SSN Lab 2 - Enigma

Lab Author: *Ahmed SalahEldin Elkashef*
Teammate: *Botir*

- ## 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.

For this sentence, It will be:

“It is so beautiful to think beforehand of my birthday present. I think for my birthday, I would like to have a new mobile phone.”

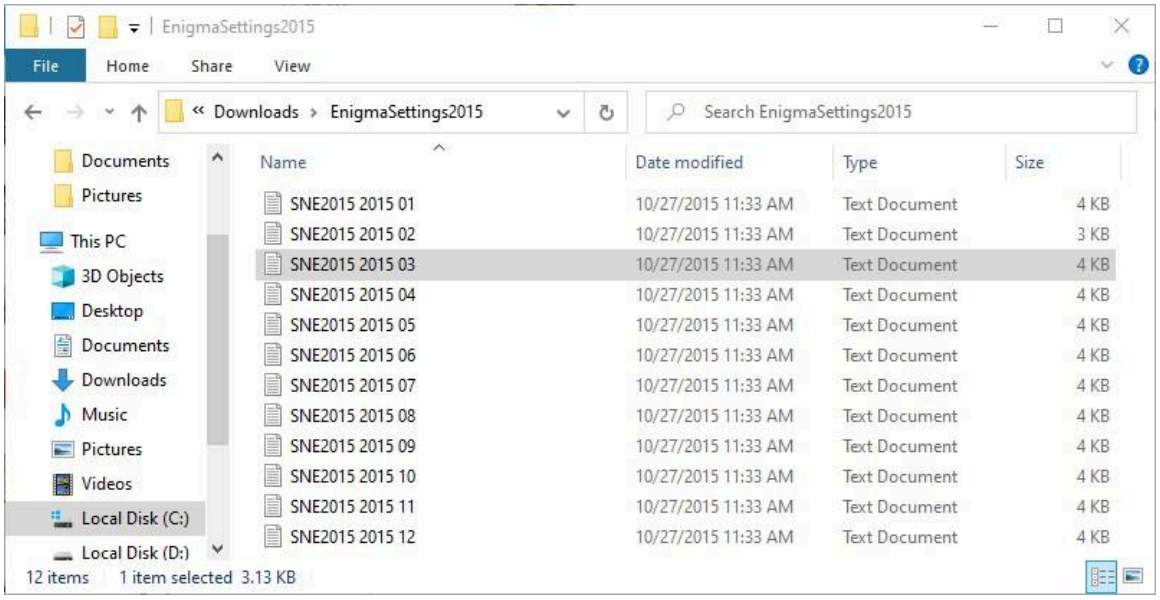
25 words.

There are many different Enigma versions available:
- Enigma with 3 rotors
- Enigma with 3 rotors + reflector
- Enigma with 4 rotors

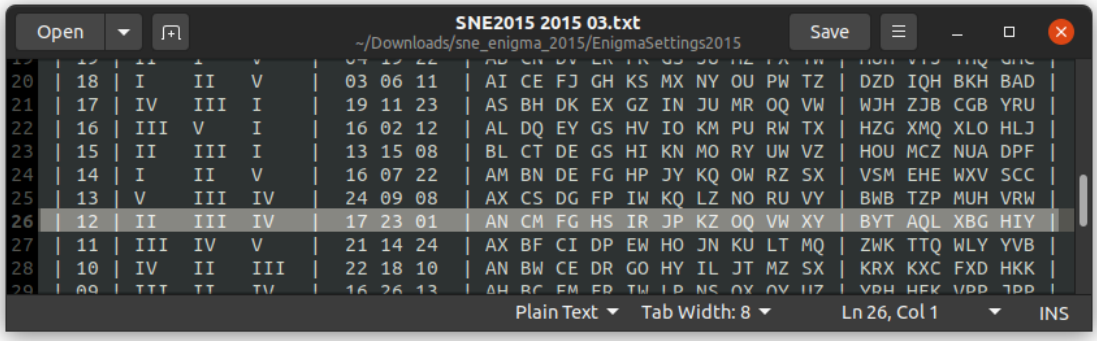
There are much more, but the same principles apply.
Another point is that the algorithm (which in this case is the enigma machine itself) can be exposed to the public, but the key should be kept secret. The key in the case of enigma is the setup that was used in order to encrypt the message in the first place, that key contains:
- Which rotors will be used
- The ordering of the rotors
- The starting orientation of each rotor
- When a rotor will nudge to the next one
- Which reflector will be used
- The plugboard settings

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.

The link was forbidden. Therefore, I used the other link.



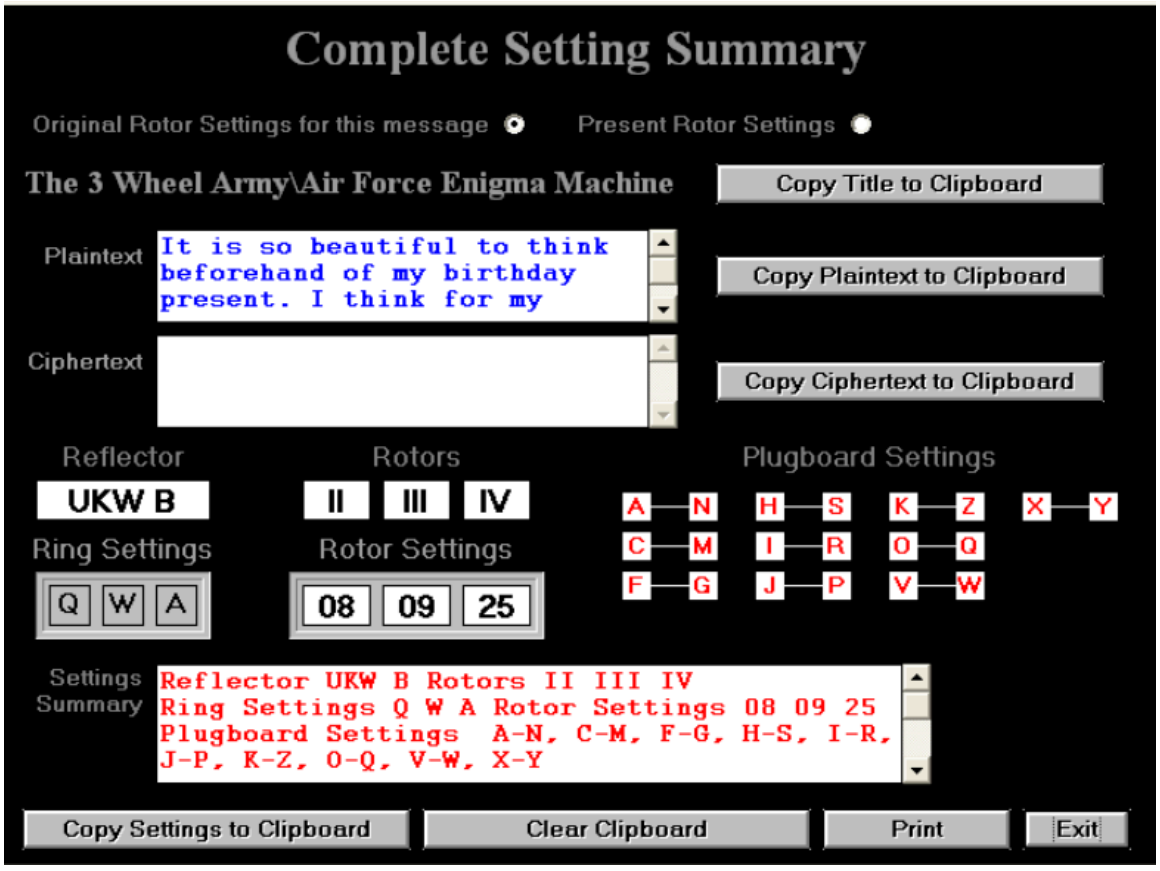
As prescribed in the task, I should look for that key in the file downloaded and look up my birthday, which is 12th of March:

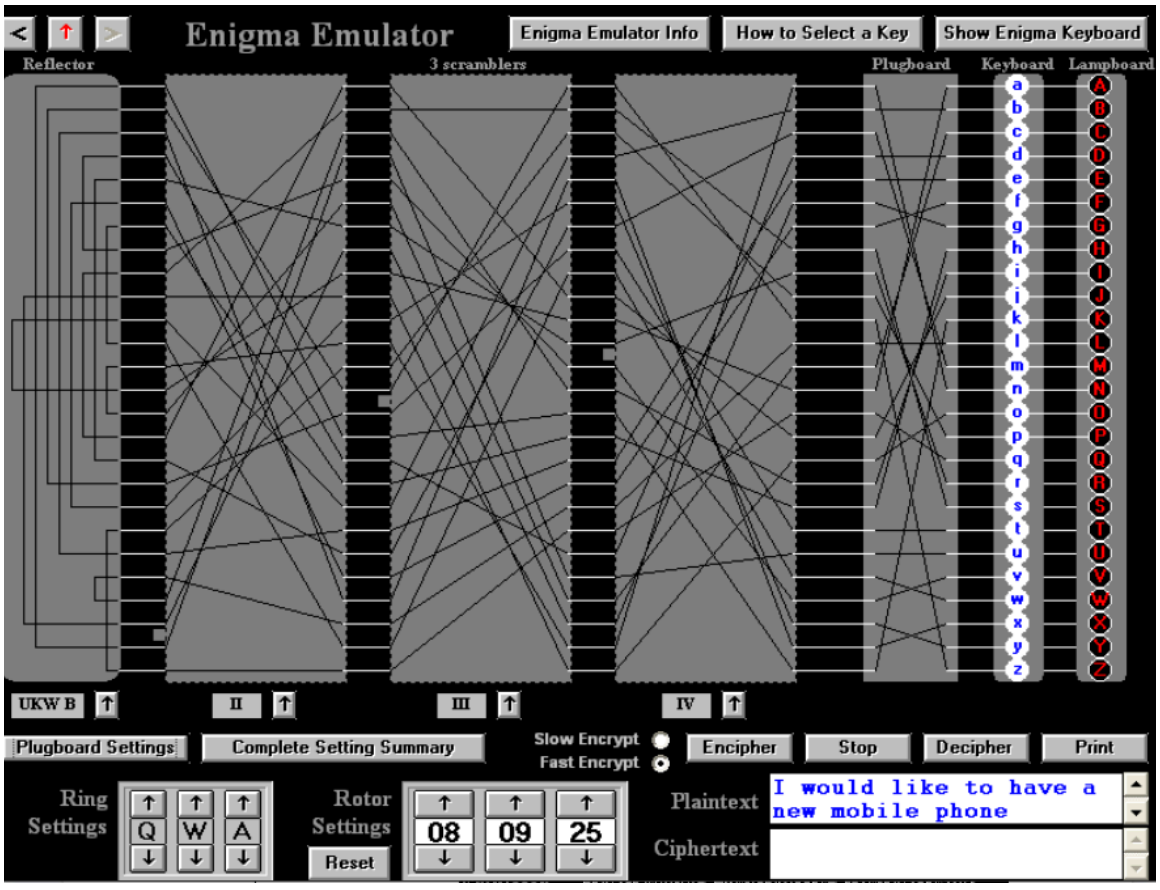


So the exact key which will be used:

Day	**Rotor Order**	**Ring Setting**	**Plugboard**	**Date discriminant**
12	II III IV	17 23 01	AN CM FG HS IR JP KZ OQ VW XY	BYT AQL XBG HIY

Then we move to the Enigma simulator that is installed on the virtualbox image and do the complete settings according to the key:


Complete Setting Summary
Original Rotor Settings for this message
Present Rotor Settings
The 3 Wheel Army\Air Force Enigma Machine
Copy Title to Clipboard
Plaintext
It is so beautiful to think beforehand of my birthday present. I think for my
Copy Plaintext to Clipboard
Ciphertext
Copy Ciphertext to Clipboard
Reflector
UKW B
Rotors
II III IV
Plugboard Settings
A N H S K Z X Y
C M I R O Q
F G J P V W
Ring Settings
Q W A
Rotor Settings
08 09 25
Settings Summary
Reflector UKW B Rotors II III IV
Ring Settings Q W A Rotor Settings 08 09 25
Plugboard Settings A-N, C-M, F-G, H-S, I-R, J-P, K-Z, O-Q, V-W, X-Y
Copy Settings to Clipboard
Clear Clipboard
Print
Exit


Enigma Emulator
Enigma Emulator Info
How to Select a Key
Show Enigma Keyboard
Reflector
3 scramblers
Plugboard
Keyboard
Lampboard
UKW B
II
III
IV
Plugboard Settings
Complete Setting Summary
Slow Encrypt
Fast Encrypt
Encipher
Stop
Decipher
Print
Ring Settings
Q W A
Rotor Settings
Reset
08 09 25
Plaintext
I would like to have a new mobile phone
Ciphertext

The enciphered message is:

“LJBCR NXTGZ XVOHK QUFQW COPSN WSRNI QFGKR RAAWS EUWIX MSZKT IDXJJ RWVMD ETAZU SATYF CZJSQ VTDBX INCFN TZXQF FJXMC SOOQW T”

Now, I sent my partner the non-secret information:

SSN Lab 2 Useful information about WW2

Ahmed Salaheldin Farouk Ahmed Elkashef
Today, 1:49 PM
BOTIRJON SHOKAMOLOV; Nikita Ulianov; Kirill Saltanov

Reply all

Hello Botir, March 12th, LJBCR NXTGZ XVOHK QUFQW COPSN WSRNI QFGKR RAAWS EUWIX MSZKT IDXJJ RWVMD ETAZU SATYF CZJSQ VTDBX INCFN TZXQF FJXMC SOOQW T

Look at the fourth window.

•••

And I get the other email from my partner:

BOTIRJON SHOKAMOLOV
Today, 1:18 PM

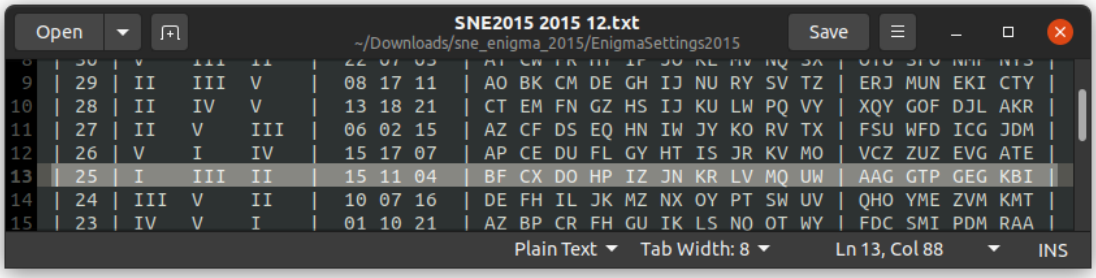
Second Message

December 25, Three Quarters,
EHFCN YVBSU BHNEL LKNSH TEOMI SDSCA QDSAH GYNKF VADBZ CGRVD QVJZA JNHQI HYLWL ZKZOH UQZAL KPEPP YNT

•••

Encrypted message:
EHFCN YVBSU BHNEL LKNSH TEOMI SDSCA QDSAH GYNKF VADBZ CGRVD QVJZA JNHQI HYLWL ZKZOH UQZAL KPEPP YNT

We lookup the date: 25th December



Day	Rotor Order	Ring Setting	Plugboard	Date discriminant
25	I III II	15 11 04	BF CX DO HP IZ JN KR LV MQ UW	AAG GTP GEG KBI

Then adjust the settings accordingly
Rotor Order -> I III II
Ring Setting -> 15 11 04 or OKD
Plugboard -> BF CX DO HP IZ JN KR LV MQ UW
Date discriminant -> three quarters, so it's GEG, or 07 05 07

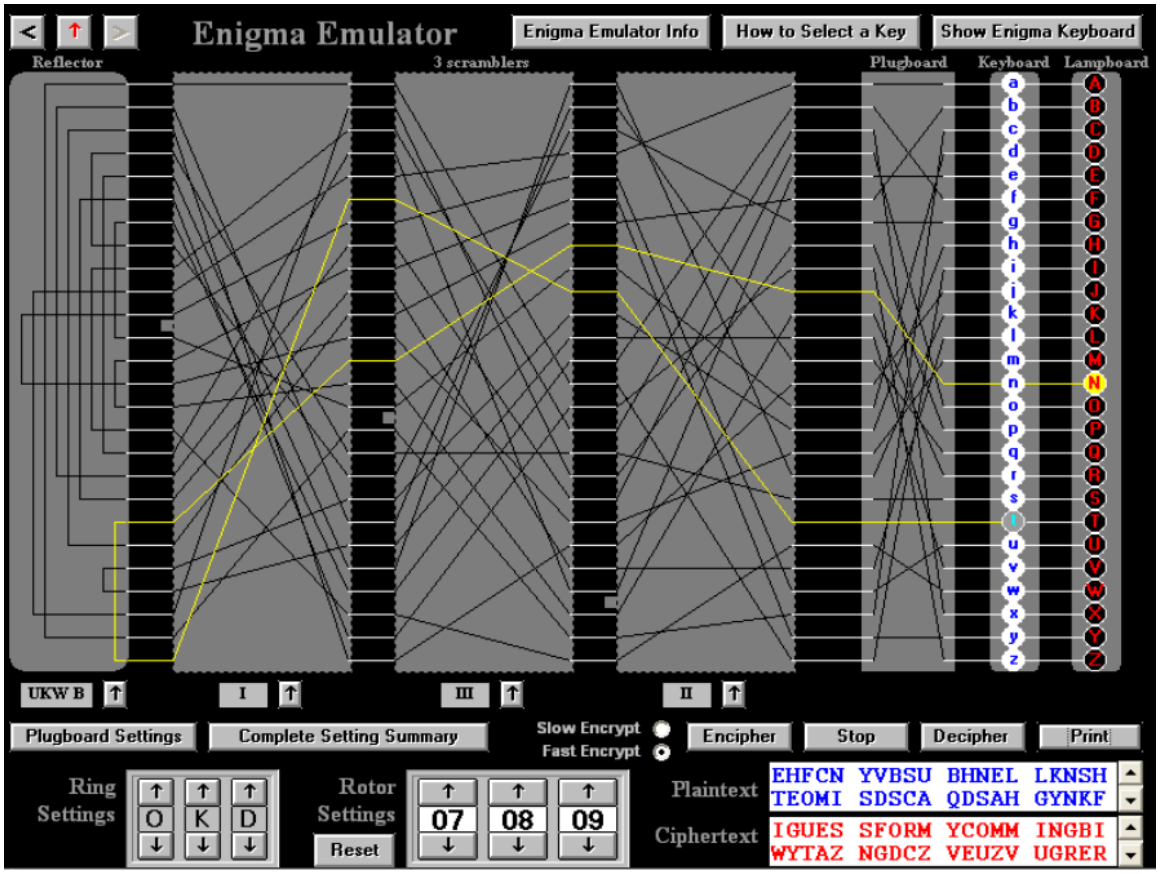
We translate characters to numbers based on their alphabetical order:

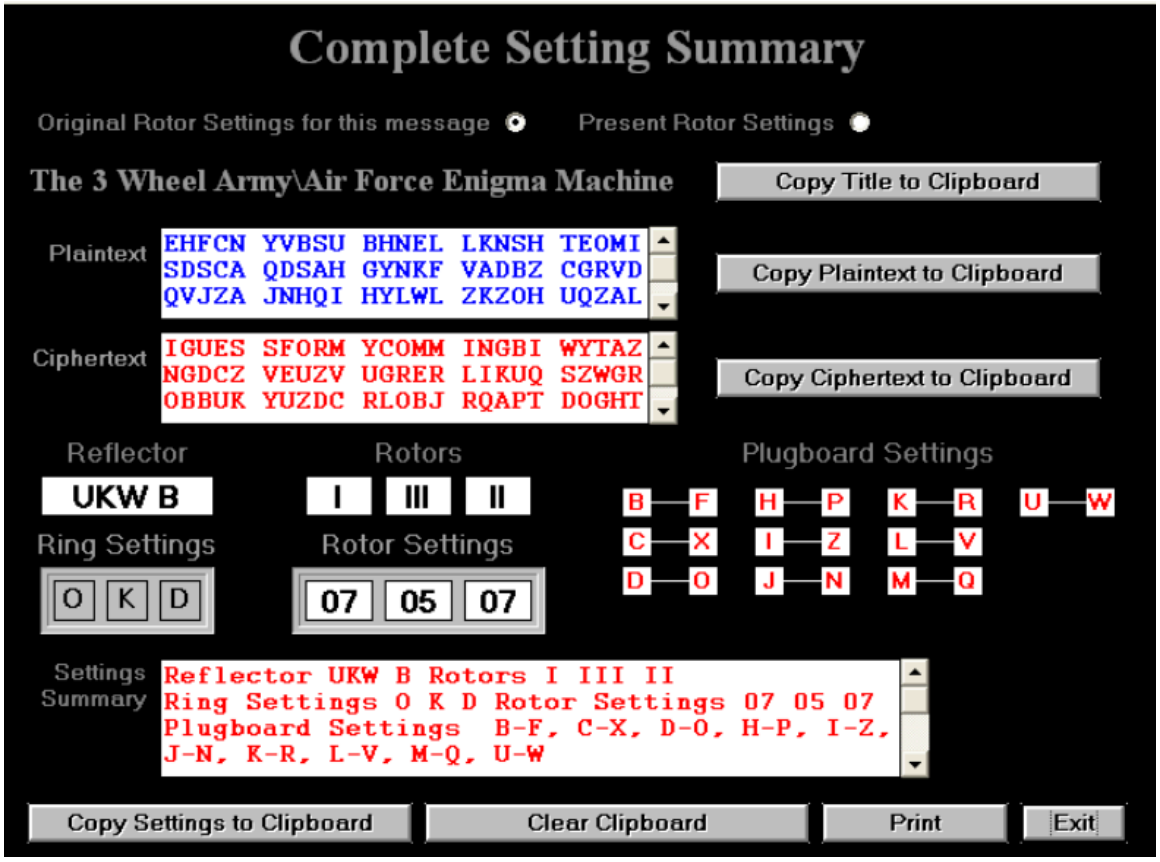
Number Substitution Cypher

A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	10

K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20

U	V	W	X	Y	Z
21	22	23	24	25	26





And the deciphering is done

The final text is
IGUES SFORM YCOMM INGBI RTHDA YIWAN TANEW LAPTO PSINC EMINE ISPRE TTYOL DTOPE RFORM INTEN DEDTA SKS

We compare it to the encrypted text to fix the spacing:
I GUESS FOR MY COMING BIRTHDAY I WANT A NEW LAPTOP SINCE MINE IS PRETTY OLD TO PERFORM INTENDED TASKS

Note: After a discussion with another classmate, I found that I made the same mistake that was done by the Germans in the World War, which is not using a secure communication of the "password" or using a Ring Setting as an AAA.

As a result, Here is the real process as done in real-life situations

The new process involves the sending of a sentence that hints to a 3 letter combination, which should be sent via Morse code, and then that code gets decrypted, and the resulting combination will be used for the rotor starting position, and hence do the decryption of the original message.
Example: Password to be decrypted first (ITA)
Decrypted password (ITA) -> (TRU)
Use (TRU) as the Ring setting and decrypt the message.

In this lab and for simplicity, that process was not done.

- **2 Viola**

2 Viola specs:

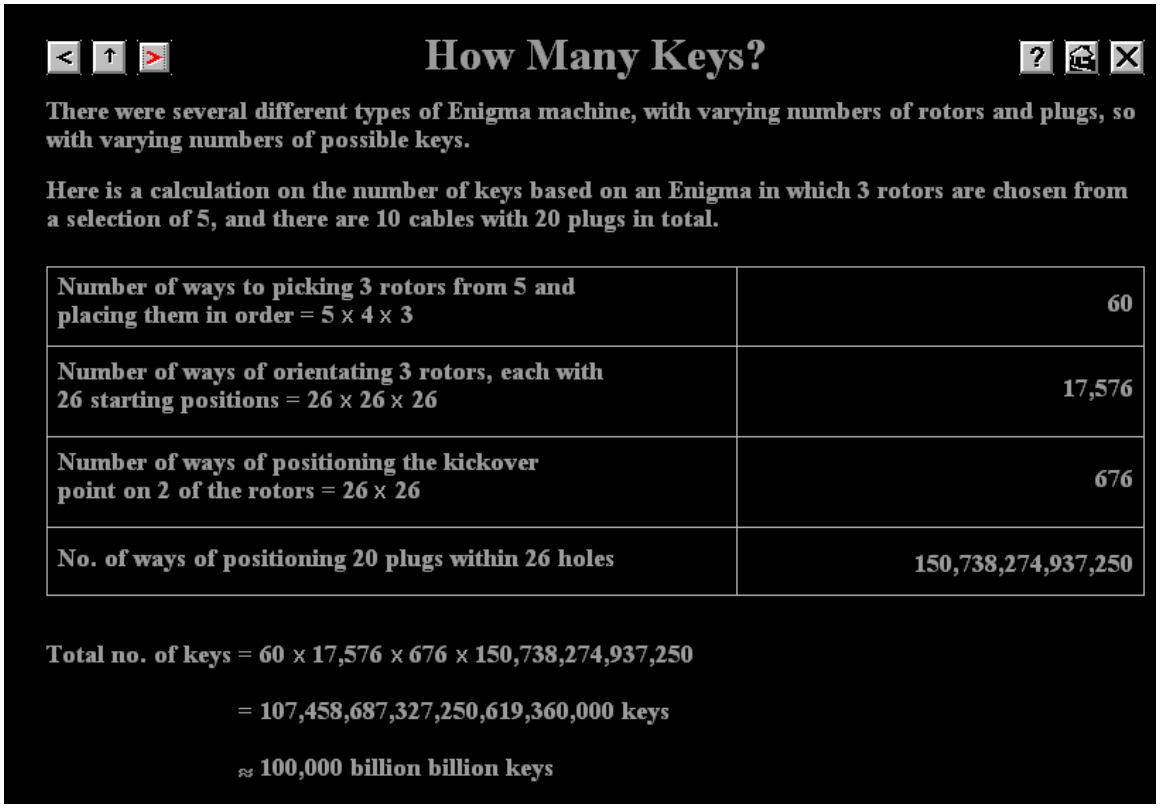
- The Viola machine can fit 1 static reflector and 10 rotors each with 30 characters.
- There are 5 unique reflectors to select from.
- There are 50 unique (under all rotations) rotors to select from.
- The machine has a standard plugboard for all 30 characters.
- It is unknown how many plugboard cables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

Enigma specs:

- 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.

How does the number of keys compare?

From the CD-ROM, we see the calculation:



How Many Keys?

There were several different types of Enigma machine, with varying numbers of rotors and plugs, so with varying numbers of possible keys.

Here is a calculation on the number of keys based on an Enigma in which 3 rotors are chosen from a selection of 5, and there are 10 cables with 20 plugs in total.

Number of ways to picking 3 rotors from 5 and placing them in order = 5 x 4 x 3	60
Number of ways of orientating 3 rotors, each with 26 starting positions = 26 x 26 x 26	17,576
Number of ways of positioning the kickover point on 2 of the rotors = 26 x 26	676
No. of ways of positioning 20 plugs within 26 holes	150,738,274,937,250

Total no. of keys = 60 x 17,576 x 676 x 150,738,274,937,250

= 107,458,687,327,250,619,360,000 keys

≈ 100,000 billion billion keys

Calculation for a typical enigma machine:

Number of ways to picking 3 rotors from 5 and placing them in order: 5x4x3 = 60
Number of ways of orienting 3 rotors, each with 26 starting position: 26x26x26 = 17,576
Number of ways of positioning the kickover point on 2 of the rotors = 26x26 = 676
Number of ways of positioning 20 plugs within 26 holes:

$$\frac{26!}{(26-20)! \times 2^{10} \times 10!} = 150{,}738{,}274{,}937{,}250$$

Total number of keys = 60 x 17,576 x 676 x 150,738,274,937,250
= 107,458,687,327,250,619,360,000 keys
= 100,000 billion billion keys

Calculation for a 2 viola machine:

Number of ways to picking 10 rotors from 50 and placing them in order:

$\frac{50!}{(50-10)!}$= 37276043023296000 or $3.7276043023296 \times 10^{16}$

Number of ways of orienting 10 rotors, each with 30 starting position:$30^{10} = 5.9049 \times 10^{14}$

Number of ways of positioning the kickover point on 9 of the rotors = $30^{9} = 1.9683 \times 10^{13}$

Number of ways of positioning 20 plugs within 30 holes (also assuming 10 plug cables):

$$\frac{30!}{(30-20)! \times 2^{10} \times 10!} = 1.96713449 \times 10^{16} \; or \; 19,671,344,900,000,000$$

Total number of keys = $3.7276043023296 \times 10^{16}$ x 5.9049×10^{14} x 1.9683×10^{13} x $1.96713449 \times 10^{16}$

= $8.522513483 \times 10^{60}$

or 8, 522, 513, 483, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000 keys

Comment:

With just increasing the number of picked rotors from 3 to 10, and choosing from 50 instead of 5, even after using the same number of plug cables 10 plug cables) and finally increasing the number of possible characters from 26 to 30, the number of possible keys has increased into a huge number in an exponential manner.

References:

1. https://www.desmos.com/scientific
2. https://crypto.stackexchange.com/questions/33628/how-many-possible-enigma-machine-settings/33631#33631

3. https://en.wikipedia.org/wiki/Enigma_machine