Slav Maksimov

smaks6@eq.edu.au

Caesar cipher

DSP10D

Contents

1. history-of-cryptography
   1. definition
   2. Historical importance
   3. Uses throughout history
2. history of Caesar cipher
   1. definition
   2. historically importance
   3. uses throughout history
   4. images and diagrams



Picture of a cipher disk (<https://gettysburgmuseumstore.com/products/csa-cipher-disc>)

1. python
   1. interface message
   2. evidence of accepting
   3. key—user interface
   4. evidence of running
   5. file system (screenshot)
2. evaluation
   1. why did you create this project?
   2. what were the objectives for the project?
   3. to what extent hove the intent objectives been achieved
   4. how could the project have been improved?
   5. what factors helped and hindered the result
   6. what lesson have been learned from this project

History of cryptography

Definition – Cryptography is the art of encrypting and decrypting communications (such as messages) as an attempt to securely transport encrypted information without a third party reading the message

C = Ek(P)

P = Dk(C)

The above formula where c is ciphertext, E is the encryption method, D the decryption method, P plaintext and k is the key.

Historical Importance – Through history cryptography has been used as a military tactic in many wars such as in the Roman Empire (Julius Caesar used Caesar cipher see 2.0), in WWI a large amount of countries used Morse code (Invented by Samuel Morse) while in WWII Germany used a Lorenz cipher and Enigma machines to encrypt high-level German documents and troop movement.

Uses through history – Through history cryptography has been used at all time in history, since the first cipher (Caesar cipher) to the complex Enigma M4 that took seven year to break, cryptography has been present through most of the world’s history. Starting from about 50BC Julius Caesar was using his three-shift cipher (where he would shift each letter by three to the right). After Caesar cipher came a more complex cipher, the Vigenere cipher (that is based on Caesar cipher) that was invented in the 16th century and was used by the Confederate States of America during the Civil War and was also used by the Swiss Army between 1914 and 1940. The Vigenere cipher was regarded as a very strong cipher even though it was broken as early as 1854 by Charles Babbage but he didn’t publish his works.

Caesar cipher

Definition—Caesar cipher is a method of encoding text messages by replacing each letter with a different one a fixed amount up (or down) the alphabet. These encoded messages can be transmitted through all messages (letter, SMS, email). The code was named after Julius Caesar because he used it to encrypt message with importance (e.g. troop positioning, military orders).

https://www.cia.gov/news-information/featured-story-archive/2007-featured-story-archive/cracking-the-code.html

Historical context- As the roman Empire grew the empire required to communicate between outpost. Although it is not confirmed the Caesar cipher was reasonably secure (mostly because most of Caesars enemy’s where most likely illiterate). During the early 20th century the Russian army used it instead of more complicated cipher (as the soldiers found it difficult to use). Caesar cipher was also used in kids toy/radio programs as seen in A Christmas Story where Little Orphan Annie club members can decipher the “secret” message. More recently Caesar cipher has been used in cites to hide joke answers or spoilers.

Uses through history -



FIGURE [] FIGURE []

<https://familyfoundry.wordpress.com/tag/code/>

<https://www.rpgnow.com/product/231576/Classic-Cipher-Disc>