Lab 02 (4 hrs): Classical Cryptography

Part 1 (3 hrs):

Program 1: Vigenère cipher (on alphabet string)

In this program, you are required to implement the Vigenère cipher algorithm from scratch, to encrypt and decrypt for alphabet string. The encrypt and decrypt method should be pure functions, i.e. without side effects.

Your program does the following:

- Read an alphabet string from the console input, where the string is only consisting of 26 uppercase letters (A-Z). The first string represents the plaintext.
- Read the second alphabet string. It is ensured that the length of second alphabet string is the same with the first string. The second string represents the key.
- Encrypt the plaintext with the key.
- Print the ciphertext alphabet string.
- Decrypt the ciphertext with the key.

Example Input & Output

Input:

```
ABCDEFG
ABCDEFG
```

Output:

```
ACEGIKM
ABCDEFG
```

Program 2: Columnar transposition (on alphabet string)

http://rumkin.com/tools/cipher/coltrans.php

A columnar transposition, also known as a row-column transpose, is a very simple cipher to perform by hand. First, you write your message in columns. Then, you just rearrange the columns. For example. I have the message, `Which wristwatches are swiss wristwatches`. You convert everything to upper case and write it without spaces. When you write it down, make sure to put it into columns and number them. Let's use five columns.

	Unencoded	Rearranged
Column #:	42531	12345
	WHICH	HHCWI
	WRIST	TRSWI
	WATCH	HACWT
	ESARE	ESREA
	SWISS	SWSSI
	WRIST	TRSWI
	WATCH	HACWT
	ES	SE

Now, you just read the columns down in the order that you number them. Above, you will see the key is `4 2 5 3 1`, which means you write down the last column first, then the second, then the fourth, the first, and finally the middle. When you are all done, you will get `HTHESTHHRASWRASCSCRSSCWWWESWWEIITAIIT`.

Your program does the following:

- Read an integer from the console, representing the column count. In the example above, the count is `5`.
- Read the encryption key, i.e. the order of columns, separated by space. In the example above, the key is `4 2 5 3 1`.
- Read the plaintext string in one line. In the example above, the plaintext is `WHICHWRISTWATCHESARESWISSWRISTWATCHES`.
- Perform the columnar transposition.
- Print the ciphertext string. In the example above, the ciphertext is `HTHESTHHRASWRASCSCRSSCWWWESWWEIITAIIT`.

Example Input & Output

Input:

```
5
4 2 5 3 1
WHICHWRISTWATCHESARESWISSWRISTWATCHES
```

Output:

```
HTHESTHHRASWRASCSCRSSCWWWESWWEIITAIIT
```

Part 2 (1 hrs):

Program 3: Vigenère cipher (on bytes)

In this program, you are required to extend the Vigenère cipher (on alphabet string) to bytes, in order to encrypt arbitrary data on the computer.

Your program does the following:

- Read a hex string from the console input. The first string represents the plaintext bytes as a hex string. Remember that you need to decode the hex string into bytes.
- Read a hex string from the console input. The second string represents the encryption key bytes as a hex string.
- Encrypt the plaintext with the key.
- Print the ciphertext bytes as a hex string.
- Print the ciphertext bytes as a Base64 string.

From now on, the alphabet string is deprecated. Cryptography methods, such as encryption and decryption, operates on bytes.

Example Input & Output

Input:

```
abcd
abcd
```

Output:

```
569a
Vpo=
```