**KINGDOM OF SAUDI ARABIA | JAZAN UNIVERSITY**
**COLLEGE OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY**
**DEPARTMENT OF INFORMATION TECHNOLOGY & SECURITY**

## GROUP ASSIGNMENT - 2023-24 (THIRD SEMESTER)

| | | | | | |
|---|---|---|---|---|---|
| **Student Name:** | | | | **Student ID:** | |
| **Level:** | 9th | | | **Section Number:** | |
| **Course Name:** | Cryptography & Data Security | | | **Course Code:** | ITEC-332 |
| **Date:** | 15/04/2024 | **Day** | Sunday | **Course Teacher:** | Masrath |
| **Duration:** | 4 Weeks | **Max. Marks:** | Total 20 marks | **Deadline:** | |

**Instructions:**

- **Students should answer all the questions. Questions are from unit-1, unit-2, unit-3, and unit-4 topics, examples alongside exercises (textbook).**
- **Students should mention their Name, University Registration, and Section Number.**
- **Students should solve it by hand, take its snapshot and add it in MS Word.**
- ***Students should submit the assignment via Blackboard only. No email no WhatsApp.***
- ***Submit your assignment copy only in Microsoft Word format. (***.doc, .docx)***

## Do as directed

**1. Using the Vernum cipher, encrypt the word "cryptographic" using the word "eng".**

| Character | ASCII | Binary |
|---|---|---|
| c | 99 | 01100011 |
| r | 114 | 01110010 |
| y | 121 | 01111001 |
| p | 112 | 01110000 |
| t | 116 | 01110100 |
| o | 111 | 01101111 |
| g | 103 | 01100111 |
| r | 114 | 01110010 |
| a | 97 | 01100001 |
| p | 112 | 01110000 |
| h | 104 | 01101000 |
| i | 105 | 01101001 |
| c | 99 | 01100011 |
| e (from eng) | 101 | 01100101 |
| n (from eng) | 110 | 01101110 |
| g (from eng) | 103 | 01100111 |

-For 'c' (99) and 'e'(101) from "eng":

01100011(99,'c')

01100101(101,'e')

XOR result:00000110 (6  in decimal)

-For 'r' (114) and 'n'(110) from "eng":

01110010 (114,'r')

01101110 (110,'n')

XOR result:00011100 (28  in decimal)

-For 'y' (121) and 'g'(103) from "eng":

01111001   (121,'y')

01100111 (103,'g')

XOR result:00011110 (30  in decimal)

-For 'p' (112) and 'e'(101) from "eng":

01110000 (112,'p')

01100101 (101,'e')

XOR result:00010101 (21 in decimal)

-For 't' (116) and 'n'(110) from "eng":

01110100 (116,'t')

01101110 (110,'n')

XOR result:00011010 (26  in decimal)

-For 'o' (111) and 'g'(103) from "eng":

01101111   (111,'o')

01100111 (103,'g')

XOR result:00001000 (8 in decimal)

-For 'g' (103) and 'e'(101) from "eng":

01100111 (103,'g')

01100101 (101,'e')

XOR result:00000010 (2 in decimal)

-For 'r' (114) and 'n'(110) from "eng":

01110010 (114,'r')

01101110 (110,'n')

XOR result:00011100 (28  in decimal)

-For 'a' (97) and 'g'(103) from "eng":

01100001   (97,'a')

01100111 (103,'g')

XOR result:00000110 (6 in decimal)

-For 'p' (112) and 'e'(101) from "eng":

01110000 (112,'p')

01100101 (101,'e')

XOR result:00010101 (21 in decimal)

-For 'h' (104) and 'n'(110) from "eng":

01101000 (104,'h')

01101110 (110,'n')

XOR result:00000110 (6 in decimal)

-For 'i' (105) and 'g'(103) from "eng":

01101001 (105,'i')

01100111 (103,'g')

XOR result:00001110 (12 in decimal)

-For 'c' (99) and 'e'(101) from "eng":

01100011 (99,'c')

01100101 (101,'e')

XOR result:00000110 (6 in decimal)

The ciphertext is "628302126822862l6126"

**2. By using the Vigenere Cipher, perform encryption and decryption. The plaintext is CRYPTOGRAPHY, and keyword is CIPHER.**

- Plaintext: CRYPTOGRAPHY
- Keyword: CIPHERCIPHERCI
- Encrypted text: DURWPIJCNHCV
- Decrypted text: CRYPTOGRAPHY

**3. Explain DES algorithm with an example.**

The DES is a symmetric block cipher that makes use of only one key for both encryption and decryption operations.

The DES is a block cipher that encrypts a 64-bit block of plaintext using a 56-bit key to produce a 64-bit block of ciphertext.

The key is presented as a 64-bit block from which an effective 56-bit key is generated for encryption and decryption operations.

In the 64-bit key value, every bits are parity bits used for parity checking which are discarded and contain no effect on DES’s security.

- Example: Encrypting the plaintext "HELLO123" using a key "KEY12345":
  - Plain text: 01001000 01000101 01001100 01001100 01001111 00110001 00110010 00110011
  - Key: 01001011 01000101 01011001 00110001 00110010 00110011 00110100 00110101
  - Encrypted text: 11011010 01100010 01111110 11001110 00010110 10011100 11100010 01111011

**4 . What is the difference between stream and block ciphers?**

Block cipher: converts the plain text into cipher text by taking plain text's block at a time.

Stream cipher: converts the plain text into cipher text by taking 1 byte of plain text at a time.

Block cipher: uses either 64 bits or more than 64 bits. While stream cipher uses 8 bits.

Block cipher: uses confusion as well as diffusion.

While stream cipher uses only confusion. Confusion achieved via the substitution technique. While the diffusion is achieved via transposition technique.

**5.Write AES key expansion algorithm.**

• The AES encryption and decryption uses a RoundKey in each round from the given 128-bit key value.

• For a 128-bit key value, totally 11 round keys are generated.

• Among the 11 keys, one key is used for the initial round, 9 for standard rounds and 1 for the final round.

• For generating 11 keys, initially the input key is copied into a (4 × 4) square matrix.

• In this matrix, the first four bytes are copied into first column and next four bytes are copied into next column

• From this matrix, four words (128 bits) are generated for each round and hence 44 words are generated in total.

• AES key expansion algorithm is depicted .

**6. The 802.11 standard protocol used RC4 for its agility and simplicity for encryption and decryption. There are a few simple steps in RC4 including the initialization of S to a number from 0 to 255, followed by permutation. Explain the stream generation, and main benefits and drawbacks of RC4.**

In RC4, after initializing arrays S and T, the permutation step involves swapping elements in array S based on the values in array T. This creates a pseudo-random permutation of numbers from 0 to 255. The stream generation process involves generating a pseudo-random keystream based on the permutation of array S. This keystream is then XORed with the plaintext to produce the ciphertext during encryption, and XORed with the ciphertext to recover the plaintext during decryption.

Main benefits of RC4:

- Simple and efficient implementation.

- Fast encryption and decryption process.

- Well-suited for streaming data encryption.

Drawbacks of RC4:

- Vulnerable to certain cryptographic attacks, such as key recovery attacks.

- Weaknesses in the key scheduling algorithm can lead to security vulnerabilities.

- Not recommended for high-security applications due to known weaknesses.

**7. Compare symmetric and asymmetric key encryption.**

• Symmetric (Secret) Key Encryption: One key is utilized for encryption and decryption processes. It is further divided to substitution and transposition techniques.

• Asymmetric (Public) Key Encryption: Two keys are utilized. One(public key) for encryption, and another (private key) for decryption processes.

**8.(i) Describe the RSA algorithm with an example.**

• The RSA stands for Rivest, Shamir and Adleman.

• The RSA is a best known and widely used public-key scheme.

• The RSA algorithm consists of three phases, namely, key generation, encryption and decryption.

• Significant steps of key generation phase are:

Step 1: Initialization

Step 2: Computation of n value

Step 3: Computes Euler's totient function

Step 4: Generation of Public keys

Step 5: Generation of Private keys

Step 6: Publish the public keys

Step 7: Make private key as secret

Key Generation:

1. Choose two large prime numbers p and q.

2. Calculate $n = p * q$ and $\varphi(n) = (p-1) * (q-1)$.

3. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.

4. Calculate d as the modular multiplicative inverse of e modulo $\varphi(n)$.

Encryption:

a plaintext message M, the ciphertext C is calculated as $C \equiv M^e \pmod{n}$.

Decryption:

a ciphertext C, the plaintext message M is calculated as $M \equiv C^d \pmod{n}$.

Example:

consider $p = 5$, $q = 11$, $e = 3$.

- Calculate $n = 5 * 11 = 55$, $\varphi(n) = (5-1) * (11-1) = 40$.
- Choose d such that $d * 3 \equiv 1 \pmod{40}$, so $d = 27$.

**(ii) 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?**

Given $C = 20$, $e = 13$, $n = 77$:

- Decrypt using RSA: $M \equiv C^d \pmod{n}$
- Calculate $d^{-1} \equiv e^{-1} \pmod{\varphi(n)} = 13^{-1} \equiv 37 \pmod{40}$
- $M \equiv C^d \equiv 20^{37} \equiv 33 \pmod{77}$

Therefore, the plaintext M is 33.