Ref. No.: EX/IT/T/322/2017

B.E. INFORMATION TECHNOLOGY
THIRD YEAR SECOND SEMESTER 2017
Subject: CRYPTOGRAPHY & NETWORK SECURITY

Time: 3 Hours **Full Marks: 100**

Answer from each group

Group I

(Answer any ten Questions) **1 * 10 = 10**

1. The ..... attack is related to confidentiality.
2. In an asymmetric-key cryptography, the sender uses the ..... key.
3. Interruption attacks are also called as ..... attack.
4. ..... rounds are present in IDEA.
5. Caesar Cipher is an example of .....
6. The mechanism of writing text as rows and reading as columns is called as .....
7. EDE stands for .....
8. DES encrypts blocks of ..... bits.
9. ..... ,..... and ..... inputs are needed in one round in MD5 .
10. After key transformation process ..... key-bit is present in DES.
11. DSA stands for .....

Group II

(Answer any ten Questions) **2 * 10 = 20**

1. What is cryptography and cryptanalysis?
2. Difference between public key and symmetric key cryptography.
3. Find gcd(60, 24) using Euclidean algorithm.
4. Determine $\varphi(37)$ using Euler's Totient Function.
5. What is Brute-force attack?
6. Simplify this binary number (1 0 1 1 0 1) using **s-box** process.
7. Explain expansion permutation in DES.
8. Define confusion and diffusion.
9. What is P in MD5, explain P in round(1).
10. Original number is 7391743, create a MD.
11. Describe round numbers, no. of plain text bits and key size are used in AES.

Group III

(Answer any five Questions) **5 * 6 = 30**

1. Explain principle of security. 6

2. What is polygram substitution cipher? Encrypt " HOW ARE YOU" using Vernam cipher. 2 + 4

3. What is bucket bridge attack? Explain the process. 1 + 5

4. Explain triple DES encryption process using three keys and two keys. 3 + 3

5. Why we use (*) in IDEA? Explain Sub-key generation process in IDEA . 3 + 3

6. Calculate N, d and e in RSA algorithm using p=7 and q=17 . 6

Group IV

(Answer any four Questions) **4 * 10 = 40**

1. a) Explain RSA algorithm.
   b) Encrypt and decrypt the message "F" using RSA algorithm with private key(119,77) and public key(119,5). 4 + 6

2. a) Explain Diffie-Hellman key exchange protocol.
   b) Prove that the result of G^{xy} mod N is the same as the result of $(G^x \bmod N)^y \bmod N$, using G = 7, x = 2, y = 3 and N = 11. 4 +6

3. Explain this mathematical expression a single MD5 operation in short form.
   $a = b + ((a + \text{Process } P(b, c, d) + M[i] + T[k]) <<< s)$ 10

4. a) What is HMAC?
   b) Use a block cipher to encrypt and decrypt a message. The plaintext blocks of this message are m1, m2 and m3, and the encryption and decryption functions of this block cipher are EK and DK, respectively. Give mathematical equations of both the encryption and decryption operations when the following modes of encryption are used, respectively: (i) ECB (Electronic Code Book mode), and (ii) CBC (Cipher-Block-Chaining mode). 2 + 8

5. What is Rijndael algorithm? In AES w[0] to w[3] contains Hex value, so calculate w[4] using previous Hex values.
   clue: tmp = Substitute(Rotate(temp)) XOR Constant [i/4]. 2 + 8