**Information Security lab(20cs71) External Question paper**

**============ =============== ========== ============**

1(a) A plaintext had its punctuation and spaces removed, and was then encrypted with a Caesar cipher.

The resulting ciphertext is: *cxknxawxccxkncqjcrbcqnzdnbcrxwfruurjvbqjtnbynjan*

Use frequency analysis to identify which ciphertext characters are most common. What was the original plaintext?

Hint: In plaintext English, the most common letter is E. Using frequency analysis, a sensible guess would be to try a shift which maps E to one of the most common ciphertext characters.

1(b) Explore any four network diagnosis tools.

============== =================== ================ ====================

2 Edith and Norman have decided to encrypt all of their messages through 'Playfair cipher'. While Norman can encrypt and decrypt on his own, Edith asks for your help with the process. Now you and Edith are both on your desk figuring it out.  
This encryption method requires the use of a **key table** - a grid of 25 alphabets in a 5 × 5 square.  
Example:

A B C D E  
F G H I K  
L M N O P  
Q R S T U  
V W X Y Z

In Playfair cipher the message is **split into digraphs**, pairs of two letters, and then encrypted by following these **rules** in order:  
  
**i)** If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively. (Also applies for the cases with same letters)  
  
Example:

A B C D E  
F G H I K  
L M N O P  
Q R S T U  
V W X Y Z  
Message: MO  
Output: NP  
**ii)** If the letters appear on the same column of your table, replace them with the letters immediately below respectively.  
  
Example:

A B C D E  
F G H I K  
L M N O P  
Q R S T U  
V W X Y Z  
Message: GR  
Output: MW  
**Note:** In cases where letters are at the edges, replace the value of the key whose isn't

present, with the key that is at the start of the row/column (according to the rules given).  
Example:

A B C D E  
F G H I K  
L M N O P  
Q R S T U  
V W X Y Z  
Message: CE BW  
Output: DA GB  
**iii)** If neither of the preceding two rules is true, form an imaginary rectangle with the two letters as edge points. Then, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle. The order is important – the first letter of the encrypted pair is the one that lies on the same row as the first letter of the plaintext pair.  
Example:

A B C D E  
F G H I K  
L M N O P  
Q R S T U  
V W X Y Z  
Message: GT  
Output: IR

In addition, Norman has also created some **additional rules** to increase credibility:  
- If the letters in the message are in lower case, they are supposed to be changed to their respective upper case.  
- If all the letters cannot be kept in pairs, the message is a **dud**.  
- Any characters that are not present in the key table are ignored from the message.  
  
**For decryption, you simply do the process in reverse.**

**3(a)** Use a railfence cipher with 3 rails – removing the rails from top to bottom – to encrypt the message

alan turing the enigma

Try decrypting this message that was encrypted with a railfence cipher with four rails:

*TTTPT QDSYP RSHII XEDOH EIUNS ESLDY TEMES*

*SERSE NELSC NEAUC FLERE GAMAE BHDIH SCUCD*

*NG*

(b) Download and install nmap. Use it with different options to scan open ports, do a ping scan, tcp port scan, udp port scan

================== ======================= ==========================

4(a) (i) Use a columnar transposition cipher with a rectangular array and keyword **mathematician** to encrypt the following message:

*Sample the electronic environment of the east*

*coast of North Korea. Emphasis is intercepting*

*coastal radars*

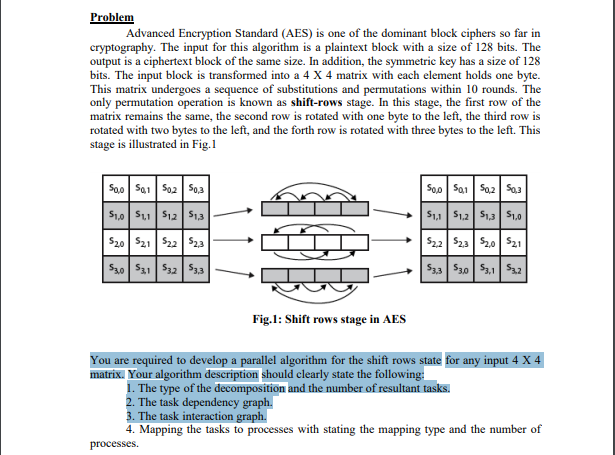
(ii) Decrypt the following message that was encrypted with a columnar transposition with keyword **welchman**.

*LAOAE CEDOS EEOHN NAHRE FESSV EGEGA SCJMS*

*WDPSD OTIAS*

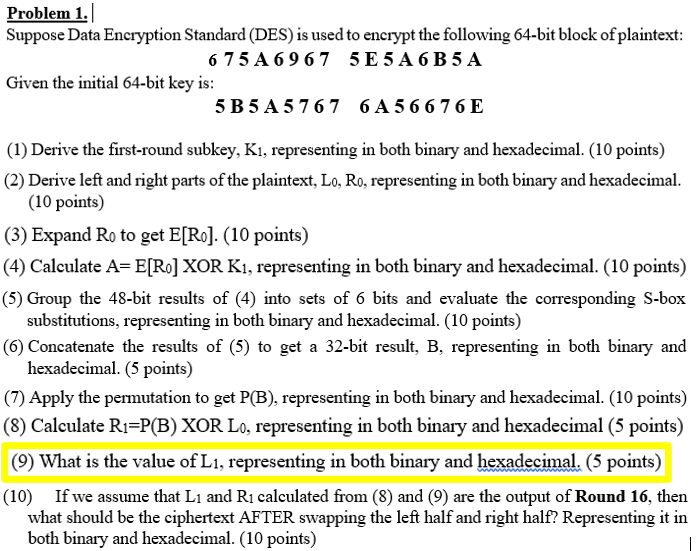
(b) Study about Wireshark packet sniffer tool in promiscuous and non- promiscuous mode.

=========== ================== ================ ========================

**5(a)** 

(b) Explore any Four Network Diagnosis Tools.

=========== ============== ==================== ============== ===============

6(a) 

(b) Explore IP Tables in Linux.

7(a) **Suppose Alice and Bob agree to use p = 47 and g = 5. Alice chooses a number between 0 and 46, say a = 18. Bob chooses a number between 0 and 46, say b = 22. Can you show the publishing of computed numbers using Deffie-Hellman-Key exchange algorithm (both of the steps)? Also find the final published public key.**

**(b)** Download and install nmap. Use it with different options to scan open ports, do a ping scan, tcp port scan, udp port scan

========== ================= ================= =============== =========

8(a) Consider an RSA cryptosystem with p = 17, q = 13 (hence, n = pq = 221), and e = 35.

i) What is the value of d?

ii)Let (e, n) be the public key of Alice. If we use it to encrypt a message m = 78, what is the ciphertext C?

iii) (d, n) be the private key of Alice. If she receives a ciphertext C = 65, what is the original message m?

iv) If you receive a message m = 93 from Alice and her digital signature 188, do you think that this message indeed comes from her?

(b) Study about Wireshark packet sniffer tool in promiscuous and non- promiscuous mode.