Cryptography Stack Exchange is a question and answer site for software developers, mathematicians and others interested in cryptography. It only takes a minute to sign up.

Sign up to join this community

Anybody can ask a question
Anybody can answer
The best answers are voted up and rise to the top

CRYPTOGRAPHY

How does the ring settings of enigma change wiring tables?

Asked 5 years, 1 month ago Active 1 year, 4 months ago Viewed 6k times

Ask Question

7

EDIT: The model I'm trying to make is "Enigma 1". I learned initially about it from a book called "Code Book" and then looked at it in detail from its wikipedia page. The site wont allow me too add more links but google "enigma rotor details" and see the wikipedia page

There is a similarly worded question here but it doesn't answer mine.

I am trying to make an enigma simulator. I have finished doing everything except the ring settings. How do they affect the substitutions?

For example suppose the initial rotor settings are:

```
abcdefghijklmnopqrstuvwxyz
ekmflgdqvzntowyhxuspaibrcj
```

```
abcdefghijklmnopqrstuvwxyz
kmflgdqvzntowyhxuspaibrcje
```

I think all I should have to do is add the ring positions to the rotor positions. But that doesn't seem to be the case. I tried decrypting the first sample message from here that way but didn't succeed. I even tried to make the program run in a loop till it finds the intended answer so I could deduce the relation between ring settings and rotor positions, but it never found it.

But using the same settings on an online enigma simulator worked. Everything seems to be the same except that according to the online simulator, the rotor wirings on a ring setting of b or 2 should be:

```
abcdefghijklmnopqrstuvwxyz
kflngdmrwauqszijytubjcsdk
```

How on earth did it turn into that?

encryption substitution-cipher enigma

share improve this question follow edited Sep 30 '15 at 4:58 asked Sep 22 '15 at 12:48 Olivera Olivera 91 1 1 4 3

I'm working on a physical enigma simulator and I'm as confused as you about what this online simulator shows in it's wiring window. At first I was thinking it's changing around so much because it is coming from the other direction or something but I can't get it to add up. However I did look at page 15 in users.telnet.net/~mmanetti/Enigma/K30Manual.pdf and there it makes things a little clearer on how the ring setting impacts the (de/en)cryption. – Ipassen Dec 18 '15 at 21:14

It should be noted that there's an updated version of the simulator and linked to at: people.physik.hu-berlin.de/~palloks/enigma/index_en.html Also another simulator that shows the wiring (uses Flash though) which might help you out too: enigmaco.de/enigma/enigma.html (or someone new by now if not you) – Pryfan May 3 at 13:49

add a comment

3 Answers

Active Oldest Votes

5

There's two missing pieces. First, the ring setting changes the output letter, it doesn't rotate the whole exit pattern. Second, the rotors are advanced *before* the letter is encrypted.

If your rotor (Enigma I Rotor I) is set up like this with the ring at A.

```
abcdefghijklmnopqrstuvwxyz
ekmflgdqvzntowyhxuspaibrcj
```

Then if you advance the ring to B all the outputs will be shifted up the alphabet by one. `A` will become `F` instead of `E`. `B` will become `L` instead of `K`. And so on.

```
abcdefghijklmnopqrstuvwxyz
flngdmrwauqszijytubjcsdk
```

This almost matches the simulator, but why is the simulator's output shifted over one?

```
abcdefghijklmnopqrstuvwxyz
kflngdmrwauqszijytubjcsd
```

> Remember that, when depressing a key, the rotors advance before the electrical signal runs through the rotors. Therefore, to examine the current flow through the rightmost rotor in A position, the rotor must be set in the Z position before depressing the key (this also counts for the other rotors if they are due to step).

Source: Technical Details of the Enigma Machine

When you press `A` the rotor advances to `B` and encrypts the letter according to `B`. Your simulator has to *first advance the rotor* and then *encrypt the letter*.

share improve this answer follow answered Feb 16 '16 at 0:02 dchaven 483 1 4 9 9

add a comment

3

The easiest way to understand the path of the current through the rotors is to make up six tables for the three wheels, three going forward and three going backwards plus a table for the reflector.

The simulator was used with rotors `III`, `II`, `I` and `B reflector`. The simulator advances the rotor when the first key is pressed, i.e., the first entry.

To simplify, set the rings to `1`, `1`, `1`. Then when you press the first key the rotor will have the fixed terminal on the terminals from keyboard matching the letters on the core of the rotor (which contains the fixed wiring of the rotor). The path is rotors `I-II-III`, `reflector`, `III`, `II`, `I`. The current path is `A-E,E-L-G` then the reflector gives path `G-L`, then using reverse tables starting at wheel `III`, the return path is `L-F,F-W,W-N`. The result of entering `A` is the letter `N`.

For the next `A` entered, the rotor shifts by one so that the letters on the rotor are shifted relative to the terminals from the keyboard (these are fixed). The letter `A` from keyboard goes to the `A` terminal but now goes to letter `B` on rotor. As before, using the tables, `B` goes to letter `E` on rotor but because of the shift goes to terminal `J` of the next rotor (assuming no shifts of other rotors). Our current path is now `J-B,B-E`, `Reflector G-L`, with return path (using reverse tables starting at rotor `III`) `H-D,D-C`. Because of the shift of the rotor, the `C` terminal is opposite the letter `D` on the core of rotor `I`.

Letter `D` on the rotor is wired to `G` and `G` is opposite the terminal `F` because of the shift. Thus the second `A` will exit as an `F`.

The rotors used were (for first three letters on rotors)

```
ROTOR.I.... A-E,B-K,C-M ..... THE RETURN IS.. A-U,B-W,C-Y ....
ROTOR.II.... A-A,B-J,C-D..... THE RETURN IS.. A-A,B-J,C-P .....
ROTOR.III.... A-B,B-D,C-F ..... THE RETURN IS.. A-T,B-A,C-G....
REFLECTOR (B)..... A-Y,B-R,C-U..
```

The rotors have a ring on the left-hand side of the rotor which has 26 letters or numerals. This ring is spring-loaded and can be pulled outward so that it can rotate relative to the main body (the core).

Beneath the ring is a dot on the main body which is fixed. This is usually set to the `A` position on the rotor. If we want to change the ring setting to `B` or position 2 then we can do this by pulling out the ring and holding the core at the `A` position (relative to the fixed keyboard position `A`), move the ring so that the letter `B` (or `2`) on the ring is opposite the dot on the core. Then release the ring and now we have letter `B` in the window instead of `A`. The rotor must now be turned so that the letter `A` on the ring shows in window. Thus `B` to `A` reverses the normal direction of rotor and the `2` position of the rotor is now opposite the fixed `A` terminal.

```
.............O..C..B..A..Z..Y..X.........fixed terminals from keyboard .....
.............O..C..B..A..Z..Y..X.........core of rotor.....................
.............O..C..B..A..Z..Y..X.........MOVABLE RING.....................
```

Now change to ring setting `B` (2):

```
.............O..C..B..A..Z..Y..X
.............O..C..B..A..Z..Y..X
.............O..C..B..A..Z..Y
```

Now rotate so that `A` shows in the window of the rotor.
This rotates the lower two rows since the ring is engaged.

```
.............O..C..B..A..Z..Y..X
.............O..C..B..A..Z..Y..X
.............C..B..C..B..A..Z..Y
.............................^....
```

The dot at `A` on the middle row which represents the core (where all the wiring is) is now in the `B` position relative to terminals from the keyboard (top row). Note that the core now has `Z` next to our `A` terminal on top row.

The window on lower row shows as `A`. If we now select a key on keyboard, then this will rotate the rotor so that `B` will show in the window. The middle row will now have `A` next to the `A` terminal from the keyboard.

This is why you can set the rings to `1`, `1`, `2` on simulator so that we get a read out from the `A` contact. The `2` setting is equivalent to the `B` setting.

share improve this answer follow edited Jun 27 '17 at 22:11 user47922 answered Jun 27 '17 at 0:52 K ROSSER 31 1 2

1 I tried to format some of this reply. I hope the blocks are still aligned properly. – user47922 Jun 27 '17 at 22:12

add a comment

2

Ok, here we go. Let's use Rotor I as an example.

The wiring for this rotor looks like this:

```
EKMFLGDQVZNTOWYHXUSPAIBRCJ
```

On every rotor, there originally was a dot, for more detail, read K ROSSER's answer. We need to know the position of this dot. It's always where the ring setting letter is (So, if the ring setting is A, it's where the A is). Since all the wiring tables on Wikipedia assume a ring setting of **A**, **we can find the dot position by finding the position of the a**, in case of rotor I, it's the 21. letter. **We need to remember this position for later**.

The next step is to shift all the letters up the alphabet by one for each letter that we go up in the alphabet. So, if we want ring setting C, we go up by 2 in the alphabet (Start out at A, B + 1; C = 2). Shifting up the alphabet means, an A becomes a B, a B a C, and so on. **Each time we shift up the alphabet, we need to add one to the dot position we remembered.** We do this addition mod 26 (Or over the length of your alphabet is).

The last step is to rotate the new wiring, until our ring setting letter is at the position of our dot.

To go back to our example (Were going to count like this now: 0,1,2; In case your wondering):

Our original wiring is "EKMFLGDQVZNTOWYHXUSPAIBRCJ" We want to get it to the Ringstellung "C".

First, we get the dot position, so we look for the A, which is at position 20. We remember this.

Now we shift all the letters up the alphabet by one for each letter that we go up the alphabet from A to get to our Ringstellung, and add one to our dot position:

```
A → B:
EKMFLGDQVZNTOWYHXUSPAIBRCJ
 ||||||||||||||||||||||||||
 FLNGMEHRWAUQPSZIVTQBJCSDK

dot position + 1 = 21
```

```
B → C:
EKMFLGDQVZNTOWYHXUSPAIBRCJ
 ||||||||||||||||||||||||||
 GMOHNIFSXBPVQYAJZWURCKDTEL

dot position + 1 = 22
```

Our new wiring look like this: "GMOHNIFSXBPVQYAJZWURCKDTEL" and our dot position is 22, our ring setting is C, so we want the letter C to be at position 22 in the wiring.

```
Rotation 1:

GMOHNIFSXBPVQYAJZWURCKDTEL
||||||||||||||||||||||||||
LGMOHNIFSXBPVQYAJZWURCKDT

Rotation 2:

LGMOHNIFSXBPVQYAJZWURCKDTE
||||||||||||||||||||||||||
ELGMOHNIFSXBPVQYAJZWURCKDT
```

C is now at position 22, we have completed all the steps. The final wiring table looks like this:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
||||||||||||||||||||||||||
ELGMOHNIFSXBPVQYAJZWURCKDT
```

Here are a few more examples. Here is a python implementation.

share improve this answer follow answered Jun 15 '19 at 11:53 Ichpuchs 187 1 1 9 9

add a comment

Your Answer

B I ~~S~~ link code

Sign up or log in

Sign up using Google
Sign up using Facebook
Sign up using Email and Password

Post as a guest

Name

Email
Required, but never shown

Post Your Answer

By clicking "Post Your Answer", you agree to our terms of service, privacy policy and cookie policy

Not the answer you're looking for? Browse other questions tagged encryption substitution-cipher enigma or ask your own question.

By using our site, you acknowledge that you have read and understand our Cookie Policy, Privacy Policy, and our Terms of Service.

Related

7 How to deduce enigma settings given a partial plaintext?
4 Could the Enigma algorithm be classified as a Feistel network?
7 Under what conditions did a Bletchley bombe stop?
2 How exactly is an enigma simulation software supposed to encrypt alphabets?
10 How many possible Enigma machine settings?
4 Why are the indicator drums of a Bombe machine labelled from A to Z clockwise?
6 Why does the Bombe not consider the Ringstellung when determining stecker pairs?

Hot Network Questions

What does "a dramatic annual shrub" mean?
Create doped structures to POSCAR files for vasp
Drawing a complete graph of 5 nodes on a torus
Applications of symplectic geometry to classical mechanics
What does the term "support loop" specifically mean?
Using a chain-type oil filter wrench as a chain whip
Which mathematician traveled to and moved in with each collaborator?
Exceeding 999999 points in SMB1
Defending a planet's surface from ships in orbit
Is a contiguous_range always a sized_range?
Matchsticks: Fix the Equation
What to do when I'm forced to make battle decisions by other players?
Terminal - different window colors?
The politicization of the supreme court
Does copyright law protect a translation of an ancient work from being translated into a third language?
Why are people protesting against supreme court nominee Amy Coney Barrett?
Wiring two pickups to a single volume pot on a bass guitar
Derivative of definite integrals - how did MWG arrived at this result? Microeconomics
Should items separated by Oxford commas be alphabetical?
Can someone be charged with the murder of unidentified victims?
Solving a sudoku with backtracking
Do I lose if I have an empty library and cast Brainstorm?
A distinction between knowledge of laws of physics and the actual laws
Teenagers discover a network of tunnels to other times

Question feed

site design / logo © 2020 Stack Exchange Inc; user contributions licensed under cc by-sa rev 2020.10.19.37639