

DEPARTMENT OF INFORMATION TECHNOLOGY

SREENIDHI INSTITUTE OF SCIENCE AND TECHNOLOGY

(An Autonomous Institution approved by UGC and Affiliated to JNTUH)

Yamnampet, Ghatkesar, Hyderabad – 501 301.

**Computer Networks Lab Project**

**Caesar Cipher in Cryptography**

**18311A12J8 Rahul Teja B**

**IT-D**

**Name of the Incharge**

**Caesar Cipher in Cryptography**

**Abstract**

The Caesar Cipher algorithm for cryptography is one of the oldest algorithms. Now much newer algorithms have arrived that are much more secure, however in terms of speed of execution Caesar cipher algorithm is still the fastest owing to its simplicity. However the algorithm is extremely easy to crack. This is because in this algorithm each character of a message is always replaced by the same fixed character that has been predetermined. To improve the algorithm and enhance it's security feature, a few changes can be added. This paper proposes an enhancement to the existing algorithm by making use first of a simple Diffie-Hellman key exchange scenario to obtain a secret key and later using simple mathematics to ensure the encryption of data is much more safer. Once a private shared key is obtained by making use of the Diffie-Hellman method, the key is subject to the mod operation with 26 to obtain a value less than or equal to 26, then the current character is taken and to this the key value obtained is added to obtain a new character. For any character in the `x' position the key is simply first multiplied with `x' and then mod is done to obtain the encrypted character. So 2nd character of the message is multiplied with 2, third character with 3 and so on. This enhances the security and also does not increase the time of execution by a large margin.

18311A12J8

RAHUL TEJA B

**Introduction**

The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Thus to cipher a given text we need an integer value, known as shift which indicates the number of position each letter of the text has been moved down.

The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.

**Program**

#A python program to illustrate Caesar Cipher Technique

def encrypt(text,s):

result = ""

# traverse text

for i in range(len(text)):

char = text[i]

# Encrypt uppercase characters

if (char.isupper()):

result += chr((ord(char) + s-65) % 26 + 65)

# Encrypt lowercase characters

else:

result += chr((ord(char) + s - 97) % 26 + 97)

return result

#check the above function

text = "ATTACKATONCE"

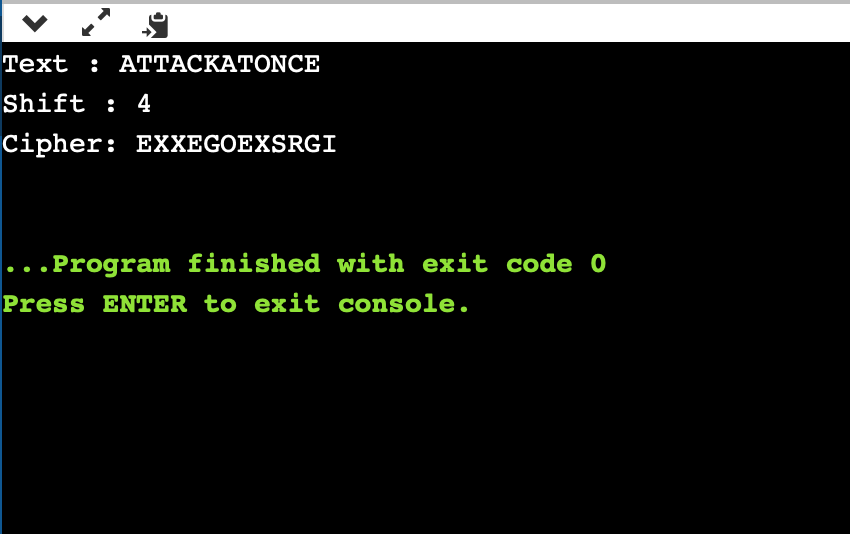
s = 4

print "Text : " + text

print "Shift : " + str(s)

print "Cipher: " + encrypt(text,s)

**OUTPUT**

****