Innopolis University

SYSTEM AND NETWORKING ENGINEERING

Security of Systems and Networks

LABORATORY REPORT 2

Enigma

Student	**ID**
Grebennikov Sergey	47611

Lecturer
Dr. Rasheed Hussain, PhD

October 23, 2017

Contents

1 Enigma

Use the Enigma simulator as installed on the VirtualBox image. Write a phrase in English, not shorter than 20 characters which states what present you want for your next birthday. Lookup the settings corresponding to your birthday in 2015 in the code book available at: `https://www.os3.nl/_media/2015-2016/courses/ssn/sne_enigma_2015.zip`, and use these to select the rotors and set the rings on the rotors. Next, follow the official German operating procedure described in `http://www.ellsbury.com/enigma3.htm` to encrypt the phrase.

Question

1. 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 Kirill and Kanwal to CC [1]). Once you receive the corresponding message from your fellow colleague, configure your Enigma machine accordingly and decrypt the message.

ENCRYPTION

BirthDay: 05 May
Daily Key: Table 1 **Rotor arrangement:** IV V II

Tag	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
05	IV V II	12 07 06	AY BI CG DQ EX FM HK LW OT RZ	BDM XOJ PEE VSP

Table 1: Daily key from the monthly list

Ring Settings: 12(L) 07(G) 06(F)
Plugboard settings: AY BI CG DQ EX FM HK LW OT RZ
Reflector: B
Kenngruppen: PEE
Rotor Settings: 01(A) 02(B) 03(C)
Message Key: 07(G) 19(S) 01(A)
Encrypted Message Key: S I B
Letter identification group: KZEEP
Plaintext:

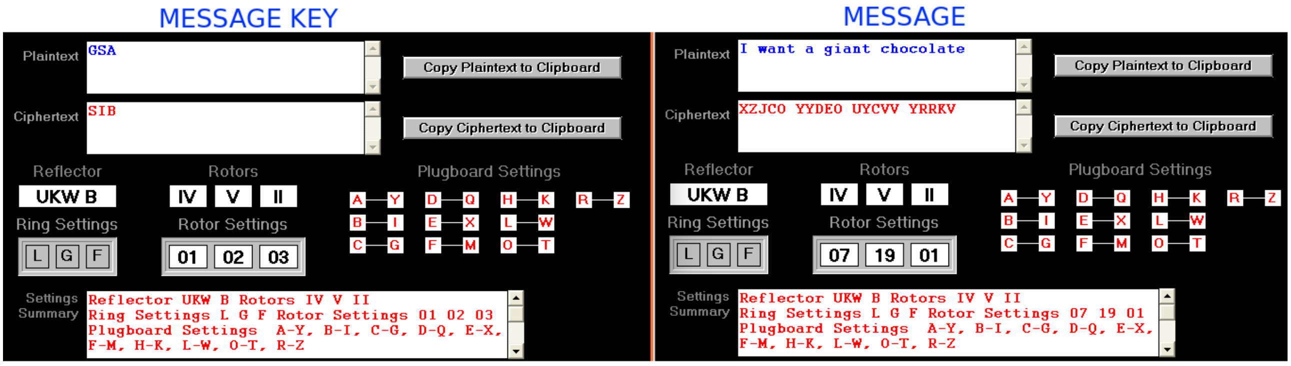
```
I want a giant chocolate
```

Ciphertext:

```
0900 1tl 1tl 25 ABC SIB

KZEEP XZJCO YYDEO UYCVV YRRKV
```

Complete Setting Summary: Figure 1



MESSAGE KEY

Plaintext: GSA
Ciphertext: SIB
Reflector: UKW B
Rotors: IV V II
Ring Settings: L G F
Rotor Settings: 01 02 03
Plugboard Settings: A–Y, D–Q, H–K, R–Z, B–I, E–X, L–W, C–G, F–M, O–T
Settings Summary:

```
Reflector UKW B Rotors IV V II
Ring Settings L G F Rotor Settings 01 02 03
Plugboard Settings  A-Y, B-I, C-G, D-Q, E-X,
F-M, H-K, L-W, O-T, R-Z
```

MESSAGE

Plaintext: I want a giant chocolate
Ciphertext: XZJCO YYDEO UYCVV YRRKV
Reflector: UKW B
Rotors: IV V II
Ring Settings: L G F
Rotor Settings: 07 19 01
Plugboard Settings: A–Y, D–Q, H–K, R–Z, B–I, E–X, L–W, C–G, F–M, O–T
Settings Summary:

```
Reflector UKW B Rotors IV V II
Ring Settings L G F Rotor Settings 07 19 01
Plugboard Settings  A-Y, B-I, C-G, D-Q, E-X,
F-M, H-K, L-W, O-T, R-Z
```

Copy Plaintext to Clipboard
Copy Ciphertext to Clipboard
Copy Plaintext to Clipboard
Copy Ciphertext to Clipboard

Figure 1: Complete setting summary for message key and message.

[1] k.saltanov@innopolis.ru, k.batool@innopolis.ru

DECRYPTION

Ciphertext:

1515 1tl 1tl 37 SNE GRK

RUFOD AMJCK YLJGX SUOLY IYRSZ WJGEL RIRTV IO

BirthDay: 21 Feb
Daily Key: Table 2
Rotor arrangement: I IV V

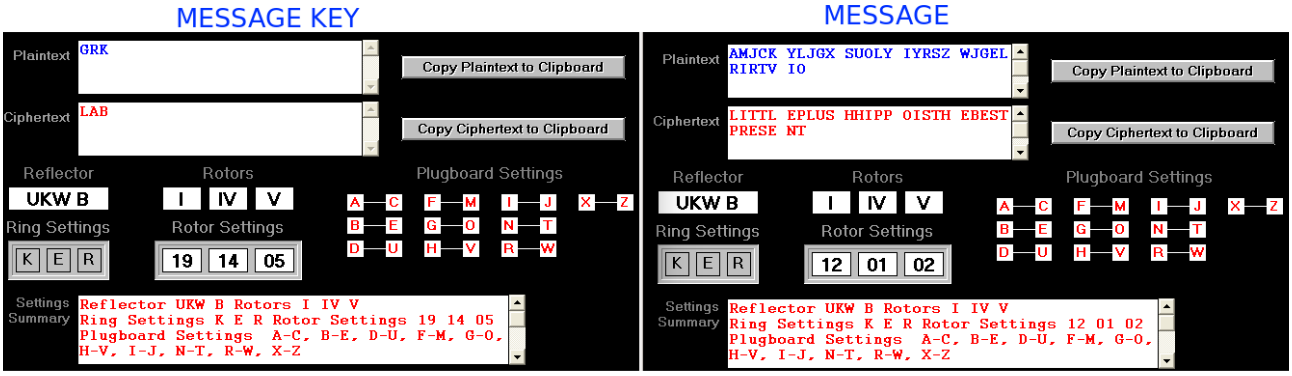
Tag	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
21	I IV V	11 05 18	AC BE DU FM GO HV IJ NT RW XZ	DOF HCA VQW UUI

Table 2: Daily key from the monthly list

Ring Settings: 11(K) 05(E) 18(R)
Plugboard settings: AC BE DU FM GO HV IJ NT RW XZ
Reflector: B
Kenngruppen: DOF
Rotor Settings: 19(S) 14(N) 05(E)
Encrypted Message Key: 07(G) 18(R) 11(K)
Message Key: 12(L) 01(A) 02(B)
Letter identification group: RUFOD
Plaintext:

LITTLE PLUSH HIPPO IS THE BEST PRESENT

Complete Setting Summary: Figure 2



MESSAGE KEY

Plaintext: GRK
Ciphertext: LAB
Reflector: UKW B
Rotors: I IV V
Ring Settings: K E R
Rotor Settings: 19 14 05
Plugboard Settings: A—C, B—E, D—U, F—M, G—O, H—V, I—J, N—T, R—W, X—Z
Settings Summary:
Reflector UKW B Rotors I IV V
Ring Settings K E R Rotor Settings 19 14 05
Plugboard Settings A-C, B-E, D-U, F-M, G-O,
H-V, I-J, N-T, R-W, X-Z

MESSAGE

Plaintext:
AMJCK YLJGX SUOLY IYRSZ WJGEL
RIRTV IO
Ciphertext:
LITTL EPLUS HHIPP OISTH EBEST
PRESE NT
Reflector: UKW B
Rotors: I IV V
Ring Settings: K E R
Rotor Settings: 12 01 02
Plugboard Settings: A—C, B—E, D—U, F—M, G—O, H—V, I—J, N—T, R—W, X—Z
Settings Summary:
Reflector UKW B Rotors I IV V
Ring Settings K E R Rotor Settings 12 01 02
Plugboard Settings A-C, B-E, D-U, F-M, G-O,
H-V, I-J, N-T, R-W, X-Z

Copy Plaintext to Clipboard
Copy Ciphertext to Clipboard
Copy Plaintext to Clipboard
Copy Ciphertext to Clipboard

Figure 2: Complete setting summary for message key and message.

2 Viola

You have just uncovered a so far unknown encryption machine called Viola which looks a bit similar to the Enigma machine. You are asked to compute the upper bound of different keys (or machine start configurations) you have to search in a brute force attack on an intercepted message.

- The Viola machine can fit 1 static reflector and 10 rotors each with 30 characters.
- There are 5 unique reflectors to select from.
- There are 50 unique (under all rotations) rotors to select from.
- The machine has a standard plugboard for all 30 characters.
- It is unknown how many plugboard cables are used so assume any number could be used.

2. How does the number of keys compare to the number of keys of a typical Enigma machine with the following specification:
   - The typical Enigma machine can fit 1 static reflector and 3 rotors each with 26 characters.
   - There are 3 unique reflectors to select from.
   - There are 5 unique (under all rotations) rotors to select from.
   - The machine has a standard plugboard for all 26 characters.
   - It is known the operator always uses 10 plugboard cables.

ENIGMA

Name	**Amount**	**Used**	**Ways**
Reflector	3	1	3
Rotor	5	3	60
Plugboard hole	26	20	150 738 274 937 250
Rotor position	26^3	1	17 576
Ring	26^2	1	676
Total			$\approx 3,22 \times 10^{23}$

VIOLA

Name	**Amount**	**Used**	**Ways**
Reflector	5	1	5
Rotor	50	10	$\approx 3727,6 \times 10^{13}$
Plugboard hole	30	0-30	$\approx 60691,7 \times 10^{13}$
Rotor position	30^{10}	1	$59,049 \times 10^{13}$
Ring	30^9	1	$1,9683 \times 10^{13}$
Total			$\approx 13 \times 10^{62}$

Used Formulas

Reflector:

$$\frac{n!}{(n-r)!} = \frac{5!}{(5-1)!}$$

Rotor:

$$\frac{n!}{(n-r)!} = \frac{50!}{(50-10)!}$$

Plugboard hole:

$$\sum_{r=0}^{\frac{n}{2}} \frac{n!}{(n-2r)\cdot r!\cdot 2^r} = \sum_{r=0}^{15} \frac{30!}{(30-2r)\cdot r!\cdot 2^r}$$

Rotor position:

$$r^c = 30^{10}$$

Ring:

$$r^{c-1} = 30^9$$

3 Conclusion

Despite the fact that from the point of view of modern cryptography, the Enigma cipher was weak, in practice only a combination of this factor with others (such as operator errors, procedural flaws, falsified messages (for example, in weather reports), capture of Enigma copies and encryption books) allowed crackers of ciphers to unravel the Enigma ciphers and read the messages.

References

[1] M. Stamp, Information Security: Principles and Practice, Second Edition, 2011, 606 pages.

[2] The Enigma Machine. Its Construction, Operation and Complexity `http://www.ellsbury.com/enigma3.htm`.

[3] Enigma Simulation `http://enigmaco.de/enigma/enigma.html`.