CYBER SECURITY ASSIGNMENT QUESTION

DAY 36

1.Explain the mathematical foundations of cryptography. Discuss the role of mathematical concepts such as number theory, algebra, and probability theory in designing secure cryptographic algorithms.

2.Define modulo arithmetic and explain its significance in cryptography. Discuss how modulo arithmetic is used in cryptographic operations such as encryption and hashing.

3.Define the greatest common divisor (GCD) and discuss its relevance in cryptography. Explain how the Euclidean algorithm is used to compute the GCD of two integers.

4. Discuss the algebraic structures commonly used in cryptography. Explain the properties and applications of groups, rings, and fields in cryptographic algorithms.

5. Explain the Chinese Remainder Theorem (CRT) and its application in cryptography. Discuss how CRT can be used to speed up modular exponentiation operations in RSA encryption.