--not usesfull here--------An Enigma system is made up of several parts including a keyboard, a lamp board, rotors, and internal electronic circuitry. Some machines, such as the ones used by the military, have additional features such as a plugboard.--------

Encoded messages would be a particular scramble of letters on a given day that would translate to a comprehendible sentence when unscrambled.

----for software use---When a key on the keyboard is pressed, one or more rotors move to form a new rotor configuration which will encode one letter as another. Current flows through the machine and lights up one display lamp on the lamp board, which shows the output letter. So if the "K" key is pressed, and the Enigma machine encodes that letter as a "P," the "P" would light up on the lamp board.------looks not useful here-----

--------Software use-----------(Each month, Enigma operators received codebooks which specified which settings the machine would use each day. Every morning the code would change.

For example, one one day, the codebook may list the settings described in the day-key below:

Plugboard settings: A/L – P/R – T/D – B/W – K/F – O/Y

A plugboard is similar to an old-fashioned telephone switch board that has ten wires, each wire having two ends that can be plugged into a slot. Each plug wire can connect two letters to be a pair (by plugging one end of the wire to one letter’s slot and the other end to another letter). The two letters in a pair will swap over, so if “A” is connected to “Z,” “A” becomes “Z” and “Z” becomes “A.” This provides an extra level of scrambling for the military.

Rotor (or scrambler) arrangement: 2 — 3 —1

The Enigma machines came with several different rotors, each rotor providing a different encoding scheme. In order to encode a message, the Enigma machines took three rotors at a time, one in each of three slots. Each different combination of rotors would produce a different encoding scheme. Note: most military Enigma machines had three rotor slots though some had more.

To accomplish the configuration above, place rotor #2 in the 1st slot of the enigma, rotor #3 in the 2nd slot, and rotor #1 in the 3rd slot.

Rotor orientations: D – K –P

On each rotor, there is an alphabet along the rim, so the operator can set in a particular orientation. For this example, the operator would turn the rotor in slot 1 so that D is displayed, rotate the second slot so that K is displayed, and rotate the third slot so that P is displayed.

Cracking the Enigma Code brute force attack

Our enigma machine can not be attacked either by black or grey hackers because we have increased the number of cogs and rotors in the code to make it harder to decrypt. Everything is written in alphabet of 26 words including nu

A major flaw with the Enigma code was that a letter could never be encoded as itself. In other words, an “M” would never be encoded as an “M.” This was a huge flaw in the Enigma code because it gave codebreakers a piece of information they could use to decrypt messages. If the codebreakers could guess a word or phrase that would probably appear in the message, they could use this information to start breaking the code. Because the Germans always sent a weather report at the beginning of the message, and usually included the phrase “Heil Hitler” at the end of the message, there were phrases decrypters knew to look for. [8]Decoders could compare a given phrase to the letters in the code, and if a letter in the phrase matched up with a letter in the code, they knew that that part of the code did not contain the phrase. The decoders could then begin cracking the code with a process of elimination approach.

In the world of Cyber crimes, brute force attack is an activity which involves repetitive successive attempts of trying various password combinations to break into any website. This attempt is carried out vigorously by the hackers who also make use of bots they have installed maliciously in other computers to boost the computing power required to run such type of attacks.

How Can I Prevent It?

Yes, you can take some precautionary measures:

Password Length.Password Complexity.Limit Login Attempts.Modifying .htaccess file.Using Captcha.Two Factor Authentication.Cloudflare.