Total No. of questions : 7] *Roll No.* BETN1CS20014

B.Tech.CS (Cyber Forensics) IV Semester Regular
End Term Examination,June-2022

CRYPTOGRAPHY AND ENCRYPTION TECHNIQUE

(CSL0462)

Time : 03:00 hours Max. Marks :40

Note: Attempt all questions.

1.1 Plan how many keys are required by two people to communicate via a cipher. CO3 *1*

1.2 Discuss any four Substitution Technique and list their merits and demerits.

OR

Encrypt the following plain-text bit pattern with the supplied key, using the XOR operation, and state the resulting cipher-text bit pattern.

Plain text : 10011
Key : 01000 CO3 *2*

1.3 Explain about Hill Cipher. Consider the plaintext "paymoremoney" and use the encryption key: $K=\begin{pmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{pmatrix}$ Find the cipher text. *3*

OR

Eve has intercepted the cipher text "UVACLYFZLJBYL". Show how she can use an exhaustive key search to break this Caesar cipher.CO5

2.1 What are the different modes of operation in DES? **CO3** *1*

2.2 Describe HMAC algorithm. Comment on the security of HMAC

OR

Mention the strengths and weakness of DES algorithm. **CO4** *2*

2.3 With a neat diagram, explain the steps involved in SHA algorithm for encrypting a message with maximum length of less than 2128 bits and produces as output a 512 bit message digest. **CO5** *3*

P.T.O.

OR

Give a detailed description of key generation and encryption of IDEA algorithm

3.1 Define Digital signature. **CO2** *1*

3.2 Find gcd (56, 86) using Euclid's algorithm. **CO5** *2*

OR

Write about key generation, encryption and decryption in ElGamal Cryptosystem.

3.3 Give Plain text "G". Using RSA algorithm and the value of E=3, D=11, N=15. Find what G encrypts value and verify that after decryption. Is it same as plain text. **CO5** *3*

OR

User Alice & Bob exchange the key using Diffie Hellman alg. Assume ?=5 q=83 XA=6 XB=10. Find YA, YB, K.

4.1 Define Kerberos. **CO2** *1*

4.2 What is the difference between TLS and SSL security?

OR

State the X.509 content. **CO3** *2*

4.3 How does PGP provide authentication and confidentiality for email services and for file transfer applications? Draw the block diagram and explain the components. CO4 *3*

OR

What is the role of Ticket Granting Server in inter realm operations of Kerberos?

5.1 What is X.509 Standard? **CO2** *1*

1 2 1

5.2 List out the cryptanalysis resources. *2*

OR

Write down the differences between Cryptography and Steganography.

5.3 Explain the term cryptanalysis and frequency analysis. *3*

OR

How Staganalysis work explain in detail.

6. Users A and B use the Diffie Hellman key exchange technique, a common prime q=11 and a primitive root alpha=7. *10*

(a) What is the shared secret key? Also write the algorithm.

(b) How man in middle attack can be performed in Diffie Hellman algorithm

OR

Encrypt the following using play fair cipher using the keyword MONARCHY. "SWARAJ IS MY BIRTH RIGHT". Use X as blank space.
