Department of Computer Science & Engineering
LOKNAYAK JAI PRAKASH INSTITUTE OF TECHNOLOGY
Chapra, Bihar

Academic Session 2018-19 (VIII Semester)

INFORMATION SECURITY (IT 1805)

Time: 2 Hour **Max Marks: 20**

Assignment-1

PART A

Q1. Which of the following security attack is threat to integrity?

a). Traffic analysis **b). Repudiation**

c). Snooping **d). Denial of Service**

Q2. Which one is not belongs to Passive attack

a) Traffic Analysis **b) Interception**

c) Interruption **d) Snooping**

Q3. Which happens first authorization or authentication?

a) Authorization **b) Authentication**

c) Both are same **d) None of the mentioned**

Q4. If an attacker stole a password file that contained one way encrypted passwords, what type of an attack would he/she perform to find the encrypted password?

a) Man- in-the middle attack **b) Birthday attack**

c) Denial of service attack **d) Dictionary attack**

Q5. The input block length in AES is:

a) 56 bits

b) 64 bits

c) 112 bits

d) 128 bits

PART B

Q.1 Differentiate between active and passive security threats with an example**.**

Q.2 Explain the problems with one-time pad with an example**.**

Q.3 Encrypt the message **"attackxatxdawn"** using a double transposition cipher with 4 rows and 4 columns**,** using

the row permutation

(1,2,3,4) ------------> (2,4,1,3)

and the column permutation

(1,2,3,4) --------------> (3,1,2,4).

Q.4 Explain simple substitution cipher with an example.

Q.5 Differentiate between feistel cipher and non-feistel cipher in detail with an example.

Q.6 Explain Project VENONA with its all features in detail.

Q.7 Write a short notes on Fingerprint recognition and Iris recognition.

Q.8 Explain Knapsack Algorithm with suitable example.

Q.9 Explain Codebook Cipher.

Q.10 Explain DES and Triple DES with suitable Diagram.

Q.11 Define the following Terms:

a. Stream Cipher

b. Block Cipher

c. Application of Public key Crypto

d. Biometric

e. Authentication Methods

Q.12 Use Chinese Remainder Theorem (CRT) to find the number which is repeatedly divided by 3 gives remainder as 2; when divided by 5 gives remainder as 3; and divided by 7 the remainder is 2. What is the Number?

Q.13 Alice wants to send a message M with a Digital Signature Sig(M) to Bob. Alice and Bob have authentic copy of each others public keys, and have agrred on using a specific hash function H. Outline the steps that Alice must follow when signing M, and the steps that Bob must follow for validating the signature Sig(M). Explain with suitable diagram.

Q.14 Explain Malware? What are the types of Malware..

Q.15) (a) Find gcd (1970, 1066) using Euclid's algorithm?

(b) Using Row Transposition technique &, given key as "2 5 4 I 3" generate the Cipher Text for the following Plain text “a convenient way to express the transposition”.

Q.16 Alice and Bob decide to communicate with each other using RSA Algorithm. Against the Advice of Cryptographers, Alice selects two random prime numbers p= 7 and q= 13 to use for RSA Algorithm. He observes that n= p*q = 7*13 = 91 and chooses an encryption key e= 5. He makes his selection of n and e public. Then

a) **Alice wishes to send the message m= 23 to Bob. Compute the Cipher Text that Bob will obtain.**
b) **Compute the Decryption key d that Bob uses to decrypt the message. Suppose he receives the Cipher Text C = 2. Decrypt this Cipher text to reveal the number that Alice sent.**

Q.17 Discuss Public key Cryptography. Also describe Diffie-Hellman Key exchange algorithm. Consider the Diffie-Hellman scheme with common prime number P=7l and primitive root G=7.

(a) If user A has a private key Xa=5, what is A’s public key.

(b) If the user A has private key Xb=9 then what is B’s public key?

(c) What is shared key?

--BEST OF LUCK--