QP CODE	2263516231

Reg.No: | | | | | | | | | | | |

DMI-ST. EUGENE UNIVERSITY
DEGREE EXAMINATION – DECEMBER – 2022

SEM:VI **351CS62 CRYPTOGRAPHY AND NETWORK SECURITY**

Time: 3 Hours Max. Marks: 100

Answer any Five questions (5 x 20 = 100 Marks)

1. a) Define cryptography and state the security objectives of cryptography. **(10 Marks)**

   b) Explain transposition cipher technique and demonstrate with a good example. **(10 Marks)**

2. a) Explain the initial permutation and the final permutation of the Data Encryption Standard. **(10 Marks)**

   b) Explain the generation of the round keys for the Advanced Encryption Standard algorithm. **(10 Marks)**

3. a) Explain the RSA algorithm. **(10 Marks)**

   b) Given that the extended Eucleadean Algorithm is given by GCD (a, b) =a.t + b.s. Find the valuers of s and t for the following GCD (41,17). **(10 Marks)**

4. a) With a neat Diagram explain the Digital Signature Algorithm. **(10 Marks)**

   b) Explain cryptographic hash function and its applications. **(10 Marks)**

5. a) What is the difference between TLS and SSL? **(6 Marks)**

   b) Draw the Secure Socket Layer and explain the handshake and change cipher protocols. **(8 Marks)**

   c) What is Transport Layer Security (TLS)? **(6 Marks)**

6. a) Define cryptography and explain the threats to data security in cryptography. **(4 Marks)**

   b) Distinguish between transposition cipher and substation cipher and give an example of each. **(8 Marks)**

c) With neat Diagrams explain the difference between symmetric and asymmetric cryptography. **(8 Marks)**

7. a) Mention two security protocols defined by IPsec. **(5 Marks)**

   b) Write a few notes on Security Associations in IPsec. **(5 Marks)**

   c) Write a few notes on Security policy. **(5 Marks)**

   d) Write a few notes on the Internet Key Exchange (IKE). **(5 Marks)**