Information Security Lab

15B17CI576

Odd 2023

Week 2 (4th August – 10th August)

Note: Students are advised to submit their solutions to respective lab faculty. The solution file must be named as "rollno_first name_w1.doc" (here w1 represents week1).

Q1. Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text. In this process, the actual plain text alphabets are not included.

Consider the plain text hello world, and let us apply the simple columnar transposition technique as shown below:

H	E	L	L
O	W	O	R
L	D		

The number of columns is taken as key. Plain text characters are placed horizontally and the cipher text is created with vertical format as: **holewdlolr**. Now, the receiver has to use the same table to decrypt the cipher text to plain text.

WAP in C/C++ to implement both encryption and decryption using this cipher.

Q2. A Mono-alphabetic cipher uses a fixed substitution for encrypting the entire message. Implement encryption and decryption functions for following types of mono-alphabetic cipher.

a) Integer key based (shifting alphabets right by "key" places for encryption and shifting alphabets left by "key" places for decryption and

b) Mapping table based (each alphabet/digit mapped to any other random alphabet/digit).

Q3. Read working of Playfair cipher from help file and implement keymatrix_generation(), encrypt() and decrypt() functions. Test the program with key = "occurrence" and plaintext="computers".

Q4. In Vigenère polyalphabetic cipher, encryption is done using a keyword instead of just one integer. For example, if the keyword is **deceptive**, the message "we are discoveredsave yourself" is encrypted as follows:

```
keyword:  deceptivedeceptivedeceptive
plaintext: wearediscoveredsaveyourself
ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Implement encryption and decryption according to this scheme.

Q5. The periodic nature of the keyword in above cipher can be eliminated by using a nonrepeating keyword that is as long as the message itself. Vigenère proposed an autokey system, in which a keyword is concatenated with the plaintext itself to provide a running key. For example:

keyword: deceptivewearediscoveredsav

plaintext: wearediscoveredsaveyourself

ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

Implement encryption and decryption according to this modified scheme.

Q6. Write a C/C++ program to implement 2x2 and 3x3 hill cipher.