**Mid Term Data Network Security Exercise**

1. Given a cipher text, “**TTB JTB EAO MHE ENL OHY”**. Show all the mathematical calculations and works involved to derive the answers. Decrypt the cipher text using the Transposition cipher and a key: **453126**. Find the original message (plain text).

**[5 Marks]**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 6 | 2 | 1 | 3 | 5 | 4 |
| O | E | M | E | J | T |
| H | N | H | A | T | T |
| Y | L | E | O | B | B |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| M | E | E | T | J | O |
| H | N | A | T | T | H |
| E | L | O | B | B | Y |

MEETJOHNATTHELOBBY

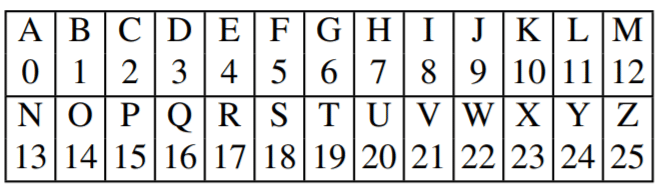
Decrpt: MEET JOHN AT THE LOBBY

1. Given a Plain text, “**CYBER FORENSIC IS FUN”**. Answer all the following question. Show all the mathematical calculations and works involved to derive the answers. Encrypt the plain text using Vigenere cipher and a key: **REPUBLIC.** Find the Encryption message (Cipher Text)

**[8 Marks]**

**Answer:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| C | Y | B | E | R | F | O | R | E | N | S | I | C | I | S | F | U | N | X | Y | Z | A | B | C |
| R | E | P | U | B | L | I | C | R | E | P | U | B | L | I | C | R | E | P | U | B | L | I | C |



| **Pi​** | **Ki​** |  | **Ci​** |
| --- | --- | --- | --- |
| 2 | 17 |  | 19 |
| 24 | 4 |  | 2 |
| 1 | 15 |  | 16 |
| 4 | 20 |  | 24 |
| 17 | 1 |  | 18 |
| 5 | 11 |  | 16 |
| 14 | 8 |  | 22 |
| 17 | 2 |  | 19 |
| 4 | 17 |  | 21 |
| 13 | 4 |  | 17 |
| 18 | 15 |  | 7 |
| 8 | 20 |  | 2 |
| 2 | 1 |  | 3 |
| 8 | 11 |  | 19 |
| 18 | 8 |  | 0 |
| 5 | 2 |  | 7 |
| 20 | 17 |  | 11 |
| 13 | 4 |  | 17 |

TCQYSQWTVRHCDTAHLR

1. In order to deliver a key in safely condition, Diffie Hillman key exchange has been applied. In this algorithm, both sender, **Alice** and receiver, **Bob** has agreed on the values for 2 parameter which are p, prime number and g, root number(p = 17 and g = 13). Find the value for shared keys.

**[7 Marks]**

|  |  |
| --- | --- |
|  |  |
|  |  |

1. Given a plain text, **“SEE YOU AT THE LOBBY NOW**”. Encrypt the plain text using the monoalphabetic substitution cipher with the key obtained from **QUESTION 3**.

**[7 Marks]**

1. Given a cipher text, “WCGXEERORYLVYTAHOPP”. Decrypt the cipher text using Rail Fence cipher with the key obtained from **QUESTION 3.**

**[5 Marks]**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| W |  |  |  |  |  | C |  |  |  |  |  | G |  |  |  |  |  | X |
|  | E |  |  |  | E |  | R |  |  |  | O |  | R |  |  |  | Y |  |
|  |  | L |  | V |  |  |  | Y |  | T |  |  |  | A |  | H |  |  |
|  |  |  | O |  |  |  |  |  | P |  |  |  |  |  | P |  |  |  |

WELOVECRYPTOGRAPHYX

WE LOVE CRYPTOGRAPHY

1. Given a plain text “HIDDEN”. Encrypt the message using RSA algorithm with **p=5**, **q=7** and public key **e=5**. Do the works for each alphabet.

**[10 Marks]**

so, d=5

Use public key to encrypt the message usin g formula

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| P: | H | I | D | D | E | N |
| M: | 7 | 8 | 3 | 3 | 4 | 13 |
|  | 7 | 8 | 33 | 33 | 9 | 13 |

Ciphertext=7, 8, 33, 33, 9, 13

Decrypt: