Name: Kehinde Oluwatoyin Martha

Matric no: 16/SCI01/023

Course code:CSC 418

1. Ceaser Cipher or Shift Cipher: In [cryptography](/wiki/Cryptography" \o "Cryptography), a Caesar Cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known [encryption](/wiki/Encryption" \o "Encryption) techniques. It is a type of [substitution cipher](/wiki/Substitution_cipher" \o "Substitution cipher) in which each letter in the [plaintext](/wiki/Plaintext" \o "Plaintext) is replaced by a letter some fixed number of positions down the [alphabet](/wiki/Alphabet" \o "Alphabet). For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after [Julius Caesar](/wiki/Julius_Caesar" \o "Julius Caesar), who used it in his private correspondence.

The encryption step performed by a Caesar cipher is often incorporated as part of more complex schemes, such as the [Vigenère cipher](/wiki/Vigen%C3%A8re_cipher" \o "Vigenère cipher), and still has modern application in the [ROT13](/wiki/ROT13" \o "ROT13) system. As with all single-alphabet substitution ciphers, the Caesar cipher is easily broken and in modern practice offers essentially no [communications security](/wiki/Communications_security" \o "Communications security).

The transformation can be represented by aligning two alphabets; the cipher alphabet is the plain alphabet rotated left or right by some number of positions. For instance, here is a Caesar cipher using a left rotation of three places, equivalent to a right shift of 23 (the shift parameter is used as the [key](/wiki/Key_(cryptography)" \o "Key (cryptography))):

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZCipher: XYZABCDEFGHIJKLMNOPQRSTUVW

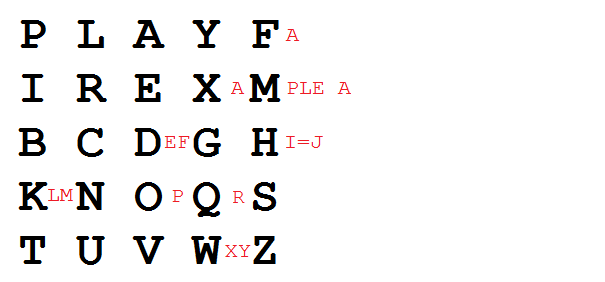
When encrypting, a person looks up each letter of the message in the "plain" line and writes down the corresponding letter in the "cipher" line.

Plaintext: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOGCiphertext: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

2. Monoalphabetic cipher or simple cipher: Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if ‘A’ is encrypted as ‘D’, for any number of occurrence in that plaintext, ‘A’ will always get encrypted to ‘D’.

3. Polyalphabetic Cipher:A polyalphabetic cipher is any [cipher](/wiki/Cipher" \o "Cipher) based on [substitution](/wiki/Substitution_cipher" \o "Substitution cipher), using multiple substitution alphabets. The [Vigenère cipher](/wiki/Vigen%C3%A8re_cipher" \o "Vigenère cipher) is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case. The [Enigma machine](/wiki/Enigma_machine" \o "Enigma machine) is more complex but is still fundamentally a polyalphabetic substitution cipher.

4. Play fair Cipher: The Playfair cipher or Playfair square or Wheatstone-Playfair cipher is a manual [symmetric](/wiki/Symmetric_key_algorithm" \o "Symmetric key algorithm) [encryption](/wiki/Encryption" \o "Encryption) technique and was the first literal [digram substitution](/wiki/Polygraphic_substitution" \o "Polygraphic substitution) cipher. The scheme was invented in 1854 by [Charles Wheatstone](/wiki/Charles_Wheatstone" \o "Charles Wheatstone), but bears the name of [Lord Playfair](/wiki/Lord_Playfair" \o "Lord Playfair) for promoting its use. Using "playfair example" as the key (assuming that I and J are interchangeable), the table becomes (omitted letters in red):



P L A Y FI R E X MB C D G HK N O Q ST U V W Z

Encrypting the message "Hide the gold in the tree stump" (note the null "X" used to separate the repeated "E"s) :

HI DE TH EG OL DI NT HE TR EX ES TU MP ^

|  |  |
| --- | --- |
| 1. The pair HI forms a rectangle, replace it with BM | IMG_257 |
| 2. The pair DE is in a column, replace it with OD | IMG_258 |
| 3. The pair TH forms a rectangle, replace it with ZB | IMG_259 |
| 4. The pair EG forms a rectangle, replace it with XD | IMG_260 |
| 5. The pair OL forms a rectangle, replace it with NA | IMG_261 |
| 6. The pair DI forms a rectangle, replace it with BE |  |
| 7. The pair NT forms a rectangle, replace it with KU |  |
| 8. The pair HE forms a rectangle, replace it with DM |  |
| 9. The pair TR forms a rectangle, replace it with UI |  |
| 10. The pair EX (X inserted to split EE) is in a row, replace it with XM | IMG_262 |
| 11. The pair ES forms a rectangle, replace it with MO |  |
| 12. The pair TU is in a row, replace it with UV |  |
| 13. The pair MP forms a rectangle, replace it with IF |  |

BM OD ZB XD NA BE KU DM UI XM MO UV IF

Thus the message "Hide the gold in the tree stump" becomes "BMODZ BXDNA BEKUD MUIXM MOUVI F". (Breaks included for ease of reading the cipher text.)

5. One time Cipher: In cryptography, a one-time pad is a system in which a [private key](https://searchsecurity.techtarget.com/definition/private-key" \t "_top) generated randomly is used only once to [encrypt](https://searchsecurity.techtarget.com/definition/encryption" \t "_top) a message that is then decrypted by the receiver using a matching one-time pad and key. Messages encrypted with keys based on randomness have the advantage that there is theoretically no way to "break the code" by analyzing a succession of messages.