligned} K_{DA} &= 7^{11} \mod 17 \\ &= 14 \end{aligned}$$~~

~~$$\begin{aligned} K_{DB} &= 7^4 \mod 17 \\ &= 4 \end{aligned}$$~~

$$\begin{aligned} K_A &= Y_{DA}^{X_a} \mod p \\ &= 4^5 \mod 17 \\ &= 14 \end{aligned}$$

$$\begin{aligned} K_B &= Y_{DB}^{X_b} \mod p \\ &= 16^4 \mod 17 \\ &= 1 \end{aligned}$$

$$\begin{aligned} K_{DA} &= Y_a^{X_{DA}} \mod p \\ &= 11^4 \mod 17 \\ &= 4 \end{aligned}$$

$$\begin{aligned} K_{DB} &= Y_b^{X_{DB}} \mod p \\ &= 4^8 \mod 17 \\ &= 1 \end{aligned}$$

② Elgamal Cryptosystem.

prime number $q = 17$

Generator value $\alpha = 11$

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

Message = 7

$$\text{public key of user B} = Y_A = \alpha^{X_A} \bmod q$$
$$= 11^6 \bmod 17$$

$$\boxed{Y_A = 8}$$

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

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

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

$$= 8^5 \bmod 17$$
$$\boxed{K = 9}$$

$$\text{Calculate } C_1 = \alpha^k \bmod q$$

$$= 11^5 \bmod 17$$

$$C_1 = 10$$

$$\text{Calculate } C_2 = KM \bmod q$$

$$= 9 * 7 \bmod 17$$

$$C_2 = 12$$

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

Decryption by User A with Private key.

$$\begin{aligned}\text{Calculate } K &= (C_1)^x \bmod q \\ &= 10^6 \bmod 17 \\ &= 9.\end{aligned}$$

$$\begin{aligned}\text{plain Text } M &= (C_2 K^{-1}) \bmod q \\ &= 12 \times 9^{-1} \bmod 17 \\ &= (12 \times 2) \bmod 17 \\ &= 24 \bmod 17\end{aligned}$$

$$\boxed{M = 7}$$

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

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

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

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

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

$$= \frac{714}{20} \bmod 23$$

$$= \frac{10}{5}$$

$$= \frac{7}{5} \bmod 23$$

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

$$= 6 //$$

$$\begin{aligned}
 x_3 &= \lambda^2 - x - x \pmod{p} \\
 &= 6^2 - 3 - 3 \pmod{23} \\
 &= 36 - 6 \pmod{23} \\
 &= 30 \pmod{23} \\
 &= 7 //
 \end{aligned}$$

$$\begin{aligned}
 y_3 &= \lambda(x - x_3) - y \pmod{p} \\
 &= 6(3 - 7) - 10 \pmod{23} \\
 &= 6(-4) - 10 \pmod{23} \\
 &= -24 - 10 \pmod{23} \\
 &= -34 \pmod{23} \\
 &= 23 - (34 \pmod{23}) \\
 &= 23 - 11 = 12 //
 \end{aligned}$$

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

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

Secret integer $k = 2$.

$$\begin{aligned}
 \text{Ciphertext } C &= [(kG), (M + kP_u)] \\
 &= [C_1, C_2]
 \end{aligned}$$

$$\begin{aligned}
 C_1 &= kG \\
 &= 2(3, 10)
 \end{aligned}$$

$$\begin{aligned}
 C_2 &= M + kP_u \\
 &= (9, 7) + 2(7, 12)
 \end{aligned}$$

$P_m = M$
 P_u - public key

$$\begin{aligned}
 C &= [2(3, 10), (9, 7) + 2(7, 12)] \\
 &= [(7, 12), (9, 7) + 2(7, 12)]
 \end{aligned}$$

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

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

$$= \frac{148}{24} \bmod 23$$

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

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

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

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

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

$$= 86 \bmod 23$$

$$= 17$$

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

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

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

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

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

$$= 23 - 20$$

$$= 3$$

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

Now compute

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

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

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

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

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

$$= -12 \bmod 23$$

$$= 23 - 12$$

$$\boxed{\lambda = 11}$$

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

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

$$= 121 - 26 \bmod 23$$

$$= 95 \bmod 23$$

$$= 3 //$$

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

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

$$= 11 \times 6 - 7 \bmod 23$$

$$= 66 - 7 \bmod 23$$

$$= 59 \bmod 23$$

$$= 13 //$$

$$\text{Cipher Text} = [c_1, c_2]$$

$$= [(1, 12), (3, 13)] //$$

4a SHA512

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

Original message Length. 16

$$\therefore 1024 + 16 = \underline{1040} \Rightarrow \text{Total message length.}$$

For SHA512

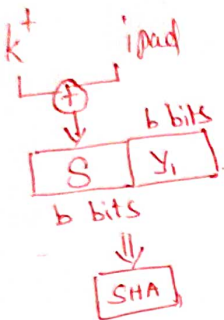
$$mL \equiv 896 \pmod{1024}$$

$$1040 \equiv 896 \pmod{1024}$$

$$16 \neq 896$$

880 bits shd be padded.

No. of blocks needed = 2



MD5

Key is padded to 512 bits.

Original message length. 16

$$\therefore 512 + 16 = \underline{528} \Rightarrow \text{Total message length.}$$

For MD5

$$mL \equiv 448 \pmod{512}$$

$$528 \equiv 448 \pmod{512}$$

$$16 \neq 448$$

432 bits shd be padded.

No. of blocks needed = 2

16) $\text{Maj}(a, b, c) = (a \text{ and } b) \oplus (a \text{ and } c) \oplus (b \text{ and } c)$

$a = 00010001000100010111011101110111000000000000000000010001000100010001$

$b = 111111111111111100100010010001000100010001000100010001000100010001$

$c = 1011101110111011100110011001100110011001100110011001100110011001$

$a \text{ and } b = 000100010001000100100010001000100000000000000000000000000000000000$

$a \text{ and } c = 000100010001000100010001000100010000000000000000000000000000000000$

$\oplus = 000000000000000000110011001100110011000000000000000000000000000000$

$b \text{ and } c = 101110111011101100$

$\oplus = 101110111011101100110011001100110000000000000000000000000000000000$

BBBB333300001111

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

$(e \text{ and } f) = 0000 \quad 0000 \quad 2222 \quad 0000$

$\text{not } e = 3333 \quad \text{DDDD} \quad \text{DDDD} \quad \text{FFFF}$

$(\text{not } e \text{ and } g) = 3333 \quad 1111 \quad 8888 \quad \text{FFFF}$

$(e \text{ and } f) \oplus (\text{not } e \text{ and } g) = 3333 \quad 1111 \quad \text{AAAA} \quad \text{FFFF}$

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

$$\begin{aligned}\text{Calculate } g &= h^{(p-1)/q} \mod p \\ &= 7^{(23-1)/11} \mod 23 \\ &= 7^2 \mod 23 \\ &= 3 //\end{aligned}$$

$$\begin{aligned}\text{Calculate } y &= g^x \mod p \\ &= 3^3 \mod 23 \\ &= 27 \mod 23 \\ &= 4 //\end{aligned}$$

2) Signature Generation

$k = 5$

$$\begin{aligned}r &= (g^k \mod p) \mod q \\ &= (3^5 \mod 23) \mod 11 \\ &= (243 \mod 23) \mod 11 \\ &= 13 \mod 11 \\ &= 2 //\end{aligned}$$

$$\begin{aligned}s &= [k^{-1} (H(M) + x r)] \mod q \\ &= 5^{-1} (4 + 3 \times 2) \mod 11 \\ &= [5^{-1} * 10] \mod 11 \\ &= (9 * 10) \mod 11 \\ &= 90 \mod 11 = 2\end{aligned}$$

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

3) Signature Verification

$$\begin{aligned}w &= s^{-1} \bmod q \\&= 2^{-1} \bmod 11 \\&= 6\end{aligned}$$

$$\begin{aligned}u_1 &= [H(m') w] \bmod q \\&= [4 \times 6] \bmod q \\&= 24 \bmod 11 \\&= 2\end{aligned}$$

$$\begin{aligned}u_2 &= (r') w \bmod q \\&= (2 \times 6) \bmod 11 \\&= 12 \bmod 11 \\&= 1\end{aligned}$$

$$\begin{aligned}V &= [(g^{u_1} \cdot y^{u_2}) \bmod p] \bmod q \\&= [(3^2 \times 4^1) \bmod 23] \bmod 11 \\&= [(9 \times 4) \bmod 23] \bmod 11 \\&= 13 \bmod 11 \\&= 2\end{aligned}$$

$$\boxed{V = 2}$$