VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of
Computer Science and Engineering (SCOPE)

BCSE309L – Cryptography and Network Security

Digital Assignment

Winter Semester 2024-2025

Class ID: VL2024250501949 **Slot: E1+TE1**

Instruction for the submission of Digital Assignment:

- Last Date for Assignment Submission: **2nd April 2025.**
- **Late Submission Policy:** If the assignment is not uploaded within the specified timeframe, **zero marks** will be awarded, and **no alternate options** will be provided for submission.
- **Format:** The assignment must be **handwritten on A4 sheets**. A scanned **soft copy should be uploaded on VTOP** before the deadline, and the **hard copy must be submitted in person** in my cabin.
- **Question Selection:** The assignment will consist of **10 questions**. You may choose any **8 questions to answer**, which will carry an 8% weightage. An **additional 2% weightage will be awarded based on the presentation** of the assignment.
- **Answer Format:** For each question, please write the question followed by the corresponding answer.
- **Front Sheet Requirements:** On the front sheet, include your **FULL NAME (as per the records in VTOP), Register Number, Course Code & Title, and indicate "Digital Assignment-1."**
- **Input Selection:** Wherever "**ZZ**" is mentioned, it should be replaced with the **last two digits of the register number**. If the last two digits of the register number fall within the range **00 to 09**, they should be replaced with the number **22**.

1. **(a)** Find the **GCD** (262200, ZZ) using the **Euclidean Algorithm**. (2)

   (b) Find the **GCD** (222600, ZZ) using the **Extended Euclidean Algorithm**. (3)

   (c) Find the value of $\mathbf{85^{ZZ}}$ **mod 11** using **Fermat's Little Theorem.** (2)

   (d) Find the value of $\mathbf{79^{ZZ}}$ **mod 11** using **Euler's Theorem.** (3)

2. **(a)** Using the **Playfair Cipher technique**, perform **encryption** and **decryption** for the given plaintext using the specified keyword. (5)

   - **Plaintext:** Use the **first 8 letters of your name** as the plaintext.
   - **Keyword:** Use "**ALLTHEBEST**" as the keyword to construct the 5x5 Playfair cipher matrix.

   (b) Using the **Hill Cipher technique**, perform **encryption** and **decryption** for the given plaintext using the specified key matrix. (5)

$$K = \begin{pmatrix} 22 & 9 \\ 85 & 26 \end{pmatrix}$$

   - **Plaintext:** Use the **last four letters of your name** as the plaintext. Convert each letter to its corresponding numerical value (A=0, B=1, ..., Z=25).

3. Using the **Hill Cipher technique**, perform **encryption** and **decryption** for the given plaintext using the specified key matrix.

$$K = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 5 \\ 6 & 7 & 8 \end{pmatrix}$$

Plaintext: Use the **last six letters of your name** as the plaintext. Convert each letter to its corresponding numerical value (A=0, B=1, ..., Z=25).

4. Perform a single-round operation in the **Data Encryption Standard (DES)** using the given plaintext and round key as specified below:
   - **Plaintext:**
     - Use the **first 8 letters of your name** as the plaintext. (64-bit)
     - Convert each letter to its corresponding **8-bit binary** representation (using **ASCII**).
   - **Round Key:**
     - Use the **last 6 letters of your name** as the round key. (48-bit)
     - Convert each letter to its corresponding **8-bit binary** representation (using **ASCII**).
   - **DES Single-Round Operation:**
     - **Round Function (f):**
       1. i. Perform the expansion permutation (E) on the right half of the data.
       2. ii. XOR the expanded right half with the round key.
       3. iii. Substitute the result using standard S-Boxes (S1 to S8). (for S-Boxes S1 to S8, refer text book)
       4. iv. Perform the permutation P on the output of the S-Boxes. (refer text book)
       5. v. XOR the result with the left half of the plaintext.

5. Generate the **2nd round key** using the **AES key expansion algorithm** with the following parameters:

   128-bit Initial Key:
   - Construct the key by concatenating the following: (Use ASCII for bit conversion)
     a. The **constant value AABBCCDD** (converted to 64 bits using ASCII).
     b. The **first 4 letters of your name** (converted to 32 bits using ASCII).
     c. The **last 4 letters of your name** (converted to 32 bits using ASCII).
     d. Combine these three parts to form a **128-bit key**.

- **Round Constant (Rcon):**
    a. Use **round constant = 2** for the second-round key.
- **AES Key Expansion Algorithm:**
    a. **Step 1:** Divide the **128-bit key** into **4 words** (32 bits each).
    b. **Step 2:** Compute the **2nd round key** as follows:
        i. Use the **previous round key** and the **AES key schedule algorithm** to generate the next words.
        ii. Apply the **SubWord**, **RotWord**, and **XOR with Rcon** where needed.
    c. **Step 3:** Concatenate the words to form the **2nd round key**.
- **Output:**
    a. Display the **2nd round key** in **binary and hexadecimal format**.

6. **(a)** A secure communication system is being designed for a small organization where each user needs to **encrypt** and **decrypt messages using RSA**. As part of the implementation, you are tasked with creating a prototype that demonstrates RSA encryption and decryption using fixed prime numbers for simplicity. (5)

The given parameters are:

- Prime numbers **p=13** and **q=23**
- Public key **e=7**
- Message **M=ZZ**

(b) An online secure messaging application uses the **ElGamal encryption algorithm** to achieve **confidentiality** during message transmission. User A wants to send a confidential message to User B using ElGamal encryption. To maintain the confidentiality of the message, the application uses the following pre-agreed parameters: (5)

- Prime number **(q) = 131**
- Primitive root **(a) = 31**

- User A's private key **(X_A) = 9**
- User B's randomly chosen integer **(k) = 26**
- Message **(M) = ZZ**

7. A secure communication application uses **Elliptic Curve Cryptography (ECC)** to **encrypt messages**. User A wants to send a confidential message to User B using ECC. The application uses the following elliptic curve parameters:

- **Elliptic Curve Equation:** E31(2, 3)
- **Base Point (Generator):** G = (13, 26)
- **Message Point: Pm** = (8, 2)
- **Private Key of User B (n_B)** = 2
- **Secret Integer (k)** = Last digit of your register number.
  - If the last digit is **0 or 1**, use **3** as the secret integer.
  - If the last digit is **more than 6**, divide it by **2** (integer division).

8. **(a)** Alice and Bob want to establish a secure communication channel using the **Diffie-Hellman Key Exchange protocol**. They agree on the following public parameters: (5)

- Prime number **p=23**
- Primitive root **g=5**

1. Alice selects a private key **X_A=6**.
2. Bob selects a private key **X_B=15**.
3. Exchange public keys and compute the shared secret key. And verify that both users derive the same shared secret.
4. Eve, an attacker, wants to intercept and manipulate the communication between Alice and Bob. Demonstrate how Eve can manipulate the keys and derive her own shared secret with both Alice and Bob.

(b) Alice wants to send a confidential and authenticated message to Bob using **RSA Digital Signature**. (5)

1. Alice generates her RSA key pair:
   - Prime numbers: **p=61, q=53**
   - Public exponent: **e=17**
2. Alice signs the hash code using her private key. Find the Hash code below based on your department.
   - BCE Students: 22
   - BCI Students: 26
   - BCT Students: 9
   - BDS Students: 8
   - BKT Students: 25
   - BCB Students: 56
3. Alice sends the signed message and her public key to Bob.
4. Bob verifies the signature using Alice's public key.

9. **(a)** Determine the **number of padding bits, total length and number of blocks used** in **HMAC** for the hash functions **MD5** and **SHA512** if the message size is 7926 bits. (3)

(b) Evaluate the values of **ch(e,f,g)** and **Maj(a,b,c)** functions as defined in the **SHA512** for the buffers a, b, c, e, f and g that contains the hexa-decimal values as follows: (4)

1234567890123456, AABBCCDDEEFFAABB, AAABBBCCCDDDEEFF, 1111222233334444, 11AA22BB33CC44DD, and **First 8 Letters of your name (Use ASCII for bit conversion)** respectively.

(c) Evaluate the value of the **F(b, c, d)** function as defined in the **MD5 algorithm** for the given 32-bit hexadecimal buffer values. (3)

The buffers a, b, c, and d contain the following hexadecimal values:

- a = 89ABCDEF
- b = 12345678
- c = 0F0F0F0F
- d = **last four letters of your name**. (Use ASCII for bit conversion)

10. (a) A company wants to ensure the authenticity and integrity of its digital documents using the **Digital Signature Standard (DSS)**. As part of the process, the following values are given: (5)

- ○ Prime modulus **p: 619**
- ○ Subprime **q: 103**
- ○ Generator **g: 5**
- ○ Private key **x: 15**
- ○ Message hash **H(M): 17**
- ○ Random value **k: 9**

(b) An IoT device generates a **digital signature using the ElGamal algorithm** to secure transmitted data. The server verifies the authenticity of the received data. The following values are given: (5)

- **p = 61**
- **g = 6**
- **x = 9**
- **H(M) = 20**
- **k = 7**