

CBCS SCHEME

18CS744



Seventh Semester B.E. Degree Examination, June/July 2023 Cryptography

Time: 3 hrs.

Max. Marks: 100

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Module-1

- 1 a. Give and explain the 3 independent dimensions of Cryptographic Systems. (06 Marks)
- b. A message received at an Australian wireless station in play fair code : KXJEY UREBE key used was ROYAL NEW ZEALAND NAVY. Decrypt the message. (08 Marks)
- c. In the One – time pad version of a Vignere Cipher , Key stream is 9 0 1 7 23 15 21 14 11 11 2 8 9. In this scheme, encryption is done by shifting with number mentioned in the key. Encrypt the plain text sendmoremoney and using the Cipher text obtained, find a key such that Cipher text decrypts to cashnotneeded. (06 Marks)

OR

- 2 a. Differentiate Confusion and Diffusion. With a structure, explain the working of Fiestel Encryption and Decryption. (07 Marks)
- b. Encrypt the message “MAM” using Hill cipher with key
$$A = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$
Further show the calculations for corresponding decryption of Cipher text to recover plain text. (08 Marks)
- c. Given data – 208 amd IP = [4 1 8 2 3 5 6 7] (IP means Initial Permutation). Find the permutation of the data and its inverse. (05 Marks)

Module-2

- 3 a. Differentiate Public Key Encryption and Conventional Encryption. Classify and explain Public Key Cryptosystems. (06 Marks)
- b. In a Public key system using RSA, you intercept the ciphertext $C = 10$ sent to a user where $n = 221$. What is the plaintext. (07 Marks)
- c. “Diffie – Hellman key exchange is vulnerable to Man – in – The – middle attack”. Substantiate with a sequence diagram. (07 Marks)

OR

- 4 a. Design Public key encryption system for secrecy and Authentication separately. (06 Marks)
- b. Consider a Diffie – Hellman scheme with common prime, $q = 11$ and primitive root $\alpha = 2$.
 - i) Show that 2 is a primitive root of 11.
 - ii) If user has public key $Y_A = 9$, what is A’s private key X_A .
 - iii) If user B has public key $Y_B = 3$, what is secret key K shared with A. (07 Marks)
- c. Consider an Elgamal scheme with common prime $q = 71$ and primitive root $\alpha = 7$. If B has public key $Y_B = 3$ and A choose random integer $K = 2$, what is Cipher text of $M = 301$. If A now chooses different value of K , so that encoding of $M = 30$ is $C = (59, C_2)$ what is C_2 ? (07 Marks)

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, $42+8 = 50$, will be treated as malpractice.

Module-3

- 5 a. Give the Geometric and Algebraic description of Addition on Elliptic curves over real number. (07 Marks)
- b. Prove that elliptic curve equation $y^2 = x^3 + 10x + 5$ does not defines group over Z_{17} . Consider elliptic curve $E_{11}(1, 6)$ defined by $y^2 = x^3 + x + 6$ with modulus = 11. Determine all points in $E_{11}(1, 6)$. (09 Marks)
- c. Cryptosystem parameters $E_{11}(1, 6)$ and $G = (2, 7)$. B's private key $n_B = 3$. Find B's Public key P_B . (04 Marks)

OR

- 6 a. Explain the working of Micali – Schnorr Pseudorandom Bit Generator. (06 Marks)
- b. Define Control Vector. Explain the Coupling and Decoupling process with control vector. (07 Marks)
- c. Consider an elliptic curve over $GF(2^4)$ with irreducible polynomial $f(x) = x^4 + x + 1$. Develop power of g , (generator with $g^4 = g + 1$) and check whether point (g^6, g^8) exists in this curve with equation $y^2 + xy = x^3 + g^4 x^2 + 1$. (07 Marks)

Module-4

- 7 a. Write and explain general format of X.509 certificate. (08 Marks)
- b. With a figure, bring out the relationship among keyelements of PKIX model. (07 Marks)
- c. With a sequence diagram, illustrate the Kerberos exchanges among the parties. (05 Marks)

OR

- 8 a. Consider one way authentication technique based on asymmetric encryption : $A \rightarrow B : IDA$
 $B \rightarrow A : E(PVa, R_2)$ $A \rightarrow B : R_2$. Explain the protocol and what type of attack this protocol is susceptible to? (05 Marks)
- b. "PGP has grown explosively and is widely used". Enlist the reasons coated for this growth. (05 Marks)
- c. Summarize the different cryptographic algorithms used in S/MIME with its function and requirement. Explain the motivating factors of DKIM and also illustrate deployment of DKIM with a simple example. (10 Marks)

Module-5

- 9 a. Depict and explain IPSec Architecture. Explain the parameters required for Security Association. (10 Marks)
- b. Write the top level format of an ESP packet and explain the fields. Differentiate Transport and Tunnel mode of Encryption. (10 Marks)

OR

- 10 Write short notes on :
- a. Protocol Operation for ESP.
- b. Basic Combinations of Security Associations.
- c. Features of key Determination in IKE.
- d. Cryptographic suites. (20 Marks)

* * * * *