Caesar Cipher is an encryption system that is based on shifting numbers down to a specific number of places. So, for instance if I had a message that said, “help me” and I shifted the numbers down 1 place the message would come out as “ifmq nf”. If you look at the letters, you know they’re all shifted one place. This is an issue because if you can figure out that’s its cryptography the code becomes stupidly easy to break. You just need to figure out how many letters everything is being shifted and it spits itself out. In contrast, a polyalphabetic cipher has a few more layers. For one the pattern for the code is determined by the word you give to decipher the code called the “shift word”. Using this word, you convert it into numbers according to their letter position in the alphabet and that shifts every letter to that same frequency pattern. The image provided is a great example of a polyalphabetic cipher. Because of the added layer of protection with the shift word the code becomes even harder to decipher. This can be changed to be even more complicated with a longer shift word. So although these both operate on similar principles, the Ceasar Cipher is a lot more simple and easy to crack while polyalphabetic ciphers add a nice extra layer of encryption.

A screenshot of a computer

Description automatically generated

Source:

Khan Academy. “Journey into Cryptography.” *Khan Academy*, 2019, www.khanacademy.org/computing/computer-science/cryptography.