PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)

Academic Year: 2025-26 **Semester: V**

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

Subject Lab Incharge: Prof. Apeksha Mohite

Experiment No. 13 (i)

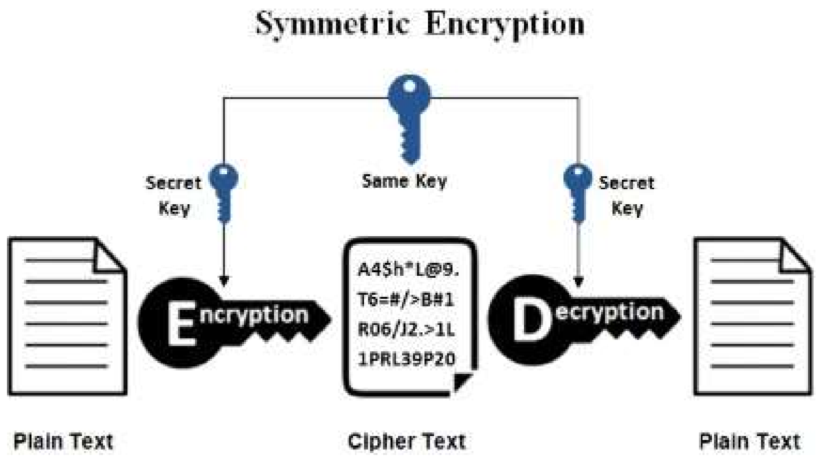
1. **Aim: To study symmetric and asymmetric encryption methods using Cryptool.**
2. **Software Required : CrypTool 1.4.41**
3. **Theory :**

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.

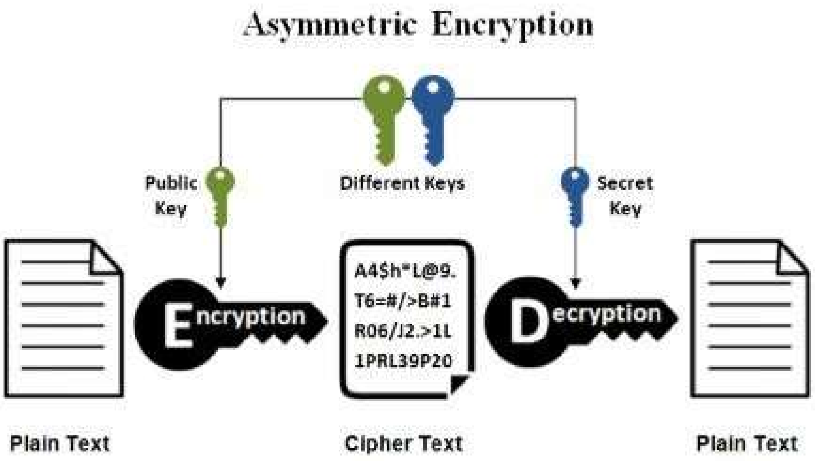
Cryptography is a method of using advanced mathematical principles in storing and transmitting data in a particular form so that only those whom it is intended can read and process it. Encryption is a key concept in cryptography – It is a process whereby a message is encoded in a format that cannot be 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

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.

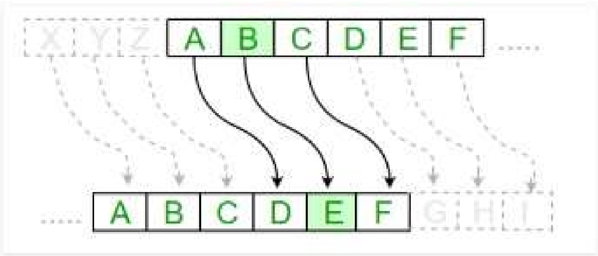
A message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key. Security of the public key is not required because it is publicly available and can be passed over the internet. Asymmetric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

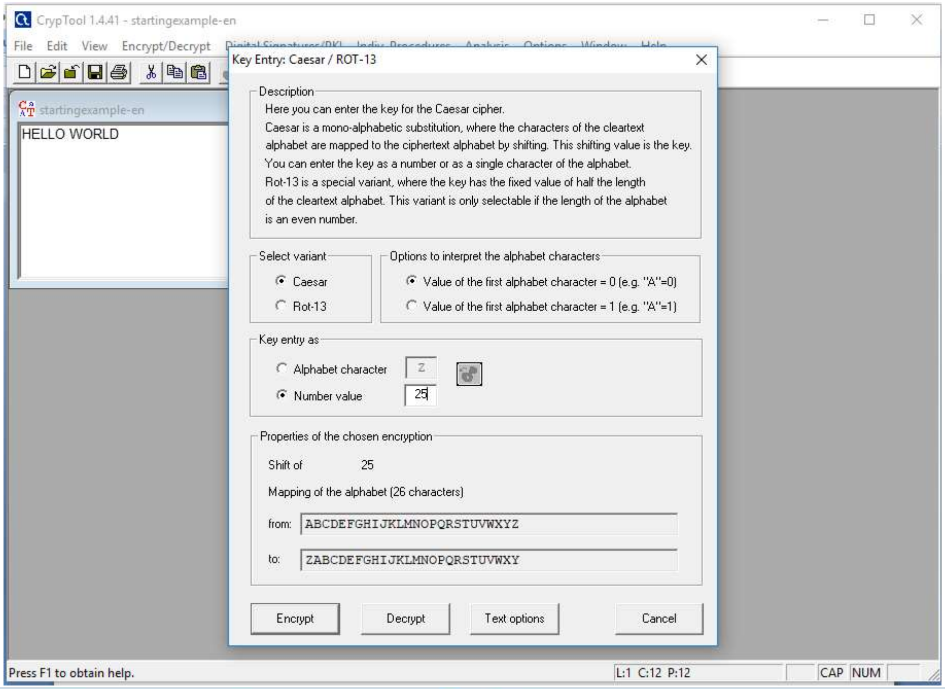
Asymmetric encryption is mostly used in day-to-day communication channels, especially over the Internet. Popular asymmetric key encryption algorithm includes EIGamal, RSA, DSA, Elliptic curve techniques.

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
Key Entry: Caesar / ROT-13
Encrypt
Decrypt
Text options
Cancel
Press F1 to obtain help.
L:1 C:12 P:12
CAP NUM

HELLO WORLD

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 Z
● Number value 25

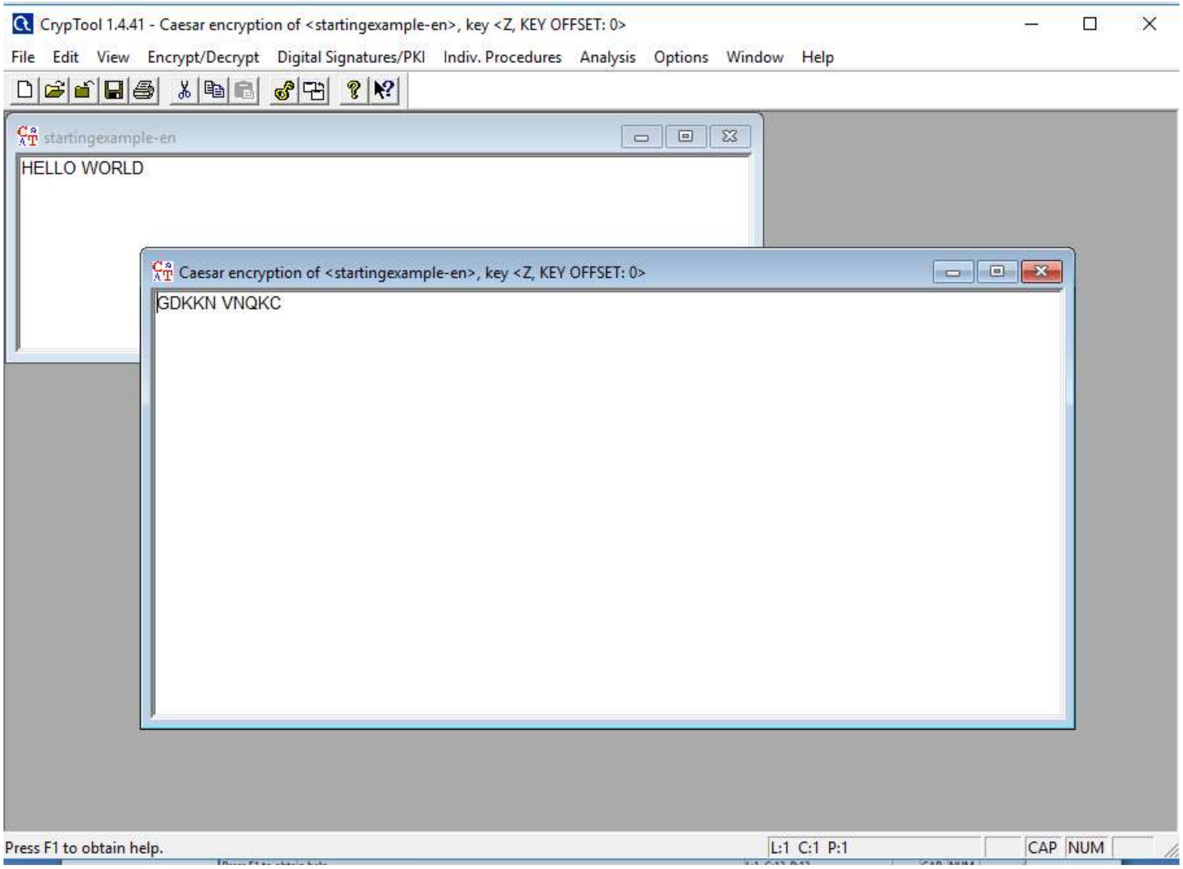
Properties of the chosen encryption

Shift of 25

Mapping of the alphabet (26 characters)

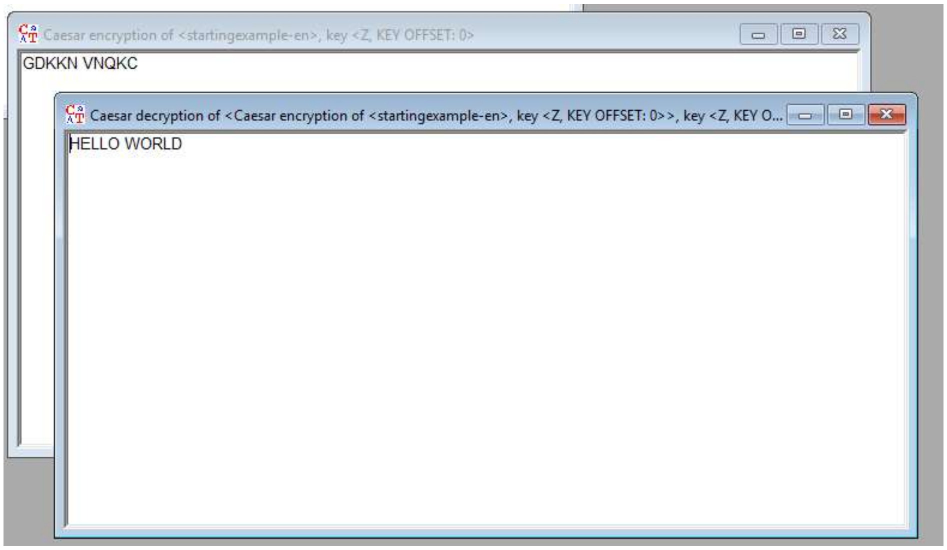
from: ABCDEFGHIJKLMNOPQRSTUVWXYZ

to: ZABCDEFGHIJKLMNOPQRSTUVWXY


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
Caesar encryption of <startingexample-en>, key <Z, KEY OFFSET: 0>
Press F1 to obtain help.
L:1 C:1 P:1
CAP NUM

HELLO WORLD

GDKKN VNQKC



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

```
GDKKN VNQKC
```

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

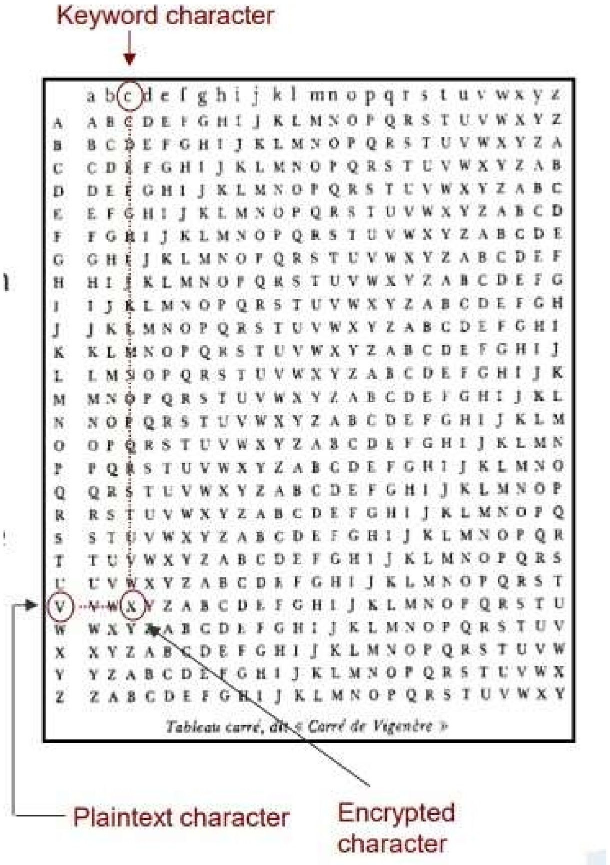
```
HELLO WORLD
```

Vigenère Cipher

Encryption with a keyword using a key table Example

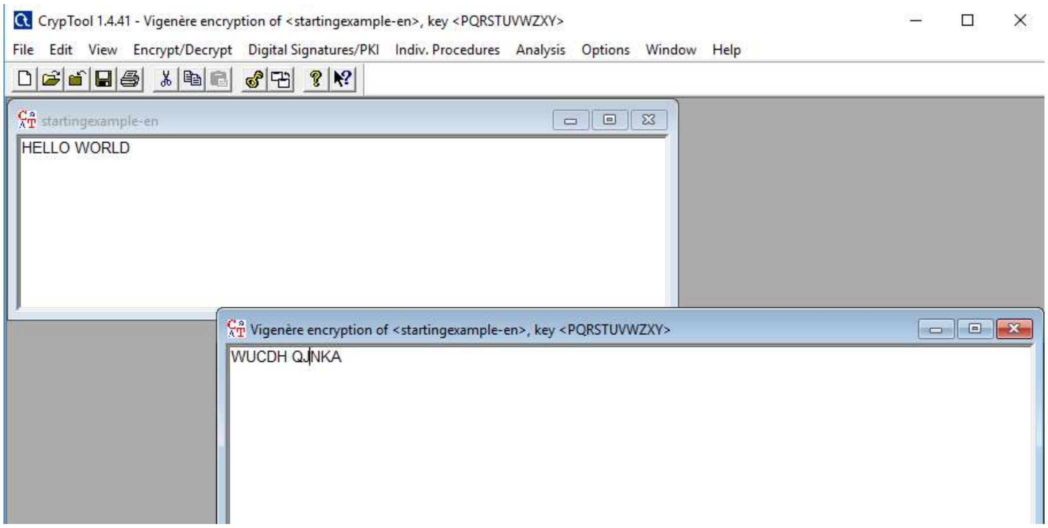
Keyword: CHIFFRE Encrypting: VIGENERE becomes XPOJSVVG

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.



	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Tableau carré, dit « Carré de Vigenère »



CrypTool 1.4.41 - Vigenère encryption of <startingexample-en>, key <PQRSTUVWZXY>

startingexample-en

HELLO WORLD

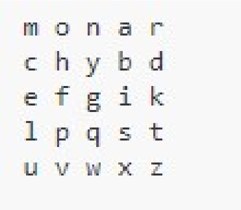
Vigenère encryption of <startingexample-en>, key <PQRSTUVWZXY>

WUCDH QJNKA

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.

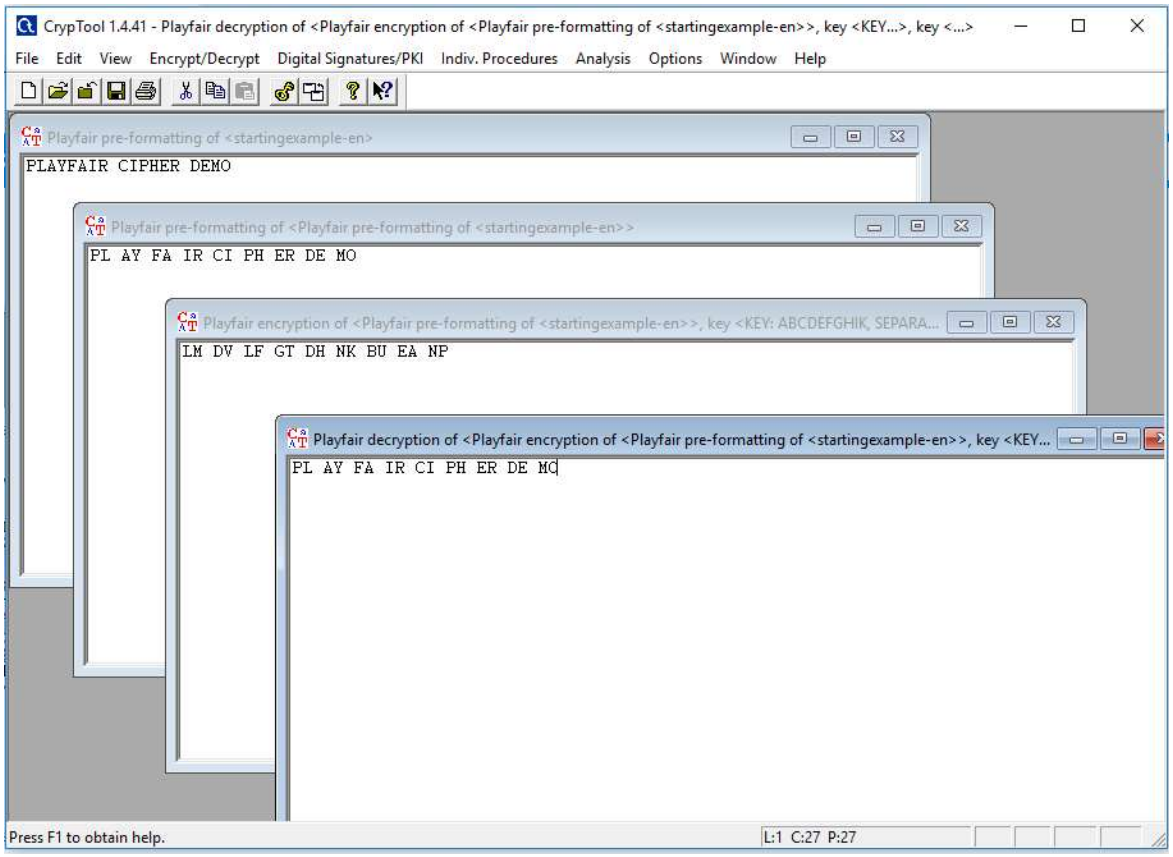


```
m o n a r
c h y b d
e f g i k
l p q s t
u v w x z
```

- 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 occurence 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'



CrypTool 1.4.41 - Playfair decryption of <Playfair encryption of <Playfair pre-formatting of <startingexample-en>>, key <KEY...>, key <...>

Playfair pre-formatting of <startingexample-en>

```
PLAYFAIR CIPHER DEMO
```

Playfair pre-formatting of <Playfair pre-formatting of <startingexample-en>>

```
PL AY FA IR CI PH ER DE MO
```

Playfair encryption of <Playfair pre-formatting of <startingexample-en>>, key <KEY: ABCDEFGHIK, SEPARA...

```
LM DV LF GT DH NK BU EA NP
```

Playfair decryption of <Playfair encryption of <Playfair pre-formatting of <startingexample-en>>, key <KEY...

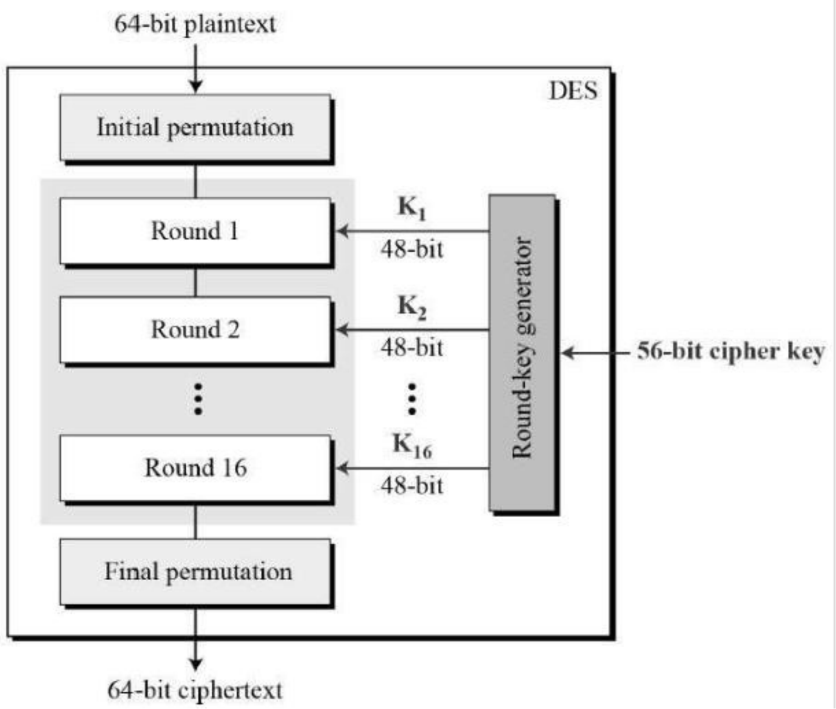
```
PL AY FA IR CI PH ER DE MO
```

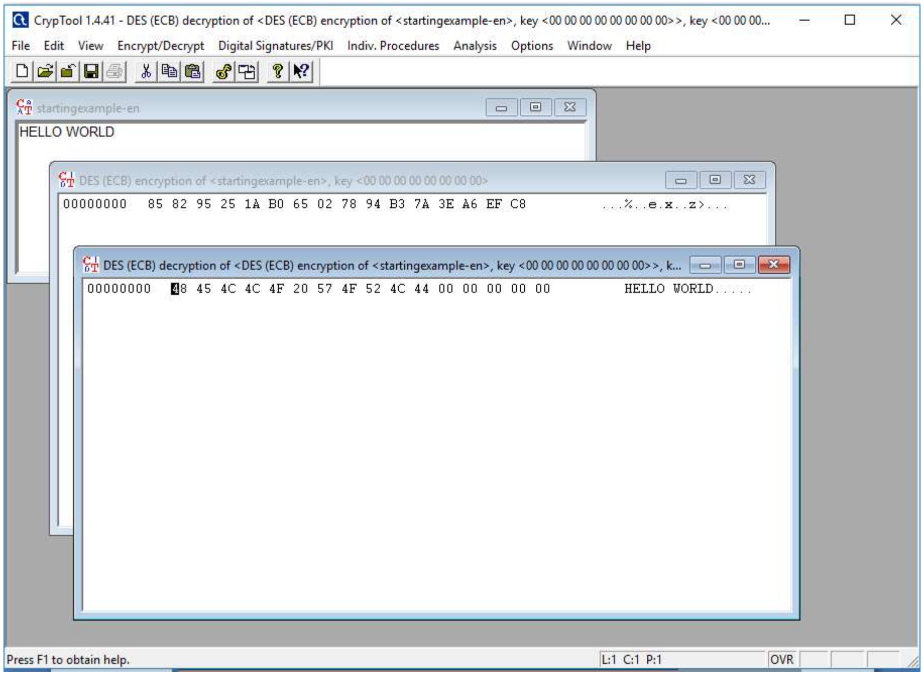
Press F1 to obtain help.
L:1 C:27 P:27

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 −




File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Press F1 to obtain help.
L:1 C:1 P:1
OVR

CrypTool 1.4.41 - DES (ECB) decryption of <DES (ECB) encryption of <startingexample-en>, key <00 00 00 00 00 00 00 00>>, key <00 00 00...

startingexample-en

HELLO WORLD

DES (ECB) encryption of <startingexample-en>, key <00 00 00 00 00 00 00 00>

```
00000000   85 82 95 25 1A B0 65 02 78 94 B3 7A 3E A6 EF C8        ...%..e.x..z>...
```

DES (ECB) decryption of <DES (ECB) encryption of <startingexample-en>, key <00 00 00 00 00 00 00 00>>, k...

```
00000000   48 45 4C 4C 4F 20 57 4F 52 4C 44 00 00 00 00 00        HELLO WORLD.....
```

Advanced Encryption Standard

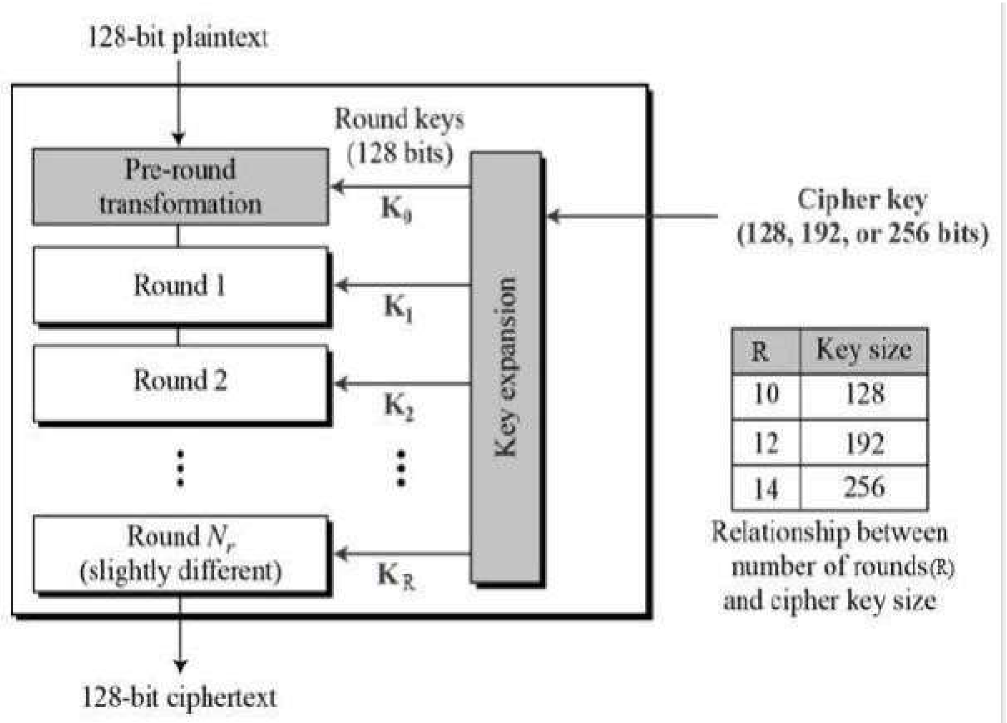
The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

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 –



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

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, $\phi(n)$ $\phi(n)=(p-1)(q-1)$.

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 ≡ me (mod 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 ≡ cd (mod n).

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

This procedure works since c ≡ me (mod n),

cd ≡(me)d (mod n), cd ≡ mde (mod n).

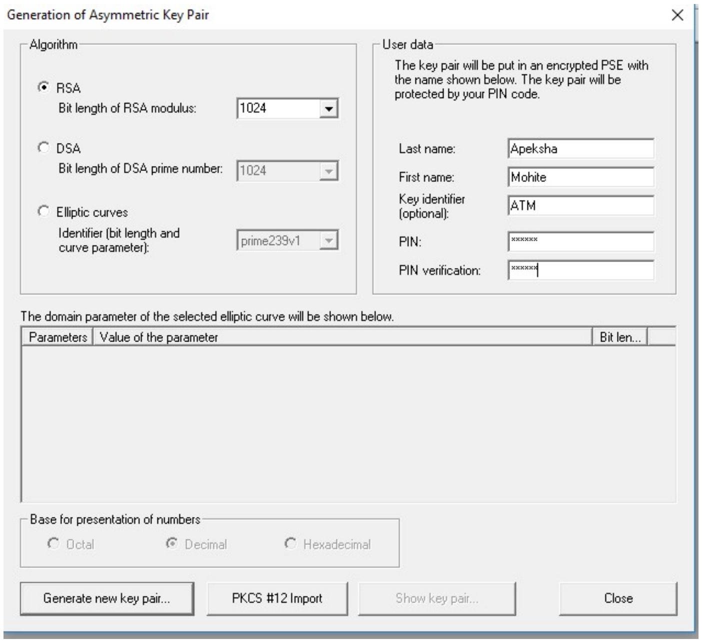
By the symmetry property of mods we have that mde ≡ mde (mod n).

Since de = 1 + kϕ(n), we can write mde ≡ m1 + kϕ(n) (mod n),

mde ≡ m(mk)ϕ(n) (mod n), mde ≡ m (mod 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 ≡ m (mod n), 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.

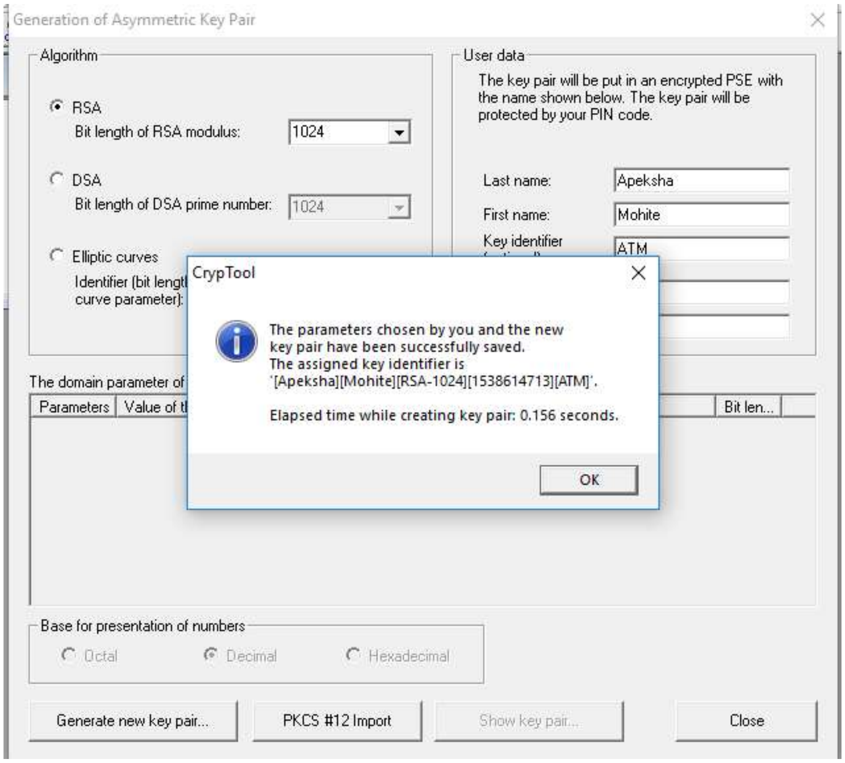
Last name:	Apeksha
First name:	Mohite
Key identifier (optional):	ATM
PIN:	******
PIN verification:	******

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



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

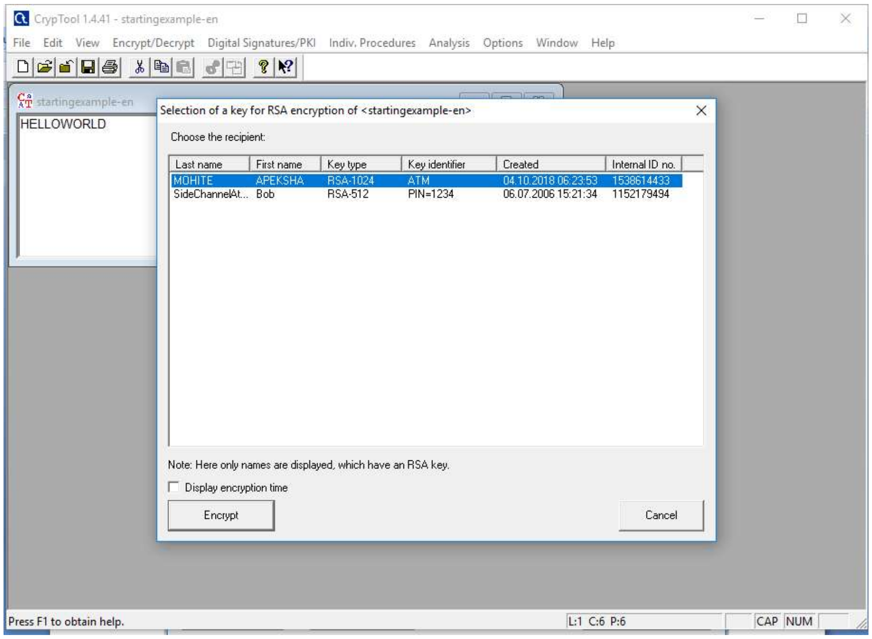
First name: Mohite

Key identifier: ATM

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.



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>

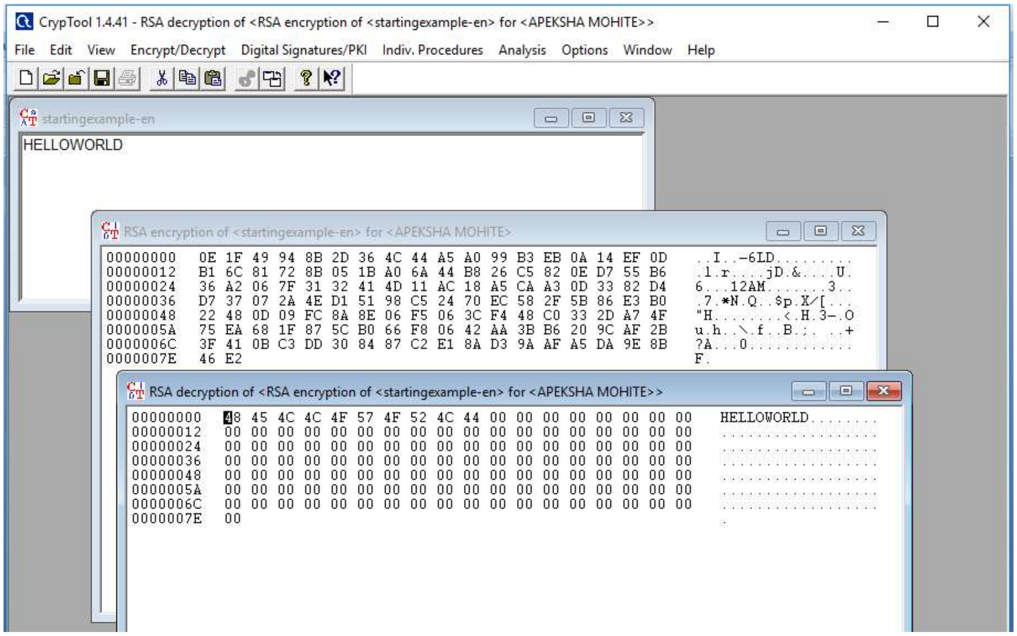
Choose the recipient:

Last name	First name	Key type	Key identifier	Created	Internal ID no.
MOHITE	APEKSHA	RSA-1024	ATM	04.10.2018 06:23:53	1538614433
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


CrypTool 1.4.41 - RSA decryption of <RSA encryption of <startingexample-en> for <APEKSHA MOHITE>>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help

startingexample-en

HELLOWORLD

RSA encryption of <startingexample-en> for <APEKSHA MOHITE>

```
00000000   0E 1F 49 94 8B 2D 36 4C 44 A5 A0 99 B3 EB 0A 14 EF 0D   ..I..-6LD.........
00000012   B1 6C 81 72 8B 05 1B A0 6A 44 B8 26 C5 82 0E D7 55 B6   .l.r....jD.&....U.
00000024   36 A2 06 7F 31 32 41 4D 11 AC 18 A5 CA A3 0D 33 82 D4   6...12AM.......3..
00000036   D7 37 07 2A 4E D1 51 98 C5 24 70 EC 58 2F 5B 86 E3 B0   .7.*N.Q..$p.X/[...
00000048   22 48 0D 09 FC 8A 8E 06 F5 06 3C F4 48 C0 33 2D A7 4F   "H.......<.H.3-.O
0000005A   75 EA 68 1F 87 5C B0 66 F8 06 42 AA 3B B6 20 9C AF 2B   u.h..\.f..B.;. ..+
0000006C   3F 41 0B C3 DD 30 84 87 C2 E1 8A D3 9A AF A5 DA 9E 8B   ?A...0............
0000007E   46 E2                                                   F.
```

RSA decryption of <RSA encryption of <startingexample-en> for <APEKSHA MOHITE>>

```
00000000   48 45 4C 4C 4F 57 4F 52 4C 44 00 00 00 00 00 00 00 00   HELLOWORLD........
00000012   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ..................
00000024   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ..................
00000036   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ..................
00000048   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ..................
0000005A   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ..................
0000006C   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ..................
0000007E   00                                                      .
```

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