University of Sussex Autumn 2018

Introduction to Computer Security – G6077

Weighting: 50% of marks for the module

Released: Monday 12th November 2018

Submission deadline: Thursday 6th December by 16:00 as an e-submission to Canvas

The coursework assigned below must be submitted online as a pdf or doc file on Canvas along with any program and data.

You must work on this assignment on your own. The standard Informatics rules for collusion, plagiarism and lateness apply. Any cases of potential misconduct discovered will be reported and investigated.
Your work should be presented to professional standards.

All questions must be answered. There are no optional questions.

Part A

Suppose you work as a junior cyber security expert in a security organisation. Your manager has forwarded you the encrypted message below and has asked you to carry out an analysis. Complete task 1 based on the cipher text listed below.

```
PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOY
QWIPBVWLXTOXBTFXQWAXBVCXQWAXFQJV
WLEQNTOZQGGQLFXQWAKVWLXQWAEBIPBFX
FQVXGTVJVWLBTPQWAEBFPBFHCVLXBQUFEVW
LXGDPEQVPQGVPPBFTIXPFHXZHVFAGFOTHFEFB
QUFTDHZBQPOTHXTYFTODXQHFTDPTOGHFQP
BQWAQJJTODXQHFOQPWTBDHHIXQVAPBFZQ
HCFWPFHPBFIPBQWKFABVYYDZBOTHPBQPQJT
QOTOGHFQAPBFEQJHDXXQVAVXEBQPEFZBVF
OJIWFFACFCCFHQWAUVWFLQHGFXVAFXQHFU
FHILTTAVWAFFAWTEVOITDHFHFQAITIXPFHX
AFQHEFZQWGFLVWPTOFFA
```

Task 1

(a) Outline your approach to decode the cipher text.

(b) Decrypt as many letters and words as you can. [32 marks]

Marking criteria

The following criteria will be used in marking part A:

1. Correctness of approach. Knowledge and understanding of ciphers and other techniques will help you to outline the steps. Correct steps need to be identified.

2. Depth of analysis. You can use online tools to perform analysis of the cipher text. Analysis can be carried at different depths. Analysis at different depths will help to identify plain text.

3. Number of words identified. There are at least eight different words to be identified.

4. Presentation of analysis and results.

Part B

Substitution and transposition used almost in all symmetric ciphers. Your task is to devise a new cipher using any or combination of these techniques.

Task 2
Write an algorithm for your cipher.

Task 3
Illustrate your cipher through an example.

Task 4
Implement your cipher using Java and test it on different inputs.

[32 marks]

Marking criteria:

The following criteria will be used in marking part B:

1. Precision: the steps are precisely defined.

2. Uniqueness: the results of each step are uniquely defined and only depend on the input and the result of the preceding steps.

3. Algorithm works on a range of inputs.

4. Algorithm produces an output of either cipher text or plain text depending on the input.

Part C

Task 5
You will need to use the DVDSwap application for this task, which is available on Canvas. There are a number of files and folders in the project. You will need to find the part which is required to complete the task. You are not required to fix errors to make the application run.

In the module, you have studied the different issues and challenges about protecting passwords. As a junior expert in cyber security, describe and analyse the password policy used in the DVDSwap application. Suggest improvements based on your analysis. Implementation of these suggestions is not required. However, you should give a detailed information about your suggested improvements.

Task 6
Describe the architectural differences between DES, 3DES and AES. Provide examples to demonstrate your understanding.

Task 7
How is the General Data Protection Regulation different from its predecessor? What are its impacts on individuals and on organisations?

[36 marks]

Marking criteria:

The following criteria will used in marking part C:

1. For task 5, marks will be awarded based on:

- Correctly identifying weaknesses in password policy.
- Suggesting how those weaknesses need to be dealt with.

2. For task 6, marks will be awarded based on:

- Identifying differences between the three ciphers.

- Accuracy of explanation.
- Use of clear examples to make understanding clear.

3. For task 7, marks will be awarded based on:

- Defining GDPR and its predecessor.
- Identifying detailed differences between GDPR and its predecessor.
- Highlighting the impact of GDPR on individuals.
- Highlighting the impact of GDPR on organisations.