# Topic 1: Introduction to Cryptography

## Week 1 Tutorial & Lab

## Tutorial 1.0 MCQ and Essay Questions

### MCQ

1. A ciphertext of a message is produced (select all apply):
   (a) before the encryption.
   (b) after the encryption.
   (c) before the decryption.
   (d) after the decryption.

2. An encryption or decryption process requires (select all apply):
   (a) a cipher.
   (b) a message.
   (c) a key.
   (d) a transmission medium.

3. The principle of _____ ensures that only the sender and the intended recipients have access to the contents of a message.

   (a) confidentiality
   (b) authentication
   (c) integrity
   (d) Availability

4. If the recipient of a message must be satisfied with the identity of the sender, the principle of _____ is required.

   (a) confidentiality
   (b) authentication
   (c) integrity
   (d) Availability

5. If we want to ensure the principle of _____, the contents of a message must not be modified while in transit.

   (a) confidentiality
   (b) authentication
   (c) integrity
   (d) availability

6. The principle of _____ ensures that the sender of a message cannot later claim that he/she never sent that message.

(a) access control
(b) authentication
(c) availability
(d) non-repudiation

7. The _____ attack is related to confidentiality.

(a) interception
(b) fabrication
(c) modification
(d) interruption

8. The _____ attack is related to authentication.

(a) interception
(b) fabrication
(c) modification
(d) interruption

9. The _____ attack is related to integrity.

(a) interception
(b) fabrication
(c) modification
(d) interruption

10. The _____ attack is related to availability.

(a) interception
(b) fabrication
(c) modification
(d) interruption

11. In _____ attacks, there is no modification to message contents.

(a) passive
(b) active
(c) both of the above
(d) none of the above

12. In _____ attacks, the message contents are modified.

(a) passive
(b) active
(c) both of the above
(d) none of the above

13. Interruption/ attacks are also called _____ attacks.

(a) masquerade
(b) alteration
(c) denial of service
(d) replay attacks

14. You made a e-payment to the supplier for a goods you purchased. What would be your **primary** cybersecurity concern in this scenario?

(a) Confidentiality
(b) Availability
(c) Integrity
(d) Non-repudiation

15. Select a **primary** cybersecurity requirement to protect a top-secret document.

(a) Confidentiality
(b) Availability
(c) Integrity
(d) Authenticity

16. Select a **primary** security requirement to proof that the email was sent by a certain individual.

(a) Confidentiality
(b) Availability
(c) Integrity
(d) Non-repudiation

17. What is the objective of data security (select all applicable).

(a) protecting the organization data
(b) protecting the personal data
(c) protecting the computing systems
(d) preserve the privacy of individuals

**Essay Questions**

18. List the applications of cryptography in cybersecurity.
19. Explain what repudiation is in email communication.
20. What are the two categories of passive attacks?
21. What are the four categories of active attacks?
22. Provide an example implementation of non-repudiation techniques by a bank at their ATM machines.
23. Discuss how can you strengthen the authentication methods to ensure only you can provide the correct credentials.

## 2.0 Research

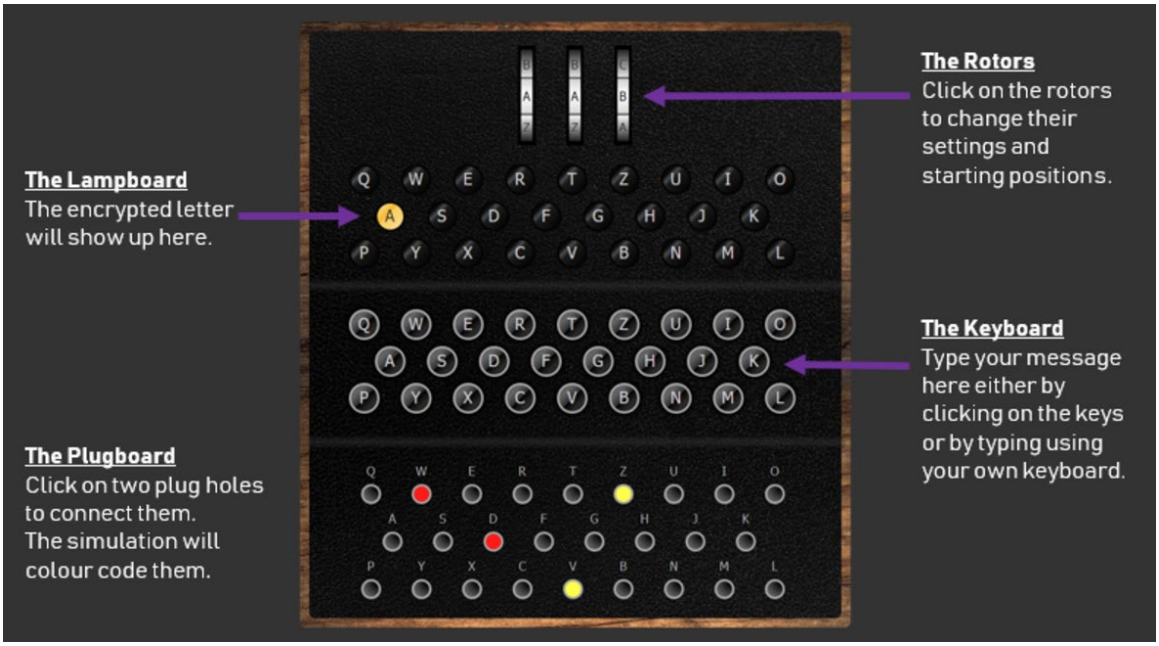
Watch the video https://www.youtube.com/watch?v=mcX7iO_XCFA that explains the workings of the enigma machine.
Discuss the following topics assigned to your group. Document your answer in Microsoft Word and present your answer. The a*nswer should not be more than one paragraph with a maximum of three sentences.*

| Group | Question |
|---|---|
| 1 | In the process of encryption, how was enigma designed to encrypt the same cleartext letter to different cipher text letters? |
| 2 | What is considered "Key(s)" in the enigma encryption and decryption process? |
| 3 | What are the requirements to decrypt a cipher text received to a correct cleartext? |
| 4 | Describe the process of sending messages and receiving them securely. |
| 5 | Share how the presenter concluded that total possible no. using the rotors alone is 17576. |
| 6 | How the British defeat the enigma encryption? (Research on Google) |

Submit your answer using the answer template provided.

## 3.0 Workshop

**3.1** Point your browser to https://www.101computing.net/enigma-machine-emulator. Familiar yourself with the emulator.



***3.2*** After understanding the Enigma operation, encrypt the following message (without quotes). Setting are provided step 3.5.

*Note: there is no space bar in Enigma. You can ignore the spaces.*

**THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG**

3.3 Take down the cipher text generate by the emulator.

3.4 Verify between the groups to ascertain that the cipher text has been decrypted to original cleartext. The table below show the group pairing.

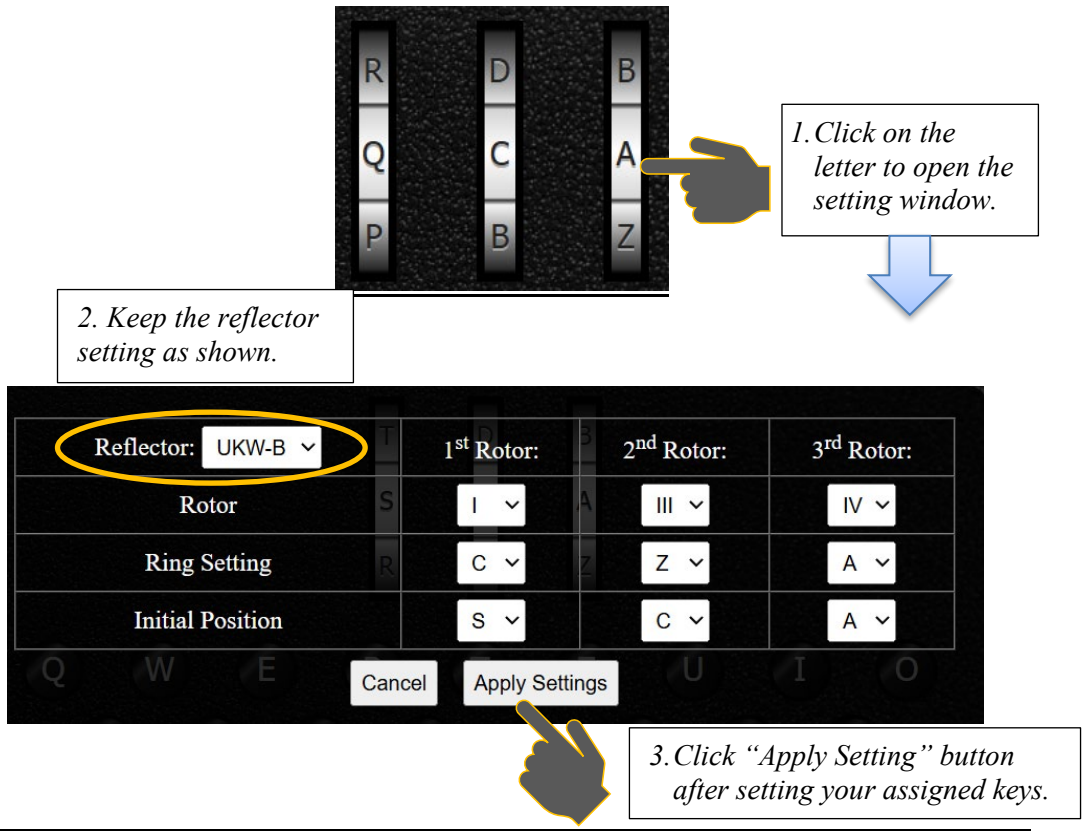
| No | Group Pairs | |
|---|---|---|
| 1 | Group 1 | Group 5 |
| 2 | Group 2 | Group 4 |
| 3 | Group 3 | Group 6 |

3.5 **Machine Setting**

The Rotor, Ring, and Initial Position settings for each group are as follows, and click on "*Apply Settings*" button. *No new setting is required for the plug-board.*

Initial Rotor Setting

*The Enigma settings for both encryption and decryption process must be the same. Use the following setting for all groups.*



**Group 1**

| | | | |
|---|---|---|---|
| Rotor | I | III | V |
| Ring setting | C | Z | A |
| Initial Position | A | B | D |

**Group 2**

| | | | |
|---|---|---|---|
| Rotor | II | III | IV |
| Ring setting | K | M | O |
| Initial Position | D | G | B |

**Group 3**

| | | | |
|---|---|---|---|
| Rotor | III | I | II |
| Ring setting | H | N | P |
| Initial Position | C | J | L |

**Group 4**

| | | | |
|---|---|---|---|
| Rotor | II | V | IV |
| Ring setting | Q | W | E |
| Initial Position | R | T | A |

**Group 5**

| | | | |
|---|---|---|---|
| Rotor | I | IV | III |
| Ring setting | A | S | D |
| Initial Position | F | C | Q |

**Group 6**

| | | | |
|---|---|---|---|
| Rotor | II | III | IV |
| Ring setting | F | G | H |
| Initial Position | B | N | M |

**Submit the cipher text produced by the Enigma using the answer template provided.**

## 4. Cryptanalysis Challenge

Download an encrypted Microsoft Word file that corresponds to your group name posted under "**decryptme**" under the Politemall folder "Topic 1".

> Rumors are that the keywords from the first lecture are used as keys to encrypt the documents.

Perform a cryptanalysis to obtain the cleartext from the ciphertext.

**Submit the Key/password to the file and the cleartext using the submission template provided.**

**End-of-Lab 1**