Birla Institute of Technology & Science, Pilani, Hyderabad Campus

BITS F463 – Cryptography (Summer Term 2020)

Assignment 1

Question 1 – Vigenere Cipher (6 marks)

Problem

Bob wants to send an encrypted message to Alice. To share the key Alice encrypts the key for Vigenere Cipher using a row transposition cipher and sends to Bob the secure key for the row transposition cipher through a secure channel. Bob encrypts his message using the Vigenere cipher with the key he decrypts from the row transposition cipher. Find out what is the encrypted message Bob finally sends to Alice.

Input:

- First line of the input contains l*l*, the length of the key of the row transposition cipher.
- The next line contains the l*l* elements of the key of the row transposition cipher.
- The next line contains a string encypted_key*encypted_key* which is the key of the Vigenere Cipher encrypted with the row transposition cipher.(Assume length of the encrypted key is a multiple of the key length given above.)
- The last line contains a string plaintext*plaintext* which is the message Bob wants to encrypt. (Assume the message contains no spaces)

Output:

- In the first line output the key of the Vigenere Cipher.
- In the second line print the ciphertext produced using the above key.

Constraints:

- $l \leq 100000$
- $len(encrypted\_key) \leq 100000$
- $len(plaintext) \leq 100000$
- The Vigenere cipher is used with repeated key
- Assume the numbering of alphabets as (a-0, b-1, .., z-25).
- All string are in lowercase alphabets and don't conatin spaces.

Sample Input:

```
7
4 3 1 2 5 6 7
ttnaaptmtsuoaodwcoixknlypetz
encryptthistextandsendittoalice
```

Sample Output:

```
attackpostponeduntiltwoamxyz
egvrazihzbhhrbwuawapgzwtflykivx
### EXPLANATION:
```

The ciphertext ttnaaptmtsuoaodwcoixknlypetz when decrypted with the key 4 3 1 2 5 6 7 using row transposition cipher gives the plaintext as attackpostponeduntiltwoamxyz. The plaintext attackpostponeduntiltwoamxyz is the key for the vigenere cipher with repeated key, the message encryptthistextandsendittoalice is encrypted as egvrazihzbhhrbwuawapgzwtflykivx.

Question 2 – Batman Hill (9 marks)

Problem
Batman sent Commisioner Gordon a message encrypted with the Hill Cipher containing the location of the next strike by the joker. The message is encrypted with Hill Cipher and the key size is 2. The message also contains how the 2 most commonly occouring digrams of the english language ("TH","HE") are encrypted. The message is in uppercase with letters A-Z. White spaces are removed and in case of an incomplete digram Z is added. You need to help Commisioner Gordon decrypt the message, to help prevent the attack.

Input:
- First line will contain a string which is the ciphertext.
- The next line contains the encrypted digrams (corresponding to "TH" and "HE") respectively separated by a space.

Output:
Output the decrypted text(you don't have to remove filler 'Z' characters).

Constraints:
$1 \leq sizeofencryptedtext \leq 100000$

Sample Input:	**Sample Output:**
ALYHAUKCRT RI JT	ARKHAMCITY

Question 3 – DES Cipher (15 marks)

Problem
Given a plaintext and key for DES encryption, output the 16 keys used in the encryption process. Also output the result of the first fiestel round (i.e. L1R1).The permutation tables and substitution boxes to be used can be found here.Take the number of left shifts (1 or 2) for generating the 16 keys as explained in the book.

Input:
- First line contains the plaintext.
- The second line has the key.

Output:
The first 16 lines contain the keys. The next line has the output of one round of encryption.

Constraints
64 bit plaintext and key.

Sample Input:

```
0123456789ABCDEF
133457799BBCDFF1
```

Sample Output:

```
1B02EFFC7072
79AED9DBC9E5
55FC8A42CF99
72ADD6DB351D
7CEC07EB53A8
63A53E507B2F
EC84B7F618BC
F78A3AC13BFB
E0DBEBEDE781
B1F347BA464F
215FD3DED386
7571F59467E9
97C5D1FABA41
5F43B7F2E73A
BF918D3D3F0A
CB3D8B0E17F5
F0AAF0AAEF4A6544
```