



---

## Department of Information Technology

**Academic Year: 2022-23**

**Semester: V**

**Class / Branch: TE IT Subject: Security Lab (SL)**

**Subject Lab Incharge: Prof. Apeksha Mohite**

---

### Experiment No. 11

- 1. Aim: To study symmetric and asymmetric encryption methods using Cryptool.**
- 2. Software Required : CrypTool 1.4.41**
- 3. Theory :**

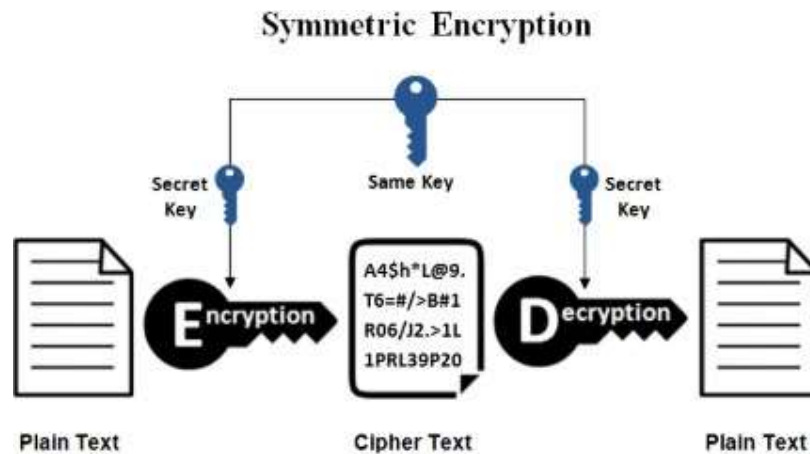
What is Cryptool?

- A freeware program with graphical user interface (GUI).
- A tool for applying and analyzing cryptographic algorithms.
- With extensive online help, it's understandable without deep crypto knowledge.
- Contains nearly all state-of-the-art crypto algorithms.
- “Playful” introduction to modern and classical cryptography.
- Not a “hacker” tool.

Cryptography is a method of using advanced mathematical principles in storing and transmitting data in a particular form so that only those whom it is intended can read and process it. Encryption is a key concept in cryptography – It is a process whereby a message is encoded in a format that cannot be read or understood by an eavesdropper. CrypTool is a free Windows program for cryptography and cryptanalysis. On Linux Platform JCrypTool can be used.

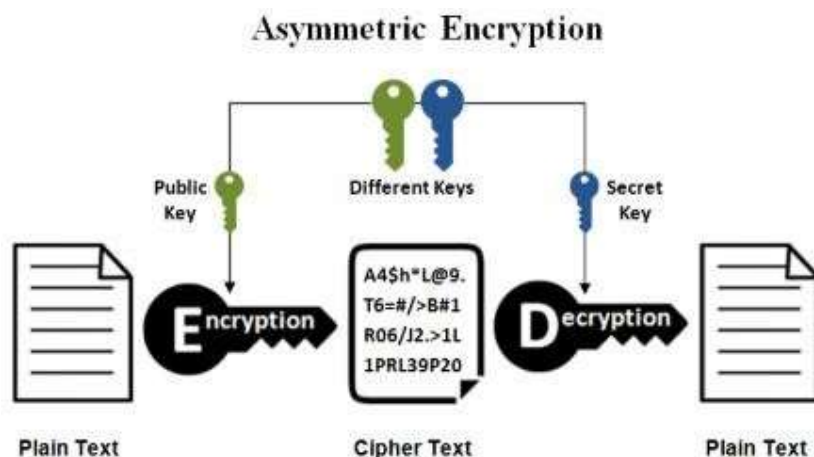
- The current version of CrypTool offers among other things:
- Visualization of several algorithms (Caesar, Enigma, RSA, Diffie-Hellman, digital signatures, AES, etc.)

- Cryptanalysis of several algorithms (Vigenère, RSA, AES, etc.)



Blowfish, AES, RC4, DES, RC5, and RC6 are examples of symmetric encryption. The most widely used symmetric algorithm is AES-128, AES-192, and AES-256.

The main disadvantage of the symmetric key encryption is that all parties involved have to exchange the key used to encrypt the data before they can decrypt it.



Asymmetrical encryption is also known as public key cryptography, which is a relatively new method, compared to symmetric encryption. Asymmetric encryption uses two keys to encrypt a plain text. Secret keys are exchanged over the Internet or a large network. It



PARSHVANATH CHARITABLE TRUST'S

**A. P. SHAH INSTITUTE OF TECHNOLOGY**

(All Branches NBA Accredited)



ensures that malicious persons do not misuse the keys. It is important to note that anyone with a secret key can decrypt the message and this is why asymmetrical encryption uses two related keys to boosting security. A public key is made freely available to anyone who might want to send you a message. The second private key is kept a secret so that you can only know.

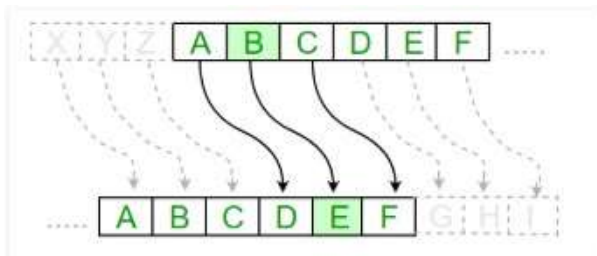
A message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key. Security of the public key is not required because it is publicly available and can be passed over the internet. Asymmetric key has a far better power in ensuring the security of information transmitted during communication.

Asymmetric encryption is mostly used in day-to-day communication channels, especially over the Internet. Popular asymmetric key encryption algorithm includes ElGamal, RSA, DSA, Elliptic curve techniques.

### Caesar Cipher

To start with the process you have to move to the Encrypt/Decrypt tab of the program. There, you will find Symmetric (Classic) tab - Choose Caesar Cipher. For further information, you can get guided by the image below.

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.





CrypTool 1.4.41 - startingexample-en

File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help

startingexample-en

HELLO WORLD

Key Entry: Caesar / ROT-13

Description

Here you can enter the key for the Caesar cipher. Caesar is a mono-alphabetic substitution, where the characters of the cleartext alphabet are mapped to the ciphertext alphabet by shifting. This shifting value is the key. You can enter the key as a number or as a single character of the alphabet. Rot-13 is a special variant, where the key has the fixed value of half the length of the cleartext alphabet. This variant is only selectable if the length of the alphabet is an even number.

Select variant

☒ Caesar  
☐ Rot-13

Options to interpret the alphabet characters

☒ Value of the first alphabet character = 0 (e.g. "A"=0)  
☐ Value of the first alphabet character = 1 (e.g. "A"=1)

Key entry as:

☐ Alphabet character   
☒ Number value

Properties of the chosen encryption

Shift of 25

Mapping of the alphabet (26 characters)

from: ABCDEFGHIJKLMNOPQRSTUVWXYZ  
to: ZABCDEFGHIJKLMNOPQRSTUVWXY

Encrypt Decrypt Text options Cancel

Press F1 to obtain help. L:1 C:12 P:12 CAP NUM

CrypTool 1.4.41 - Caesar encryption of <startingexample-en>, key <Z, KEY OFFSET: 0>

File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help

startingexample-en

HELLO WORLD

Caesar encryption of <startingexample-en>, key <Z, KEY OFFSET: 0>

GDKKN VNQKC

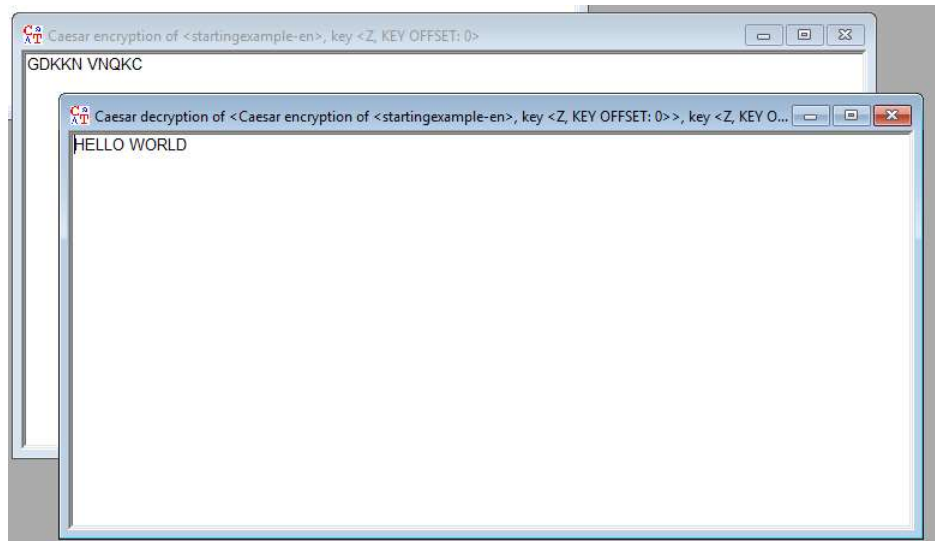
Press F1 to obtain help. L:1 C:1 P:1 CAP NUM



PARSHVANATH CHARITABLE TRUST'S

**A. P. SHAH INSTITUTE OF TECHNOLOGY**

(All Branches NBA Accredited)



## Vigenère Cipher

Encryption with a keyword using a key table Example

Keyword: CHIFFRE Encrypting: VIGENERE becomes XPOJSVVG

The plaintext character (V) is replaced by the character in the corresponding row and in the column of the first keyword character (c). The next plaintext character (I) is replaced by the character in the corresponding row and in the column of the next keyword character (h), and so on. If all characters of the keyword have been used, then the next keyword character is the first key character.



PARSHVANATH CHARITABLE TRUST'S

# A. P. SHAH INSTITUTE OF TECHNOLOGY

(All Branches NBA Accredited)



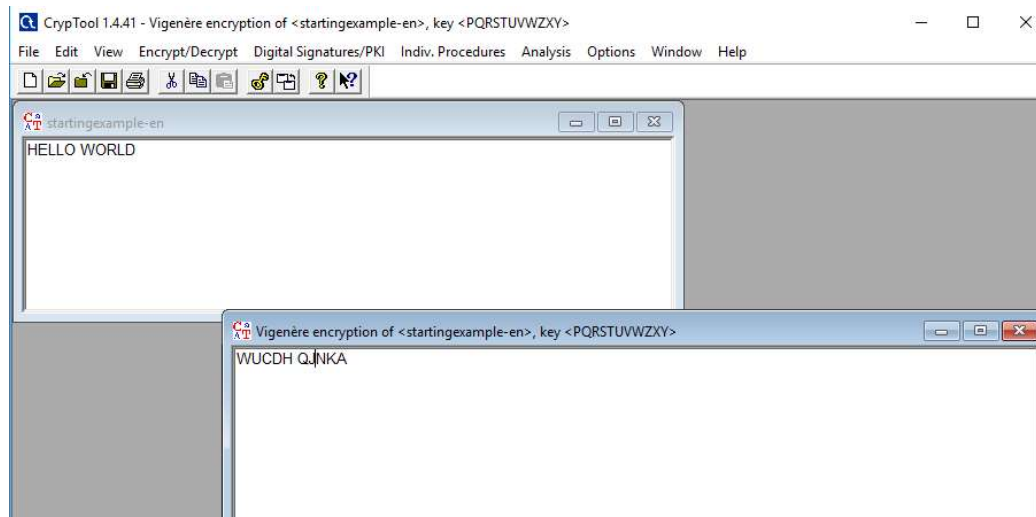
Keyword character

The diagram shows a Vigenère square, a 26x26 grid of letters. A keyword 'KEYWORD' is written vertically in the first column, and a plaintext 'HELLO WORLD' is written horizontally in the first row. The intersection of the keyword 'KEYWORD' and the plaintext 'HELLO WORLD' is circled in red, showing the encrypted character 'W'. The grid is labeled 'Tableau carré, dit « Carré de Vigenère »' at the bottom.

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
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
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	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	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

Plaintext character

Encrypted character







PARSHVANATH CHARITABLE TRUST'S

# A. P. SHAH INSTITUTE OF TECHNOLOGY

(All Branches NBA Accredited)



## Playfair cipher

The Playfair cipher was the first practical digraph substitution cipher.

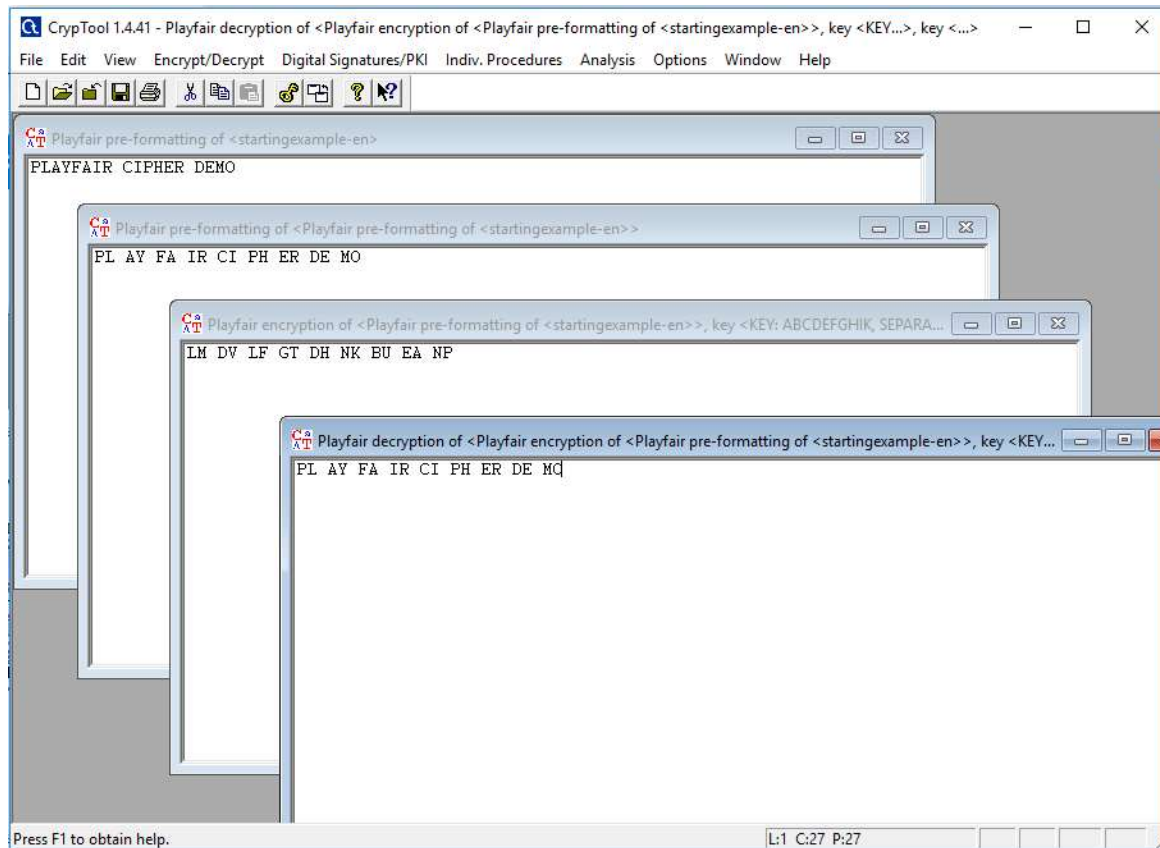
The 'key' for a playfair cipher is generally a word, for the sake of example we will choose 'monarchy'. This is then used to generate a 'key square', e.g.

m	o	n	a	r
c	h	y	b	d
e	f	g	i	k
l	p	q	s	t
u	v	w	x	z

- Any sequence of 25 letters can be used as a key, so long as all letters are in it and there are no repeats. Note that there is no 'j', it is combined with 'i'. We now apply the encryption rules to encrypt the plaintext.
- Remove any punctuation or characters that are not present in the key square (this may mean spelling out numbers, punctuation etc.).
- Identify any double letters in the plaintext and replace the second occurrence with an 'x' e.g. 'hammer' -> 'hamxer'.
- If the plaintext has an odd number of characters, append an 'x' to the end to make it even.
- Break the plaintext into pairs of letters, e.g. 'hamxer' -> 'ha mx er'
- The algorithm now works on each of the letter pairs.
- Locate the letters in the key square, (the examples given are using the key square above)
- If the letters are in different rows and columns, replace the pair with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important – the first encrypted letter of the pair is the one that lies on the same row as the first plaintext letter. 'ha' -> 'bo', 'es' -> 'il'
- If the letters appear on the same row of the table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row). 'ma' -> 'or', 'lp' -> 'pq'
- If the letters appear on the same column of the table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the



original pair was on the bottom side of the column). 'rk' -> 'dt', 'pv' -> 'vo'

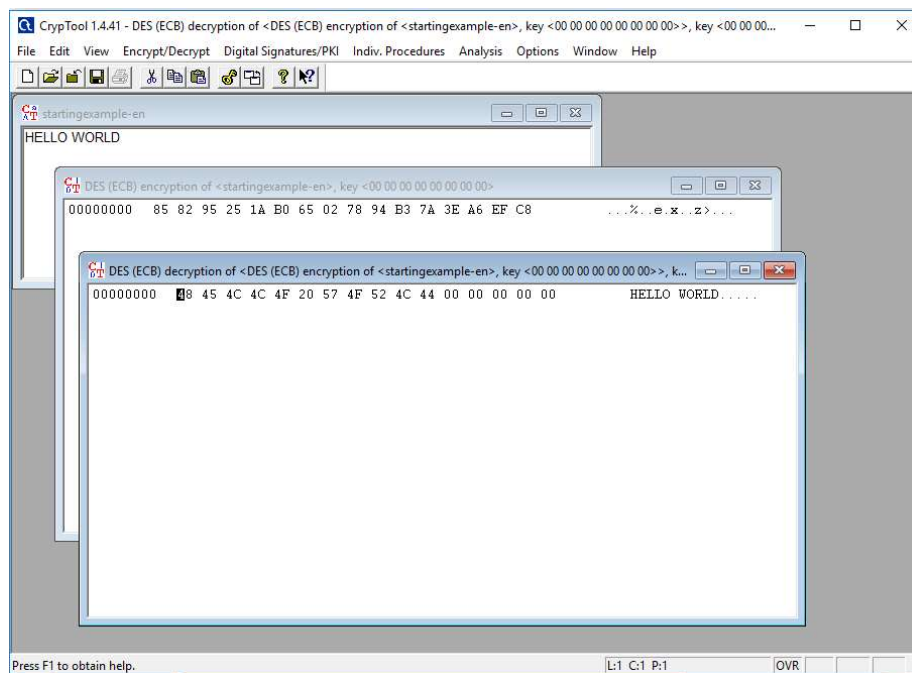
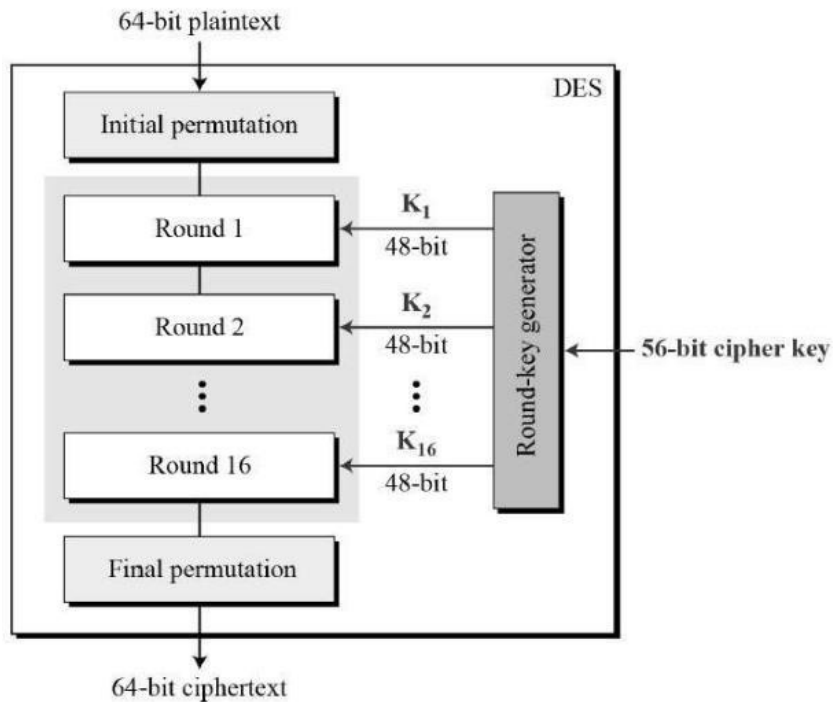


### Symmetric Algorithm DES

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration –







## Advanced Encryption Standard

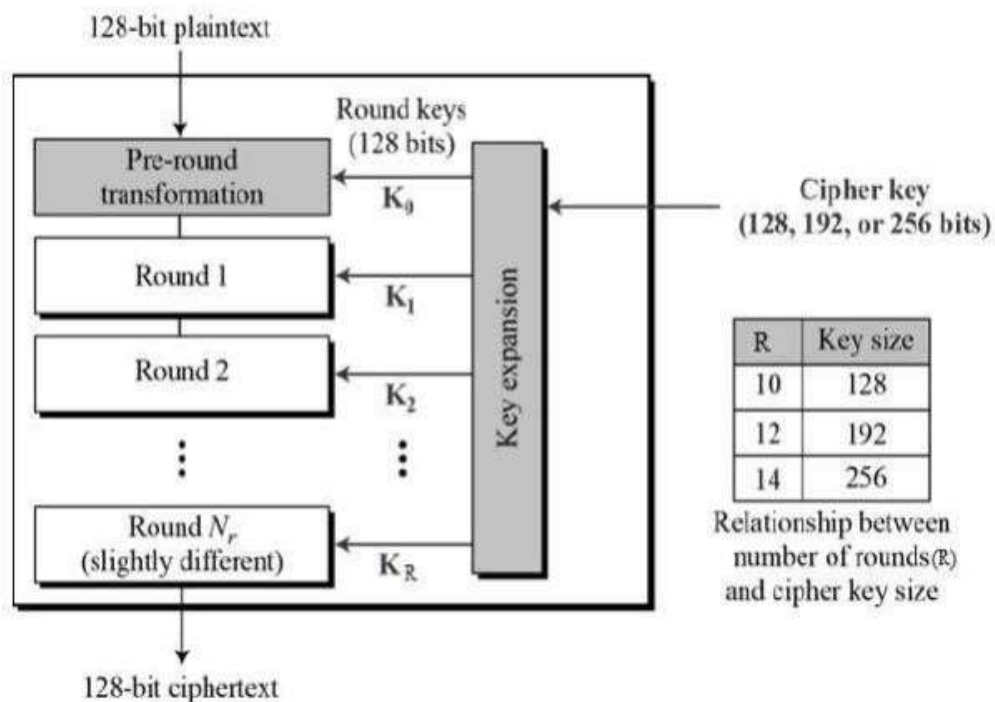
The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

The schematic of AES structure is given in the following illustration –





## Asymmetric Algorithm

### RSA Encryption and Decryption

RSA encrypts messages through the following algorithm, which is divided into 3 steps:

#### 1. Key Generation

I. Choose two distinct prime numbers  $p$  and  $q$ .

II. Find  $n$  such that  $n = pq$ .

$n$  will be used as the modulus for both the public and private keys.

III. Find the totient of  $n$ ,  $\phi(n) = (p-1)(q-1)$ .

IV. Choose an  $e$  such that  $1 < e < \phi(n)$ , and such that  $e$  and  $\phi(n)$  share no divisors other than 1 ( $e$  and  $\phi(n)$  are relatively prime).

$e$  is kept as the public key exponent.

V. Determine  $d$  (using modular arithmetic) which satisfies the congruence relation  $de \equiv 1 \pmod{\phi(n)}$ .

In other words, pick  $d$  such that  $de - 1$  can be evenly divided by  $(p-1)(q-1)$ , the totient, or  $\phi(n)$ .

This is often computed using the Extended Euclidean Algorithm, since  $e$  and  $\phi(n)$  are relatively prime and  $d$  is to be the modular multiplicative inverse of  $e$ .  $d$  is kept as the private key exponent.

The public key has modulus  $n$  and the public (or encryption) exponent  $e$ . The private key has modulus  $n$  and the private (or decryption) exponent  $d$ , which is kept secret.

#### 2. Encryption

I. Person A transmits his/her public key (modulus  $n$  and exponent  $e$ ) to Person B, keeping his/her private key secret.

II. When Person B wishes to send the message " $M$ " to Person A, he first converts  $M$  to an integer such that  $0 < m < n$  by using agreed upon reversible protocol known as a padding scheme.

III. Person B computes, with Person A's public key information, the ciphertext  $c$  corresponding



to

$$c \equiv me \pmod{n}.$$

IV. Person B now sends message "M" in ciphertext, or  $c$ , to Person A.

### 3. Decryption

I. Person A recovers  $m$  from  $c$  by using his/her private key exponent,  $d$ , by the computation  $m \equiv cd \pmod{n}$ .

II. Given  $m$ , Person A can recover the original message "M" by reversing the padding scheme.

This procedure works since  $c \equiv me \pmod{n}$ ,

$$cd \equiv (me)d \pmod{n}, cd \equiv mde \pmod{n}.$$

By the symmetry property of mods we have that  $mde \equiv mde \pmod{n}$ .

Since  $de = 1 + k\phi(n)$ , we can write  $mde \equiv m1 + k\phi(n) \pmod{n}$ ,

$$mde \equiv m(mk)\phi(n) \pmod{n}, mde \equiv m \pmod{n}.$$

From Euler's Theorem and the Chinese Remainder Theorem, we can show that this is true for all  $m$  and the original message

$$cd \equiv m \pmod{n}, \text{ is obtained.}$$

Generation of Asymmetric Key Pair

Algorithm

☒ RSA  
Bit length of RSA modulus: 1024

☐ DSA  
Bit length of DSA prime number: 1024

☐ Elliptic curves  
Identifier (bit length and curve parameter): prime239v1

User data

The key pair will be put in an encrypted PSE with the name shown below. The key pair will be protected by your PIN code.

Last name: Apeksha

First name: Mohite

Key identifier (optional): ATM

PIN: 000000

PIN verification: 000000

The domain parameter of the selected elliptic curve will be shown below.

Parameters	Value of the parameter	Bit len...
------------	------------------------	------------

Base for presentation of numbers

☐ Octal ☒ Decimal ☐ Hexadecimal

Generate new key pair... PKCS #12 Import Show key pair... Close



Generation of Asymmetric Key Pair

Algorithm

☒ RSA  
Bit length of RSA modulus: 1024

☐ DSA  
Bit length of DSA prime number: 1024

☐ Elliptic curves  
Identifier (bit length curve parameter):

User data

The key pair will be put in an encrypted PSE with the name shown below. The key pair will be protected by your PIN code.

Last name: Apeksha  
First name: Mohite  
Key identifier: ATM

The domain parameter of

Parameters Value of t

Base for presentation of numbers

☐ Octal ☒ Decimal ☐ Hexadecimal

Generate new key pair... PKCS #12 Import Show key pair... Close

**CrypTool**

The parameters chosen by you and the new key pair have been successfully saved.  
The assigned key identifier is '[Apeksha][Mohite][RSA-1024][1538614713][ATM]'.  
Elapsed time while creating key pair: 0.156 seconds.

OK

CrypTool 1.4.41 - startingexample-en

File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help

startingexample-en

HELLOWORLD

Selection of a key for RSA encryption of <startingexample-en>

Choose the recipient:

Last name	First name	Key type	Key identifier	Created	Internal ID no.
Mohite	Apeksha	RSA-1024	ATM	04.10.2018 09:22:53	1538614713
SideChannelAt...	Bob	RSA-512	PIN-1234	06.07.2006 15:21:34	1152179494

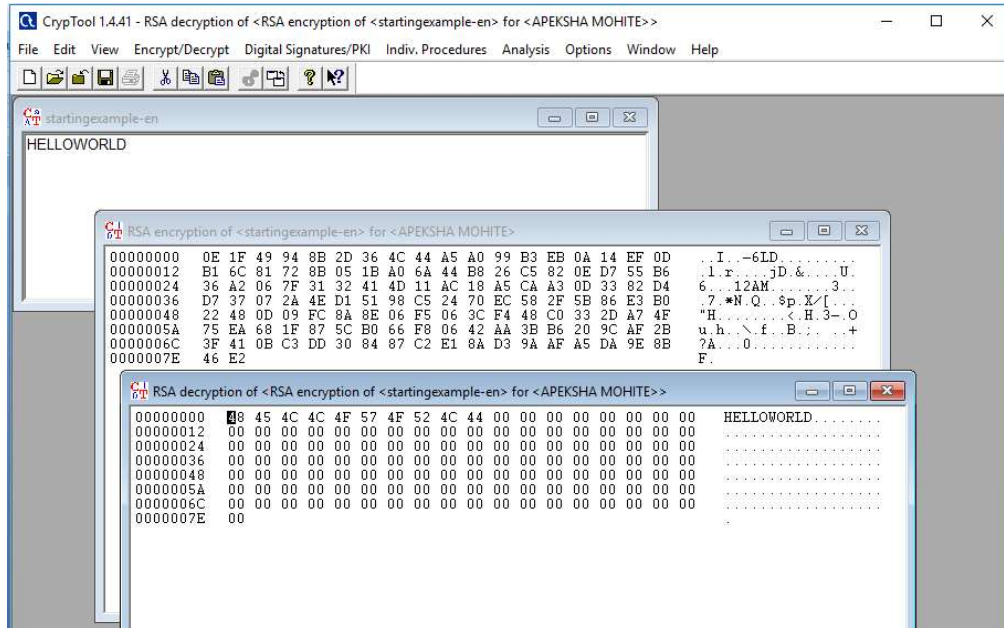
Note: Here only names are displayed, which have an RSA key.

☐ Display encryption time

Encrypt Cancel

Press F1 to obtain help.

L:1 C:6 P:6 CAP NUM



4. **Conclusion :** Thus we have implemented and studied various symmetric and asymmetric algorithms using CrypTool.