The
Enigma Machine Simulator
Ciphering Algorithm

Document holds a brief explanation of the algorithm used in The Engima Machine Simulator.

I. Settings

This simulator is based on the settings of real Enigma Machine used in World War II.

Enigma I was the main ciphering machine used by the German Military. Although, Enigma was used before the war, it was modified to provide higher security standards for encrypted messages. The machine also had several commercial versions, but none of them was as complex as these used by military.

Discussed simulator uses following components and settings:

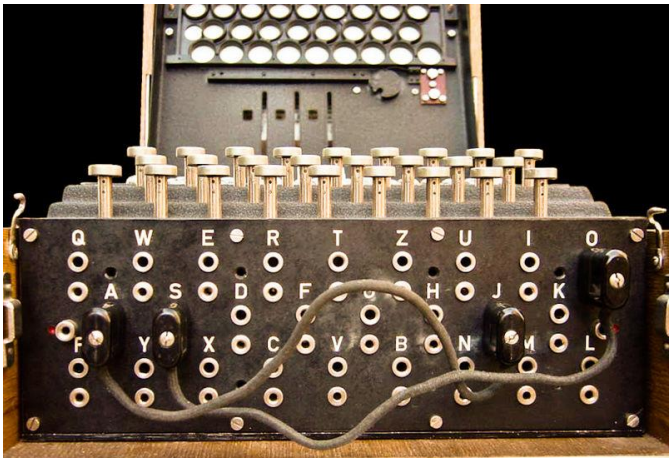
	Input/Output Alphabet Conversion A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
FIRST ROTOR (ALPHA)	E K M F L G D Q V Z N T O W Y H X U S P A I B R C J
SECOND ROTOR (BETA)	A J D K S I R U X B L H W T M C Q G Z N P Y F V O E
THIRD ROTOR (GAMA)	B D F H J L C P R T X V Z N Y E I W G A K M U S Q O
REFLECTOR A (UKW-A)	E J M Z A L Y X V B W F C R Q U O N T S P I K H G D
REFLECTOR B (UKW-B)	Y R U H Q S L D P X N G O K M I E B F Z C W V J A T
REFLECTOR C (UKW-C)	F V P J I A O Y E D R Z X W G C T K U Q S B N M H L

(tab.1.1)

i. Steckerbrett (plug board)

Mechanism of conjungtion two letters from alphabet. Operator used this setting to ensure that a letter would be changed for further encryption steps. It is not required to use this setting.

Będkowski Patryk
Warsaw University of Technology

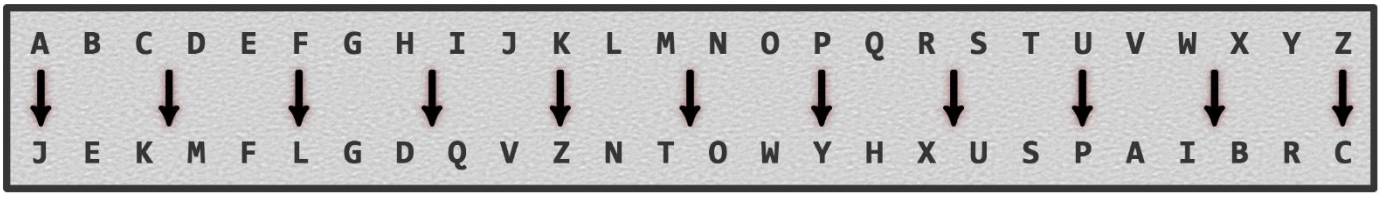


(source en.wikipedia.org/wiki/Enigma_machine)

ii. Rotors

Each of three rotors can be set in one from 26 positions. This element ensures that a letter will be specifically changed to another. However, the process of changing letter to another depends on **model of the rotor and its position** (value 1-26).

In base position (position 1), rotor **model: A** changes letters as shown below:



(pic.1.1) e.g. if letter **L** is inserted into the rotor, it is changed to letter **T.**

After one letter has been inserted into machine, the value of each rotor changes:

When rotor alpha changes position from 26 to 1, rotor beta's position increments by value 1. Similarly when rotor beta changes position from 26 to 1, rotor gamma's position is incremented by value 1.

Notice that output alphabet of the original **rotor A** (tab.1.1) is little bit different than one presented above(pic1.1). That is because, before each letter is changed, alpha's rotor setting value is increased by 1. Thus shifting output alphabet one time to the right, causing change of alpha's setting from value **1** to value **2.**

But what does position of the rotor means? Position of the rotor defines how output alphabet is shifted compared to the base position coding. If alpha rotor's position value is 10, its output alphabet is shifted 9 times to the right.

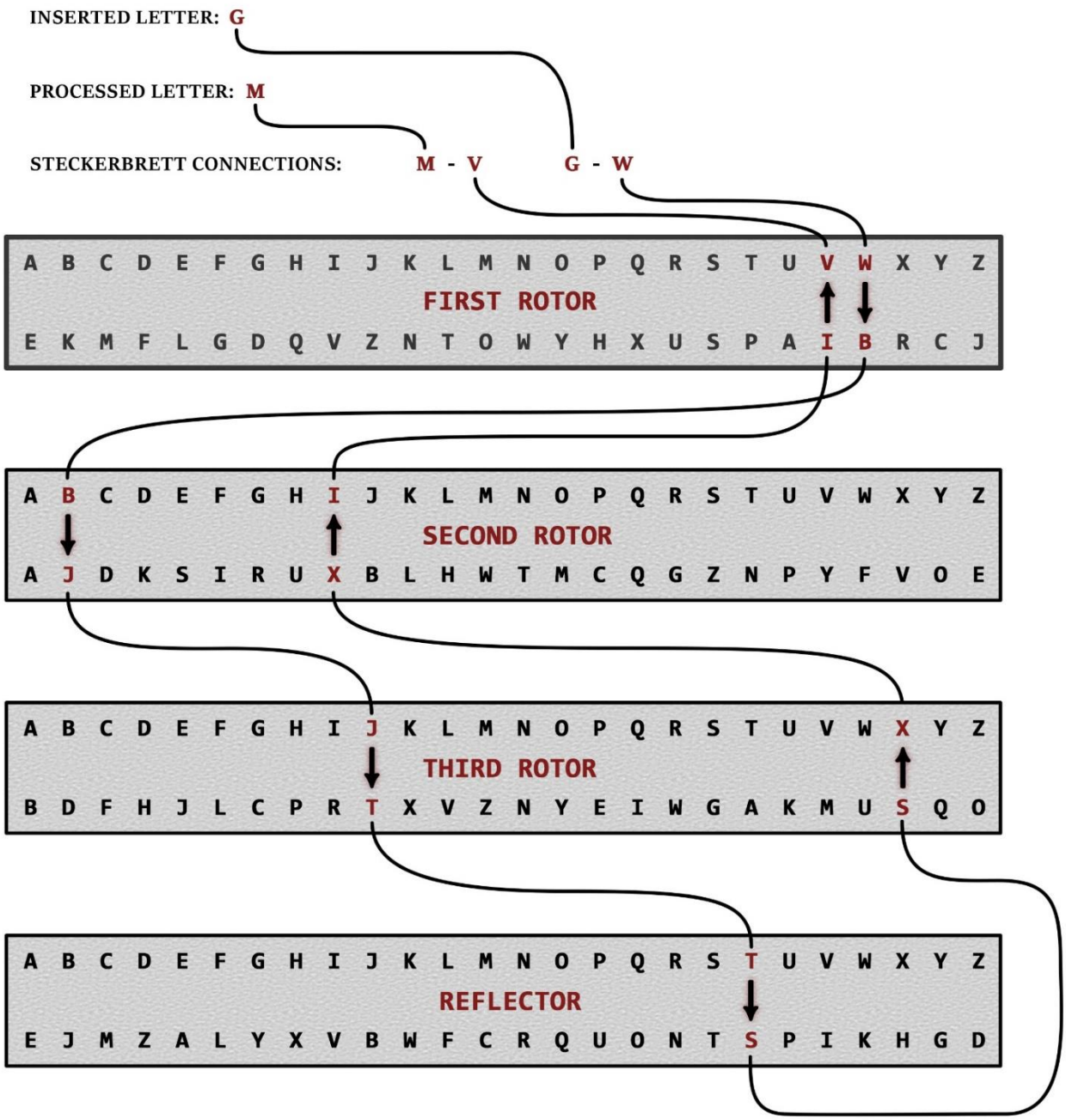
iii. Reflectors

There are three available reflectors **A, B, C.** Each of them change letter in a unique way.

II. Below is a representation of the algorithm ciphering inserted letter.

Settings of the simulator during this encryption are:

- alpha = 1
- beta = 1
- gamma = 1
- Steckerbrett = MV,GW
- Relfector = A



III. Mathematical analysis

How many configurations are possible with an Enigma machine with these specifications?

$$\Lambda = SBM$$

$S -$ *is a permutation describing the steckerbrett transformation*
$B -$ *is a permutation describing the reflector transformation*
$M -$ *is a permutation* describing transformation of the three rotors

Total number of possible settings:

$$\Lambda = \frac{26!}{13! \times 2^{13}} \times 3 \times 26^3 = 416'859'847'599'195'000 =$$

$$= 4.16859847599195 \times 10^{17}$$

More information about Original Enigma Machine can be found on these websites:

- https://www.cryptomuseum.com/crypto/enigma
- https://en.wikipedia.org/wiki/Enigma_machine

This documents describes project: https://gitlab-stud.elka.pw.edu.pl/pbedkows/enigma-simulator