Computer Security - Assignment 3

1. Manual Padding Oracle Attack (20 points)

We use:

- CBC mode
- Block size = 4 bytes
- PKCS#7 padding

You intercept:

```
C0 | C1
```

The server decrypts:

$$P_1 = D(C_1) \oplus C_0$$

The server responds:

- “VALID”
- “INVALID PADDING”

Given:

Original last byte of C0:

```
C0[4] = A3 (hex)
```

You modify it and send:

```
C0'[4] = B6 (hex)
```

The server returns:

```
VALID
```

Original second-to-last byte of C0:

```
C0[3] = 34 (hex)
```

You modify it and send:

```
C0'[3] = 35 (hex)
```

The server returns:

```
VALID
```

Question:

- What is the last byte of plaintext P_1? Derive the formula you used and Show all XOR steps. (10 points)
- Then second-to-last byte of plaintext P_1? Derive the formula you used and Show all XOR steps. (10 points)

2. Security Analysis (20 points)

Consider the following encryption scheme:

- Key $k \in \{0,1\}^n$
- Encryption:

$$Enc_k(m) = (r, m \oplus k \oplus r)$$

where r is a random n-bit string

Question:

- Is this scheme deterministic or randomized? Why? (5 points)
- Construct a Chosen Plaintext Game for this encryption scheme. Describe the detailed procedure. (10 points)
- Suppose an adversary wins the CPA game with probability: $P[Win] = 0.72$, Compute adversary advantage. If we repeat the experiment 1000 times, what is expected number of wins? (5 points)

3. Diffie–Hellman Key Exchange (24 points)

Two users, Alice and Bob, wish to establish a shared secret using the Diffie–Hellman key exchange protocol.

They publicly agree on:

$$q = 353, \quad g = 3$$

Alice chooses private key:

$$a = 97$$

Bob chooses private key:

$$b = 233$$

Question:

- Compute Alice’s public key. (You must calculate by hand. Show the detailed calculation for exponent decomposition.) (10 points)
- Compute Bob’s public key. (You must calculate by hand. Show the detailed calculation for exponent decomposition.) (10 points)
- Compute the shared secret from either Alice's or Bob's side. (You can just list the formulas) (4 points)

4. RSA Encryption and Decryption (24 points)

Alice wants to generate an RSA key pair.

She chooses two prime numbers:

$$p = 17, \quad q = 11$$

Alice chooses public exponent:

$$e = 7$$

Suppose Bob wants to send:

$$m = 88$$

Question:

- Compute the private key exponent d (You must calculate by hand. Show the detailed process finding d.) (8 points)
- Compute ciphertext of m (You must calculate by hand. Show the detailed calculation for exponent decomposition.) (8 points)
- Show decryption of ciphertext (You must calculate by hand. Show the detailed calculation for exponent decomposition.) (8 points)

5. Public-Key Cryptography Standards (PKCS) (12 points)

Public-Key Cryptography Standards (PKCS) define many widely used cryptographic formats and protocols. You must research **at least 3** PKCS standards listed below. For each standard, research and find **at least 2** real-world application examples where the standard is used. For each example you provide:

1. Clearly identify the name of the system / software / product / protocol
2. Describe the real-world application scenario
3. Explain how the PKCS standard is used or implemented
4. Provide a link or reference to at least one official technical document supporting your claim (e.g., RFC, standard spec, vendor documentation, OpenSSL docs, PKCS official docs)
5. Use your own words, do not copy large chunks directly

- **PKCS #1** – RSA Cryptography Standard
- **PKCS #3** – Diffie–Hellman Key Agreement Standard
- **PKCS #5** – Password-Based Cryptography Standard
- **PKCS #7** – Cryptographic Message Syntax Standard
- **PKCS #8** – Private-Key Information Syntax Standard
- **PKCS #10** – Certification Request Syntax Standard
- **PKCS #11** – Cryptographic Token Interface Standard
- **PKCS #12** – Personal Information Exchange Syntax Standard