**Assignment 02**

**Total Marks: 20 Cyber Security** Answer the following questions.

Q1: What is the difference between symmetric and asymmetric encryption? Q2: What is the purpose of a hashing algorithm in cryptography?

Q3: What are the strengths of the Advanced Encryption Standard (AES) algorithm? Q4: How does a digital signature ensure integrity and non-repudiation?

Q5: What is the purpose of a certificate in a Public Key Infrastructure (PKI)? Q6: What are the potential security risks associated with using weak encryption algorithms? Q7: What is the significance of key management in cryptography?

Q8: What are some challenges or limitations of implementing asymmetric encryption algorithms? Q9: What is post-quantum cryptography, and why is it gaining importance? Q10: What are the potential applications of homomorphic encryption?