CRYPTOGRAPHY

MULTIPLE CHOICE QUESTIONS-

1. Find 3^{201}mod11.

a) 4 b) 3

c) 12 d) 0

Ans:- a),3

2. Find a number a between 0and 9 such that a iscongurent to 7^{1000} modulo 10.

a) 6 b) 7

c) 1 d) 0

Ans:- (c),1

3. Value of Phi(440).

a) 120 b) 160

c) 440 d) 240

Ans:- (b),160

4. Which of the following attacks are addressed by messageauthentication.

a) Masquerade b) content modification

c) sequence modification d) timming modification

Ans:-a,b,c and d

5.Consideran Eigamal scheme with a common prime q= 71 and a primitive prime root r=7 if Y_B=3 AND A RANDOM INTEGER K=2 WHAT IS CYPHERTEXT OF m=30 .

a) (49, 57) b) (48,56) c) (0,0) d) none of the above.

Ans:- a) (49, 57)

6. Which of the following is/are principal elements of public key Cryptosystem.

a) plaintext b) encryption algorithm

c) ciphertext d) none of the above

Ans:-a,b,c

7. Which of the following is/are basic arithmetical and logical functions are used in whirlpool .

a) XOR b) addition over finite field

c) circular shifts d) none of the above

Ans:–a,b,c

8.For the groups S_n of all permutations of n distinct symbols then what is the number of elements in S_n .

a) n! b) n c) (n-1) d) n^2

Ans:- (a),n!

9. The value of x in 9*x is congruent to 8 modulo 7.

a) 4 b) 5 c) 6 d) 0

Ans:– (a), 4

10. The process of every possible key untill an intelligible translation of the cipher text in plaintext is obtained is called

a) Brute-Force attack b) Computationally secure

c) Unconditionally secure d) None of the above

Ans:- (a), Brute-Force attack.

11. Which of the followings are the parameters of Feistel network

a) block size b) number of rounds

c) key size d) all of the above

Ans:- (a),(b),(c) and (d).

12. In which of the following year The Data Encryption Standard (DES) was adopted

a) 1999 b) 1998

c) 1977 d) 1996

Ans:- (c), 1977.

13. gcd(60,24) is equal to

a) 10 b) 12

c) 15 d) 19

Ans:- (b), 12.

14. If a is an integer and n is a positive integer , a mod n is the remainder when a is divided by n. The integer n is called

a) Dividend b) Modulus

c) Divisor d) None of the above

Ans:- (b), Modulus.

15. The value of 4(mod 23) is equal to

a) 90 b) 99
c) 70 d) 73
Ans:- (d), 73.

16. The equation
gcd(a,b) = gcd(b , a mob b)
a) is true b) is false
c) may or may not be true d) None of the above
Ans:= (a), is true.

SUBJECTIVE QUESTIONS-

1. Define rail fence.
Ans. In rail fence the plaintext is written down as a sequence of diagonals and then read off as asequence of rows.

2. What is substitution in Feistel Cipher?
Ans. The process of uniquely replacing each plaintext element or group of elements by a corresponding cipher text element or group of elements is called substitution.

3. Name the two criteria used to validate that the sequence of numbers is random.
Ans. (a) Uniform distribution
(b)Independence.

4. Name unpredictability of pseudorandom numbers.
Ans. A stream of pseudorandom numbers should exhibit two forms of unpredictability:

a) Forward unpredictability
b) Backward unpredictability.

5. What is the difference between mechanism diffusion and confusion?
Ans. The mechanism of diffusion seeks to make the statistical relation between the plaintext and ciphertext as complex as possible in order to thwart attempts to deduce the key.

On the other hand, confusion seeks to make the relationship between the statistics of the ciphertext and the value of encryption key as complex as possible.

6. Write the three properties of modular arithmetic.
Ans. i) [(a mod n) + (b mod n)] mod n = (a+b)mod n
ii) [(a mod n) - (b mod n)] mod n = (a-b)mod n
iii) [(a mod n) * (b mod n)] mod n = (a*b)mod n

7. What are two general approaches to attacking a cipher?
Ans. The two general approaches to attacking a cipher are:-

a) Cryptanalysis
b) Brute-Force attack.

8. Encrypt the word 'explanation' using the key leg.
Ans.Key :legleglegle
Plaintext : explanation
Ciphertext : PBVWETLXOZR.

9. Statement of Fermat's theorem.

Ans – $a^{p-1}=1(\text{mod } p)$

10. What are some approaches tp produce message authentication ?

Ans – Message encryption, message authentication, hash function.

11. What are two different uses of public key cryptography related to key distribution?

Ans – 1.The distribution of public keys.

2. The use of public key encryption to distribute secret keys.

12. The digital signature technique to avoid triple encryption of the entire message?

Ans- The use of a hash function avoids the need for triple encryption.

13. What are three broad categories of applications of public key cryptosystem?

Ans-Encryption/decryption, digital signature, key exchange.

15. What are basic arithmetical and logical functions are used in SHA?

Ans- Addition modulo, circular shift Boolean functions based on AND, OR, NOT and XOR.