Sant Dnyaneshwar Shikshan Sanstha's
Annasaheb Dange College of Engineering and Technology (ADCET), Ashta
An Autonomous Institute, Affiliated to Shivaji University, Kolhapur, Approved By AICTE, New Delhi & Govt. of Maharashtra, Accredited by NAAC 'A++' Grade, Bangalore
Department of CSE (IOT and Cyber Security including Blockchain Technology)

Class: SY B.Tech Sem VI

AY: 2023-2024

Course: Information Theory for Cyber Security (Laboratory)

Couse Code: 1ICPC210

Experiment No. 2

Title: Implement Symmetric cipher technique using c/c++/python.

- Caesar cipher

Objectives:

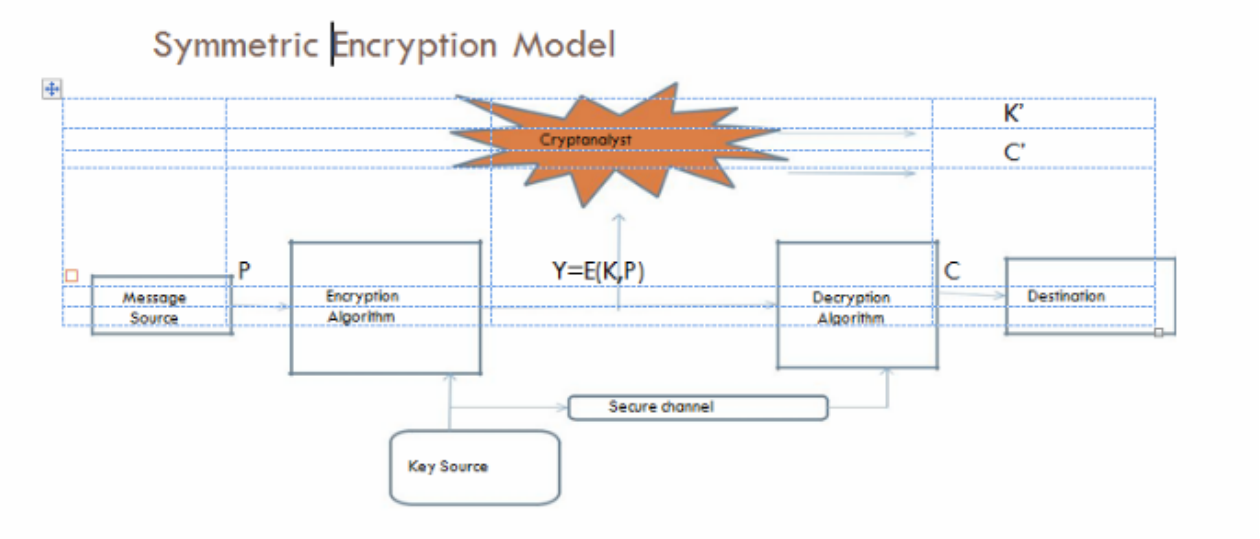
1. Understanding Symmetric Cryptography
2. Understanding Symmetric Cipher Techniques
3. Implementing Symmetric Cipher Algorithms
4. Understanding Encryption and Decryption Processes

Symmetric Cryptography:

Symmetric Cipher Model – Key Terms

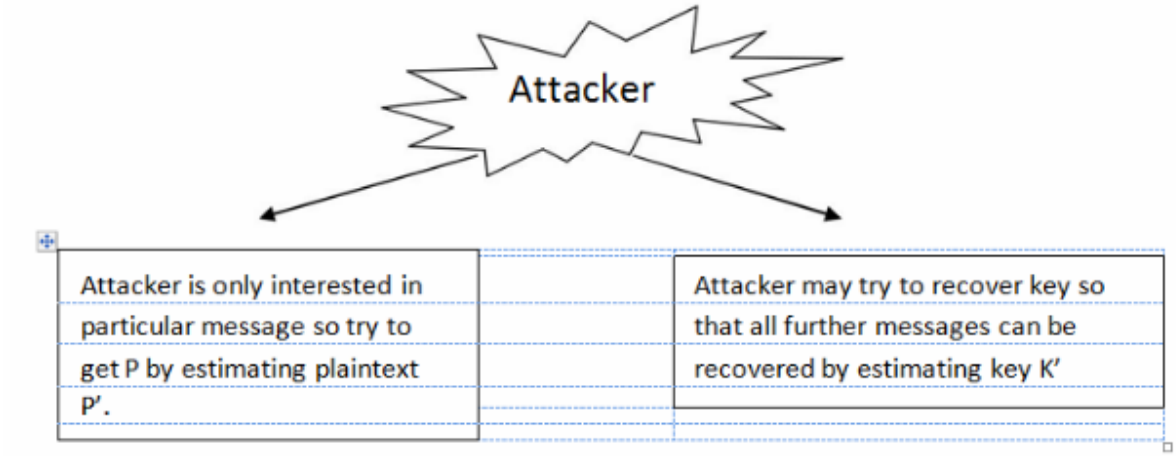
1. Plaintext – Original message or Data that is input to the algorithm.
2. Encryption Algorithm – The algorithm that generates text by performing substitution or permutation.
3. Secret Key – Key that decides substitution and transformation that is to be applied to the algorithm.
4. Ciphertext – The substituted or permuted message which is produced by inputting plaintext and key to algorithm.
5. Decryption Algorithm –The algorithm takes ciphertext and key as input and generates plaintext.
6. For secure communication using encryption following requirements must be satisfied:
7. Strong encryption algorithm – Given the algorithm and one or more ciphertexts attacker can neither decrypt the ciphertext nor find key.
8. The key must be exchanged in secret manner by communicating entities.

Symmetric Encryption Model:



Symmetric Encryption Scheme:

1. Input is, Message P and the encryption key K – Algorithm forms the Ciphertext C denoted as C=E(K,P) .
2. The receiver has key K. P = D(K,C)



Three dimensions specify characteristics of Cryptographic systems:

1. The form of operations used for converting plaintext to ciphertext
2. The number of key used
3. The method used to process plaintext – block cipher, stream cipher

Block cipher - Input is divided into blocks. For a block of elements at a particular time instance, output generated is also a block of elements.	Stream cipher – Elements of input are processed in continuous manner, one element at a time and one element at a time is produced as output.

Substitution Technique:

1. Each letter of the plaintext is replaced by other letter or by number or by symbol.
2. Plaintext is bit sequence, ciphertext is also bit sequence

Caesar cipher – Developed by Julius Caesar

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

- Each letter in the word is replaced by 3 places ahead in the alphabet.
- Plaintext : play

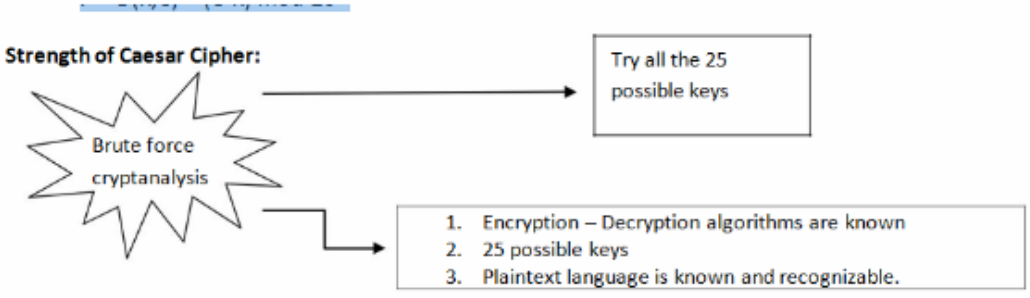
	15	11	0	24
+	3	3	3	3

Ciphertext : SODB

18 mod 26 = 18	14 Mod 26 = 14	3 mod 26 = 3	27 mod 26 = 1

- C = E(3, P)

C = E(3, P)
=(p + 3) mod 26
General form,
C = E(K,P) = (P+K) mod 26 P = D(K,C) = (C-K) mod 26



Caesar Cipher Implementation:

```
// A C++ program to illustrate Caesar Cipher Technique
#include <iostream>
using namespace std;

// This function receives text and shift and
// returns the encrypted text
string encrypt(string text, int s)
{
    string result = "";

    // traverse text
    for (int i = 0; i < text.length(); i++) {
        // apply transformation to each character
        // Encrypt Uppercase letters
        if (isupper(text[i]))
            result += char(int(text[i] + s - 65) % 26 + 65);

        // Encrypt Lowercase letters
        else
            result += char(int(text[i] + s - 97) % 26 + 97);
    }

    // Return the resulting string
    return result;
}

// Driver program to test the above function
int main()
{
    string text = "ATTACKATONCE";
    int s = 4;
    cout << "Text : " << text;
    cout << "\nShift: " << s;
    cout << "\nCipher: " << encrypt(text, s);
    return 0;
}
```

Output:

```
Text : ATTACKATONCE
```

Sant Dnyaneshwar Shikshan Sanstha's
Annasaheb Dange College of Engineering and Technology (ADCET), Ashta
An Autonomous Institute, Affiliated to Shivaji University, Kolhapur, Approved By AICTE, New Delhi & Govt. of Maharashtra, Accredited by NAAC 'A++' Grade, Bangalore
Department of CSE (IOT and Cyber Security including Blockchain Technology)

Shift: 4

Cipher: EXXEGOEXSRGI