Logbook: how to uses crack to crack code

|  |  |  |
| --- | --- | --- |
| Nov 3 2023 | start of research | I will be doing three different codes that I will use a program to crack. The three cods I will use programming to crack will be enigma, Caesar and one other which I haven’t decided yet.    Enigma: the enigma code was used by the Germans in WW2 and a very hard code to crack at the time, this is why I will be comparing how they cracked in WW2 to how we could crack it today.    Caesar: the Caesar cypher was used by Jules Caesar. Although we it is not the hardest code to crack now; back then it was very hard to crack. |
| Nov 20 2023 (did not use) | Final research for some of the codes | History: The enigma was made in 1918 by Arthur Scherbiu; its main use was in WW2 by the German or the Nazis at the time. This code was cracked in 1932 by a man named Marian Rejewski. At the time they had very limited tech for cracking this code because it used random letters each press of the keyboard that would change every day, this proved hard to solve because the solving key would change every night. Marian Rejewski came up with a machine to crack this code by finding similarity’s through everyday messages such as “Hail Hitler,” At the end of all the messages; for there the worked backwards to eventually cracking it.  How it worked:  1.     Input letter on keyboard  2.     The letter goes through a set of wheels that rotate each time a key is pressed. It goes through this wheel twice to completely scramble the letter.  3.     It would go down to a pin board that can switch seitan letters with another letter (example K-->X whenever a K appears after the wheel it would switch it to an X)  4.     After it would a appear on the lights above the keyboard.  5.     To unscramble you need to take the given text and put it into the exact same scramble set up to get results |
| Nov 21 2023 | Research for the first Caesar cypher | Using the book of code |
| Dec 29-jan 1 2023 | Basic steps to set up the program | I made a list of thing a program should do to crack the caesar cipher, I also made some of the programming using the help of chatgpt and my dad. |
| Jan 20 2024 | Got the basic code cracking to work | Got the java code to crack to crack the Caesar cypher to work, the time it takes is around one second (because it has to search the dictionary for every out come) |
| Jan 25 | Started working on the a Program that will crack a randomized censor cypher | Started working on a program that will take in the alphabet and completely randomize it |
| Feb ? | Started the work on the program that will scramble the randomized Caesar cipher |  |
| Feb 4 | Started the decoding of randomized censor cypher | Decoding this censor cypher is very hard because there way to many outcomes, it has to run through every possible Letter combination in the alphabet. |
| Feb 18 | Got the program to work |  |
| More Logs On GitHub where I stored my code |  |  |

A white board with writing on it

Description automatically generated

Credits:

* + - [how it works?](https://www.theguardian.com/technology/2014/nov/14/how-did-enigma-machine-work-imitation-game)
    - [demo](https://www.101computing.net/enigma-machine-emulator/)
    - [Programming](https://code.visualstudio.com/docs/?dv=osx)
    - [The book of code](http://www.it-docs.net/ddata/788.pdf)
    - <https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/caesar-cipher>
    - https://en.wikipedia.org/wiki/Caesar\_cipher

Steps/Plan:

A diagram of a diagram

Description automatically generated

Ceasar:

Multi-Alpha Caesar

Enigma

Vocabulary

|  |
| --- |
| Clear Text/plain text - unencrypted information |
| Cypher Text - encrypted text |
| Algorithm -a process or set of rules to be followed in calculations or other problem-solving operations |
| Key - when processed through a cryptographic algorithm, can encode or decode cryptographic data. |
| Symmetric Algorithm -a single key for encryption and decryption of information |
| Asymmetric Algorithm- Algorithm- one key is used to encipher the data, and a different but corresponding key is used to decipher the data. |

Using ChatGPT as a tool

Since I have never coded in Java, and my Dad (who helped me) has not coded in Java in many years, I used chatGPT to help me generate code. I would provide ChatGPT will text description of functions I’d like to perform, and used the resulting response as code samples, which were altered and combined to create a new program.