WILFRID LAURIER UNIVERSITY

LAURIER

Inspiring Lives.

CP460– Applied Cryptography – Fall 2024
Assignment 1

Due: Oct 21, 2024, 11:59 pm

Assignment Overview (10 Marks)

There are three tasks. Tasks 1 and 2 are programming part. You are allowed to use any programming languages to implement the function. I will recommend to use Google Collab for Tasks 1 and 2. Submit two files (your code (.ipynb file) and a .pdf file for Task 3 to 5) to Assignment 1 Dropbox folder.

Task 1 (2.5 Marks):

We received the following ciphertext which was encoded with a shift (Caeser) cipher:

Xultpaajcxitltlxaarpjhtiwtgxktghidhipxciwtvgtpilpitghlxiwiwtxgqadds.

a) Implement a function that performs a letter frequency attack based on the table 1.1 in section 1.2.2. from the textbook.

b) For the above cipher text, how many letters do you have to identify through a frequency count to recover the key? What is the cleartext?

Task 2 (2.5 Marks):

a) Implementation of the Affine Cipher- Encryption and Decryption method:

Encryption method - **AffineEncrypt(k, plaintext)**

Decryption method - **AffineDecrypt(k, ciphertext) ,**

given a key **k** that consists of a pair of integers (a,b), both in {1,2,..,25} with a not divisible by 2 or 13. The functions should work on strings, and leave any non-

alphabetic characters unchanged. Show the operation of your functions using an example.

Sample execution of your function is below:

```
> plaintext = john smith is the culprit!
  >k = (17, 8)
>ciphertext = AffineEncrypt(k, plaintext)
>ciphertext = fmxv ceotx oc txy qkndlot!
>AffineDecrypt(k, ciphertext)
>'john smith is the culprit!'
```

b) Consider k= (7,22), decrypt the following cipher text using **AffineDecrypt(k, ciphertext)** method.

Ciphertext **= falszztysyjzyjkywjrztyjztyynaryjkyswarztyegyyj**

Task 3 (1.5 Marks):

The OTP can be used to encrypt data of arbitrary length by encrypting binary symbols xi ε {0,1}. Decrypt the following ciphertext by hand. The ciphertext is given in hexadecimal notation:

26 34 05 18 0c 06 07 15 1c 2a 13 3c 0c 23 04 27 07 27 18

The key is given by:

6a 51 71 6b 49 68 64 67 65 5a 67 68 64 4a 77 65 68 48 73

Compute the plaintext, which is encoded in ASCII symbols.

Task 4 (2 Marks):

We conduct a known-plaintext attack on an LFSR-based stream cipher. We know that the plaintext sent was:

1001 0010 0110 1101 1001 0010 0110

By tapping the channel we observe the following stream:

1011 1100 0011 0001 0010 1011 0001

1. What is the degree m of the key stream generator?

2. What is the initialization vector?

3. Determine the feedback coefficients of the LFSR.

4. Draw a circuit diagram and verify the output sequence of the LFSR.

Task 5 (1.5 Marks):

What is the output of the first round of the DES algorithm when the plaintext and the key are both all zeros? Also, justify your answer with one example.

Good luck with your assignment!