Overview of Cryptography

PKI Outreach Programme (POP)

Nationwide Awareness Programme,
Centre for Development of Advanced Computing (C-DAC)
Electronics City, Bangalore.

Agenda

- **Introduction to Cryptography**
  - Substitution Ciphers, Transposition Ciphers
- **Hash Functions**
- **Symmetric Key Cryptography**
- **Asymmetric key Cryptography**

What is Information security?

- General definition: Information security involves providing appropriate levels of assurance of

Privacy/Confidentiality: preventing disclosure of information to unauthorized individuals or systems

Authenticity: Ensuring that the user, data, transactions, communications or documents are genuine

Integrity : Data cannot be modified without authorization

Non-Repudiability: One party of a transaction can not deny having sent/received a transaction

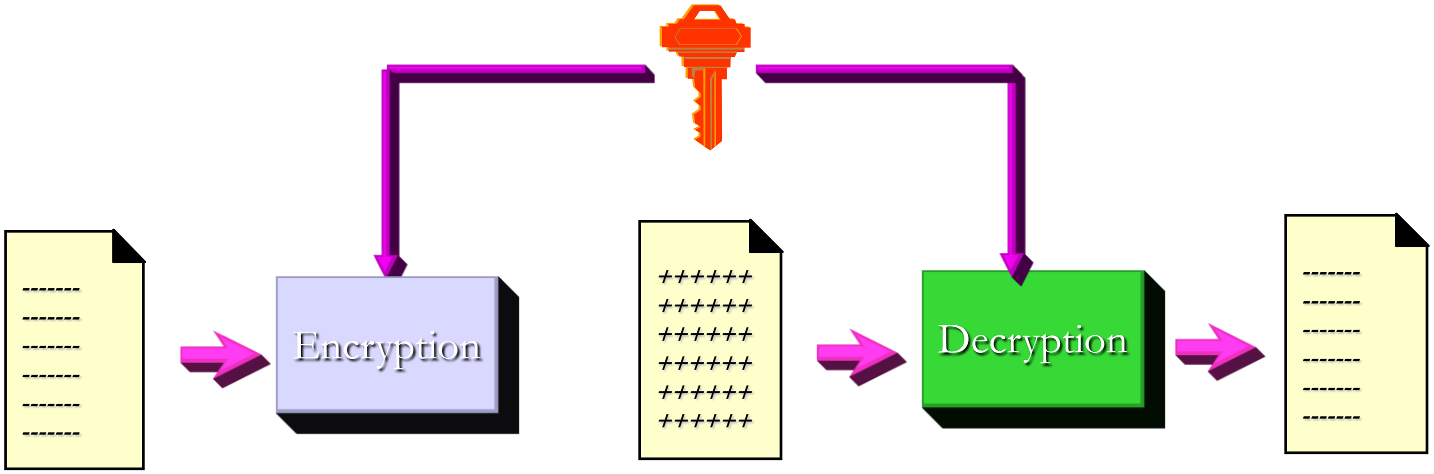
Cryptography

- The study & practice of hiding, encrypting or secret writing;
- It uses mathematical & logical principles to secure information
  - **Plaintext:** The message which has to be sent to other party.
  - **Encryption / Decryption**: The process of transforming plain text input to an un-interpretable form is called Encryption. Decryption is reverse of Encryption. Therefore, this is a two-way function.

Cryptography …

- **Cipher text:** The message after it is encoded
- **Key**. This is a unique value (bit pattern, alphabetical sequence) that is used by the cipher for encryption/decryption
- The Cryptosystems are broadly classified into two:
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography

Encryption / Decryption



“The quick
brown fox
jumps over
the lazy dog”

“AxCv;5bmEseTfid3)fG
smWe#4^,sdgfMwir3:d
kJeTsY8R\s@!q3%”

“The quick
brown fox
jumps over
the lazy dog”

History

- Cryptography is quite old – at least about 4000 years.
- Ancient Egyptians use Symbols to represent things, an early form of writing (1900 BC)
- 1500 BC The Phoenicians developed an alphabet
- 600 BC Palestinians use the Atbash cipher
- 500 BC The Spartans use the encryption process Scytale

History Contd…

- In 50 BC, Julius Caesar used an alphabet with a shift of three and hence named as Caesar cipher.
- Blaise de Vigenère discussed Vigenere cipher in 1585 AD
- 1917 AD American, Gilbert S. Vernam, develops the One-time-pad
- 1976 AD Diffie-Hellman key exchange protocol is developed
- 1977 AD DES is developed by IBM
- 1977 RSA is developed, this method is still widely used today
- 2000 AD AES is chosen as the successor to DES

Hiding Message

Have you ever wanted to hide something from:

- Your friends?
- Your family?
- The Government?

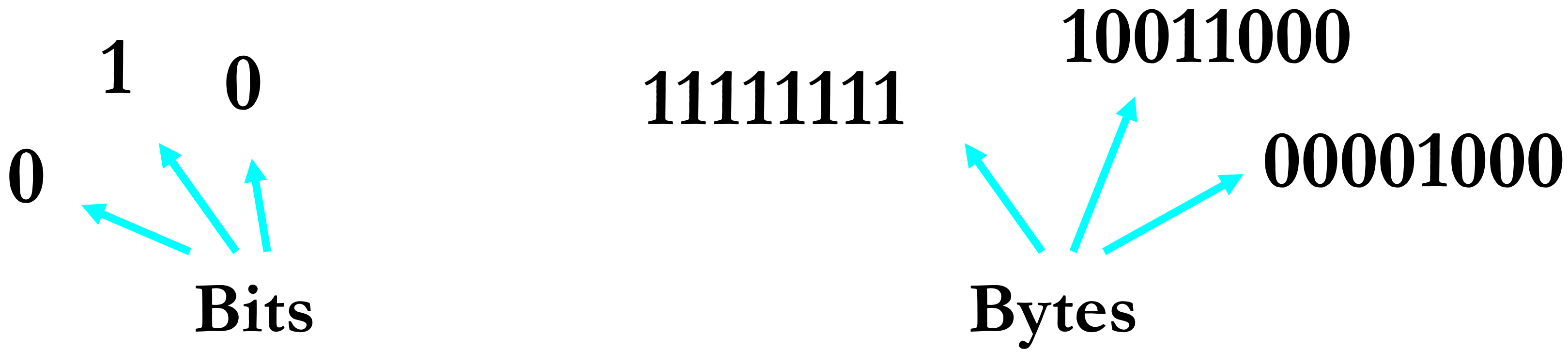
Ancient Steganography

ϹΟΦΟΥΠΑΡΑΝΔΡΟϹΠΡΟϹΔΕΧΟΥϹΥΜΒΟΥΛΙΑΝ
ΜΗΠΑϹΙΝΕΙΚΗΤΟΙϹΦΙΛΟΙϹΠΙϹΤΕΥΕΤΑΙ

ΟΦΟΥΠΑΡΑΝΔΡΟϹΠΡΟϹΔΕΧΟΥϹΥΜΒΟΥΛΙΑΝ
ΜΗΠΑϹΙΝΕΙΚΗΤΟΙϹΦΙΛΟΙϹΠΙϹΤΕΥΕΤΑΙ
ΟΦΟΥΠΑΡΑΝΔΡΟϹΠΡΟϹΔΕΧΟΥϹΥΜΒΟΥΛΙΑΝ
ΜΗΠΑϹΙΝΕΙΚΗΤΟΙϹΦΙΛΟΙϹΠΙϹΤΕΥΕΤΑΙ

One hiding method was to engrave a message in a block of wood, then cover it with wax, so it looked like a blank wax tablet. When they wanted to retrieve the message,
they would simply melt off the wax.

Digital Steganography



1 0

0

Bits

11111111

10011000

00001000

Bytes

One byte can be used to represent each letter of the alphabet. This is what is used in text files.

01000001 = A

01000010 = B

01000011 = C

Colour Image Pixels

11111000 11001001 00000011

248 201 3

Each byte is interpreted as a number, which is how much of that color is used to make the final color of the pixel.

248 + 201 + 3 = Orange Color

Eg: Digital Steganography

Message: A **01000001**

Image with 3 pixels: 🟨🟨🟨

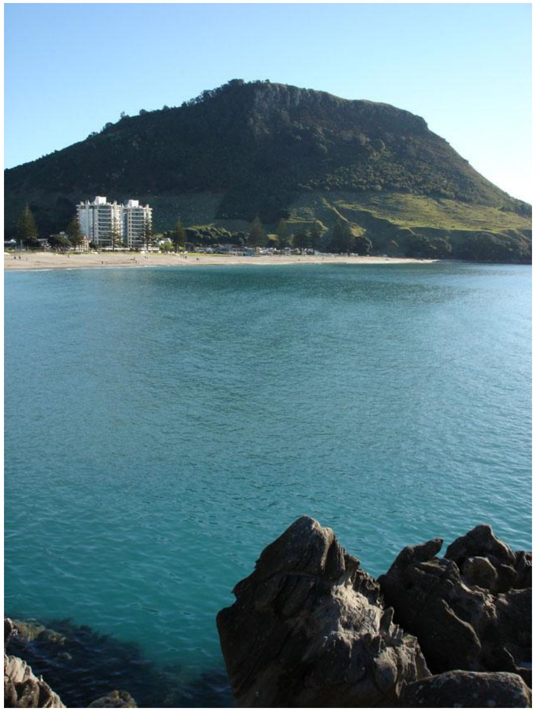
Pixel 1:	11111000	11001001	00000011
Pixel 2:	11111000	11001001	00000011
Pixel 3:	11111000	11001001	00000011

Now we hide our message in the image:

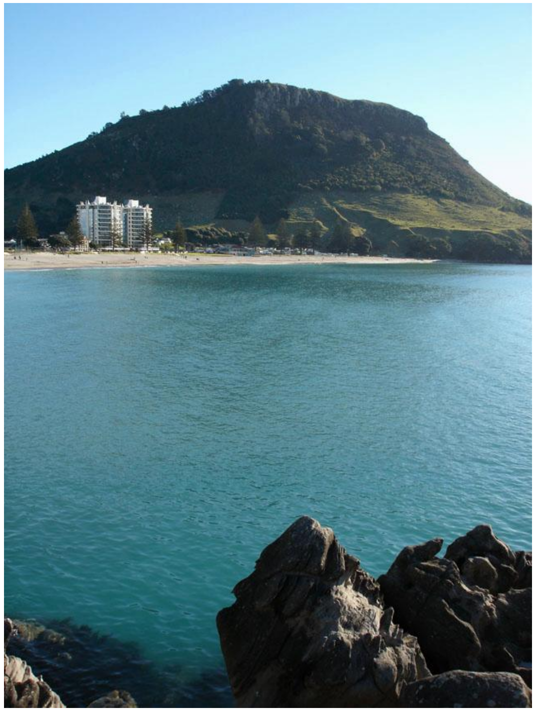
Pixel 1:	11111000	11001001	00000010
Pixel 2:	11111000	11001000	00000010
Pixel 3:	11111000	11001001	00000011

New image: 🟨🟨🟨

Eg: Digital Steganography



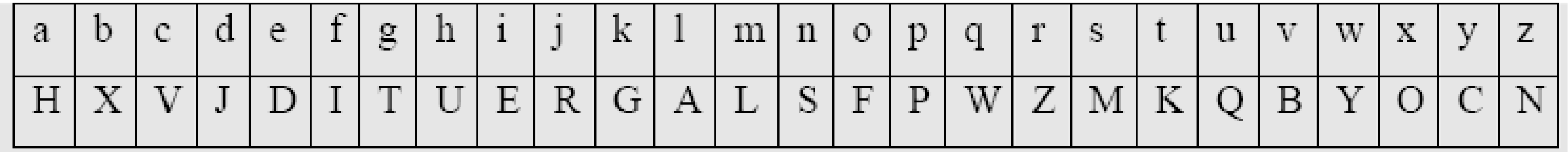
Original



With Hidden Message

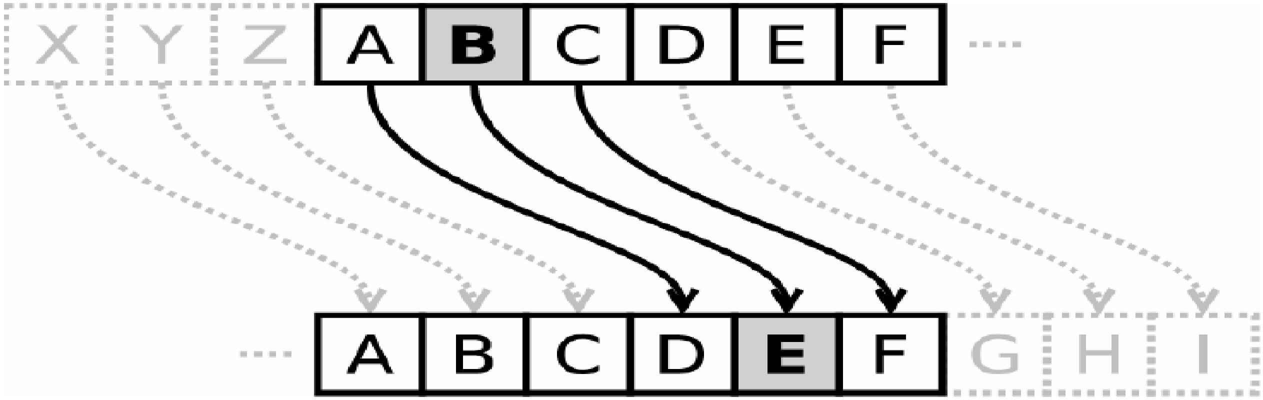
Substitution Ciphers

- Here each character is simply represented by another 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
H	X	V	J	D	I	T	U	E	R	G	A	L	S	F	P	W	Z	M	K	Q	B	Y	O	C	N

- In its simplest form there is no logic in order of representation.
- A type of substitution cipher is Caesar Cipher (Shift cipher) where each character in cipher text is shifted by 'k' letters.



Eg: Caesar Ciphers

KRISHNA → nulvkqd ….. obvious

Shift by k letters (here k = 3)

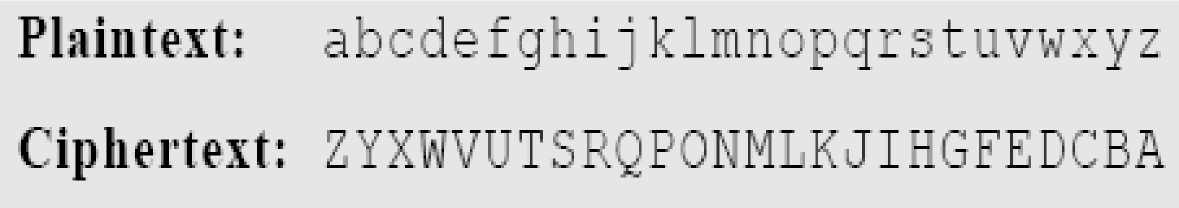
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Shift by k letters (here k = 6)

KRISHNA → qxoyntg … still obvious(?!)

Atbash

This cipher simply represents letters of the alphabet in reverse order: Eg:



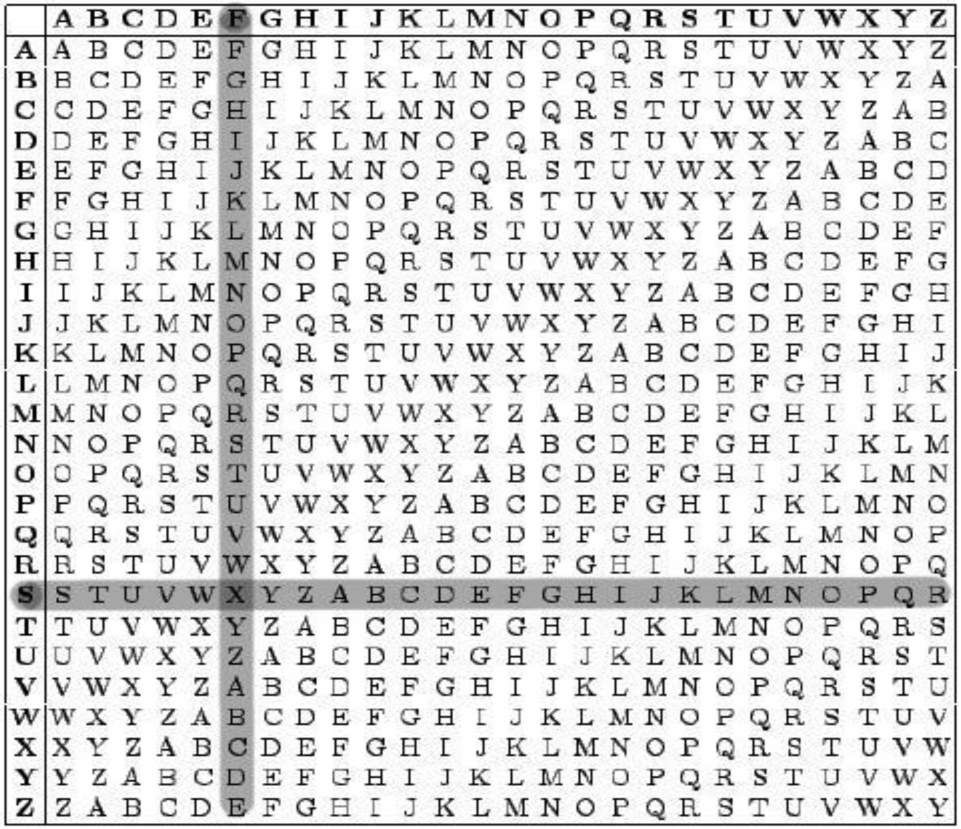
Plaintext:	abcdefghijklmnopqrstuvwxyz
Ciphertext:	ZYXWVUTSRQPONMLKJIHGFEDCBA

Vigenère cipher

- Encryption process combines one character of plain text and corresponding character of Key to get a character of cipher text from Vigenere Square
- Eg: Text: SQUARE

  Key: FROGFR

Cipher Text: XHIGWV



	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

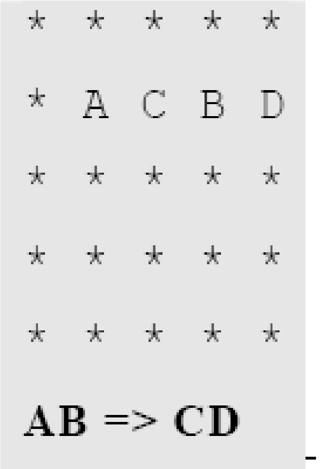
Playfair Cipher

- Makes use of diagrams and comprises of several small steps
  - **Key:** Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months
    - TREAYOUPSWDLIKHBNGVXMCFQZ
- Plain Text: “Information is not knowledge”

  “IN FO RM AT IO NI SN OT KN OW LE DG EX”

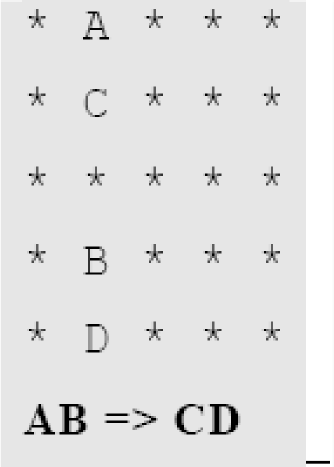
T	R	E	A	Y
O	U	P	S	W
D	L	I	K	H
B	N	G	V	X
M	C	F	Q	Z

- Cipher Text: LG MP TC YR DP GL UV DO LV UO IR IB YG
- “Information is not knowledge”
- = lgmptcyrdpgluvdolvuoiribyg



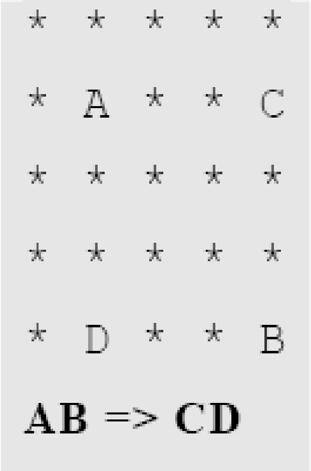
*	*	*	*	*
*	A	C	B	D
*	*	*	*	*
*	*	*	*	*
*	*	*	*	*

AB => CD



*	A	*	*	*
*	C	*	*	*
*	*	*	*	*
*	B	*	*	*
*	D	*	*	*

AB => CD



*	*	*	*	*
*	A	*	*	C
*	*	*	*	*
*	*	*	*	*
*	D	*	*	B

AB => CD

Transposition Ciphers

- Here the order of the character is changed

Rail Fence Cipher *(Capture fox)*

Cipher Text

C P U E O
 A T R F X

CPUEOATRFX

Route Cipher *(We are discovered Flee at once)*

Cipher Text

W R I O R F E O E
E E S V E L A N J
A D C E D E T C X

EJXCTEDECDAEWRIORFEONALEVSE

Columnar Transposition *(Deposit Four Crore Rupees in our Citi Bank Account)*

K R I S H N A -- Key
D E P O S I T
F O U R C R O
R E R U P E E
S I N O U R C
I T I B A N K
A C C O U N T

Cipher Text

TOECKTSCPUAUPURNICDFRSIAIRERNNEOEITCORUOBO

Hash Function

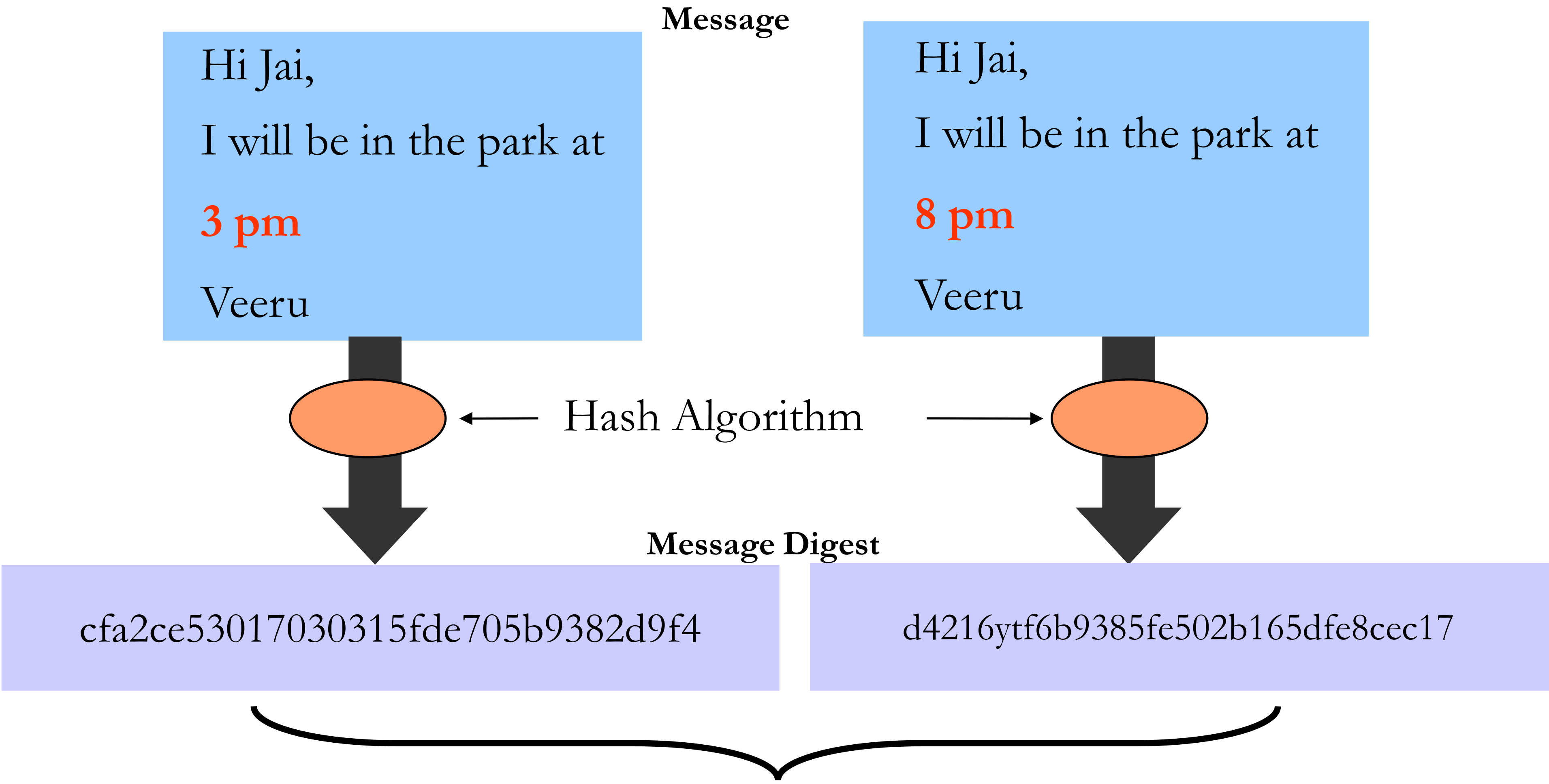
- A hash function is a cryptographic mechanism that operates as one-way function
  - Creates a digital representation or "fingerprint“ (Message Digest)
  - Fixed size output
  - Change to a message produces different digest

Examples : MD5 , Secure Hashing Algorithm (SHA)

Hash function -Properties

- **Consistency**
  - Same input must produce the same message digest. No randomness
- **Uniqueness**
  - Computationally infeasible to identify two messages that will generate the same message digest
- **One way**
  - Computationally infeasible to identify the input given the message digest

Hash - Example



Message

Hi Jai,

I will be in the park at

3 pm

Veeru

Hi Jai,

I will be in the park at

8 pm

Veeru

Hash Algorithm

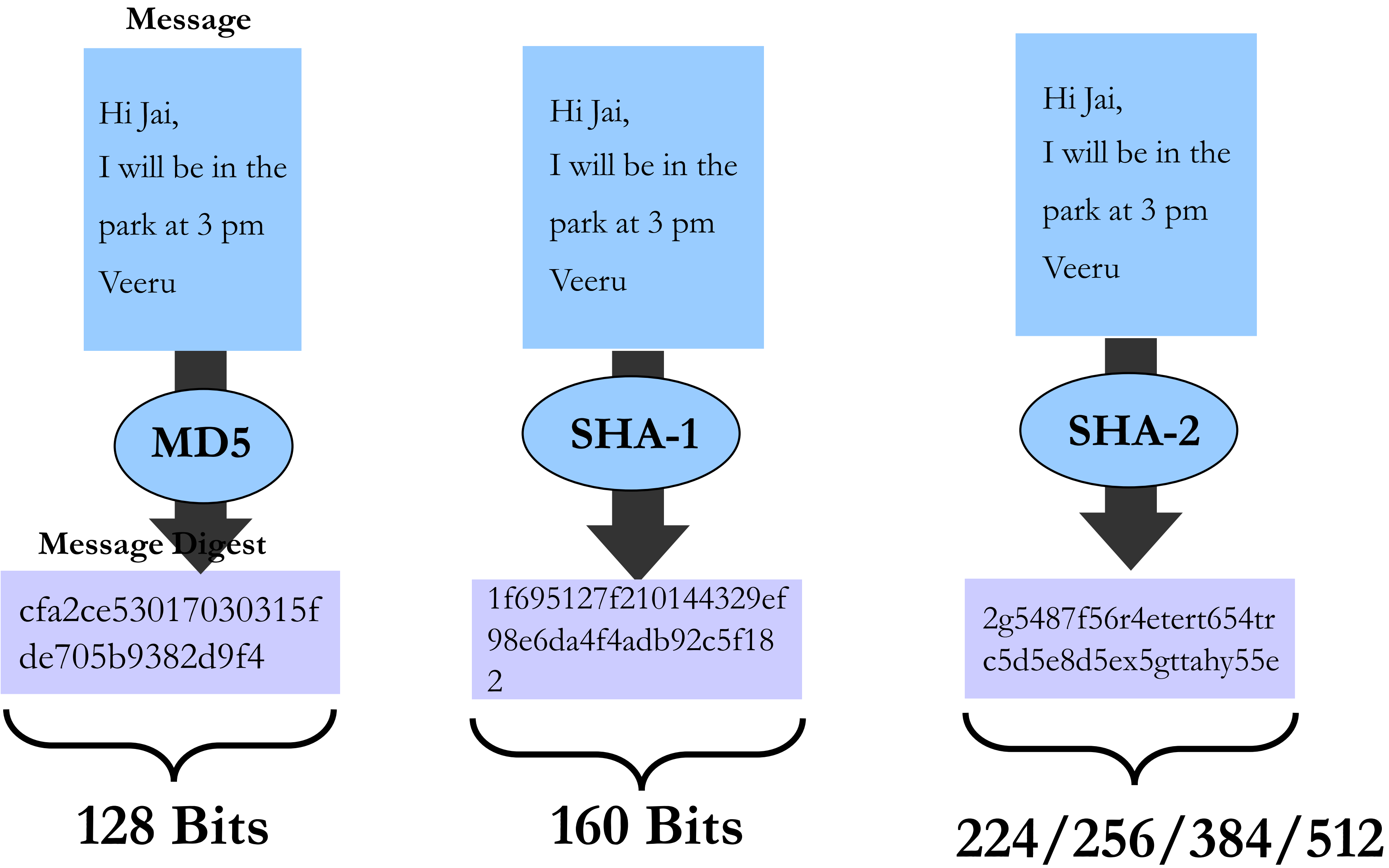
Message Digest

cfa2ce53017030315fde705b9382d9f4

d4216ytf6b9385fe502b165dfe8cec17

Digests are Different

MD5 and SHA



Message

Hi Jai,
I will be in the
park at 3 pm
Veeru

MD5

Message Digest

cfa2ce53017030315f
de705b9382d9f4

128 Bits

Hi Jai,
I will be in the
park at 3 pm
Veeru

SHA-1

1f695127f210144329ef
98e6da4f4adb92c5f18
2

160 Bits

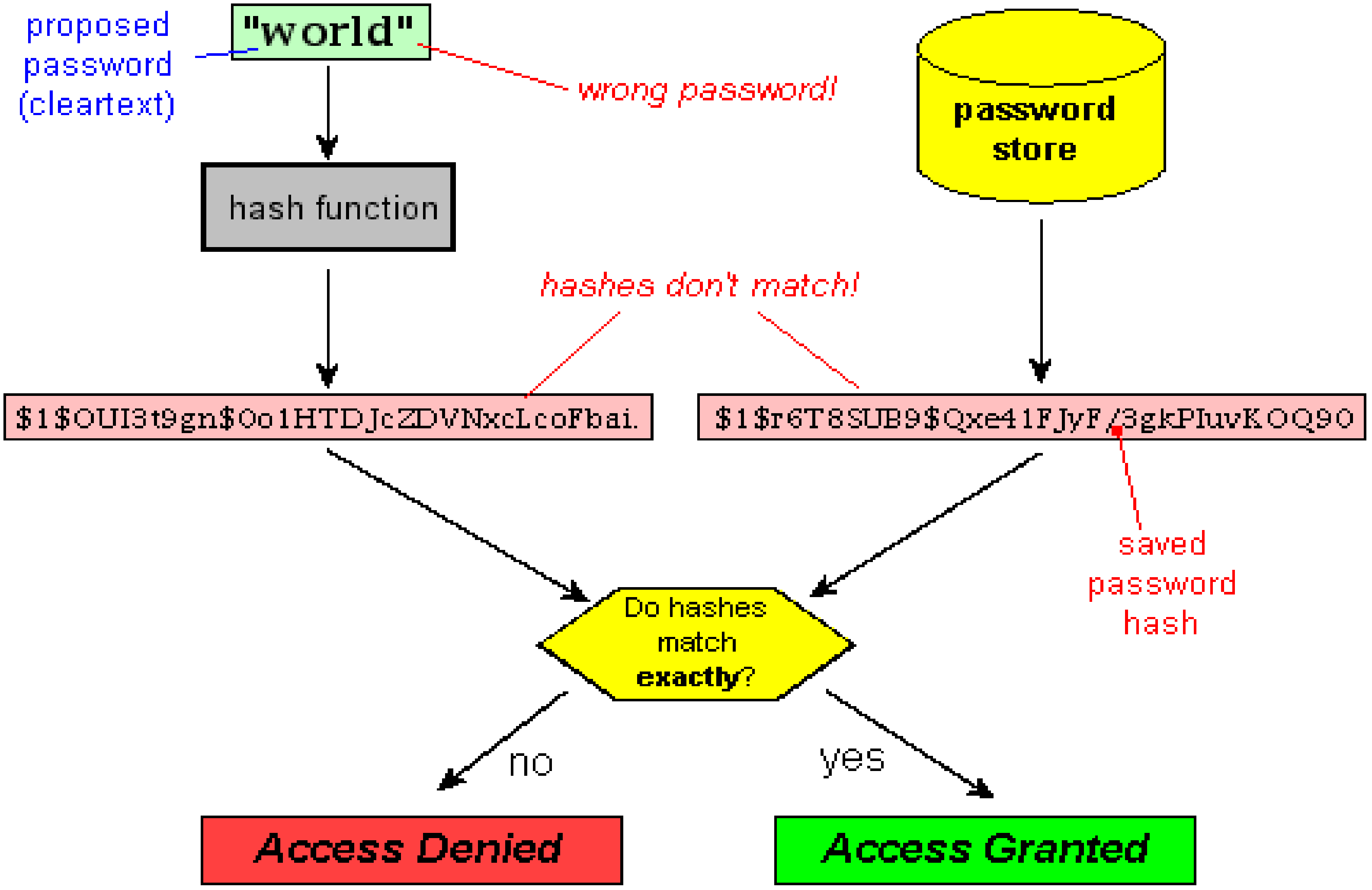
Hi Jai,
I will be in the
park at 3 pm
Veeru

SHA-2

2g5487f56r4etert654tr
c5d5e8d5ex5gttahy55e

224/256/384/512

Example of Hash functions

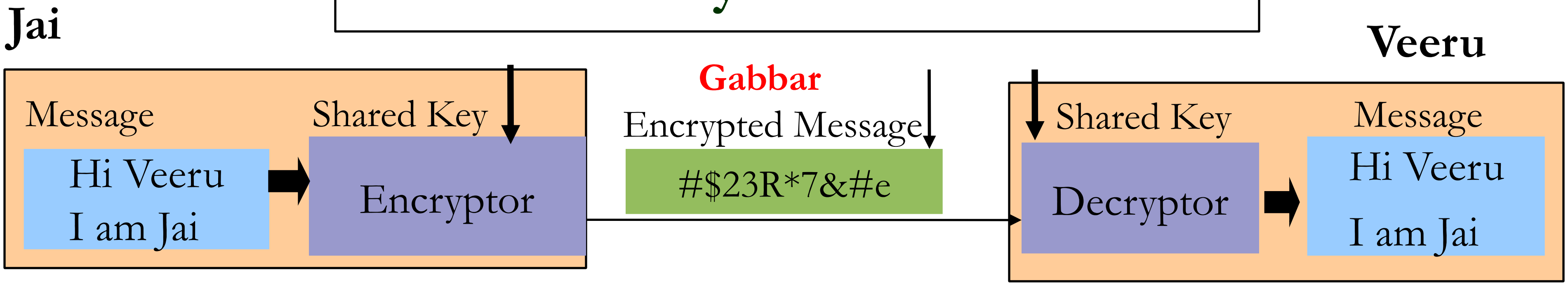


Symmetric Key Cryptography

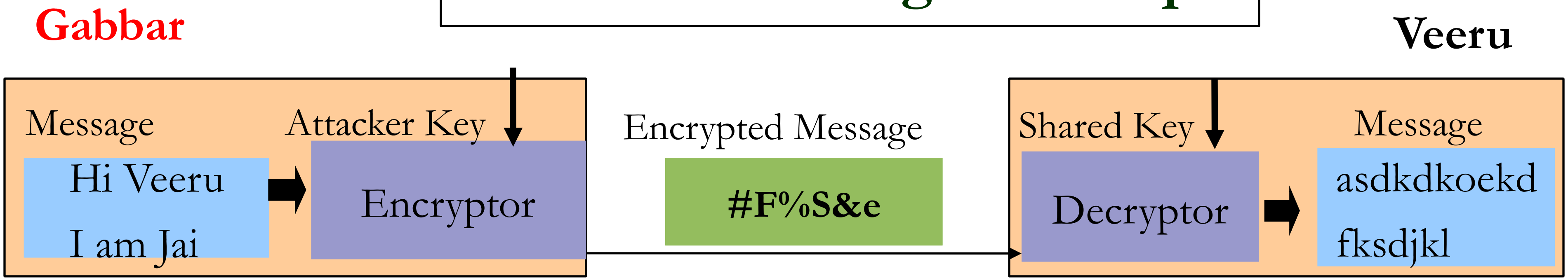
- Also called as Secret Key Cryptography or Single Key Cryptography.
- Uses one key shared by both sender and receiver.
- This key is used for both encryption and decryption.
- Both parties have to agree on the key before start of the communication
- Encryption and Decryption is extremely fast comparing to asymmetric cryptography

Symmetric Key Cryptography

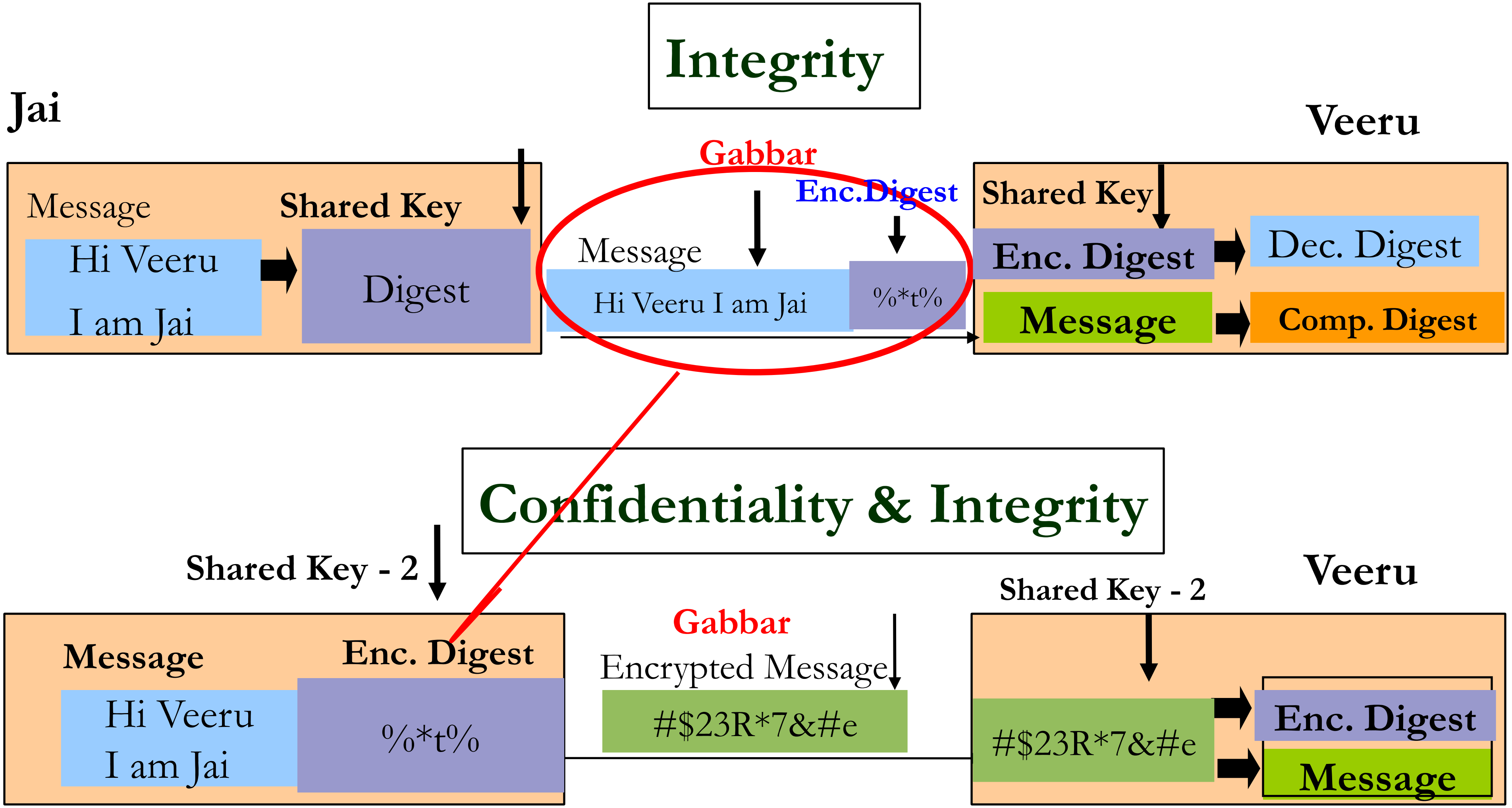
Confidentiality & Authentication



Unauthorized Login Attempt



Symmetric Key Cryptography



Symmetric Key Cryptography

Issues:

- Jai and Veeru must agree on the secret key without anyone else finding out
- Compromise of shared key leads to compromise of communication
- Secure Key Distribution and Scaling

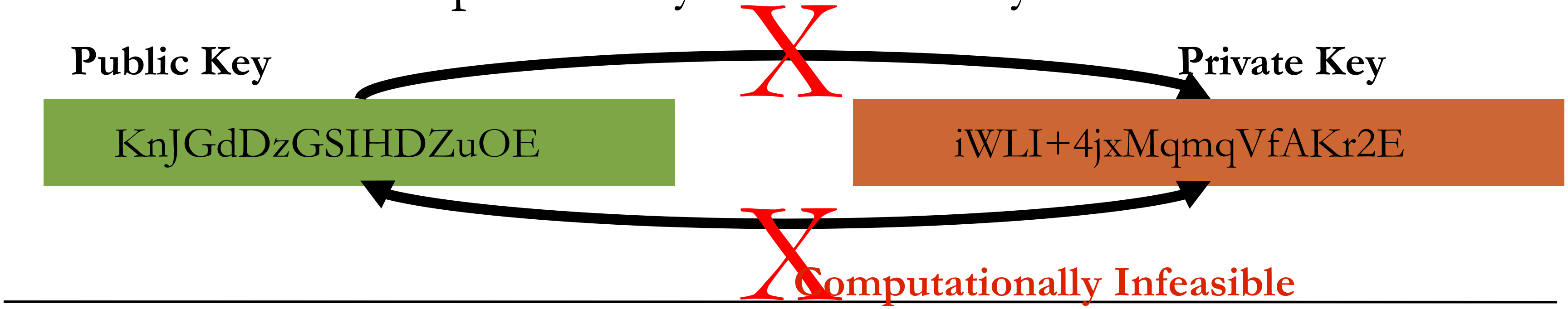
What can be achieved using Symmetric Key ?

- Confidentiality
- Integrity
- Authentication

What about Non-repudiation ?

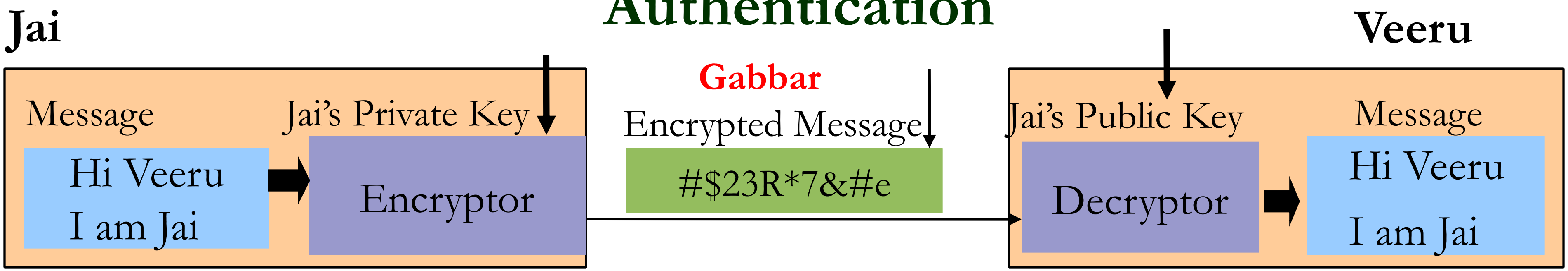
Asymmetric Key Cryptography

- Also called as Public Key Cryptography
- Uses a related key pair wherein one is Private key and another is Public key
  - One for encryption, another for decryption
- Knowledge of the *encryption* key doesn't give you knowledge of the *decryption* key
- A tool generates a related key pair (public & private key)
  - Publish the public key in a directory



Asymmetric Key Cryptography

Authentication



Jai

Veeru

Message

Jai's Private Key

Hi Veeru

I am Jai

Encryptor

Gabbar

Encrypted Message

#$23R*7&#e

Jai's Public Key

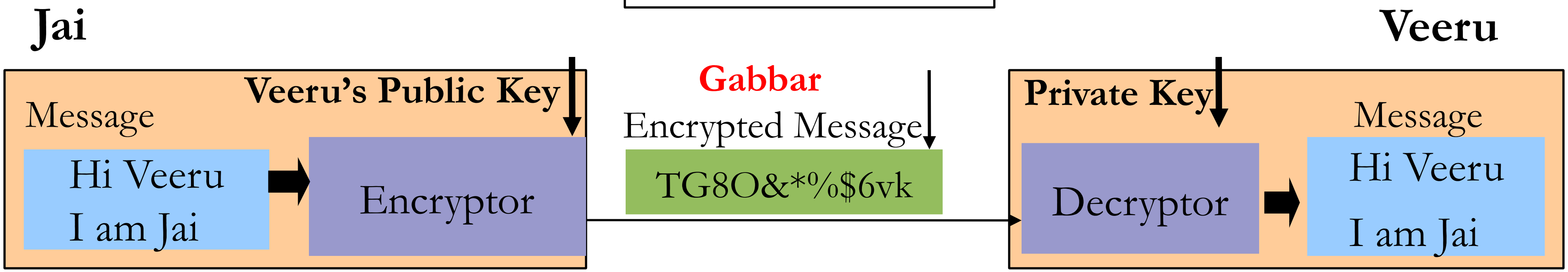
Message

Decryptor

Hi Veeru

I am Jai

Encryption



Jai

Veeru

Veeru's Public Key

Message

Hi Veeru

I am Jai

Encryptor

Gabbar

Encrypted Message

TG8O&*%$6vk

Private Key

Message

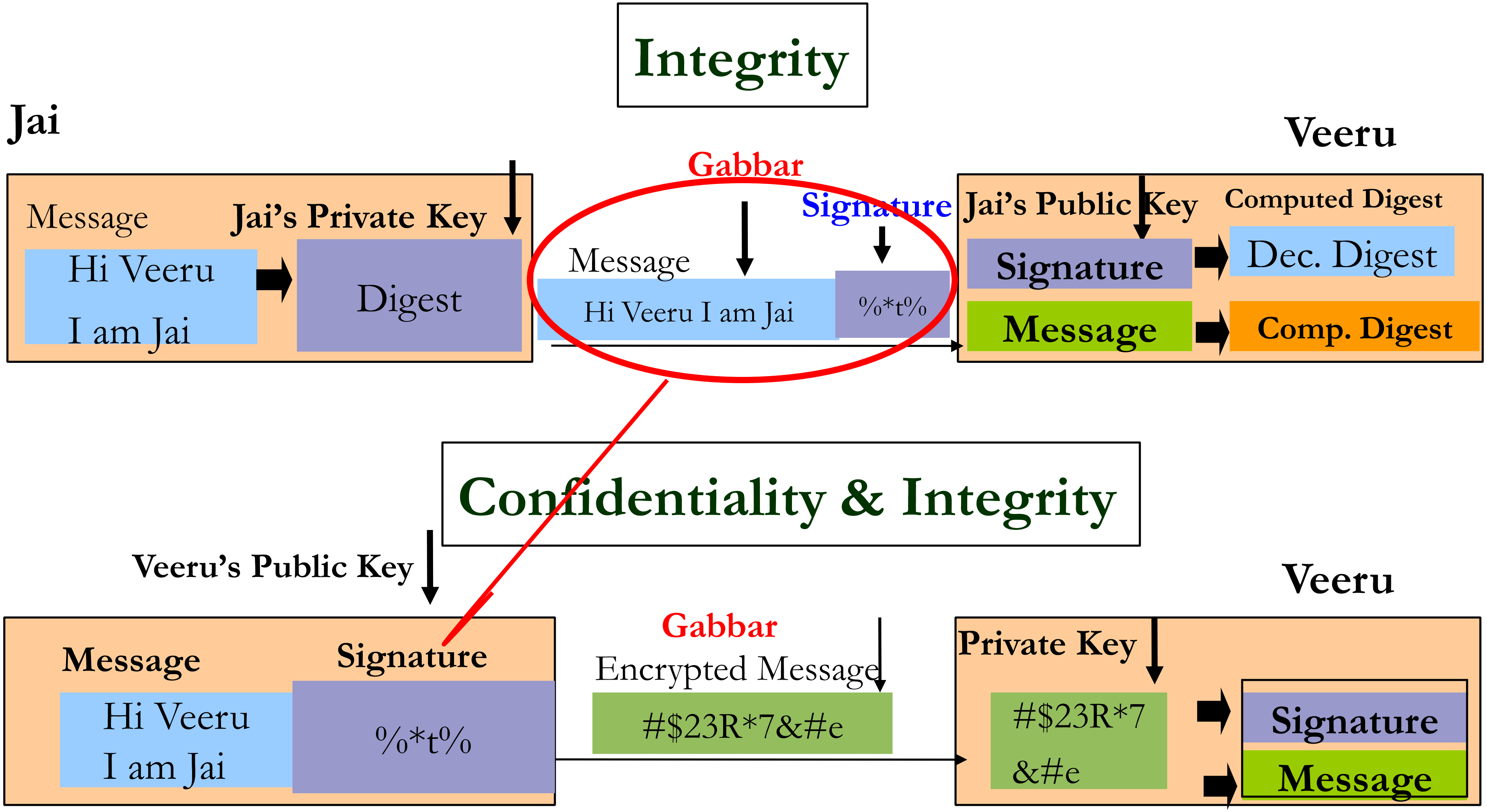
Decryptor

Hi Veeru

I am Jai

© C-DAC, EC, Bangalore

Asymmetric Key



Integrity

Jai

Message

Hi Veeru I am Jai

Jai's Private Key

Digest

Gabbar

Message

Hi Veeru I am Jai

Signature

%*t%

Veeru

Jai's Public Key

Signature

Message

Computed Digest

Dec. Digest

Comp. Digest

Confidentiality & Integrity

Veeru's Public Key

Message

Hi Veeru I am Jai

Signature

%*t%

Gabbar

Encrypted Message

#$23R*7&#e

Veeru

Private Key

#$23R*7 &#e

Signature

Message

Public Key Pros and Cons

Weakness

– Extremely slow

Strength

– Solves problem of passing the key

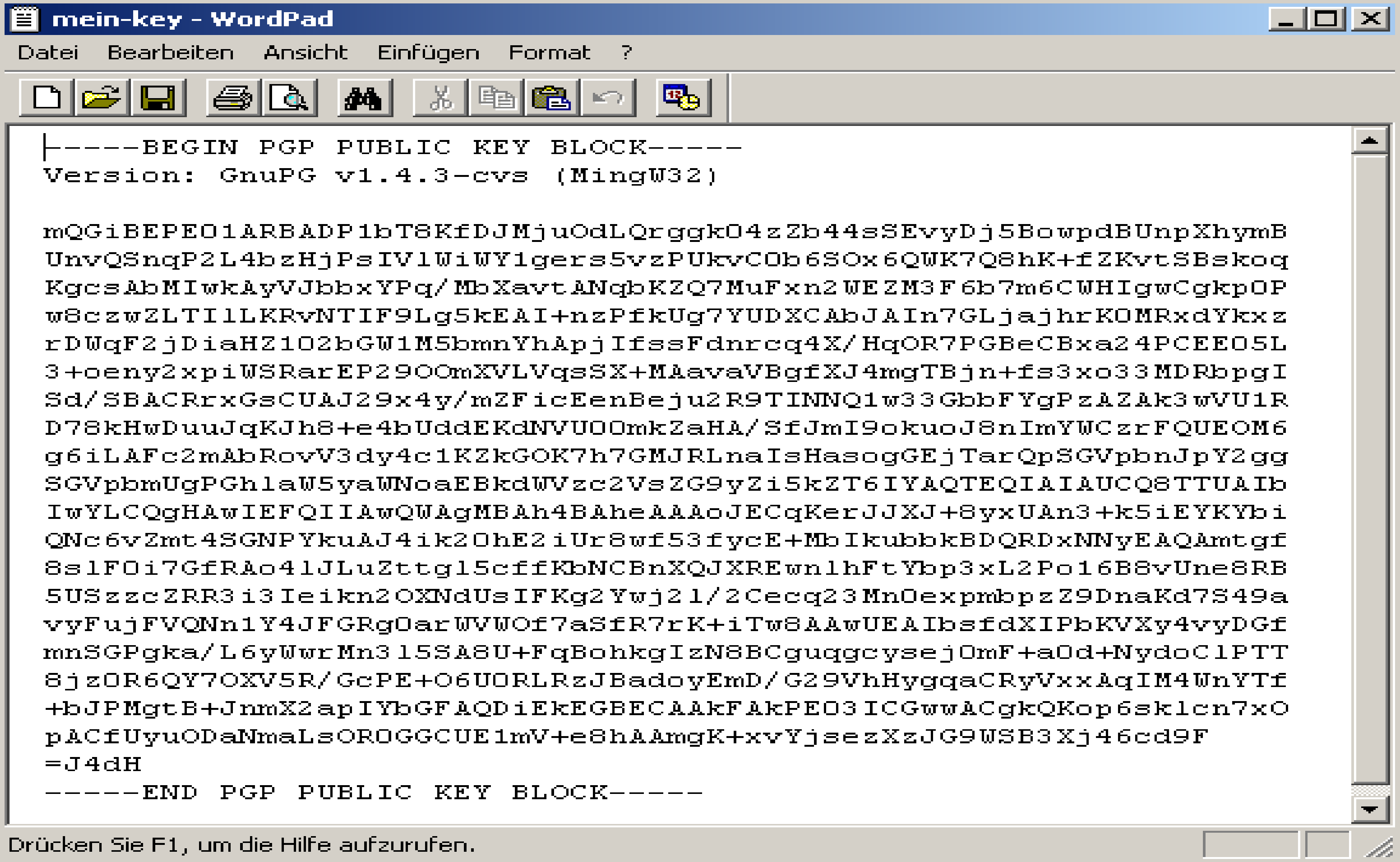
Key Aspects

- Public key encryption; RSA

Misconceptions

- More secure
- Has made Symmetric encryption obsolete

Example Public Key



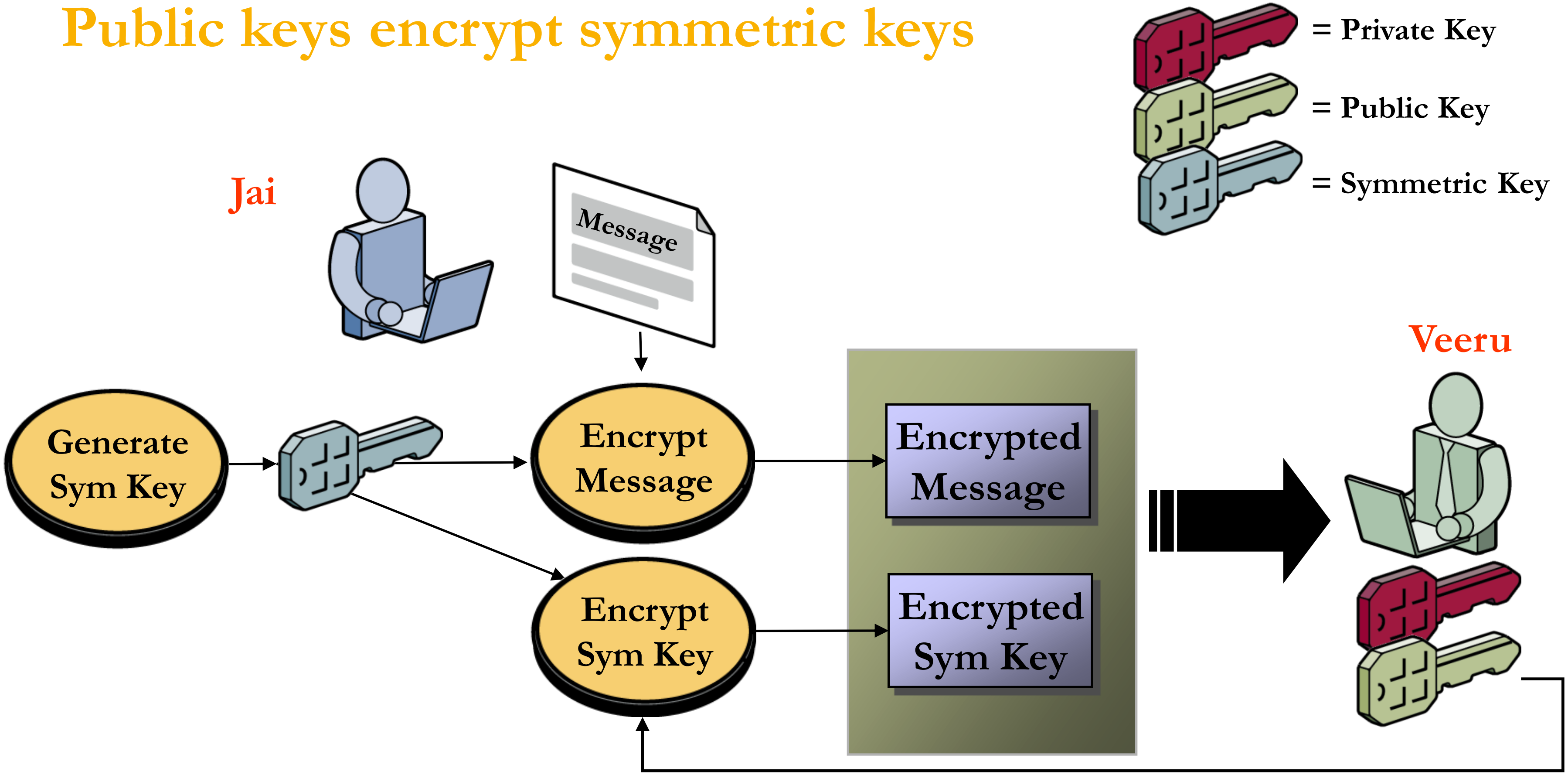
```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.3-cvs (MingW32)

mQGiBEPEO1ARBADP1bT8KfDJMjuOdLQrggkO4zZb44sSEvyDj5BowpdBUnpXhymB
UnvQSnqP2L4bzHjPsIVlWiWY1gers5vzPUkvCOb6SOx6QWK7Q8hK+fZKvtSBskoq
KgcsAbMIwkAyVJbbxYPq/MbXavtANqbKZQ7MuFxn2WEZM3F6b7m6CWHIgwCgkpOP
w8czwZLTIlLKRvNTIF9Lg5kEAI+nzPfkUg7YUDXCAbJAIn7GLjajhrKOMRxdYkxz
rDWqF2jDiaHZ1O2bGW1M5bmnYhApjIfssFdnrcq4X/HqOR7PGBeCBxa24PCEEO5L
3+oeny2xpiWSRarEP29OOmXVLVqsSX+MAavaVBgfXJ4mgTBjn+fs3xo33MDRbpgI
Sd/SBACRrxGsCUAJ29x4y/mZFicEenBeju2R9TINNQ1w33GbbFYgPzAZAk3wVU1R
D78kHwDuuJqKJh8+e4bUddEKdNVUOOmkZaHA/SfJmI9okuoJ8nImYWCzrFQUEOM6
g6iLAFc2mAbRovV3dy4c1KZkGOK7h7GMJRLnaIsHasogGEjTarQpSGVpbnJpY2gg
SGVpbmUgPGhlaW5yaWNoaEBkdWVzc2VsZG9yZi5kZT6IYAQTEQIAIAUCQ8TTUAIb
IwYLCQgHAwIEFQIIAwQWAgMBAh4BAheAAAoJECqKerJJXJ+8yxUAn3+k5iEYKYbi
QNc6vZmt4SGNPYkuAJ4ik2OhE2iUr8wf53fycE+MbIkubbkBDQRDxNNyEAQAmtgf
8slFOi7GfRAo4lJLuZttgl5cffKbNCBnXQJXREwnlhFtYbp3xL2Po16B8vUne8RB
5USzzcZRR3i3Ieikn2OXNdUsIFKg2Ywj2l/2Cecq23MnOexpmbpzZ9DnaKd7S49a
vyFujFVQNn1Y4JFGRg0arWVWOf7aSfR7rK+iTw8AAwUEAIbsfdXIPbKVXy4vyDGf
mnSGPgka/L6yWwrMn3l5SA8U+FqBohkgIzN8BCguqgcysej0mF+a0d+NydoClPTT
8jzOR6QY7OXV5R/GcPE+O6UORLRzJBadoyEmD/G29VhHygqaCRyVxxAqIM4WnYTf
+bJPMgtB+JnmX2apIYbGFAQDiEkEGBECAAkFAkPEO3ICGwwACgkQKop6sklcn7xO
pACfUyuODaNmaLsOROGGCUE1mV+e8hAAmgK+xvYjsezXzJG9WSB3Xj46cd9F
=J4dH
-----END PGP PUBLIC KEY BLOCK-----
```

Drücken Sie F1, um die Hilfe aufzurufen.

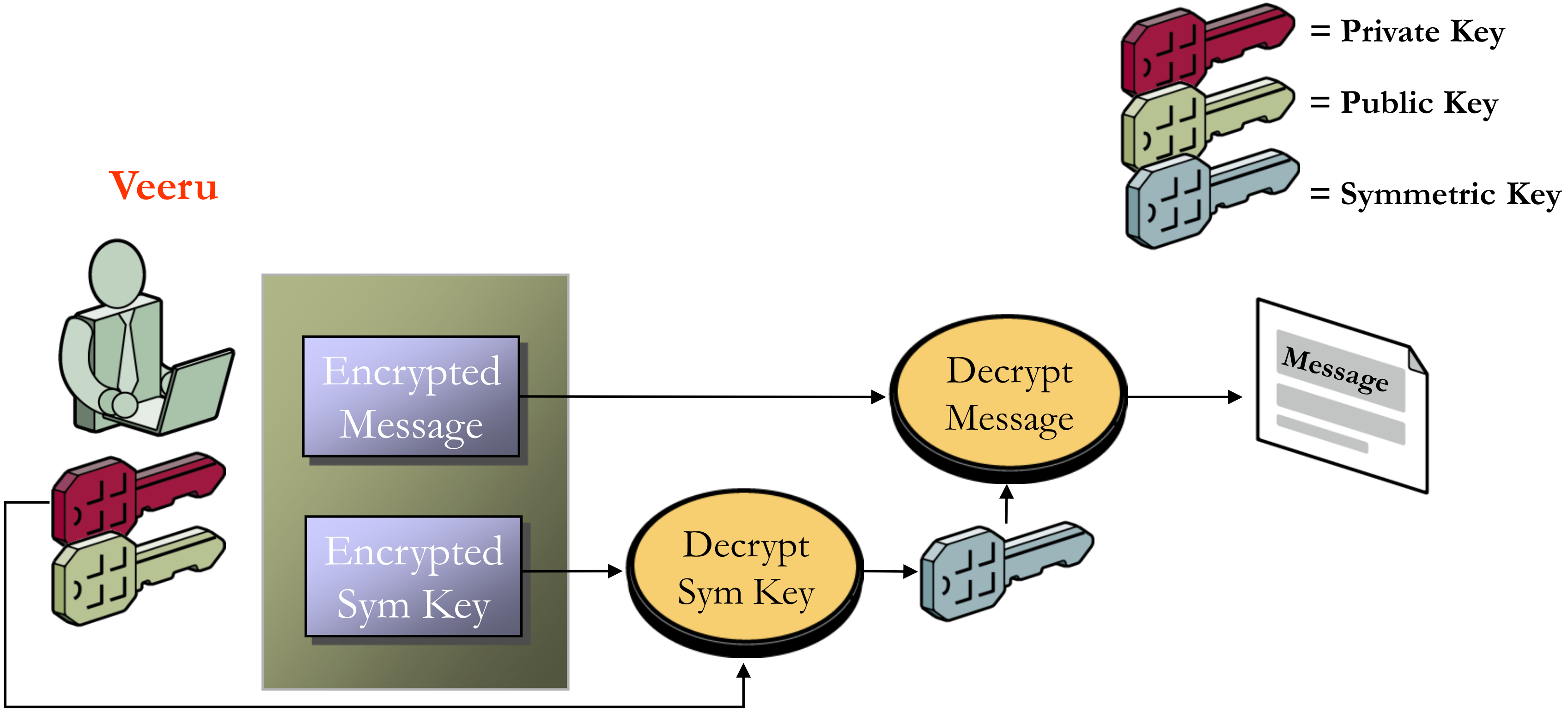
Public Key Encryption

Symmetric keys encrypt data;
Public keys encrypt symmetric keys



Encrypt with Veeru's Public Key

Public-Key – Decryption



Decrypt with Veeru's Private Key

Public key and symmetric key cryptography are complementary technologies

© C-DAC, EC, Bangalore

References

- Cryptography and Network security – principles and practice : William Stallings
- Applied Cryptography, Second Edition: Bruce Schneier
- www.certicom.com/index.php/ecc-turorial
- http://campustechnology.com/articles/39190_2
- http://csrc.nist.gov/
- Handbook of Applied Cryptography, by Menezes
- http://en.wikipedia.org
- Cryptographic Techniques for N/w Security

Thank You