IS Assignment

Instructor	**Dr. Umar Aftab**
Session	**Spring 2025**
Section	**BCS 8D**

- **General Guideline**
  Try to do your assignment by your own in order to learn.

Diffie–Hellman

- Alice and Bob use the Diffie–Hellman key exchange technique with a common prime q = 157 and a primitive root a = 5.

a. If Alice has a private key XA = 15, find her public key YA.

b. If Bob has a private key XB = 27, find his public key YB.

c. What is the shared secret key between Alice and Bob?

- This problem illustrates the point that the Diffie–Hellman protocol is not secure without the step where you take the modulus, i.e. **the "Indiscrete Log Problem**" is not a hard problem! You are Eve and have captured Alice and Bob and imprisoned them. You overhear the following dialog.

Bob: Oh, let's not bother with the prime in the Diffie–Hellman protocol, it will make things easier.

Alice: Okay, but we still need a base a to raise things to. How about a = 3?

Bob: All right, then my result is 27.

Alice: And mine is 243. What is Bob's private key XB and Alice's private key XA? What is their secret combined key? (Don't forget to show your work.)

Elgamal

- Suppose Alice and Bob use an **Elgamal** scheme with a common prime q = 157 and a primitive root a = 5.

a. If Bob has public key YB = 10 and Alice chose the random integer k = 3, what is the ciphertext of M = 9?

b. If Alice now chooses a different value of k so that the encoding of M = 9 is C = (25, C2), what is the integer C2?

RSA

- In a public-key system using RSA, you intercept the ciphertext C=20 sent to a user whose public key is e =13, n=77. What is the plaintext M?
- In an RSA system, the public key of a given user is e = 65, n = 2881. What is the private key of this user? Hint: First use trial-and-error to determine p and q; then use the extended Euclidean algorithm to find the multiplicative inverse of 31 modulo f(n).

Modes of Operations

Write the equations for each of the following modes of operation used in block ciphers like DES:

- ECB (Electronic Codebook Mode)
- CBC (Cipher Block Chaining Mode)
- CFB (Cipher Feedback Mode)
- OFB (Output Feedback Mode)
- CTR (Counter Mode**)**