University of Southampton	School of Electronics and Computer Science	Coursework Instructions
Module: ELEC6242	Cryptography	Lecturer: Dr. Basel Halak
Deadline: 07/03/2018	Feedback: 07/04/2018	Weighting: 20%

Instructions

This coursework is in three parts. You should complete each part, working independently of other individuals.

1. **Decrypt the following cipher**

   You will receive your unique cipher by email

2. **Decrypt the hidden message contained in the attached file (secret.hex)**

   Hint: The first letter of the original message is **A**

3. **Decrypt the following cipher**

   You will receive your unique cipher by email

   Hint: The original message contains alphabetical letters only, and it is encrypted using a two stage cryptosystem.

File Submission

Please submit your report in PDF format using the ECS electronic hand-in system. Submission in any other formats will not be considered as valid submissions, and therefore they may lead to the application of late penalties (10% deduction of the awarded mark for each working day).

Learning Outcomes (LOs)

Having successfully completed the module, you should be able to:

1. Apply a number of cryptanalysis methods to decipher encrypted messages
2. Write a concise report to describe your proposed solutions, methods of analysis design, how they were arrived at and how they perform.

Marking Scheme

Criterion	Description	Outcomes	Marks
Challenge 1	The thoroughness of deciphering methodology and the accuracy of the solution	1,2	10
Challenge 2	The thoroughness of methodology and the accuracy of the solution	1,2	7
Challenge 3	The thoroughness of methodology and the accuracy of the solution	1,2	3

Report Structure

Your report should have the following structure:

1. **Outline Section** which summarises the content of the reports
2. **Solution for Cipher 1**: this section only includes the plaintext for cipher 1 and the decryption key
3. **Cipher 1 Cryptanalysis**: This section provides a summary of the techniques you have used to solve the cipher. It should include evidence of all analysis you have performed in order to solve the cipher such (e.g. frequency analysis), in addition it should refer to any programs you have developed in order to perform cryptanalysis (**500 words)**
4. **Solution for Cipher 2**: this section only includes the plaintext for cipher 2 and the decryption key
5. **Cipher 2 Cryptanalysis**: This section provides a summary of the techniques you have used to solve the cipher. It should include evidence of all analysis you have performed in order to solve the cipher such (e.g. frequency analysis), in addition it should refer to any programs you have developed in order to perform cryptanalysis (**500 words)**
6. **Solution for Cipher 3**: this section only includes the plaintext for cipher 2 and the decryption key
7. **Cipher 3 Cryptanalysis**: This section provides a summary of the techniques you have used to solve the cipher. It should include evidence of all analysis you have performed in

order to solve the cipher such (e.g. frequency analysis), in addition it should refer to any programs you have developed in order to perform cryptanalysis (**500 words)**.

8. **Appendix A:** includes any software scripts you have developed to solve cipher 1
9. **Appendix B**: includes any software scripts you have developed to solve cipher 2
10. **Appendix C**: includes any software scripts you have developed to solve cipher 3

Please note failure to follow this structure will lead to a loss of mark

Late submissions will be penalised at 10% per working day. No work can be accepted after feedback has been given.
Please note the University regulations regarding academic integrity.