2023

COMPUTER SCIENCE

Paper : CSMC-204

(Cryptography and Network Security)

Full Marks : 70

The figures in the margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable.

Answer ***Question nos.*** **1, 2** and ***any four*** from the rest.

1. Answer ***any five*** questions : 2×5

(a) State the role of Trap door one way function in Cryptography.

(b) Test the primality of the integer 19 using square root test.

(c) Is it possible to perform an encryption algorithm in parallel on multiple blocks of Plaintext?

(d) What is Euler's Totient function? Compute the value of Φ (32).

(e) Is AES a Feistel cipher? Justify your answer.

(f) A club has only 100 members. How many secret keys are needed for the given cases?

(i) If everyone trusts the President of the club, i.e., messages are transferred between members through President.

(ii) If President decides that two members should communicate, then the President creates a temporary key to be used between the two. The temporary key is encrypted and sent to both members.

(g) Give an example of Cryptanalysis attack. How is it different from Brute force attack?

2. Answer ***any five*** questions : 4×5

(a) In the elliptic curve E(l, 2) over G(l 1) field, state the equation of the curve and find all the points on the curve.

(b) Discuss the importance behind choosing the algebraic structure $< Z\Phi(n)^*, x >$.

(c) Show that the group $< Z_7, X >$ is a cyclic group.

(d) Compare between the principal ideas followed by the entity authentication schemes : Password based, Challenge Response, and Zero Knowledge Proof.

(e) Why do you think the mixing transformation (MixColumn) is not needed in DES, but is essential in AES?

(f) "Sub-key generation process also affects the strength of an encryption technique." — Comment with justification in the context of DES algorithm.

(g) Determine the multiplicative inverse of $X^3 + X + 1$ in GF (2^4) with irreducible polynomial $X^4 + X + 1$.

3. (a) Illustrate the working principle of Hill Cipher considering Plaintext = "We live in an insecure world" and Key is equal to K = [03 02].
[05 07]

(b) Describe the trust model used by PHP protocol through an example. 6+4

4. (a) Describe the Elgamal Cryptosystem.

(b) Show that the complexity of the encryption algorithm is computationally easy.

(c) Show that finding out the PT from CT by an intruder becomes computationally infeasible whereas for an authorised person it is computationally easy. 5+3+2

5. (a) State the conditions that a hash function should satisfy.

(b) Prove that the difficulty of the Pre-image attack in message integrity is proportional to 2^n, where n is the number of bits.

(c) Describe the Needham-Schroeder algorithm for both way authentications. 3+3+4

6. (a) Describe the Clogging attack in context of Key Exchange protocol. How can it be prevented?

(b) Define the term "authentication" and "Integrity".

(c) How the HMAC algorithm differs from MD5? (3+2)+2+3

7. (a) Why are the probabilistic algorithms preferable over deterministic algorithm for finding prime number?

(b) Describe Miller-Rabin test for generating strong pseudo-prime.

(c) How the CFB mode is used for generating stream cipher? 2+5+3

8. (a) Describe the RSA based Digital Signature scheme.

(b) Is it possible to offer the service 'non-repudiation' through Digital Signature? Justify your answer. 5+5