Programming Assignment

Cryptography (BITS F463)

Problem #1 (Breaking of a Classical Cipher)

The python script (**encrypt_classical.py**) provided along with this assignment implements an encryption algorithm (cipher), that takes a plaintext message file as input and produces an encrypted file as the output. As a sample to demonstrate the working of the cipher, a **sample_plaintext_p1.txt** and its corresponding **sample_ciphertext_p1.txt** is also provided. The key that has been used to produce this sample ciphertext is **bits@f463.** As part of this problem of the assignment you are supposed to do the following tasks.

1. Explain the encryption algorithm implemented by the python script **encrypt_classical_p1.py**.
2. Write the corresponding decryption script which will take output generated by the encryption script and generate the same plaintext as the output that was given to the encryption script as the input. Consider that both the encryption and decryption scripts are executed with the same key.
3. You are supposed to submit a CRACK code (**crack_classical_p1.py**) which when supplied with a ciphertex generated by the cipher should produce the corresponding plaintext. Note that, producing complete plaintext may not be feasible. So, even if your code is able to generate the partially correct plaintext, it is fine. In one sense, we are performing a ciphertext only attack to get the plaintext. It would be good if you use python language to write your code. However, you can convert the python script provided herewith into a C program and then write the CRACK in C.

Problem #2 (Multi Time Pad is not Secure)

In class, we discussed that OTP has perfect security but when the same key used multiple times it could lead to an insecure cipher.

1. Write the encryption (**encrypt_mtp_p2.py**) and decryption (**decrypt_mtp_p2.py**) and a key generation (**key_mtp_p2.py**) program for MTP (Multi time pad) cipher. Assume the plaintext is encoded as ASCII characters.
2. Develop a CRACK code (**CRACK_p2.py**) which when supplied with a number of ciphertext (say 10) generated by the cipher using the same key, should produce the corresponding plaintext for all the ciphers. Note that, producing complete plaintext may not be feas ible. So, even if your code is able to generate the partially correct plaintext, it is fine. In one sense, we are performing a ciphertext only attack to get the plaintext. It would be good if you use python language to write your code. However, you can convert the python script provided herewith into a C program and then write the CRACK in C.

Problem #3 (DES 2-Round is not Secure)

The DES performs 16 rounds. You are provide plaintext and a corresponding cipheterext pair in the files **sample_plaintext_p3.txt** and **sample_ciphertext_p3.txt** respectively. The ciphertext has been generated using the DES algorithm with 2 rounds only. The 56-bit key used for encryption is derived for a password containing exactly 7 Ascii characters (8 bit character), where the last character of the password is the character 'a'. Please note that the password contains ascii characters not the alphabets. Your task is to find the plaintext of the ciphertext given in the file named **target_ciphertext_p3.txt.** The last character of the password is reveled to reduce your effort of performing bruteforce attack and make the attack feasible.

Submission Details (Deadline Saturday, April 30, 2023, 11:55 PM)

1. Submit a zipped file with the name ***studentID_assignment.zip***

2. The zipped file should contain three different directories namely **Assignment_1a, Assignment_1b and Assignment_1c.** Submit the solutions to problems 1, 2 and 3 in the **Assignment_1a, Assignment_1b and Assignment 1c** directories respectively.

3. The **Assignment_1a** directory should contain the following
    - **report_1a.pdf** for the task 1 of the problem #1.
    - **decrypt_classical.py** for the task 2 of the problem #1.
    - **crack_classical.py** for the task 3 of the problem #1. The **crack_classical.py** file submitted by you should take the ciphertext as the input from the file with name "**ciphertext.txt**". The output (plaintext) generated by your code should be written in the file with name "**recoveredtext.txt**".

4. The **Assignment_1b** directory should contain the following
    - **report_1b.pdf, encrypt_mtp_p2.py, decrypt_mtp_p2.py, key_mtp_p2.py** for the task 1 of problem 2
    - **crack_mtp_p2.py** for the task 2 of the problem 2. The **crack_mtp_p2.py** file submitted by you should take the ciphertext as the input from the file with name "**ciphertext_p2.txt**". The output (plaintext) generated by your code should be written in the file with name "**recoveredtext_p2.txt**".

5. The **Assignment_1c** directory should contain the following
    - Decoded plaintext **(des_plaintext_p3.txt)**
    - Source code of the crack (**crack_des_p3.py)**

* **BORROWING or COPYING the source code will lead to heavy punishment. All the submissions will undergo a plagiarism check.**