

2016

Time : 3 hours

Full Marks : 80

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

The questions are of equal value.

*Answer **five** questions in which Q. No. 1 is compulsory.*

1. Choose the correct option of the following :

   (a) There are n stations in a slotted lab. Each station attempt to transmit with a probability p in each time slot. What is the probability that only one station transmit in a given slot ?

   (i) $pn(1-p)n-1$ (ii) $P(1-p)^{n-1}$

   (iii) $n(1-p)^{n-1}$ (iv) $1-(1-p)^{n-1}$

   (b) Using data p = 3, q = 11, n = p × q and = 7 in RSA algorithm. Find the cipher text of the given plain text SUZANNE :

   (i) ENNAZUS (ii) BUTAEEZ

   (iii) SUZANNE (iv) BUTAZEN

(c) Match the following cryptographic algorithms with their design issued :

List 1	List 2
(a) DES	(1) Message digest
(b) AES	(2) Public key
(c) RSA	(3) 56-bit key
(d) SHA-1	(4) 128-bit key

Codes :

	(a)	(b)	(c)	(d)
(i)	2	1	4	3
(ii)	3	1	4	2
(iii)	3	4	2	1
(iv)	4	1	2	3

(d) The period of a signal is 100 ms. What is its frequency in kHz ?

(i) 100 kHz (ii) 10^2 kHz

(iii) 10^{-3} kHz (iv) 10^{-2} kHz

(e) In crytography OTP stands for :

(i) One time password

(ii) One true pairing

(iii) None of these

(iv) One time pad

(f) To guarantee the detection of up to serrors in all cases, the minimum hamming distance d_{min} in a block code must be :

(i) S

(ii) S + 1

(iii) S^2

(iv) $S^2 + 1$

(g) Find reminder when 41 devides 220 – 1 :

(i) 0

(ii) 1

(iii) 2

(iv) 3

(h) Duty cycle for a clock is always :

(i) 10%

(ii) 35%

(iii) 50%

(iv) 75%

7. Explain cryptography & Discuss cryptanalysis

2. List the sequence of steps used in the DES function box in the DES algorithm.

3. Define Diffie Hellman key agreement algorithm with a suitable example.

8. Explain Network Sec. & discuss data comm

4. What are the Equivalence Classes ? How many equivalence classes under modulus are possible ? Compute the residue of (200) ; using equivalence classes.

5. Define digital signature, illustrate some difference between a digital signature and digital certificate.

6. Define Euclid Algorithm with their suitable properties, write code for calculating the GCD.

7. What is the difference between ARP and RARP ?

8. What is Authentication Protocol ? Discuss their PAP, CHAP and EAP types and purpose.

9. Discuss Chinese Reminder Theorem and prove that for any, such that and there is an integer such that : and.

9. Explain OSI System structure
Discuss diff layer.