Stony Brook University

CSE331: Computer Security Fundamentals

Assignment 1: Cryptography

In this assignment, you will implement the Vigenère cipher and break it!

Notes

- Your encryption/decryption should only consider the standard English alphabet (ABCDEFGHIJKLMNOPQRSTUVWXYZ)
- Preserve the spacings, word capitalizations, punctuations, and numbers in the plaintext.
- Cipher key is always in all caps.

Task 1: Implement the Vigenère cipher encoder

Write a program to encrypt an input using the Vigenère cipher. In the first line, the user shall provide the plaintext. In the second line, the user will provide the cipher key used for encryption. Your program should print out the ciphertext resulting from encrypting the plaintext using the cipher key.

Example 1

Input:

```
Hello world123!
SECURITY
```

Output:

```
Zinff ehpdh123!
```

Example 2

Input:

```
hell-o wor ld!
SECURITY
```

Output:

```
zinf-f ehp dh!
```

Task 2: Implement the Vigenère cipher decoder

Write a program to decrypt an input encrypted using the Vigenère cipher. In the first line, the user shall provide the ciphertext. In the second line, the user will provide the cipher key used for encryption. Your program should print out the plaintext resulting from decrypting the ciphertext using the cipher key.

Example 1

Input:

```
Zinff ehpdh123!
SECURITY
```

Output:

```
Hello world123!
```

Example 2

Input:

```
zinf-f ehp dh!
SECURITY
```

Output:

```
hell-o wor ld!
```

Task 3: Break the Vigenère cipher, knowing the key length

Write a program to crack an input encrypted using the Vigenère cipher, given its key length. In the first line, the user shall provide the ciphertext. In the second line, the user will provide the length of the cipher key used for encryption. In separate lines, your program should print out the cipher key, and the plaintext resulting from decrypting the ciphertext using the cipher key.

P.S. Don't worry! the ciphertext will be long enough to make frequency analysis possible.

Example 1

Input:

```
Zinff ehpdh123!
8
```

Output:

```
SECURITY
Hello world123!
```

Example 2

Input:

```
zinf-f ehp dh!
8
```

Output:

```
SECURITY
hell-o wor ld!
```

Task 4: Completely break the Vigenère cipher

Write a program to crack an input encrypted using the Vigenère cipher. In the first line, the user shall provide the ciphertext. In separate lines, your program should print out the cipher key, and the plaintext resulting from decrypting the ciphertext using the cipher key.

Example 1

Input:

```
Zinff ehpdh123!
```

Output:

```
SECURITY
Hello world123!
```

Example 2

Input:

```
zinf-f ehp dh!
```

Output:

```
SECURITY
hell-o wor ld!
```

What to submit

Submit a tarball to Brightspace, using your student ID number as its name (e.g. "123456789.tar.gz"). The tarball should contain:

- A report, describing your code and how you accomplished each task in PDF format titled "**report.pdf**".
- Your codes.
- Shell script to run each of the tasks. These files should be named "**taskN.sh**" where N is the task number (e.g., "task1.sh"). Out autograder will use these scripts to run and grade your code so make sure they are functioning correctly.

Lateness

Assigned work is due on 11:59PM on the dates listed in the class calendar. We strongly recommend that you get started early. Late submissions will be penalized by 10% of the maximum attainable score, plus an additional 10% every 4 hours until received. The instructors may grant individual extensions, but only under extraordinary circumstances.

Collaboration

Acts of cheating, plagiarism, and unacceptable collaboration will be reported to the Academic Judiciary. Cheating is when you copy, with or without modification, someone else's work that is not meant to be publicly accessible. Plagiarism is the practice of taking someone else's work or ideas and passing them off as one's own without providing attribution. Unacceptable collaboration is the knowing exposure of your own solutions, or the use of someone else's answers or solutions.

At the same time, we encourage students to help each other learn the course material. As in most courses, there is a boundary separating these two situations. You may give or receive help on any of the concepts covered in lecture. You are allowed to consult with other students about the conceptualization of a project, or the general approach for solving problems. However, all work, whether in scrap or final form, must be done by you.

If you have any questions as to what constitutes unacceptable collaboration or exploitation of prior work, please talk to an instructor right away. You are expected to exercise reasonable precautions to protect your own work, including not posting solutions publicly.