A Brief Study On Cryptography

Dipendu Ghosh
3rd year, Computer Science, Vidyasagar College, Kolkata.

Abstract: This paper is a brief study of the interesting topic Cryptography. We have tried to explain the different techniques adopted to encode and decode a text.
We implemented one of the models in a code in C++.

Keywords: Cryptography, Secret Key Cryptography, Public-Key Cryptography, Hash Functions, Morse Code, Pigpen Cipher, Steganography.

1 Introduction

Cryptography (or **cryptology**; from Greek, *kryptos*, "hidden, secret"; and *grapho*, "I write". It is the practice and study of hidden information.Cryptography is the science of writing a secret code (encryption) by converting ordinary information (i.e., plaintext) into unintelligible gibberish (i.e., cipher-text). Decryption is the reverse, moving from unintelligible cipher-text to plaintext. A cipher (or cypher) is a pair of algorithms which creates the encryption and the reversing decryption. The operation of a cipher is controlled by the algorithm and by another instance, called the key. This key is a secret parameter (known only to the communicants). For a specific message exchange the key is unique to it. Keys are important, as ciphers without keys would be unbreakable and without them the encrypted code cannot be decrypted. It is needed to protect information from being stolen.
Cryptography is performed mainly to ensure secrecy in communications between

- Spies & Military leaders,
- Diplomats,
- Religious applications.

Cryptography is performed to ensure

- Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation: A mechanism to prove that the sender really sent this message.

So cryptography not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals : secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography and hash functions.

2 Simple Cipher Cryptography techniques

- **Transposition Ciphers:** Rearrange the order of letters in a message. For example 'help me' becomes 'ehpl em'.
- **Substitution Ciphers:** Systematically replace letters or groups of letters with other letters or groups of letters. 'fly at once' becomes 'gmz bu podf' by replacing each letter with the one following it in the alphabet.
- **Caesar Cipher:** Each letter in the plaintext was replaced by a letter some fixed number of positions further down the alphabet. Named after Julius Caesar who is reported to have used it, with a shift of 3, to communicate with his generals during his military campaigns.

3 Some formats used in modern Cryptography

In modern days cryptography is performed in some of the following forms:

- Secure Communications
  - Document / Data / Email Encryption
  - VPN
- Identification and Authentication
- Secret Sharing
- Electronic Commerce and Payments
  - ATMs / Credit Cards
  - Net Banking / Web Shopping
- Certification
  - Digital Signature (not Digitized Signature)
- Key Recovery
- Remote Access
  - Secure ID
- Entertainment
  - Cable TV: Set-top Box – Pay-per-view (Encryption)
  - Satellite TV: Select Channel (Scrambling)
- Mobile Communication
  - Voice Encryption
- Anti-Spamming
  - CAPTCHA™ (from Carnegie Mellon University)
    - Completely Automated Public Turing test to tell Computers and Humans Apart
- Steganography
  - Invisible ink,
  - Microdots,
  - Digital Watermarking

4. The three types of cryptographic schemes

4.1 Secret Key Cryptography(Symmetric encryption): With secret key cryptography, a single key (known to both the sender and the receiver) is used for both encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher-text to the receiver. The receiver applies the same key (or rule-set) to decrypt the message and recover the plaintext. The biggest difficulty with this approach, of course, is the distribution of the key.

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same cipher-text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher-text in a stream cipher.

4.2 Public-Key Cryptography(PKC): This has been said to be the most significant new development in cryptography in the last 4 decades. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key.PKC depends upon the existence of so-called one-way functions, or mathematical functions that are easy to compute whereas their inverse function is relatively difficult to compute. A couple of examples illustrate the fact:

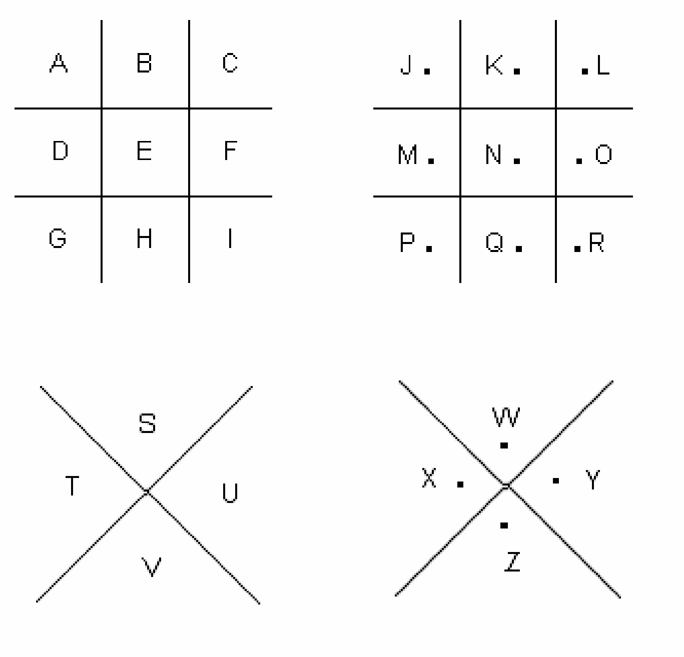
Multiplication vs. factorization**:** in no time the result of multiplying 9 with 16 which is 144, can be found. But if we suppose instead that we have the number 144, and we need to find out the pair of integers whose product is 144.Then we would get a number of solutions and obtain the final solution after many trials. Similar is the case of exponentiation and logarithms.

4.3 Hash Functions: Also called message digests and one-way encryption, are algorithms that, in some sense, use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents, often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.

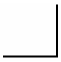
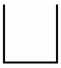
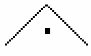
5. Some codes used in cryptography

5.1 The International Morse Code Symbols : Dash and dots were used to send short telegraphic messages from one place to another.

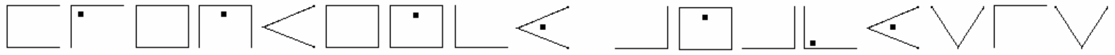
5.2 The Pigpen Cipher: The mono-alphabetic substitution cipher persists through the centuries in various forms. For example the pigpen cipher was used by Freemansons in the 1700s to keep their records private, and still used today by schoolchildren. The cipher does not substitute one letter for another, rather it substitutes each letter for a symbol according to the following pattern.



To encrypt a particular letter, its position is found and selected in one of the four grids. Hence:

a =  ,b = , .. z = 

If the key is known then it is easy to decipher the pigpen cipher. If not then it is easily broken by :



5.3 The ADFGVX Cipher: This cipher features both substitution and transposition. Encryption begins by drawing up 6 x 6 grid, and filling the 36 squares with a random arrangement of the 26 letters and 10 digits. Each row and column of the grid is identified by one of the six letters A,D,F,G,V and X. the arrangement of the elements in the grid acts as part of the key, so the receiver needs to know the details of the grid in order to decipher messages. We illustrate with an example**.**

	A	**D**	**F**	**G**	**V**	**X**
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

The first stage of encryption is to take each letter of the message, locate its position in the grid and substitute it with the letters that label its row and column.

For the Message : attack at 10 pm

Plain text : a t t a c k a t 1 0 p m

Stage 1 cipher text : DV DD DD DV FG FD DV DD AV XG AD GX

So far this is a simple mono-alphabetic substitution cipher, and frequency analysis would be enough to crack it. However, the second stage of the ADFGVX is a transposition, which makes cryptanalysis much harder. The transposition depends on a keyword, which in this case happens to be the word MARK, and which must be shared with the receiver. Transposition is carried out according to the following recipe. First, the letter of the keyword is written in the top row of a fresh grid. Next, the stage 1 cipher is written underneath it in a series of rows, as shown below. The column of the grid is then re-arranged so that the letters of the keyword are in alphabetical order. The final cipher is achieved by going down each column and then writing out the letters in this new order.

M	**A**	**R**	**K**
D	V	D	D
D	D	D	V
F	G	F	D

Re-arrange columns so that the letters of the keyword are in

A	**K**	**M**	**R**
V	D	D	D
D	V	D	D
G	D	F	F

D	V	D	D
A	V	X	G
A	D	G	X

alphabetic order

V	D	D	D
V	G	A	X
D	X	A	G

Final cipher-text: V D G V V D D V D D G X D D F D A A D D F D G

The final cipher-text would then be transmitted in Morse code, and the receiver would reverse the encryption process in order to retrieve the original text. The entire cipher-text is made up of just six letters (i.e. A,D,F,G,V,X), because these are the labels of the rows and columns of the initial 6 x 6 grid. A,D,F,G,V and X are highly dissimilar from one another when translated into Morse dots and dashes, so this choice of letters minimize the risk of errors during transmission.

5.4 Encryption using the ASCII binary numbers: This is done by changing the ASCII value of letters, symbol and digits to their equivalent binary number. The ASCII assigns a 7-digit binary number to each letter of the alphabet. There are 128(2^7) ways to arrange a combination of 7 binary digits, so ASCII can identify 128 distinct characters. For example, let us suppose we want to encrypt the message HELLO, employing computer version of a transposition cipher. Before encryption we must translate the message using the ASCII code of representing the letters.

Plaintext =HELLO=10010001000101100110010011001001111

One of the simplest way to find the encrypted text is to swap the first and the second digits, third and the fourth digits and so on. In this case the final digit would remain unchanged because there are an odd number of digits. We get the following

Cipher-text: 01100010001010011001100011000110111

Another way can be by the method of transpositioning the bits of the neighbouring letter. For example, by swapping the seventh and eighth numbers, the final 0 of H is swapped with the initial 1 of E. The encrypted message is a single string of 35 binary digits, which can be transmitted to the receiver, who then reverses the transposition to recreate the original string of binary digits. Finally the receiver reinterprets the binary digits via ASCII to regenerate the message HELLO.

Another way, which is a bit complicated, is to encrypt the plain text using a key and sending the key with the original message. Let us suppose we want to encrypt the word HELLO using this technique with the key being DAVID. First we convert both the words to their binary equivalent and then we apply logical XOR on each bit.

Message : HELLO

Message in ASCII : 10010001000101100110010011001001111

Key : DAVID

Key in ASCII: 10001001000001101011010010011000100

Cipher-text: 00011000000100001101000001010001011

The encrypted message is sent along with the key, the receiver decrypts the message by applying the reverse of the encryption process.

6 Cryptanalysing a Cipher-text: Let us consider the following cipher text

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CI SX’XJMI, KBO JCKO XPV EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: ‘DJOXL EYPD, ICJ X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?’

OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK

Assumptions before we start to decipher this cipher-text are:

i) The text is in English
ii) Ciphered using mono-alphabetic substitution cipher
iii) Blanks are preserved
iv) Case is ignored
v) No idea of the key so we go for frequency analysis found by the Arabs in 1000AD.

Now the steps used to decipher the text are:

*Step 1***:** We find the frequency of each letter in the given piece of text as shown in the table below:

Letter	Frequency	
	Occurrences	Percentage
A	3	0.9
B	25	7.4
C	27	8
D	14	4.1
E	5	1.5
F	2	0.6
G	1	0.3

Letter	Frequency	
	Occurrences	Percentage
N	3	0.9
O	38	11.2
P	31	9.2
Q	2	0.6
R	6	1.8
S	7	2.1
T	0	0

H	0	0	U	6	1.8
I	11	3.3	V	18	5.3
J	18	5.3	W	1	0.3
K	26	7.7	X	34	10.1
L	25	7.4	Y	19	5.6
M	11	3.3	Z	5	1.5

Step 2: From the above table we can see the letter ‘O’ is most commonly used in the given text. And we can also assume that it represents the most common letter in English, ‘e’. We can also assume that the eighth most frequent letter in the given text, ‘Y’ represents the eighth most frequent letter in English, ‘h’ as given in the table below:

This table of relative frequency is based on passages taken from newspapers and novels, and the total sample was 100, 362 alphabetic characters. The table was compiled by H. Beker and F. Piper, originally published in Cipher Systems: The Protection of Communication.

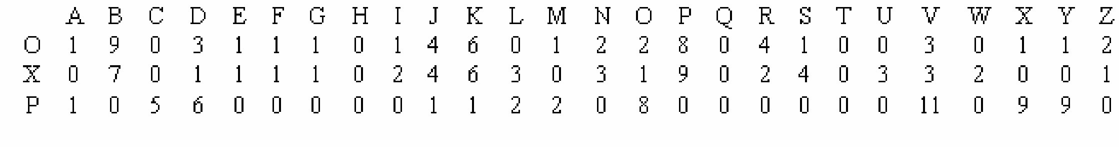
Letter	Percentage	Letter	Percentage
A	8.2	n	6.7
B	1.5	o	7.5
C	2.8	p	1.9
D	4.3	q	0.1
E	12.7	r	6
F	2.2	s	6.3
G	2	t	9.1
H	6.1	u	2.8
I	7	v	1
J	0.2	w	2.4
K	0.8	x	0.2
L	4	y	2
M	2.4	z	0.1

If we apply this technique then we lead to a gibberish deciphered text. Now we focus our attention on the 3 letters having the highest frequency of occurrence in the given text. They are ‘O’, ‘X’ and ‘P’. In the given text the precedence of occurrence of the letters are ‘O’, ‘X’ and ‘P’ and we cannot be sure that O = e, X = t and P = a as ‘e’, ‘a’ and ‘t’ are in their precedence of most occurrence in the English. But we can make the assumption that

O = e, t or a,   X = e, t or a,   P = e, t or a

Step 3: By just counting the number of times the occurrence of the letters and making the above assumption we would take a long time to decipher the given piece of text. So, now we find the number of times the letters ‘O’, ‘X’ and ‘P’ appear next to all the other letters in the given text. This will give an indication if ‘O’ represents a vowel or a consonant. If

‘O’ is a vowel then it should appear before or after most of the other letters, else it will tend to avoid many of the other letters. In the table below we represent the occurrence of the letters ‘O’, ‘X’ and ‘P’ before and after the other letters:

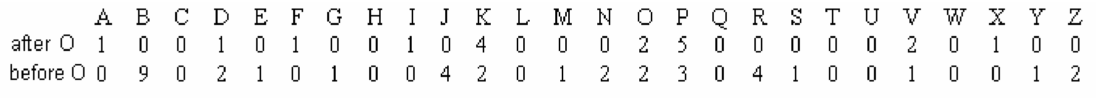


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
O	1	9	0	3	1	1	1	0	1	4	6	0	1	2	2	8	0	4	1	0	0	3	0	1	1	2
X	0	7	0	1	1	1	1	0	2	4	6	3	0	3	1	9	0	2	4	0	3	3	2	0	0	1
P	1	0	5	6	0	0	0	0	0	1	1	2	2	0	8	0	0	0	0	0	0	11	0	9	9	0

Now what is the value in each box? Take an example, O appears before A on 1 occasion, but never appears after it, giving a total of 1 in the first box and so on.

Also we see that the letters ‘O’ and ‘X’ appears more number of times than the letter ‘P’ which avoids 15 of the other letters. So it is clear that ‘O’ and ‘X’ represents vowels while ‘P’ represents a consonant.

Step 4: Next we have to determine which letter among ‘O’ and ‘X’ represents which vowel. The vowels are probably ‘a’ or ‘e’ as the are the most frequently used letters in English language. Next, is O = e and X= a or O = a and X = e? This can be found out from the ciphered text. We see the combination ‘OO’ appears twice whereas ‘XX’ does not appear at all. Since in plaintext English the letters ‘ee’ appear more number of times than ‘aa’ so it is likely that O = e and X = a. Also ‘X’ appears on its own also, so it is clear that X = a. Also another letter ‘Y’ appears on its own, and this letter can be the other English letter that appears on its own which is ‘i’. Now the trick is to spot ‘h’. It can be identified easily as in plain English ‘h’ appears most frequently after ‘e’(as in the, then, they, their, them, there, etc.) but rarely before ‘e’. Since in the cipher-text we have O = e so we need to find out which other letter occur more frequently after ‘O’ in the given text as in the table below:



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
after O	1	0	0	1	0	1	0	0	1	0	4	0	0	0	2	5	0	0	0	0	0	2	0	1	0	0
before O	0	9	0	2	1	0	1	0	0	4	2	0	1	2	2	3	0	4	1	0	0	1	0	0	1	2

From the above table we see that ‘B’ appears more frequently after ‘O’ than any other letter, so B = h.

Step 5: So we have found out that

O → e

X → a

Y → i

B→ h

Now the ciphered text is partially deciphered as

PCQ VMJiPD LhiK LiSe KhahJaWaV haV ZCJPe EiPD KhahJiUaJ LhJee KCPK. CP Lhe LhCMKaPV aPV IiJKL PiDhL, QheP Khe haV ePVeV Lhe LaRe CI Sa'aJMI, Khe JCKe aPV EiKKeV Lhe DJCMPV ZeICJe hiS, KaUiPD: 'DJeaL EiPD, ICJ a LhCMKaPV aPV CPe PiDhLK i haNe ZeeP JeACMPLiPD LC UCM Lhe IaZReK CI FaKL aDeK aPV Lhe ReDePVK CI aPAiePL EiPDK. SaU i SaEe KC ZCRV aK LC AJaNe a IaNCMJ CI UCMJ SaGeKLU?'

eFiRCDMe, LaReK IJCS Lhe LhCMKaPV aPV CPe PiDhLK

Step 6: This simple step helps us to determine some other letters because we can guess some of the words in the cipher-text. For example the 2 most common words used in plain English are 'the' and 'and'. In the partially ciphered text we find 'Lhe' which appears six times and 'aPV' which appear five times. So we have L = t, P = n and V = d

So we find that

L → t

P → n

V → d

Now the ciphered text is partially deciphered as

nCQ dMJinD thiK tiSe KhahJaWad had ZCJne EinD KhahJiUaJ thJee KCnK. Cn the thCMKand and IiJKt niDht, Qhen Khe had ended the taRe CI Sa'aJMI, Khe JCKe and EiKKed the DJCMnd ZeICJe hiS, KaUinD: 'DJeat EinD, ICJ a thCMKand and Cne niDhtK i haNe Zeen JeACMntinD tC UCM the IaZReK CI FaKt aDeK and the ReDendK CI anAient EinDK. SaU i SaEe KC ZCRd aK tC AJaNe a IaNCMJ CI UCMJ SaGeKtU?'

eFiRCDMe, taReK IJCS the thCMKand and Cne niDhtK

Step 7: Now we see that the first word of the second sentence is 'Cn'. In plain text English, every word has a vowel so 'C' must be a vowel. There are only two vowels remaining 'u' and 'o'. Here 'u' does not fit so C = o. Also, we have a word 'Khe', which implies 'K' can be 't' or 's'. But 'L' is already assigned the letter 't' so K = s.

So we find that

C → o

K → s

Now the ciphered text is partially deciphered as

noQ dMJinD this tiSe shahJaWad had ZoJne EinD shahJiUaJ thJee sons. on the thoMsand and IiJst niDht, Qhen she had ended the taRe oI Sa’aJMI, she Jose and Eissed the DJoMnd ZeIoJe hiS, saUinD: ‘DJeat EinD, IoJ a thoMsand and one niDhts i haNe Zeen JeAoMntinD to UoM the IaZRes oI Fast aDes and the ReDends oI anAient EinDs. SaU i SaEe so ZoRd as to AJaNe a IaNoMJ oI UoMJ SaGestU?’

eFiRoDMe, taRes IJoS the thoMsand and one niDhts

Step 8: From the last line we see the phrase ‘thoMsand and one niDhts’. A sensible guess this would be ‘thousand and one nights’. And it seems likely that the final line is telling us that the passage is from ‘Tales from the thousand and one nights’. This implies M = u , I = f , J = r , D = g , R = l and S = m.

So we find that

M → u

I → f

J → r

D → g

R → l

S → m

Now the ciphered text is partially deciphered as

noQ during this time shahraWad had Zorne Eing shahriUar three sons. on the thousand and first night, Qhen she had ended the tale of ma’aruf, she rose and Eissed the ground Zefore him, saUing: ‘great Eing, for a thousand and one nights i haNe Zeen reAounting to Uou the faZles of Fast ages and the legends of anAient Eings. maU i maEe so Zold as to AraNe a faNour of Uour maGestU?’

eFilogue, tales from the thousand and one nights

Step 9: Now the first word of the text is ‘noQ’ so ‘Q’ can be ‘t’, ‘n’, ‘r’ or ‘w’. But ‘t’, ‘n’ and ‘r’ are already assigned so Q = w. From the last line we have ‘maU’, where ‘U’ can be ‘y’ to form ‘may’. So U = y. Also the word ‘Eing’ is present, where ‘E’ can be ‘k’ or ‘s’ to form a meaningful word. But ‘s’ is already assigned a letter so E = k.

So we find that

Q → w

U → y

E → k

Now the ciphered text is partially deciphered as

now during this time shahraWad had Zorne king shahriyar three sons. on the thousand and first night, when she had ended the tale of ma’aruf, she rose and kissed the ground Zefore him, saying: ‘great king, for a thousand and one nights i haNe Zeen reAounting to you the faZles of Fast ages and the legends of anAient kings. may i make so Zold as to AraNe a faNour of your maGesty?’

eFilogue, tales from the thousand and one nights

Step 10: We find a word ‘Zefore’ which is clear that Z = b. Another word is ‘anAient’ which is clearly ‘ancient’ so A = c. Another word is ‘haNe’ where N = v as ‘r’ is assigned a letter, ‘t’ is assigned a letter which could form a meaningful word.

So we find that

Z → b

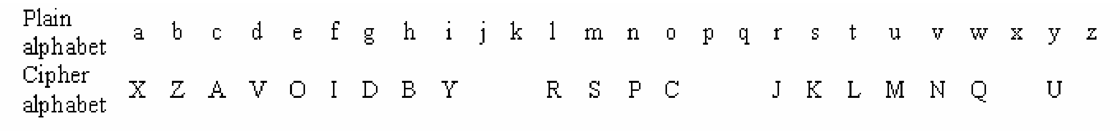
A → c

N → v

Now the ciphered text is partially deciphered as

now during this time shahraWad had borne king shahriyar three sons. on the thousand and first night, when she had ended the tale of ma’aruf, she rose and kissed the ground before him, saying: ‘great king, for a thousand and one nights i have been recounting to you the fables of Fast ages and the legends of ancient kings. may i make so bold as to crave a favour of your maGesty?’

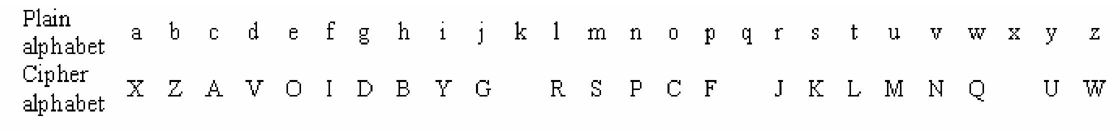
Step 11:From the almost deciphered text we form the following table



Plain alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cipher alphabet	X	Z	A	V	O	I	D	B	Y			R	S	P	C			J	K	L	M	N	Q		U	

Also we find the word ‘maGesty’ where G = j to form ‘majesty’ the other letters does not form a meaningful word. Another word is ‘Fast’ can form ‘past’ so F = p. The only word left is ‘shahraWad’ where ‘W’ can be ‘k’, ‘q’, ‘x’ or ‘z’. If W = z then it forms the name of a person as ‘shahrazad’. So W = z.

Now the table is



Plain alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cipher alphabet	X	Z	A	V	O	I	D	B	Y	G		R	S	P	C	F		J	K	L	M	N	Q		U	W

We can see from the above table the keyphrase is found ‘AVOIDBYGERSPC’ by a bit of guess work. So we have E = k. And thereafter putting the letters in alphabetic order. So we have H = q and T = x.

So we find that

G → j

E → k

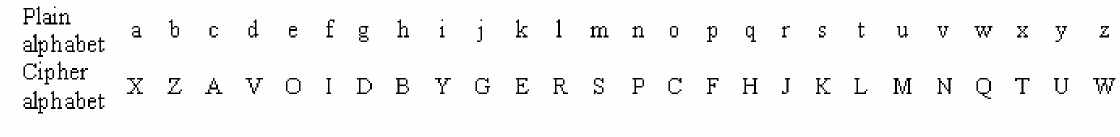
F → p

W → z

H → q

T → x

So the final table is



Plain alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cipher alphabet	X	Z	A	V	O	I	D	B	Y	G	E	R	S	P	C	F	H	J	K	L	M	N	Q	T	U	W

The fully deciphered text is

Now during this time Shahrazad had borne king Shahriyar three sons. On the thousand and first night, when she had ended the tale of Ma’aruf, she rose and kissed the ground before him, saying: ‘Great King, for a thousand and one nights I have been recounting to you the fables of past ages and the legends of ancient kings. May I make so bold as to crave a favour of your majesty?’

Epilogue, Tales from the Thousand and One Nights

In this paper we have tried to implement the above procedure using C++ programming. A part of the source code and the output of the program is given below:-

Source Code:-

```
main()
{
	crypto ob1(2),ob2(1);
	while(1)
	{
		cout<<"\t\t\tMENU"<<endl;
		cout<<"\t\t1.To Encrypt a entered text"<<endl;
		cout<<"\t\t2.To Decrypt a entered text"<<endl;
		cout<<"\t\t3.Exit"<<endl;
		cout<<"\tEnter choice - ";
		cin>>c;
		switch(c)
		{
			//Encrypting the Decrypted message
			case 1:
				ob1.get_encrypt();/*The “get_encrypt()” function takes the original text as input for the object ‘ob1’ of the class ‘crypto’ to be encrypted*/
				ob1.encrypt();/*The “encrypt()” function encrypts the original text entered using the “get_encrypt()” function.*/
				ob1.display_encrypt();/*Displays the encrypted text of the original text entered using “get_encrypt()” function and encrypting it using “encrypt()” function.*/
			break;
			//Decrypting the Encrypted message
			case 2:
				ob2.get_decrypt();/*The “get_decrypt()” function takes the encrypted text as input for the object ‘ob2’ of the class ‘crypto’ which is to be decrypted*/
				ob2.decrypt();/*The “decrypt()” function decrypts the encrypted text entered using the “get_decrypt()” function.*/
```

```
                ob2.display_decrypt();/*Displays the decrypted text of the
encrypted text entered using “get_decrypt()” function and decrypting it using “decrypt()”
function.*/
            break;
            case 3:
                exit(0);
            default:
                cout<<"Wrong Choice"<<endl;
            break;
        }
        //For infinite loop termination
        cout<<"Do you want to continue?(Enter Y or y to continue - ";
        cin>>d;
        if(d!='y' || d!='y')
            break;
    }
}
```

Output:-

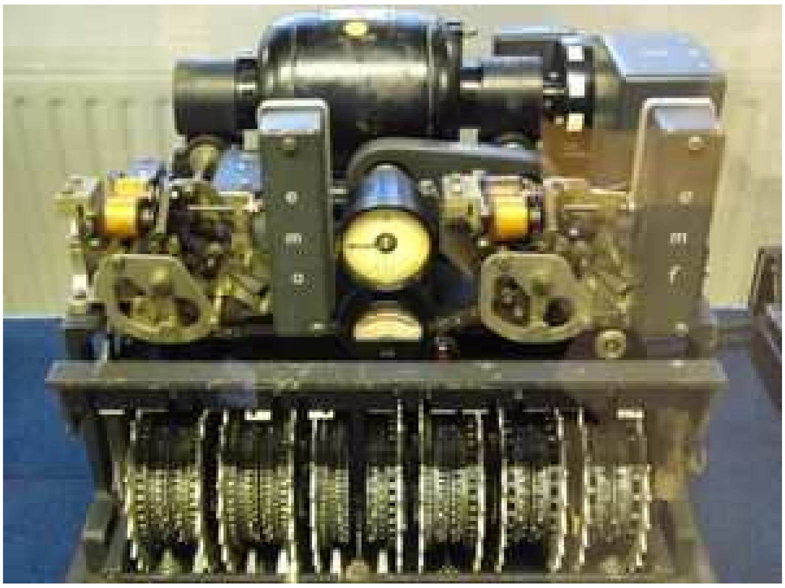
```
                MENU
        1.To Encrypt a given text
        2.To Decrypt a given text
        3.Exit
        Enter choice –  1

Enter Original Text –

Now during this time Shahrazad had borne king Shahriyar three sons. On the thousand
and first night, when she had ended the tale of Ma’aruf, she rose and kissed the ground
before him, saying: ‘Great King, for a thousand and one nights I have been recounting to
you the fables of past ages and the legends of ancient kings. May I make so bold as to
crave a favour of your majesty?’

The Encrypted Text is -

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ
LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP KBO BXV
OPVOV LBO LXRO CI SX’XJMI, KBO JCKO XPV EYKKOV LBO DJCMPV
ZOICJO BYS, KXUYPD: ‘DJOXL EYPD, ICJ X LBCMKXPV XPV CPO PYDBLK Y
BXNO ZOOP JOACMPLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO
RODOPVK CI XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X
IXNCMJ CI UCMJ SXGOKLU?’

Do you want to continue?(Enter Y or y to continue) – y
```

```
                              MENU
               1.To Encrypt a given text
               2.To Decrypt a given text
               3.Exit
               Enter choice –  2

Enter Ciphered Text -

pcq vmjypd lbyk lyso kbxbjxwxv bxv zcjpo eypd kbxbjyuxj lbjoo kcpk. cp lbo lbcmkxpv
xpv iyjkl pydbl, qbop kbo bxv opvov lbo lxro ci sx’xjmi, kbo jcko xpv eykkov lbo
djcmpv zoicjo bys, kxuypd: ‘djoxl eypd, icj x lbcmkxpv xpv cpo pydblk y bxno zoop
joacmplypd lc ucm lbo ixzrok ci fxkl xdok xpv lbo rodopvk ci xpayopl eypdk. sxu y sxeo
kc zcrv xk lc ajxno x ixncmj ci ucmj sxgoklu?’

The Deciphered Text is –

NOW DURING THIS TIME SHAHRAZAD HAD BORNE KING SHAHRIYAR
THREE SONS. ON THE THOUSAND AND FIRST NIGHT, WHEN SHE HAD
ENDED THE TALE OF MA’ARUF, SHE ROSE AND KISSED THE GROUND
BEFORE HIM, SAYING: ‘GREAT KING, FOR A THOUSAND AND ONE NIGHTS I
HAVE BEEN RECOUNTING TO YOU THE FABLES OF PAST AGES AND THE
LEGENDS OF ANCIENT KINGS. MAY I MAKE SO BOLD AS TO CRAVE A
FAVOUR OF YOUR MAJESTY?’

Do you want to continue?(Enter Y or y to continue) – y

                              MENU
               1.To Encrypt a given text
               2.To Decrypt a given text
               3.Exit
               Enter choice –  3

Exiting Program-
```

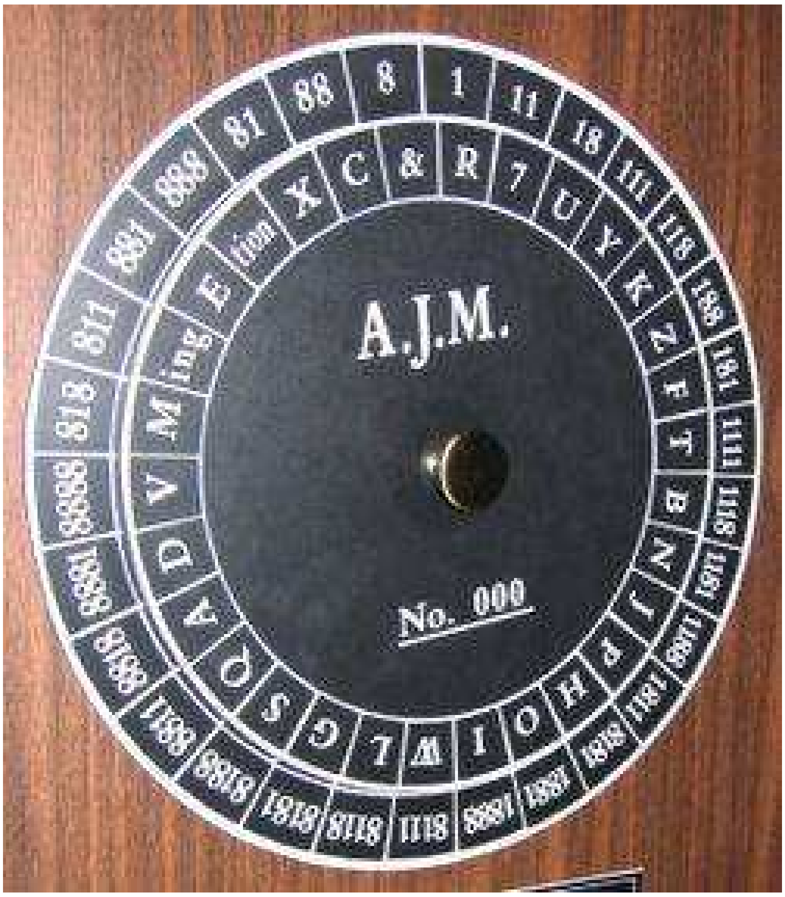
7.The RSA Algorithm

. RSA (the Republic of South Africa) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

Machines used in cryptography



The German Lorenz Cipher machine, used in World War II for encryption of very high-level general staff messages



A cipher Disk. Developed in 15th century by Leon Battista Alberti

The Ancient Greek scytale (rhymes with Italy), probably much like this modern reconstruction, may have been one of the earliest devices used to implement a cipher.

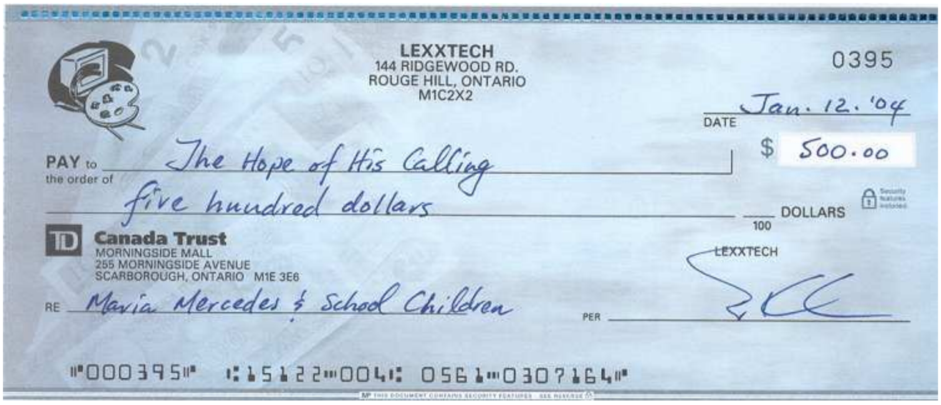
The Enigma machine, used in several variants by the German military between the late 1920s and the end of World War II, implemented a complex electro-mechanical poly-alphabetic cipher to protect sensitive communications. Breaking the Enigma at the Biuro Szyfrow, and the subsequent large-scale decryption of Enigma traffic at Bletchley Park, was an important factor contributing to the Allied victory in WWII

The rotor stack from Tatjana van Vark's Enigma-inspired rotor machine, constructed in 2002. The rotors of this machine contain 40 contacts.

Typex was a printing rotor machine used by the United Kingdom and its Commonwealth, and was based on the Enigma patents.

SIGABA, an American rotor machine, used 15 rotors. 5 were used to scramble the letters, while the other 10 determined the rotor stepping.

This is not a machine but is an identification of a person. A credit card with smart card capabilities. The 3 by 5 mm chip embedded in the card is shown enlarged in the insert. Smart cards attempt to combine portability with the power to compute modern cryptographic algorithms.



LEXXTECH
144 RIDGEWOOD RD.
ROUGE HILL, ONTARIO
M1C2X2

0395

DATE Jan. 12. '04

PAY to the order of The Hope of His Calling $ 500.00

five hundred dollars 100 DOLLARS

TD Canada Trust
MORNINGSIDE MALL
255 MORNINGSIDE AVENUE
SCARBOROUGH, ONTARIO M1E 3E6

RE Maria Mercedes & School Children

LEXXTECH

PER

⑈000395⑈ ⑆15122⑈004⑆ 0561⑈0307164⑈

This is another example of secrecy. The code at the bottom of the check gives all the details of the customer and the bank.

0 123456 789005

This is a bar code that has all the details of a product or for the purpose for which it is used.

7. Conclusion

Cryptography plays a very important role for maintaining the security and safety of a country. The defense system of a country greatly uses several methods of cryptography to transmit important information from a source to a destination. Cryptography is also used in other systems to protect the systems from unintended intrusions. In modern times, cryptography is considered as a branch of both mathematics and computer science, and is affiliated closely with information technology, computer security, and engineering. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords, and electronic commerce, which all depend on cryptography New cryptographic techniques are developed by experts which are difficult to decrypt by the hackers. It is very difficult to use Cryptography in languages other than English.

Reference:-

- Simon Singh, *The Code Book – The Secret History of Codes and Codebreaking*, 1st edition, Fourth Estate Limited, 1999
- Henk C. A. Van. Tilborg, Editor in chief, *Encyclopedia of Cryptology and Security*, New York : Springer Science+Business Media, Inc., 2005
- D. E. Newton, *Encyclopedia of Cryptology*, ABC-CLIO, Inc, 1997
- Gary C. Kessler, *An Overview of Cryptography*, May 1998 (Revised 1 August 2006) http://www.garykessler.net/library/crypto.html
- “Cryptography” on Wikipedia: http://en.wikipedia.org/wiki/Cryptography