The Enigma Machine

Sending secret, “uncrackable” messages in World War II

Imagine you're Britain in 1937…

You need a way to communicate with your armies

You can use a telegraph to send Morse code over the radio, but the enemy can intercept your messages

You need a way to **encrypt** your messages so that only your armies and your allies will understand

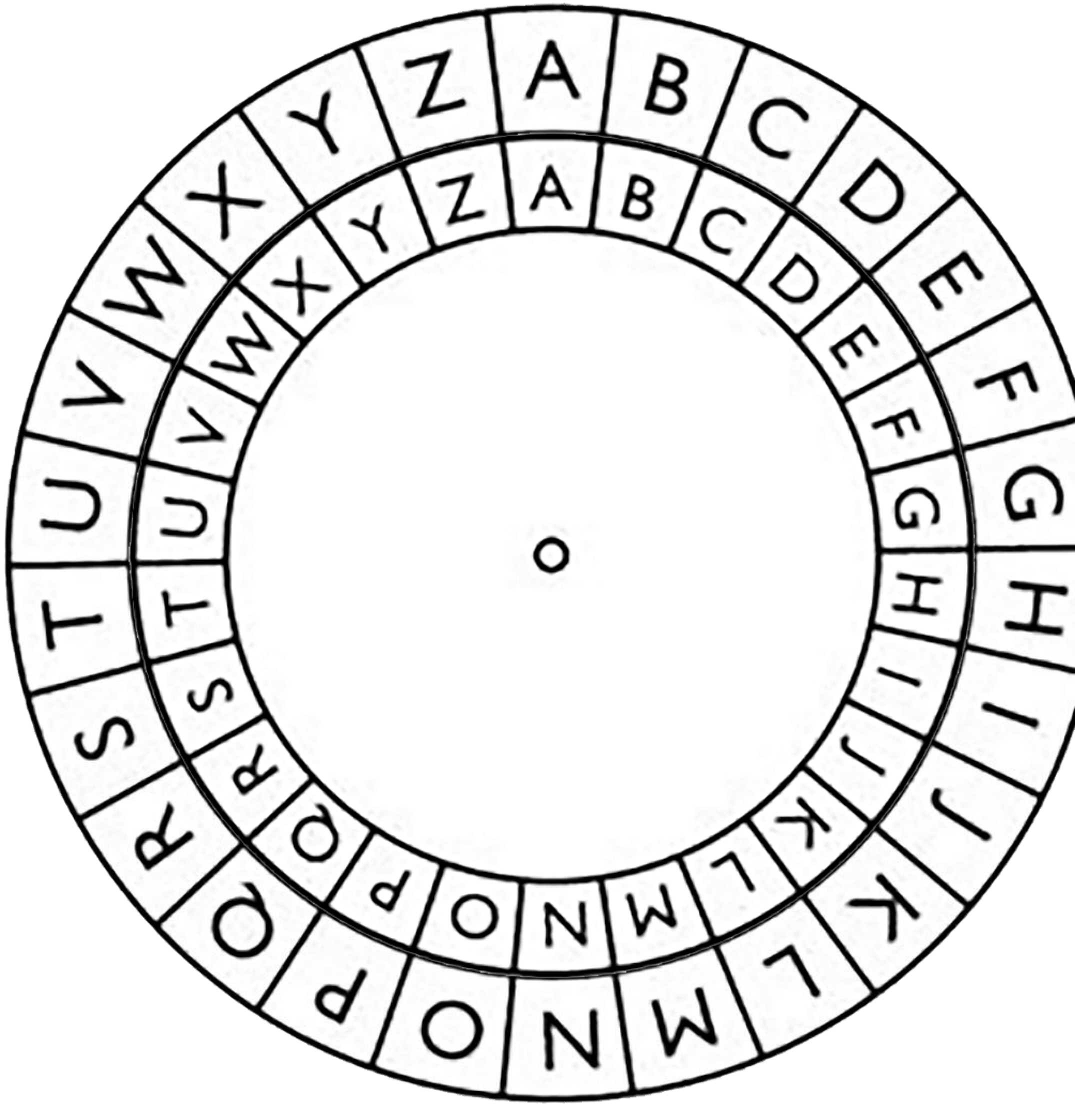
Enter… cryptography!

Some quick vocab

- **Cryptography** – the science of encrypting and decrypting messages into cipher text
- **Encryption** – converting plain text into cipher text
- **Decryption** – converting cipher text into plain text
- **Plain text** – the original message that you can ready normally
- **Cipher text** – the secret message that you cannot read normally
- **Key** – the algorithm or settings used to encrypt and decrypt

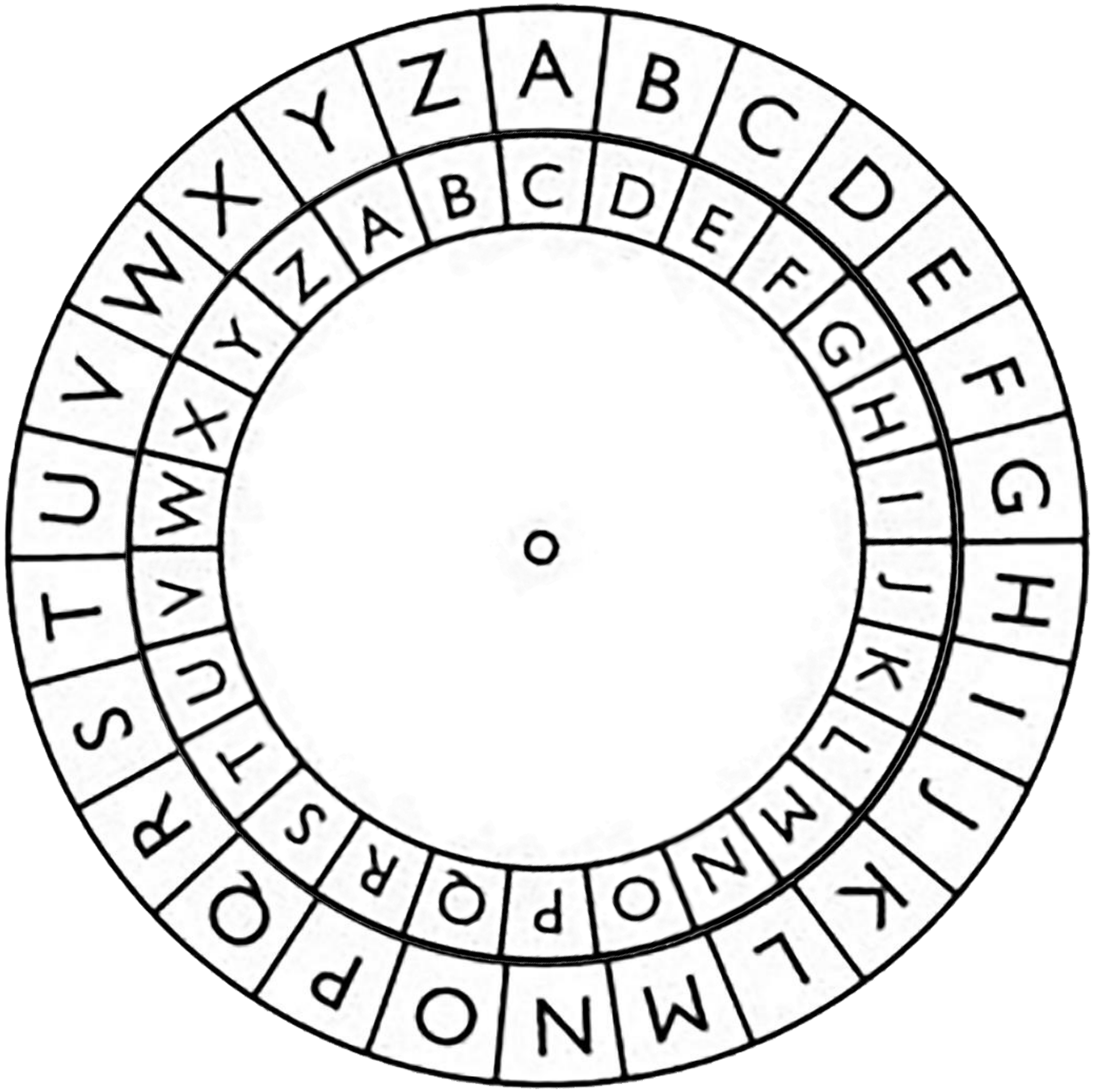
The simplest cipher is a shift cipher

- Each letter maps to a new letter
- The letters stay in order – the key is just a rotation (a shift) of the inner wheel
- For example, if we shift from A on the outer wheel lining up with A on the inner wheel (key = 0) to A on the outer wheel lining up with C on the inner wheel…


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
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

The simplest cipher is a **shift cipher**

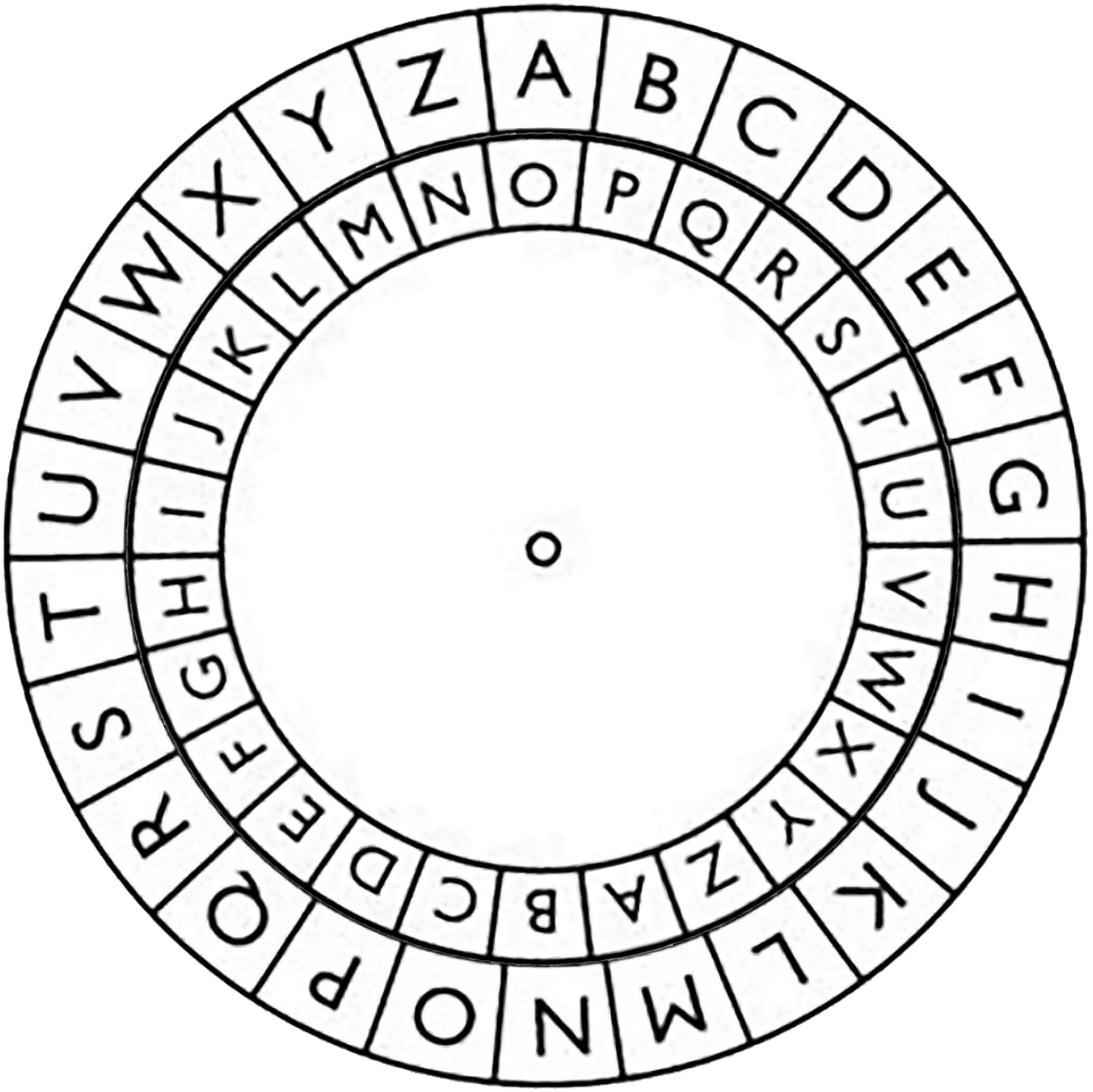
- The key is now 2, since A has been shifted by 2 letters
- If we rotate further, so A is now lined up with O (the fifteenth letter of the alphabet)…



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
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

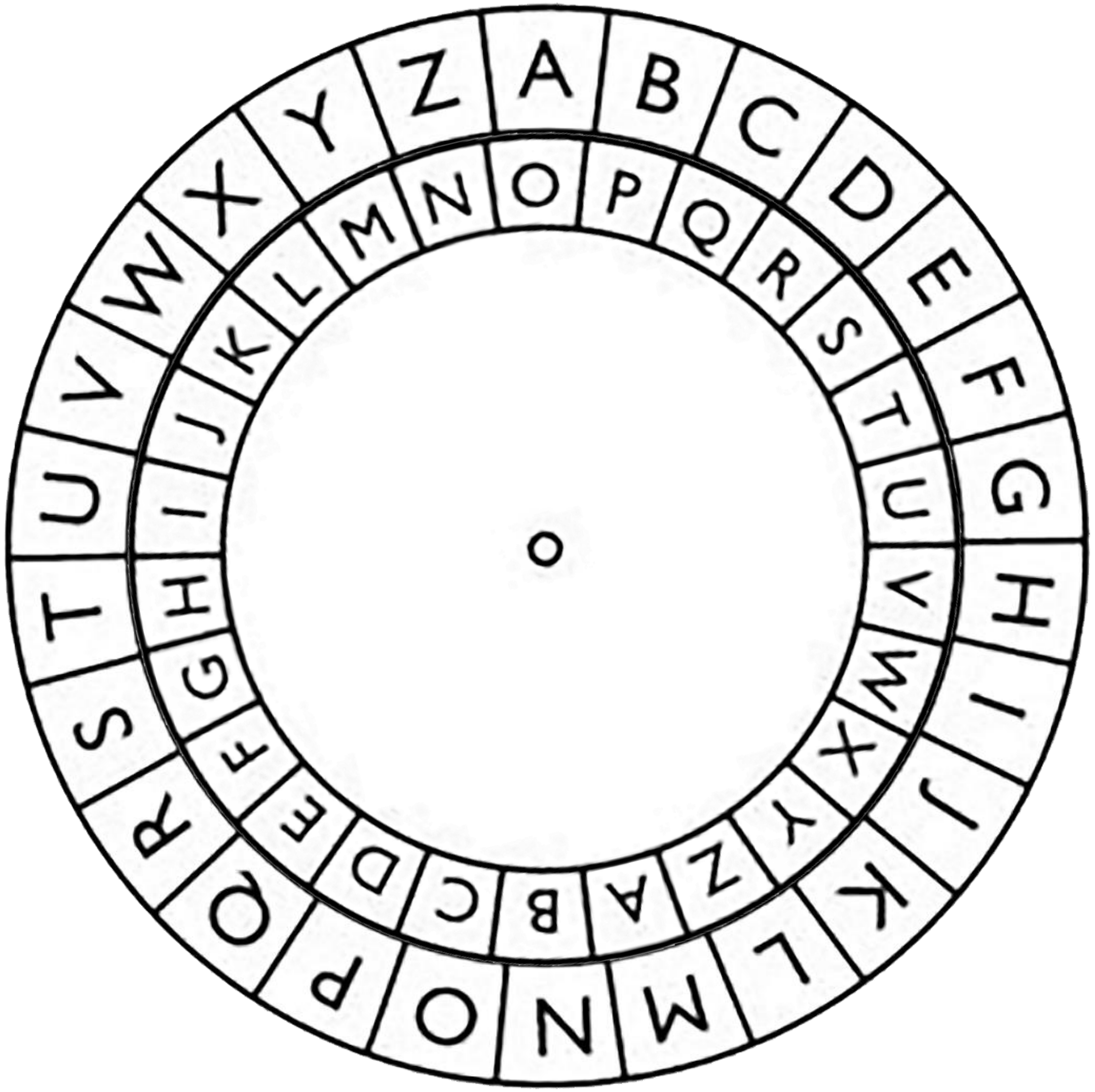
The simplest cipher is a **shift cipher**

- The key is now 15, since A has been shifted by 15 letters
- Now let's encrypt a message. The plain text is "TROOPS TO POLAND"
- T on the outer wheel lines up with H on the inner wheel
- R lines up with F
- O lines up with C…


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
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N

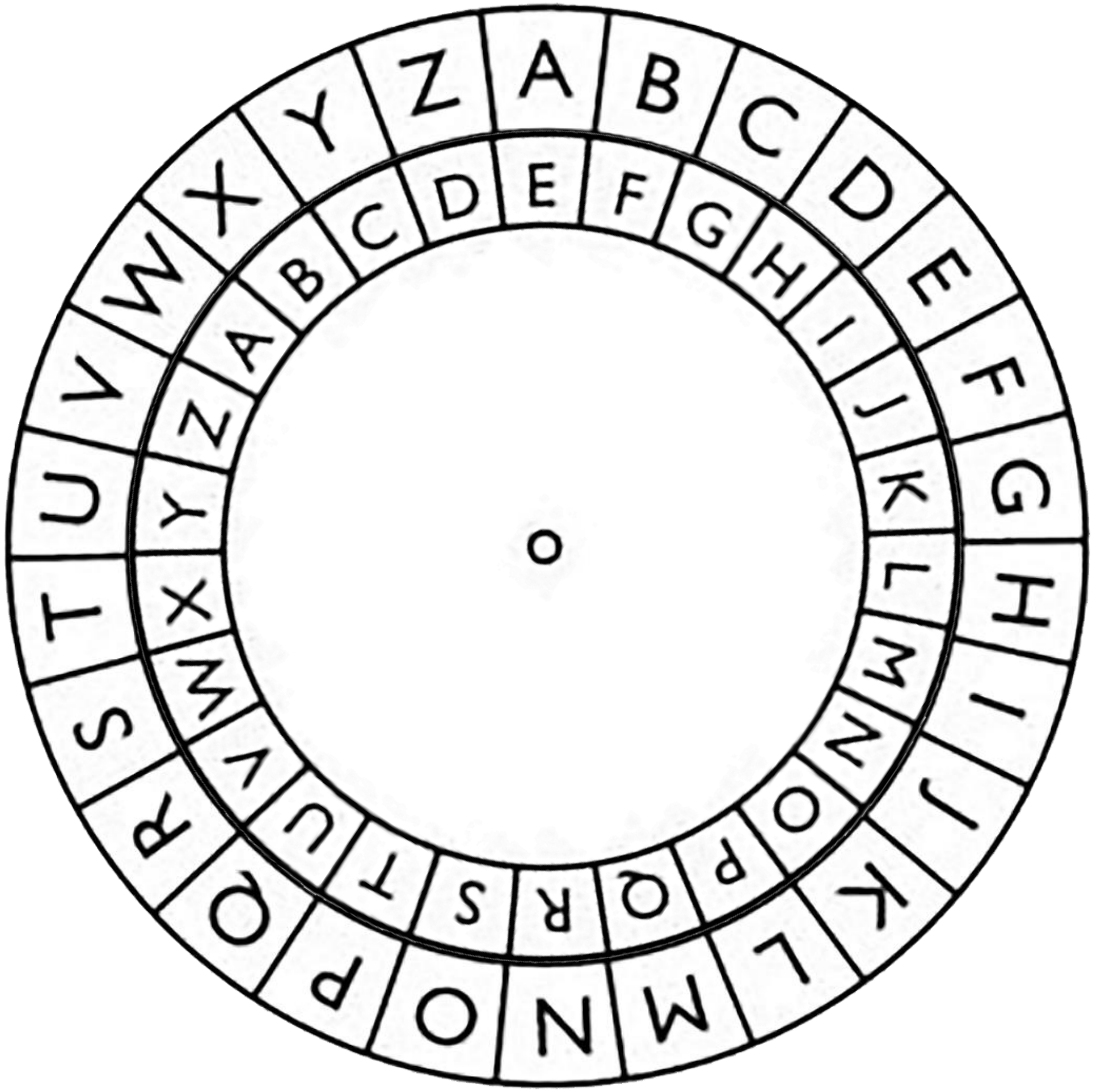
The simplest cipher is a **shift cipher**

- "TROOPS TO POLAND" becomes "HFCCDG HC DCZOBR" with key = 15
- If whoever receives that cipher text has the key, they can decrypt it by finding the letters on the inner wheel
- H on the inner wheel lines up with T
- F lines up with R
- C lines up with O…


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
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N

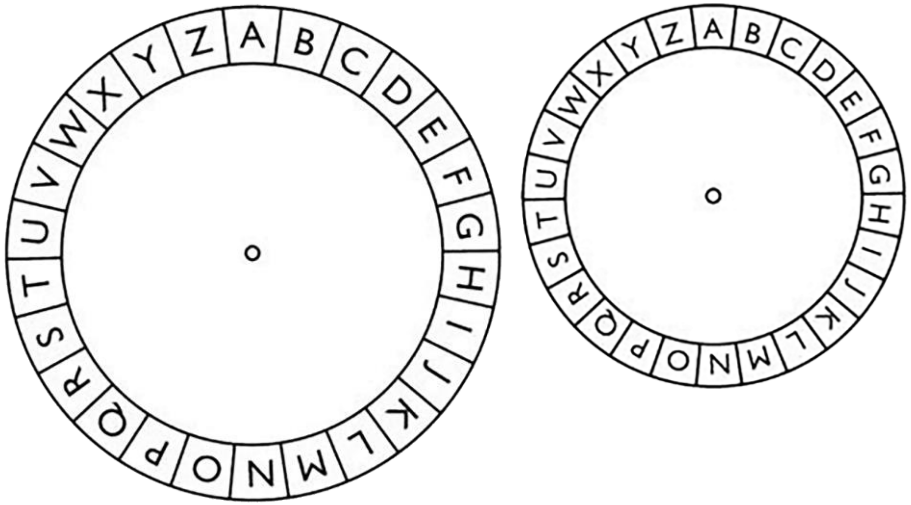
Practice time!

- Decode this message: "CSY KSX MX VMKLX"
- Note that the key is now 5


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
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Now, if you'd like to, you can create your own cipher wheel: If you have a printer, you can print out the PDF saved in the year 6 home learning folder (The Enigma Machine PDF).

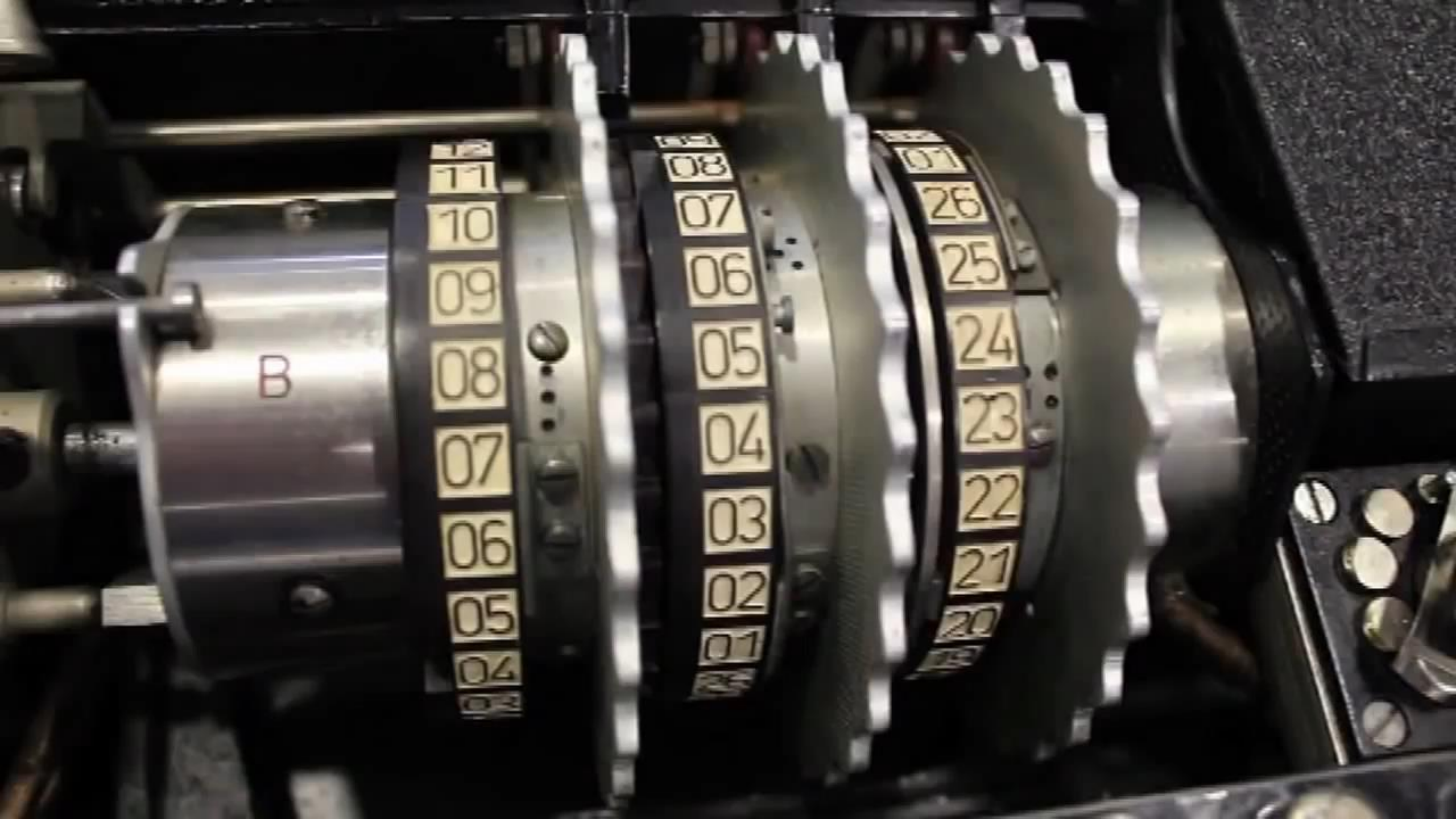
Or you can try and draw and measure it out (maybe try tracing it from the screen?!)


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
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

- Cut out the outer and inner wheels and connect them with a fastener
- Create a secret message and pass the cipher text and key to a partner – make sure your message is **school appropriate**
- Decode your partner's secret message using your own cipher wheel

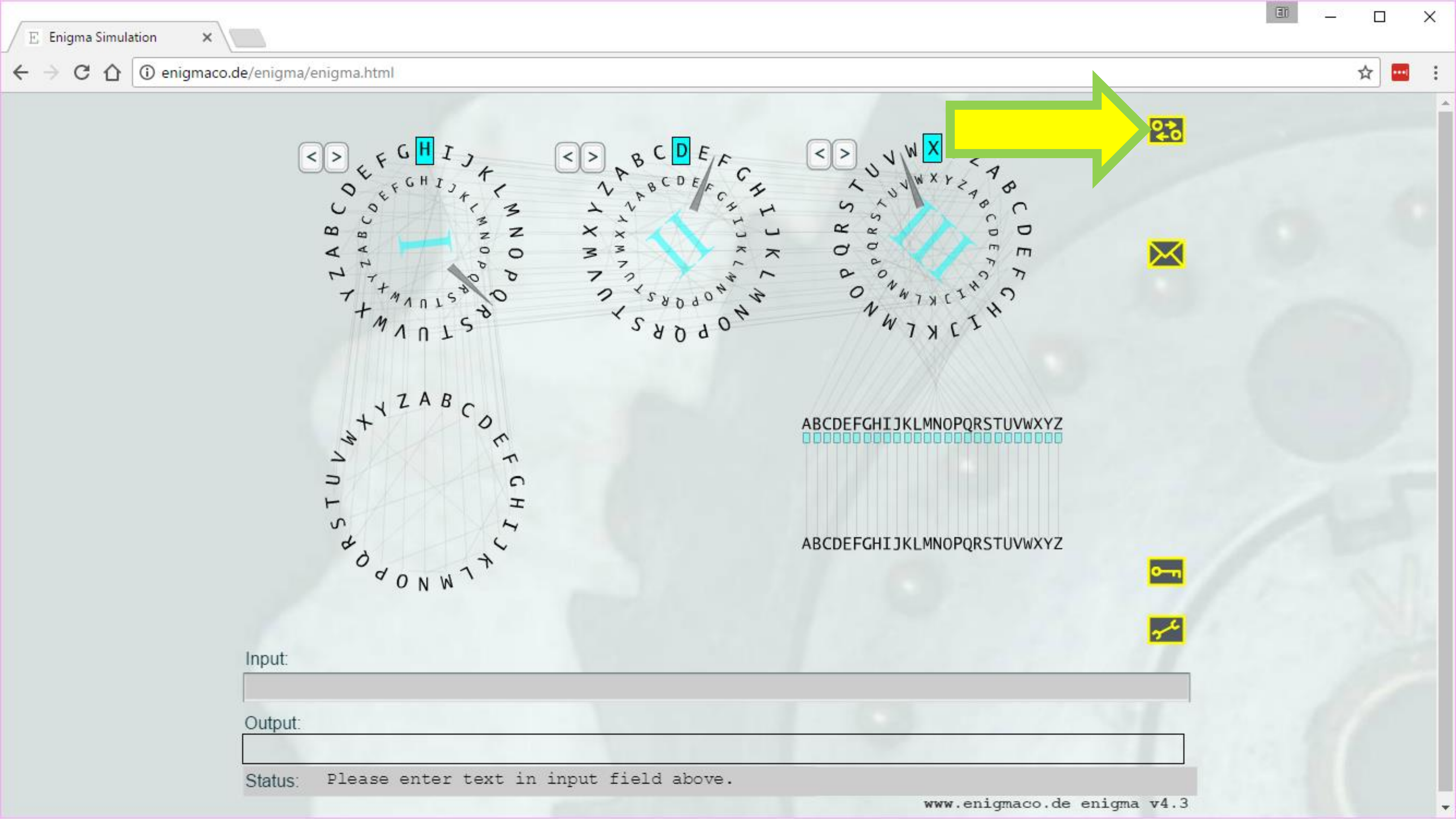
The shift cipher is **not very strong**

- How many possible keys are there?
- How long do you think it would take to crack the algorithm, even if you didn't know the key?
- How could the cipher be strengthened?


B
12
11
10
09
08
07
06
05
04
08
07
06
05
04
03
02
01
01
26
25
24
23
22
21
20

158,962,555,217,826,360,000

- That’s how many different keys there are for the Enigma Machine
- Even if you cracked it in a day, the key would already have changed
- Compared to the 26 keys of the shift cipher, this certainly seems nearly uncrackable

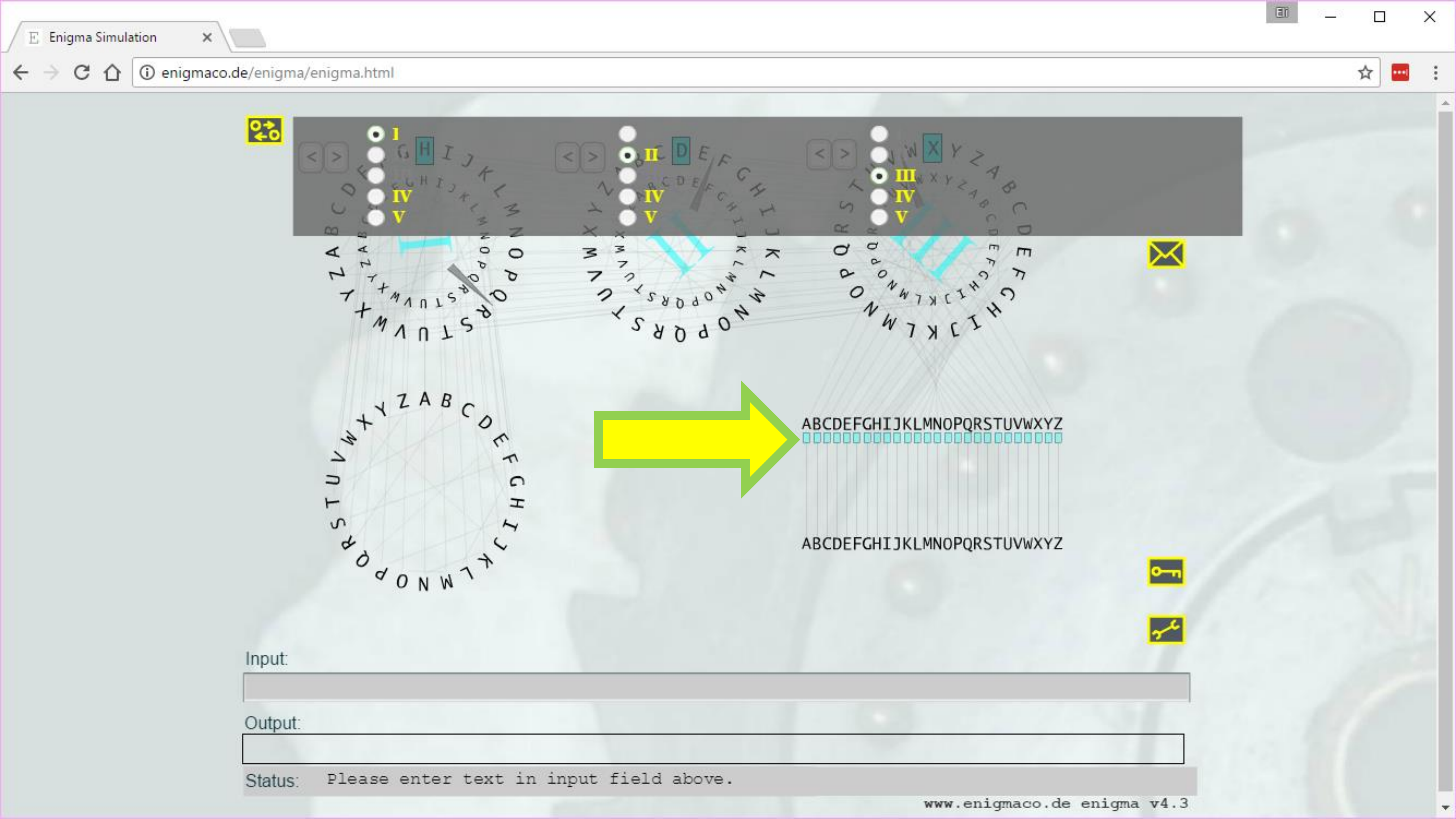

Enigma Simulation
enigmaco.de/enigma/enigma.html
< >
H
D
X
I
II
III
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Input:

Output:

Status: Please enter text in input field above.

www.enigmaco.de enigma v4.3



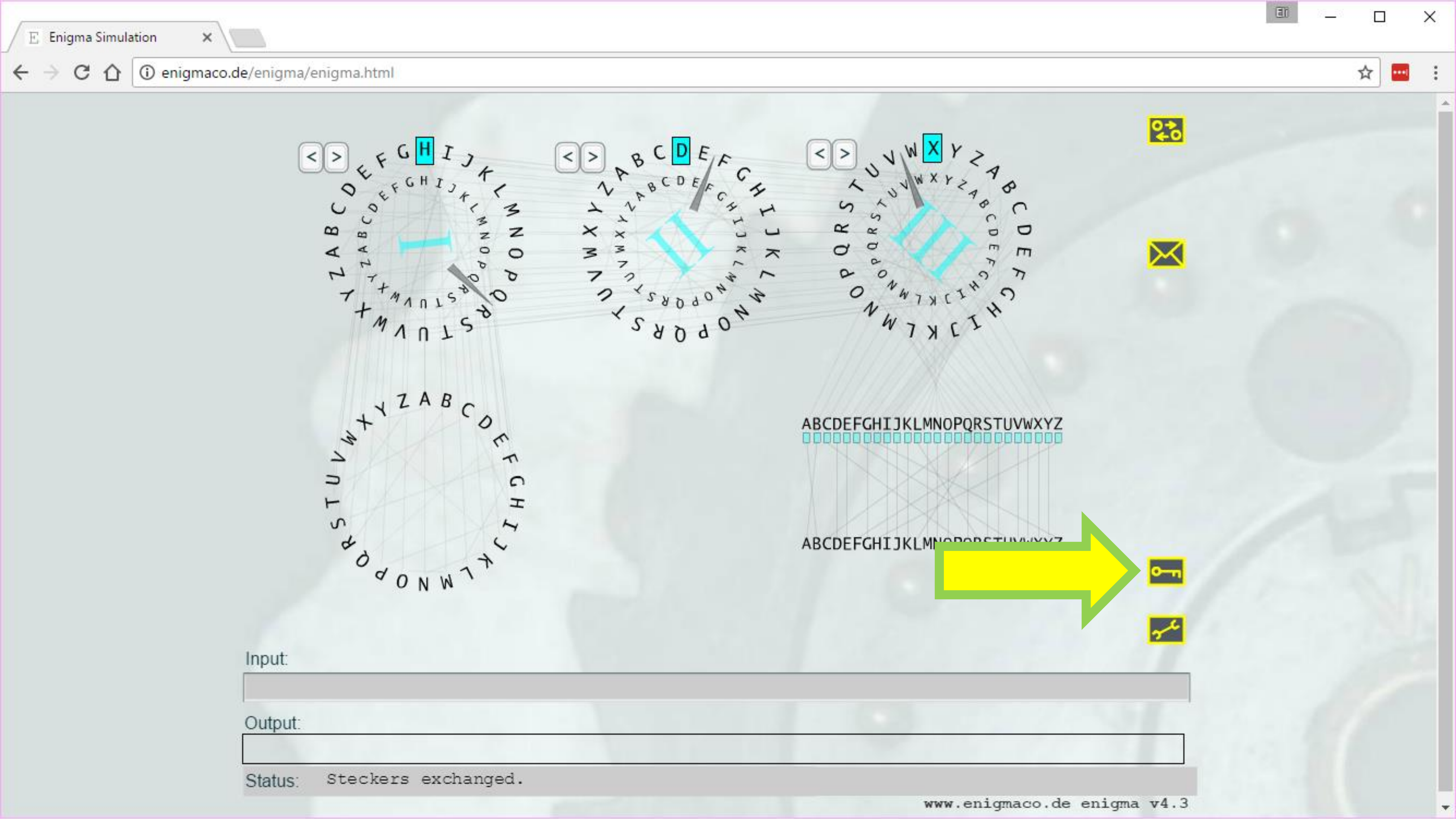
Enigma Simulation
enigmaco.de/enigma/enigma.html
● I
○ IV
○ V
● II
○ IV
○ V
● III
○ IV
○ V
H
D
X
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Input:

Output:

Status: Please enter text in input field above.

www.enigmaco.de enigma v4.3



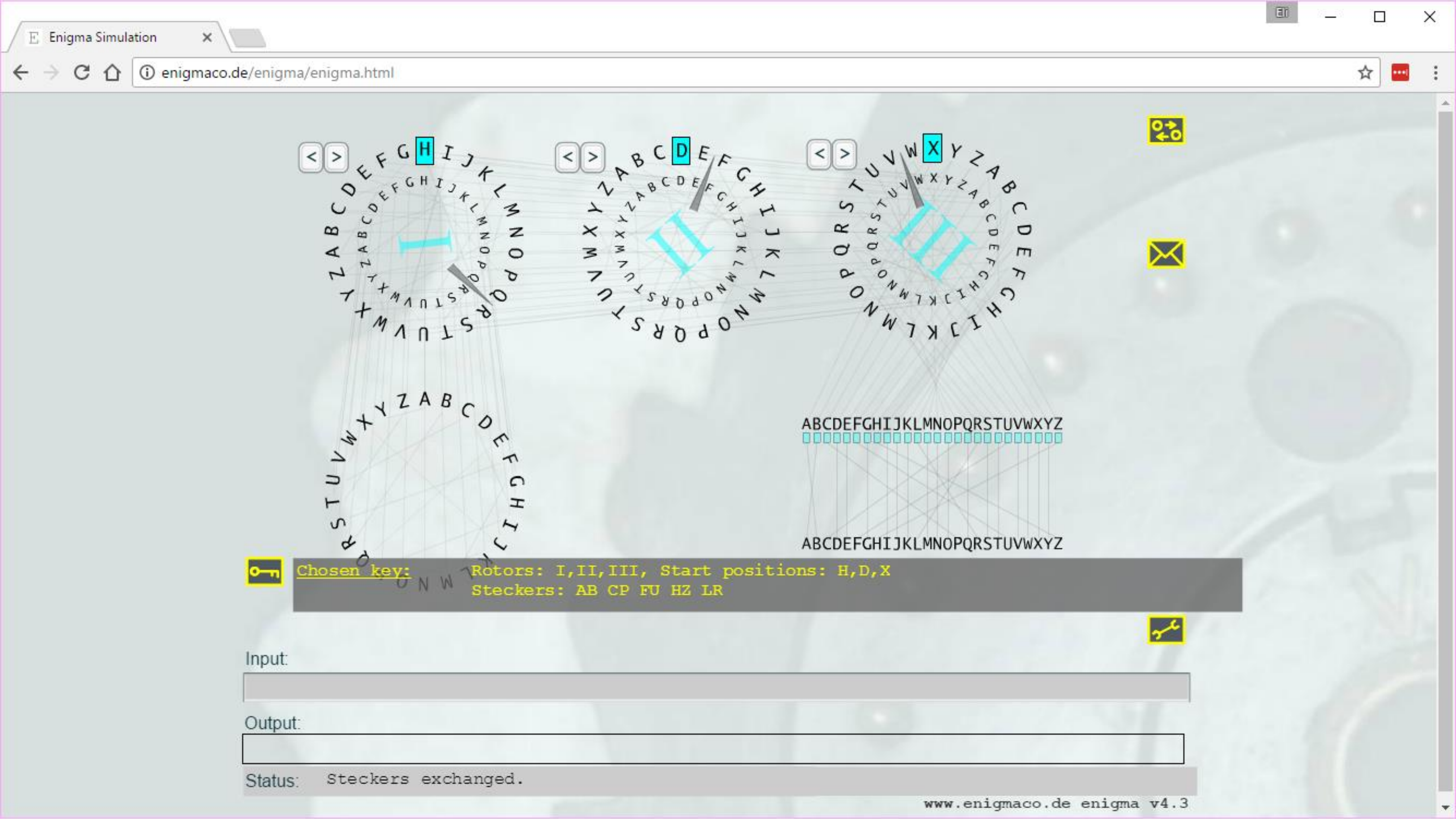
Enigma Simulation
enigmaco.de/enigma/enigma.html
H
D
X
I
II
III
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Input:

Output:

Status: Steckers exchanged.

www.enigmaco.de enigma v4.3


Enigma Simulation
enigmaco.de/enigma/enigma.html
I
II
III
H
D
X
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Chosen key: Rotors: I,II,III, Start positions: H,D,X
Steckers: AB CP FU HZ LR

Input:

Output:

Status: Steckers exchanged.

www.enigmaco.de enigma v4.3

Optional extra: Try out the Enigma machine!

- If you have Flash player, you can go to: enigmaco.de
- Create a secret message and pass the cipher text and complete key someone at home or a friend – make sure your message is **school appropriate**
- Work with someone else in year 6 and decode your each other's secret message using your own cipher machine