**#include<bits/stdc++.h>**

**using namespace std;**

**int x, y, n, t, i, flag;**

**long int e[50], d[50], temp[50], j;**

**char en[50], m[50];**

**string msg;**

**int prime(long int);**

**void encryption\_key();**

**long int cd(long int);**

**void encrypt();**

**void decrypt();**

**int main()**

**{**

**cout << "\nEnter two prime numbers : ";**

**cin >> x >> y;**

**getchar();**

**cout << "\nEnter Message : \n";**

**getline(cin,msg);**

**for(i = 0; msg[i] != NULL; i++)**

**m[i] = msg[i];**

**n = x \* y;**

**t = (x - 1) \* (y - 1);**

**encryption\_key();**

**cout<<"Public Key : ("<<e[1]<<", "<<n<<")\n";**

**cout<<"Private Key : ("<<d[1]<<", "<<n<<")";**

**encrypt();**

**decrypt();**

**return 0;**

**}**

**int prime(long int pr)**

**{**

**int i;**

**j = sqrt(pr);**

**for(i = 2; i <= j; i++)**

**{**

**if(pr % i == 0)**

**return 0;**

**}**

**return 1;**

**}**

**void encryption\_key()**

**{**

**int k;**

**k = 0;**

**for(i = 2; i < t; i++)**

**{**

**if(t % i == 0)**

**continue;**

**flag = prime(i);**

**if(flag == 1 && i != x && i != y)**

**{**

**e[k] = i;**

**flag = cd(e[k]);**

**if(flag > 0)**

**{**

**d[k] = flag;**

**k++;**

**}**

**if(k == 99)**

**break;**

**}**

**}**

**}**

**long int cd(long int a)**

**{**

**long int k = 1;**

**while(1)**

**{**

**k = k + t;**

**if(k % a == 0)**

**return(k/a);**

**}**

**}**

**void encrypt()**

**{**

**long int pt, ct, key = e[0], k, len;**

**i = 0;**

**len = msg.size();**

**while(i != len)**

**{**

**pt = m[i];**

**pt = pt - 96;**

**k = 1;**

**for(j = 0; j < key; j++)**

**{**

**k = k \* pt;**

**k = k % n;**

**}**

**temp[i] = k;**

**ct= k + 96;**

**en[i] = ct;**

**i++;**

**}**

**en[i] = -1;**

**cout << "\n\nAfter Encryption : \n";**

**for(i=0; en[i] != -1; i++)**

**cout << en[i];**

**}**

**void decrypt()**

**{**

**long int pt, ct, key = d[0], k;**

**i = 0;**

**while(en[i] != -1)**

**{**

**ct = temp[i];**

**k = 1;**

**for(j = 0; j < key; j++)**

**{**

**k = k \* ct;**

**k = k % n;**

**}**

**pt = k + 96;**

**m[i] = pt;**

**i++;**

**}**

**m[i] = -1;**

**cout << "\n\nAfter Decryption : \n";**

**for(i = 0; m[i] != -1; i++)**

**cout << m[i];**

**cout << endl;**

**}**

**Cryptography** is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication. Earlier cryptography was effectively synonymous with encryption but nowadays cryptography is mainly based on mathematical theory and computer science practice.

Modern cryptography concerns with:

Confidentiality - Information cannot be understood by anyone

Integrity - Information cannot be altered.

Non-repudiation - Sender cannot deny his/her intentions in the transmission of the information at a later stage

Authentication - Sender and receiver can confirm each

Cryptography is used in many applications like banking transactions cards, computer passwords, and e- commerce transactions.

Three types of cryptographic techniques used in general.

1. Symmetric-key cryptography

2. Hash functions.

3. Public-key cryptography

**Symmetric-key Cryptography:** Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.

**Public-Key Cryptography**: This is the most revolutionary concept in the last 300-400 years. In Public-Key Cryptography two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key, remains a secret. The public key is used for encryption and for decryption private key is used.

**Hash Functions:** No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.

**Applications of Cryptography**

**Digital Currency**

A much-known application of cryptography is digital currency wherein cryptocurrencies are traded over the internet. Top cryptocurrencies like Bitcoin, Ethereum, and Ripple have been developed and traded over time. With cashless economies emerging, digital currencies have grabbed the attention of the world. Unregulated by any government or banks, cryptocurrencies are our upcoming future. Blockchain technology has a lot to do with this application. Several nodes in the blockchain are empowered with cryptography that enables the secure trade of a cryptocurrency in a digital ledger system. These ledgers are protected, preserved, and cannot be accessed by any other person or organization.

**E-commerce**

With the current pandemic shackling us to our homes, the rise of e-commerce has been tremendous. Well, who wouldn't like to enjoy the comfort of shopping in your living room and receiving your hampers the next morning?

However, there's something we should know about e-commerce in order to understand how it works. E-commerce startups enable us to shop items online and pay for them online.

These transactions are encrypted and perhaps cannot be altered by any third party. Moreover, the passwords we set for such sites are also protected under keys to ensure that no hacker gets access to our e-commerce details for harmful purposes.

**Military Operations**

The applications of cryptography in the military are well-known. Military operations have also derived great use from cryptography for a long time. Used for encrypting military communication channels, military encryption devices convert the real communication characters so that the enemies cannot come to know about their upcoming plans.

Simply put, cryptography safely transmits messages from one end to the other without letting the enemy forces intercept the real meaning. This is a very important application of cryptology as it can be of both public and private use.

On the large scale, it can be widely used for declaring wars and sending crucial messages without the involvement of a messenger. Unlike traditional times, this technology can be precisely used to enhance the military strength of a nation.