Assignment 1

This set consists of 3 questions with a total marks of 62. Maximum you can score is 60.

1 Cyptanalysis of Classical Ciphers using chosen plaintext attack

Write algorithms to cryptanalyse the following ciphers. Assume the ciphers are written in English language on the alphabets A-Z.

(a) Shift Cipher: Write an algorithm $Break\_Shift$ that takes a ciphertext c as input and generates a plaintext m as output. You are given access to an encryption oracle $\mathcal{E}_{shift}$ that produces a ciphertext c' given a plaintext m'. You can access this oracles as many times as you want but $c' \neq c$. An efficient algorithm queries the oracle as few times as required.

(b) Substitution Cipher: Write an algorithm $Break\_Sub$ that takes a ciphertext c as input and generates a plaintext m as output. You are given access to a encryption oracle $\mathcal{E}_{sub}$ that produces a ciphertext c' given a plaintext m'. You can access this oracles as many times as you want but $c' \neq c$. An efficient algorithm queries the oracle as few times as required.

(c) Vigenere Cipher: Write an algorithm $Break\_Vigenere$ that takes a ciphertext c as input and generates a plaintext m as output. You are given access to a encryption oracle $\mathcal{E}_{Vigenere}$ that produces a ciphertext c' given a plaintext m'. You can access this oracles as many times as you want but $c' \neq c$. An efficient algorithm queries the oracle as few times as required.

What is minimum number of oracle queries in each case (1), (2), (3), to recover the ciphertext. For each of the above algorithms, you should first describe the idea and then provide a pseudocode. Write your answer in q1.txt.

Marks

1. Correct idea for (a) : 3 marks
2. Correct pseudocode (a): 2 marks
3. Minimum oracle queries for (a): 1 marks

4. Correct idea for (b) : 3 marks
5. Correct pseudocode (b): 2 marks
6. Minimum oracle queries for (b): 1 marks
7. Correct idea for (c) : 5 marks
8. Correct pseudocode (c): 4 marks
9. Minimum oracle queries for (c): 4 marks

Total: 25 marks

2 Perfect Secrecy

For each of the following encryption schemes, state whether the scheme is perfectly secret. Justify your answer in each case. Write your answer in q2.txt.

(a) The message space is $\mathcal{M} = \{0, \cdots, 6\}$. Algorithm `KeyGen` chooses a uniform key from the key space $\{0, \cdots, 7\}$. $Enc_k(m)$ returns $[k + m \mod 7]$, and $Dec_k(c)$ returns $[c - k \mod 7]$.

(b) The message space is $\mathcal{M} = \{m \in \{0,1\}^l |$ the last bit of m is $0\}$. `KeyGen` chooses a uniform key from $\{0,1\}^{l-1}$. $Enc_k(m)$ returns ciphertext $m \oplus (k||0)$, and $Dec_k(c)$ returns $c \oplus (k||0)$.

Marks

1. Correct answer for (a) : 2 marks
2. Correct justification for (a): 4 marks
3. Correct answer for (b) : 2 marks
4. Correct justification for (b): 4 marks

Total: 12 marks

(Programming task) Easy Vigenere Attack

Your task is design and implement an algorithm that takes as input a Vigenere ciphertext and length of the key and generates the plaintext message as output.

For example:

Input Ciphertext: iq q jed l eqvlo wh qy zep ivpzaxhtvi aoftf fe ywpweyag
Input length of key: 5
Output Key: alice
Output Plaintext: if i had a world of my own everything would be nonsense

Input

Ciphertext string in english language, might have only blank separator. Seperators will not be considered in encryption. Frequency table (if needed), which contains English alphabets and their frequencies. You can hardcode the data in your code.

Functions

Your code should have the following Functions:

1. findKey: Finds the key and prints it.
2. findPlaintext: Finds the plaintext and prints it.

Output

Your algorithm should print the following:

1. Key
2. Plaintext. Plaintext string with the same separators.

Marks

1. Correct output of findkey: 20 marks. You will receive partial marks if some keys are correct.
2. Marks Correct execution of findkey findPlaintext: 5 Marks

Total: 25 Marks

Full Submission

1. Q1: Write answer in q1.txt file.
2. Q2: Write answer in q2.txt file
3. Q3: Write the full code with the relevant functions: $q3.c$. You MUST submit a Makefile/script along with your code.
4. Upload a zip file with all three answers. $\langle zid \rangle \langle ass1 \rangle .zip$
5. The last question will be checked in-person during the tutorial session.