Was the Enigma's double stepping mechanism intentional?

Asked 1 year, 11 months ago Active 1 year, 11 months ago Viewed 709 times

Ask Question

2

It's sometimes refered to as the double stepping anomaly, so was it just a design flaw or was it put in place deliberately?

encryption classical-cipher substitution-cipher enigma

Share Improve this question Follow

edited Jun 17 '19 at 13:36
AleksanderRas
6,087 7 18 50

asked Jun 17 '19 at 12:59
b3nj4m1n
207 2 10

Add a comment

2 Answers

Active Oldest Votes

5

I suspect it was a semi-deliberate feature. That is, while it probably wasn't a design goal in and of itself, it neatly solved a mechanical issue that would otherwise have required a more complicated and failure-prone solution.

What was the issue? Simply, it was making the third wheel only advance one step at a time, rather than 26 steps in a row. That's what would happen if the Enigma's notch, pawl and ratchet mechanism was modified to eliminate double stepping without making any other changes to it.

To see why this would happen, you need to note a couple of things about the way the Enigma stepping mechanism works:

- Each wheel has 26 different positions it can be in, corresponding to 26 different shifts of the cipher alphabet. Every time a key is pressed, a pawl tries to push each wheel one position forward.
- Each wheel has a flange (an "index ring") with a notch at one (or, in some of the later wheels, several) of these 26 positions. When the wheel is *not* in the notched position, the index ring holds up the next wheel's pawl and prevents it from rotating the wheel.

What this means is that:

- The first wheel rotates one step on every keypress (since there's no other wheel before it to disengage its pawl).
- The second wheel (normally) rotates on every 26th keypress, whenever the first wheel is in the notched position.
- The third wheel only rotates when the second wheel is in the notched position — and if the second wheel would *stay* in the notched position when that happened, then it would *keep rotating 26 times in a row* (i.e. a full turn) until the second wheel would move out of the notched position again!

If the Enigma worked like that, its wheel positions would repeat with a period of only 26 × 26 = 676 keypresses, far less than intended and potentially less than the length of a single longish message. But by letting the third wheel's pawl also engage the second wheel via the index ring and push it immediately *out* of the notched position as soon as the third wheel has rotated once — i.e. "double stepping" it — the period is extended to 26 × 25 × 26 = 16900 keypresses, i.e. to over 96% of the theoretical maximum of $26^3 = 17576$ keypresses.

Also, the mechanical effect behind the double stepping, i.e. the pawl also pushing the notch it has dropped into, is something that kind of happens naturally in a mechanism like this. While it probably could have been avoided by suitably adjusting the shape of the pawls and the notches, in this case it would've been counterproductive to do so.

The alternative solution, of course, would have been to redesign the mechanism to only rotate the third wheel when the second wheel *moves into* (or out of) the "notched" position. That would certainly have been possible, even with early 1900s tech: a mechanical odometer, like you'd find in any old car, works exactly like that.

But the pin and gear mechanism used in odometers has more moving (and potentially breakable) parts than the Enigma's simple pawl and ratchet, and would probably have made swapping the wheels more complicated and error prone. And, perhaps more importantly, odometers are often subject to "gear lash", especially if the mechanism is worn down, causing the later wheels to fail to rotate a full step when engaged. While such misalignment is harmless in an odometer, and tends to correct itself on the next step, it could be a serious problem for something like the Enigma that relies on the wheels making a precise electrical contact with each other.

So I suspect the designers of the Enigma chose to go with the simpler pawl and ratchet mechanism, and accept an about 4% shorter period in exchange for mechanical simplicity and robustness.

Share Improve this answer Follow

answered Jun 17 '19 at 17:26
Ilmari Karonen
42.3k 3 93 165

Add a comment

3

It was very likely not put in place deliberately, since it doesn't seems to make sense to have it or not have it in place deliberately. I assume it was just overlooked.

Since double-stepping occured only in the middle rotor it just slightly changed the period of the machine.

The machine (with 3 rotors) was originally meant to have a period of $26 \times 26 \times 26 = 17576$. But the double-stepping changed this to a period of $26 \times 25 \times 26 = 16900$.

> [...] was it just a design flaw [...] ?

It could have been theoretically a design flaw but (historically) messages were limited to a few hundred letters, and so there was no chance of repeating any combined rotor position during a single session, denying cryptanalysts valuable clues.

Share Improve this answer Follow

answered Jun 17 '19 at 13:50
AleksanderRas
6,087 7 18 50

Add a comment

Your Answer

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 classical-cipher substitution-cipher enigma or ask your own question.