EBU6010

Cryptography and Cyber Security

September 2023

Tutorials 1 (For teaching block1)

Office Hour

If you have any questions, or if you wish to discuss anything relating to the module, please raise them during the lectures and tutorials or make use of the office hour

Revision

- **What is the difference between a <u>block cipher</u> and a <u>stream cipher</u>?**

- **What is the purpose of the S-box in DES? How is it used? Explain.**

Revision

- **How does a one-time pad work and how secure it is?**

- **What is cryptography?**

1. Briefly explain the security services of confidentiality, integrity and availability.

2. Consider a student attendance information system in which the students provide a password for accessing their accounts. Give examples of the security services the system should provide in terms of confidentiality, integrity, access control and availability.

3. Why is Caesar cipher substitution technique vulnerable to a brute-force cryptanalysis?

4. Why is the one-time pad scheme unbreakable? What are the practical problems of one-time pad?

5. Construct a Playfair matrix with the key ***Reasons***. Make a reasonable assumption about how to treat redundant letters in the key. Encrypt the message: **See some light in the darkness**.

6. Using Vigenere Cipher, encrypt the word “**examination**” using the key “***grades***”.

7. Briefly define the terms **substitution** and **permutation**.

8. Which are the two main areas of concern related to the level of security provided by DES?

9. What is the purpose of the key expansion algorithm used in AES?

10. A typical round of AES encryption consists of four stages (Substitution bytes, Shift Rows, Mix Columns and Add Round Key). Describe the functionality of each stage.

- When PT109 was sunk by a Japanese destroyer in WWII (this was JFK's command), the following message was received at an Australian monitoring station in Playfair code:

KX JEY UREBE ZWEHE WRYTU HEYFS

KREHE GOYFE WTTTU OLKSY CA JPO

BOTE I ZONTX BYBWT GONEY CUZWR

GDSON SXBOU YWRHE BAAHY USEDQ

- The key is *royal new zealand navy*: decrypt the message.