Enigma Template

Q1. Explain the following terms:

(a) Ringstellung (ring setting)

The ring setting adjusts the position of the rotor’s alphabet ring relative to its internal wiring. This setting shifts the rotor’s electrical paths, adding complexity to the encryption.

(b) Grundstellung (indicator setting)

The initial rotor positions before encrypting a message. The sender and recipient both set their machines to this shared position to synchronize encryption and decryption.

(c) Message setting

The specific rotor positions chosen by the sender for encrypting the actual message. After setting the Grundstellung, the message setting is encrypted and transmitted to the recipient along with the main message.

(d) Kenngruppen

A three-letter identification code included at the start of a message to indicate the correct key settings (rotor orders and plugboard connections) for decryption.

Q2. Send the non-secret information required to decrypt the message (which includes the encrypted text and your birthday) to one of your colleagues by email (make sure that you add the lab teachers to CC) Once you receive the corresponding message from your fellow colleague configure your Enigma machine accordingly and decrypt the message

Using the software available on Labs 2 folder inside the VM I encrypted my message using the settings:

- Unordered List ItemKenngruppe: NSM
- Indicator: DBM
- Message setting: YMG
- Message: “For my birthday I would like to visit my grandmother”
- Birthday: 23-09-1998 (dd-mm-yyyy)
- The encrypted message is the following: “BD ZXSGT SKXCT UUYTO RTVMI VFGJV NFLZL QYDDB ERWLJ JDZVD OZWMN MVDQ”

From my pair student I received the following email:

- Kenngruppen: WIP
- Indicator: BCD
- Message Indicator: KEL
- Message: EJMGFRZYCJBVVHWZGZXHZEUKTMG
- Birthday: 15-10-1997 (dd-mm-yyyy)

Q3. How does the number of keys compare to the number of keys of a typical Enigma machine with the following specification.

Violetta Key Space Calculation The key space for the Violetta can be divided into several components: chosen rotors, rotor ring rotations, reflector choice, ring settings, and plugboard configurations.

Choosing Rotors:

The number of ways to choose 12 rotors from 53, maintaining the order: $$ \frac {53!} {(53−12)!}= 1.278 × 10^{20} $$

Rotor Ring Rotations:

Each of the 12 rotor rings has 32 positions, giving: $$ 32^{12}=1.153×10^{18} $$

Choosing Reflector:

There are 7 reflectors available, so there are 7 possible configurations. Ring Settings:

There are 3 rings, but only 2 contribute to the key space. Each has 32 possible orientations, so: $$ 32^{(3−1)}=32^2=3.603×10^{16} $$

Plugboard Configuration:

With a maximum of 16 cables and 32 plugs available, the total number of configurations is: $$ C_{\text{total}} = \sum_{i=0}^{16} \frac{32!}{(32-2i)! \cdot i! \cdot 2^i} $$

Putting all these components together, the total key space for the Violetta is: $$ 1.278 \times 10^{20} \times 1.153 \times 10^{18} \times 7 \times 3.603 \times 10^{16} \times 2.248 \times 10^{19} = 8.354 \times 10^{74} $$

Enigma Machine Key Space Calculation The Enigma machine's key space also consists of multiple components: rotor selection, rotor ring rotations, reflector choice, ring settings, and plugboard configuration. Choosing Rotors: The number of ways to choose 3 rotors out of 5: $$ \frac{5!}{(5-3)!} = 60 $$ Rotor Ring Rotations: Each of the 3 rotors has 26 positions, so: $$ 26^3 = 17,576 $$ Choosing Reflector: There are 3 reflectors, giving 3 configurations. Ring Settings: With 3 rings and one not contributing, the configuration count is: $$ 26^{(3-1)} = 26^2 = 676 $$ Plugboard Configuration: For 10 cables and 26 plugs, the total number of configurations is: $$ C_{10} = \frac{26!}{(26-20)! \cdot 10! \cdot 2^{10}} = 1.507 \times 10^{14} $$ The total key space for the Enigma machine is: $$ 60 \times 17,576 \times 3 \times 676 \times 1.507 \times 10^{14} = 3.223 \times 10^{23} $$

Comparison of Key Spaces The Violetta's key space $$ (8.354 \times 10^{74}) $$ is approximately $$ 2.592 \times 10^{51} $$ times larger than that of the Enigma machine $$ (3.223 \times 10^{23}) $$ This enormous difference indicates that, in the context of exhaustive search attacks, the

Violetta offers far greater security than the Enigma machine.

- The Violetta's key space is significantly larger due to its higher number of rotors, more possible rotor rotations, and a greater number of plugboard configurations. As result, the Violetta is much more resistant to brute-force attacks compared to the Enigma machine.