**Lab 1 Submission**

|  |  |  |
| --- | --- | --- |
| **Tutorial group** | **Group No.** | **Members’ Names** |
| **AA2402** | **2** | **Kriston** |
| **Boon Khai** |
| **Dhiraj** |
| **Yu En** |

**2.0 Research**

|  |  |
| --- | --- |
| 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?  In the Enigma encryption and decryption process, the "key(s)" refer to the initial configuration settings that determine how messages are encoded and decoded. These keys include the rotor order, ring settings, plugboard connections, and the starting positions of the rotors. Both the sender and receiver must use identical keys to ensure successful encryption and decryption. |
| 3 | What are the requirements to decrypt a cipher text received to correct cleartext? Why?  We need the co |
| 4 | Describe the process of sending messages and receiving messages 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)  They utilised a combination of mathematicians, who designed a machine called the “Bombe” to decipher Enigma messages, along with captured Enigma machines, human analysis of messages, and exploiting operational errors made by German operators. |

**3.1**

Submit the cipher text produced by the Enigma:

**3.2**

The password/Key to the Microsoft word file:

The content of the file.