SL.NO:CAA 187381

# SRI SIVASUBRAMANIYA NADAR COLLEGE OF ENGINEERING

(An Autonomous Institution, Affiliated to Anna University, Chennai)
Rajiv Gandhi Salai (OMR), Kalavakkam - 603 110

## THEORY EXAMINATIONS

88%

| | | | |
|---|---|---|---|
| Register Number | 205001085 | | |
| Name of the Student | V. Sabariyasan | | |
| Degree and Branch | BE CSE | Semester | V |
| Subject Code and Name | UCS1505 Introduction to Cryptographic Techniques | | |
| Assessment Test No. | III | Date | 17/11/2022 |

**Details of Marks Obtained**

| Part A Question No. | Part A Marks | Part B Question No. | Part B (a) Marks | Part B (b) Marks | Part B Total Marks | Part C Question No. | Part C (a) Marks | Part C (b) Marks | Part C Total Marks |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 7 | 5 | | 5 | 10 | 9 | | 9 |
| 2 | 2 | | | | | | | | |
| 3 | 2 | 8 | 4 | | 4 | 11 | | | |
| 4 | 2 | | | | | 12 | | | |
| 5 | 2 | 9 | 5 | | 5 | 13 | 10 | | 10 |
| 6 | 1 | | | | | | | | |
| Total (A) | 11 | Total (B) | | | 14 | Total (C) | | | 19 |

| | | | |
|---|---|---|---|
| Grand Total (A+B+C) | 44 | Marks (In Words) | Four Four |
| Signature of the Faculty | | | |

ssn

## PART-C

(10)

**RSA Algorithm (Rivest-Shamir-Adleman)**

1) This is an algorithm used for public-key cryptograph.

2) Choose two large prime numbers (p, q).

3) Calculate $n = p \times q$.

4) Find the Euler totient $\phi(n)$

$$\phi(n) = (p-1)(q-1)$$

5) Choose a value for 'e' (encryption) where it should be $1 < e < \phi(n)$ and $\gcd(\phi(n), e) = 1$.

6) Find the value of 'd' (decryption) where, $d = e^{-1} \bmod \phi(n)$.

7) The public key is denoted by $<e, n>$.

8) The private key is denoted by $<d, n>$.

ssn

⇒ Encryption:

The ciphertext value (c) is derived by $c = m^e \bmod (n)$ where $m < n$.

⇒ Decryption:

The message value (m) is derived by $m = c^d \bmod (n)$.

Problem

$p = 17$, $q = 11$, $e = 7$, $M = 88$.

⇒ $n = pq = 17 \times 11 = 187$

⇒ $\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$

⇒ $e = 7$ and $\gcd(7, 160) = 1$

⇒ $d = e^{-1} \bmod \phi(n)$

$ed \bmod \phi(n) = 1$

$(7 \times 23) \bmod 160 = 1$

$161 \bmod 160 = 1$

$\therefore \boxed{d = 23}$

ssn

⇒ Public key = $<7, 187>$

⇒ Private key = $<23, 187>$

⇒ Encryption:

$c$ — $m$ Let $m = 2$.

$c = 2^7 \bmod (187)$

$\boxed{c = 128}$

⇒ Decryption:

$m = 128^{23} \bmod (187)$

$\boxed{m = 2}$

15

## Elgamal signature and Encryption

⇒ The algorithm is used for encryption and decryption in public-key cryptography.

⇒ A large prime number is chosen (q).

⇒ After choosing, calculate the primitive root of the choosen prime number ($\alpha$).

⇒ Choose a random value for $X_A$ where $1 < X_A < q-1$ and $X_A$ is the private key for user A.

⇒ Derive $Y_A = \alpha^{X_A} \bmod q$ where $Y_A$ is the public key for user A.

⇒ Finally the generated keys for user A are,

Private key = $X_A$.

Public key = $\{q, \alpha, Y_A\}$

⇒ A hashcode is generated using a hash function for the message where $m = H(M)$ and $0 \leq m \leq q-1$.

⇒ After that a random integer k is choosen, where $1 < k \leq q-1$ and

⇒ $\gcd(k, q-1) = 1$.

⇒ Calculate the values of $S_1, S_2$ where $S_1 = \alpha^k \bmod q$ and

$S_2 = k^{-1}(m - X_A S_1) \bmod (q-1)$

⇒ Final signature pair is $(S_1, S_2)$.

### Now at User B side

⇒ Find values of $V_1$ and $V_2$ where

$V_1 = \alpha^m \bmod q$.

$V_2 = (Y_A)^{S_1} (S_1)^{S_2} \bmod q$.

⇒ If $V_1 = V_2$, then both signatures are valid, otherwise both are invalid.

Eg:

$\Rightarrow q = 3$

$\Rightarrow$ Find $\alpha$ (primitive root)

$\alpha^1 \bmod q \Rightarrow 5 \bmod 3 = 2.$

$\alpha^2 \bmod q \Rightarrow 25 \bmod 3 = 1$

$\therefore \boxed{\alpha = 5}$

$\Rightarrow$ Let $\boxed{X_A = 2}$

$\Rightarrow Y_A = \alpha^{X_A} \bmod q$

$= 5^2 \bmod 3$

$\boxed{Y_A = 1}$

$\Rightarrow$ Private key $= 2.$

$\Rightarrow$ Public key $= \{3, 5, 1\}$

$\Rightarrow$ Calculate hashcode value

$m = H(m)$

Let $m = 2$ //

$\Rightarrow$ Random integer $k = 2$

$\Rightarrow S_1 = \alpha^k \bmod q$

$= 5^2 \bmod 3 = 1.$

$\Rightarrow S_2 = k^{-1}(m - X_A S_1) \bmod (q-1)$

$k^{-1} \bmod q-1$

$2^{-1} \bmod 2$

$5x = 1 \pmod 2$

$k^{-1} = 2$ //

$S_2 = 2(2 - 2(1)) \bmod (2)$

$= 2(1) \bmod (2)$

$= 2$ //

$\Rightarrow$ Signature pair $= (1, 2).$

In User B side

$V_1 = \alpha^m \mod q$

$= 5^2 \mod 3 = 1$

$V_2 = (Y_A)^{s_1} (S_1)^{s_2} \mod q$

$= 1 \cdot 1^2 \mod 3 = 1.$

$\therefore V_1 = V_2$

$\therefore$ Both signatures are valid.

PART-B

11

(7) → Before introducing public key cryptography technique, private key cryptography was used before.

⇒ In private-key cryptography, same algorithm and a single key is used by both the users. Hence it is also known as symmetric key cryptography.

⇒ The problem in private key cryptography is if any attacker gets involved ~~in between~~ in a communication held between 2 users, there are high chances of the private key can be known to the attacker.

⇒ After that public key cryptography was introduced which brings the concept of using a private key and a public key.

⇒ The public key is used for encryption and is known only to both the users. But the private key is used for decryption and is known only by the user itself.

⇒ If an attacker gets into a communication and acquires the public key, it is highly impossible for the attacker to get the private key from the public key.

⇒ Same algorithm and key is used by two users in case of symmetric key cryptograph. But in public key cryptograph, one algorithm is used for encryption and decryption and each user has a private key.

⇒ That is why public key cryptography is also known as asymmetric key cryptography.

⇒ Hence, online services can be benefit from public-key cryptography.

PART - A

ssn

(2) Disputes in digital signature

1) Fraud or forgery.

2) Reliability.

---

(3) Properties of digital signature

(1) A signature sent cannot be modified again

(2) A signature must be unique.

(3) A signature must be highly impossible to be lead to forgery

(4) Must maintain reliability.

---

(4) $p = 17, q = 13.$

$\Rightarrow n = pq = 17 \times 13 = 221$ //

$\Rightarrow \phi(n) = (p-1)(q-1) = 16 \times 12 = 192$ //

(5)

(1) Applications of public-key cryptography ssn

$\Rightarrow$ Encryption / Decryption

$\Rightarrow$ Key generation

$\Rightarrow$ Digital signature.

---

(6) Given = 11.

$\Rightarrow$ Set = $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$\Rightarrow$ Primitive roots = $\{2, 3, 4, 5, 6, 7, 8, 9, 10\}$ $\alpha$

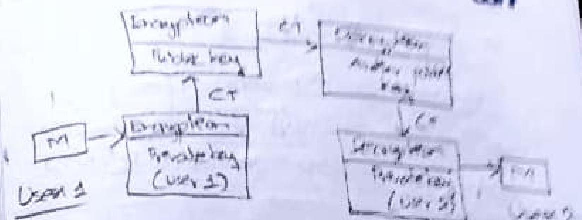
$\therefore$ 9 primitive roots.

(8) Hybrid encryption.

=> Hybrid encryption is a type of encryption algorithm in which both private keys and public keys are used for encryption process.

=> The encryption is initiated by usage of private key of user A. After that, an additional layer of cipher text is added but encrypting again with the usage of public key of user B.

=> For in case of user B, the ciphertext gets decrypted first by the another public key holded by user A. After that the final layer of cipher text is decrypted by the private key of user B.




(9) Key Generation

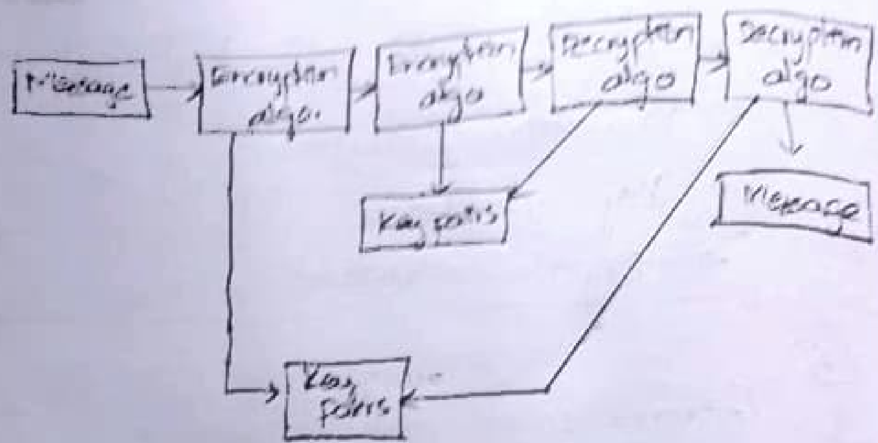
=> At first, key generation is done first. In key generation process, both private and public keys are generated.

=> public key is represented by (p,q,g) where p and q are large prime numbers and 'g' is the generating random value.

=> Private key is represented by large prime number (q).

=> Value of g can be $g = h^{(p-1)/q}$ where 'h' is hash value.

5




⇒ The encryption algorithm is applied on the message with the use of public key

⇒ The decryption algorithm is applied on the ciphertext with the use of private key.

⇒ The key-pairs are nothing but hold the private and public key information.

ssn

⇒ Private key ($x < q$)

⇒ Public key ($y = g^x \bmod p$)

Signature creation

⇒ In this method, a signature is added to message M from the sender.

⇒ At first, random signature key is generated ($k < q$)

⇒ signature pairs will be $(r, s)$ where

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

$$s = (k^{-1}(H(M) + r)) \bmod q.$$

⇒ Sends the signature pair $(r, s)$ with the message.

Signature verification

ssn

⇒ In this process, the message is received along with signature pair $(r, s)$

⇒ Calculate $w = s^{-1} \bmod q$.

⇒ $u_1 = [H(m)w] \bmod q$.

⇒ $u_2 = [rw] \bmod q$.

⇒ $v = (g^{u_1} y^{u_2} \bmod p) \bmod q$.

⇒ If the value of v is valid is receiver side, the signature pair is said to be valid, otherwise they are not valid.