|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| D:\sep2k3\COLLEG~1\LOGO.JPG | SHRI SANT GAJANAN MAHARAJ COLLEGE OF ENGG. SHEGAON | | | **LABORATORY MANUAL** | |
| **PRACTICAL EXPERIMENT INSTRUCTION SHEET** | | | | |
| LABORATORY MANUAL NO.:SSGMCE/WI/IT/BCF/7IT08/15 | | ISSUE NO.: 00 | | ISSUE DATE: 18/07/2022 | |
| REV.DATE: | | DEPTT:INFORMATION TECHNOLOGY | | | |
| LABORATORY: Block Chain Fundamental | | | SEMESTER: 4N/VII | | PAGE: 1 OF 3 |

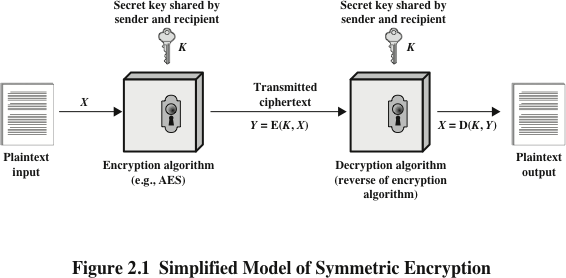
1. **AIM: Study of Cryptographic Primitives Part –I**

**Symmetric (Shift Cipher) & Asymmetric Cryptographic (RSA) algorithm**

1. **THEORY**

A symmetric encryption scheme has five ingredients.

1. **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.
2. **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
3. **Secret Key:** The secret key is also input to the encryption algorithm. The key is the value independent of the plaintext. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.
4. **Cipher text:** This is the scrambled message produced as output. It depends on the plaintext and the key.
5. **Decryption algorithm:** This is the encryption algorithm in reverse. It takes the cipher text and the secret key and produces the original plaintext.

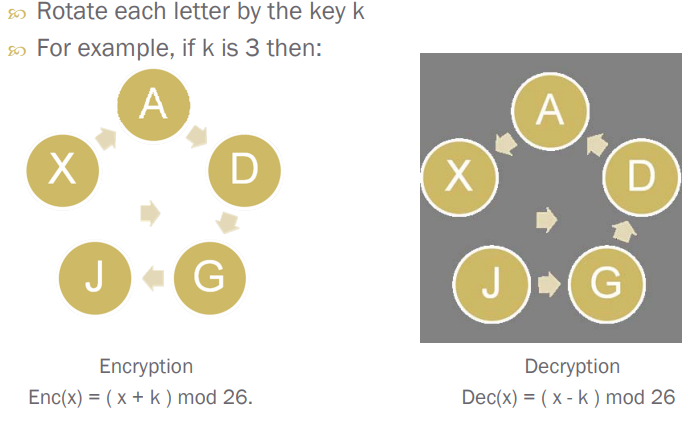


Following are the two basic functions used in the encryption algorithm. All the encryption algorithms are based on two general principles:

**Substitution:** In which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element. A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.1 If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| D:\sep2k3\COLLEG~1\LOGO.JPG | SHRI SANT GAJANAN MAHARAJ COLLEGE OF ENGG. SHEGAON | | | **LABORATORY MANUAL** | |
| **PRACTICAL EXPERIMENT INSTRUCTION SHEET** | | | | |
| LABORATORY MANUAL NO.:SSGMCE/WI/IT/BCF/7IT08/15 | | ISSUE NO.: 00 | | ISSUE DATE: 18/07/2022 | |
| REV.DATE: | | DEPTT:INFORMATION TECHNOLOGY | | | |
| LABORATORY: Block Chain Fundamental | | | SEMESTER: 4N/VII | | PAGE: 2 OF 3 |

In **transposition cipher technique**, rearranges the position of the plain text’s characters. The identity of the characters remains unchanged, but their positions are changed to create the cipher text



**For demonstration purpose refer Virtual Lab IIT Bombay (Cryptographic Lab**)

RSA algorithm is a public key encryption technique and is considered as the most secure way of encryption. It was invented by Rivest, Shamir and Adleman in year 1978 and hence name **RSA** algorithm.

The RSA algorithm holds the following features −

* RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
* The integers used by this method are sufficiently large making it difficult to solve.
* There are two sets of keys in this algorithm: private key and public key.

# RSA Algorithm

**Step-1: Choose two prime number** p & q

**Step-2: Compute the value of** n=p x q and Ø=(p-1)(-1)

# Step-3:

Consider number e as a derived number which should be greater than 1 and less than (p-1) and (q-1). The primary condition will be that there should be no common factor of (p-1) and (q-1) except 1

# Step4

Compute the value of d (private key)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| D:\sep2k3\COLLEG~1\LOGO.JPG | SHRI SANT GAJANAN MAHARAJ COLLEGE OF ENGG. SHEGAON | | | **LABORATORY MANUAL** | |
| **PRACTICAL EXPERIMENT INSTRUCTION SHEET** | | | | |
| LABORATORY MANUAL NO.:SSGMCE/WI/IT/BCF/7IT08/15 | | ISSUE NO.: 00 | | ISSUE DATE: 18/07/2022 | |
| REV.DATE: | | DEPTT:INFORMATION TECHNOLOGY | | | |
| LABORATORY: Block Chain Fundamental | | | SEMESTER: 4N/VII | | PAGE: 3 OF 3 |

Private Key d is calculated from the numbers p, q and e. The mathematical relationship between the numbers is as follows −

ed = 1 mod (p-1) (q-1)

# Step-5: Do the encryption and decryption

Encryption is given as, C = Pe mod n

Decryption is given as, Plaintext = Cd mod n

**RSA Encryption and Decryption -Illustration**

<https://www.devglan.com/online-tools/rsa-encryption-decryption>

**Below is python implementation of RSA algorithm for small values:**

# Python for RSA asymmetric cryptographic algorithm.

# For demonstration, values are

# relatively small compared to practical application

import math

def gcd(a, h):

    temp = 0

    while(1):

        temp = a % h

        if (temp == 0):

            return h

        a = h

        h = temp

p = 3

q = 7

n = p\*q

e = 2

phi = (p-1)\*(q-1)

while (e < phi):

    # e must be co-prime to phi and

    # smaller than phi.

    if(gcd(e, phi) == 1):

        break

    else:

        e = e+1

# Private key (d stands for decrypt)

# choosing d such that it satisfies

# d\*e = 1 + k \* totient

k = 2

d = (1 + (k\*phi))/e

# Message to be encrypted

msg = 12.0

print("Message data = ", msg)

# Encryption c = (msg ^ e) % n

c = pow(msg, e)

c = math.fmod(c, n)

print("Encrypted data = ", c)

# Decryption m = (c ^ d) % n

m = pow(c, d)

m = math.fmod(m, n)

print("Original Message Sent = ", m)

**03 CONCLUSION:**. **In this way, we studied, Symmetric (Shift Cipher) & Asymmetric Cryptographic (RSA) algorithm**