

Overview of Cryptography

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

- **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

Availability: The information must be available when it is needed

- 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 across
 - **Cipher.** The encryption/decryption algorithms which are used in the transformation of plaintext to ciphertext and vice-versa
 - **Ciphertext.** The message after it is encoded

Cryptography ...

- **Key.** This is a unique value (bit pattern, alphabetical sequence) that is used by the cipher for encryption/decryption
- **Cryptanalyst.** A person who analyses the cryptosystem with an aim to discover the plaintext message and/or the key
- ***Cryptology*** is cryptography + cryptanalysis

Classification of Cryptographic Techniques

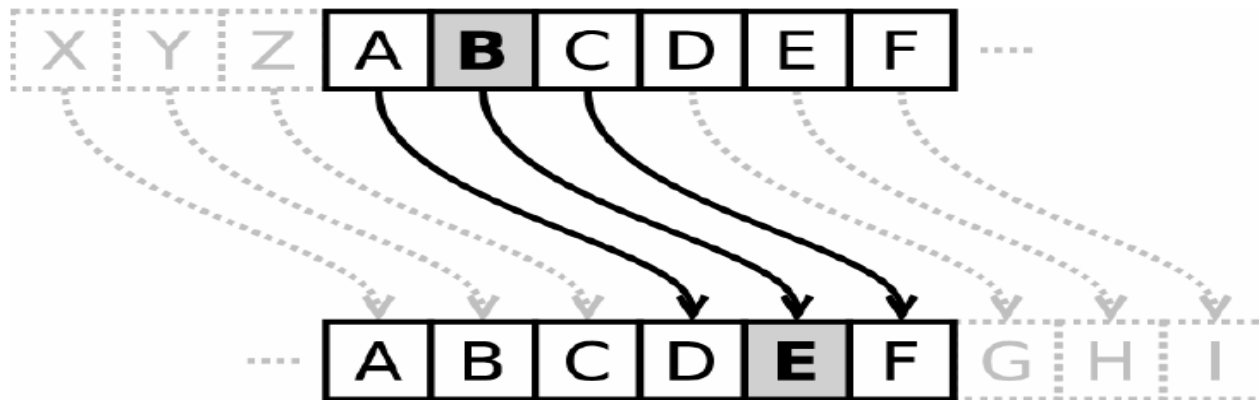
- Cryptosystems can be classified based on
 - Type of operations - Substitution/Transposition
 - Way in which plaintext is processed - Block/Stream
 - Number of keys used - Symmetric / Asymmetric

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 \longrightarrow nulvkqd obvious

Shift by k letters (here $k = 3$)

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Shift by k letters (here $k = 6$)

KRISHNA \longrightarrow qxoyntg ... still obvious(?!)

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

Transposition Ciphers

- Here the order of the character is changed

Rail Fence Cipher (*Capture fox*)

C P U E O

A T R F X

Cipher Text

CPUEOATRFX

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

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

Cipher Text

EJXCTEDECDAEWRIORFEONALEVSE

Hash Function

- A hash function is an algorithm
 - 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

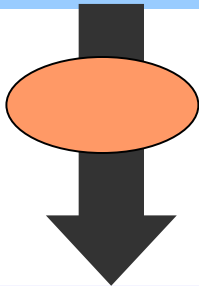
- Computationally infeasible to identify the input given the message digest

Hash - Example

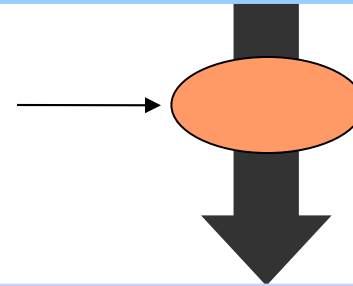
Message

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

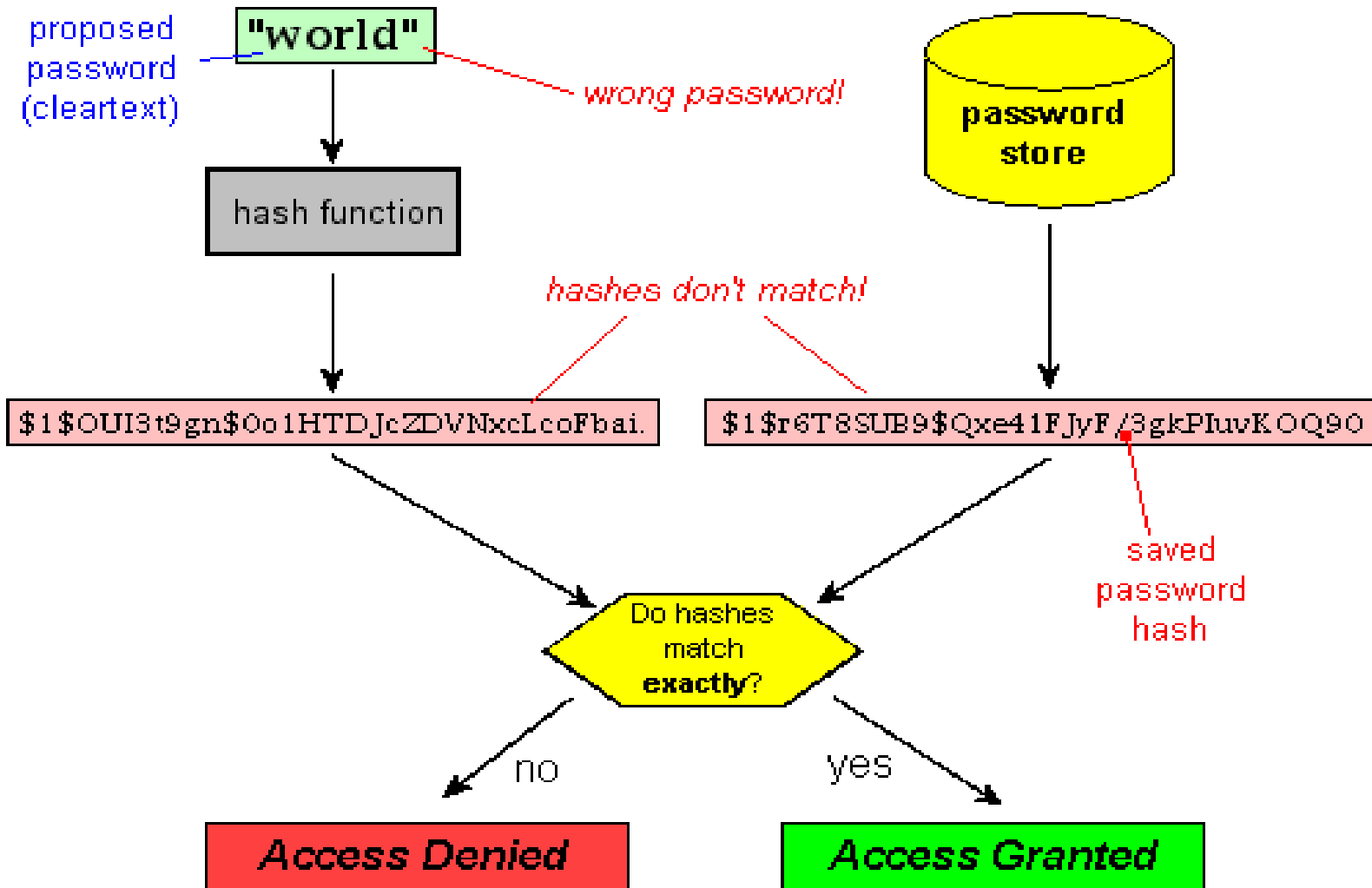
Hi Jai,
I will be in the
park at 3 pm
Veeru

SHA-2

2g5487f56r4etert654tr
c5d5e8d5ex5gttahy55e

224/256/384/512

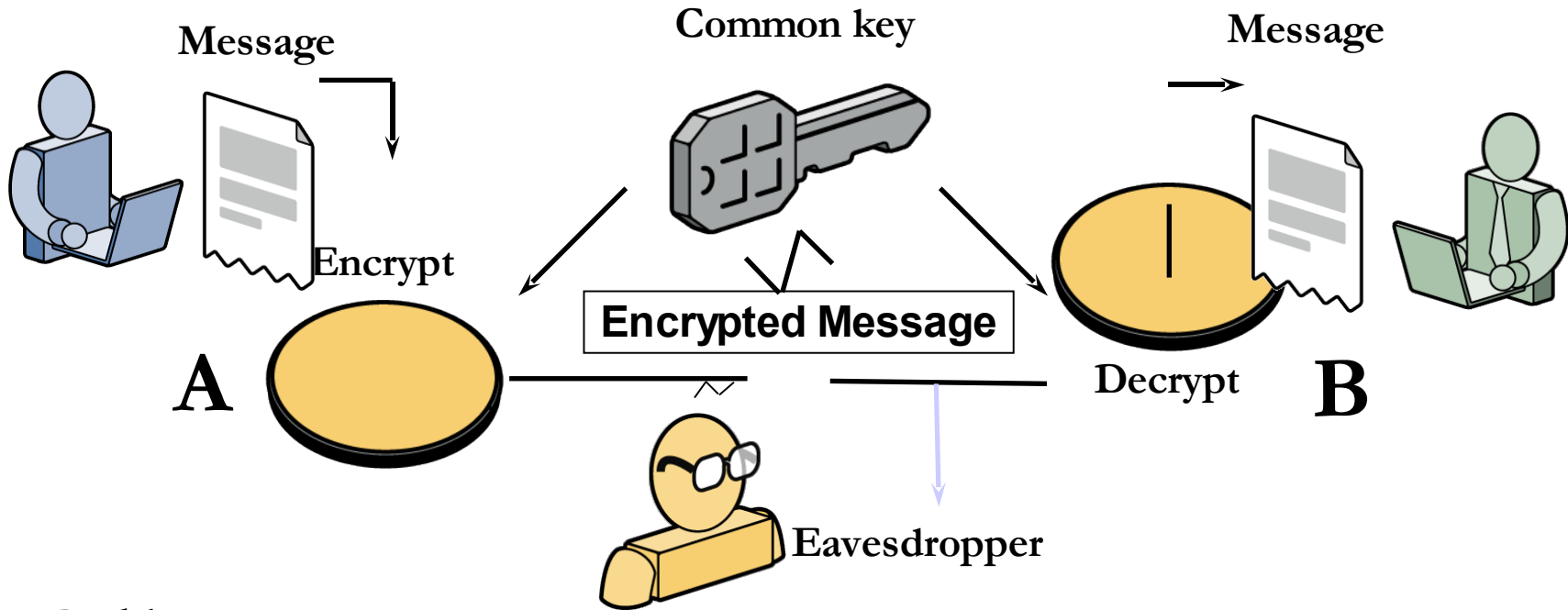
Example of Hash functions



Symmetric Key

- **Symmetric/Secret key cryptography**
- Uses one key shared by both sender and receiver
- If this key is disclosed communications are compromised
- Does not protect sender from receiver forging a message & claiming it is sent by sender
- Problem of Key distribution & scaling

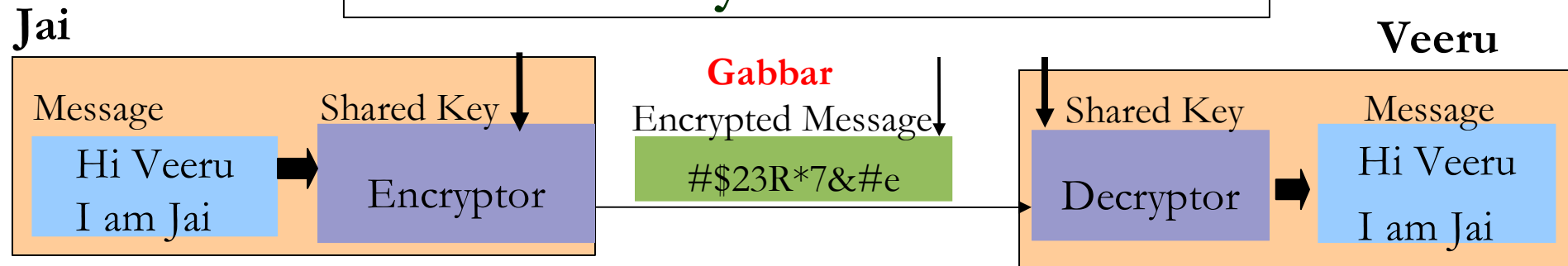
Symmetric Key Encryption



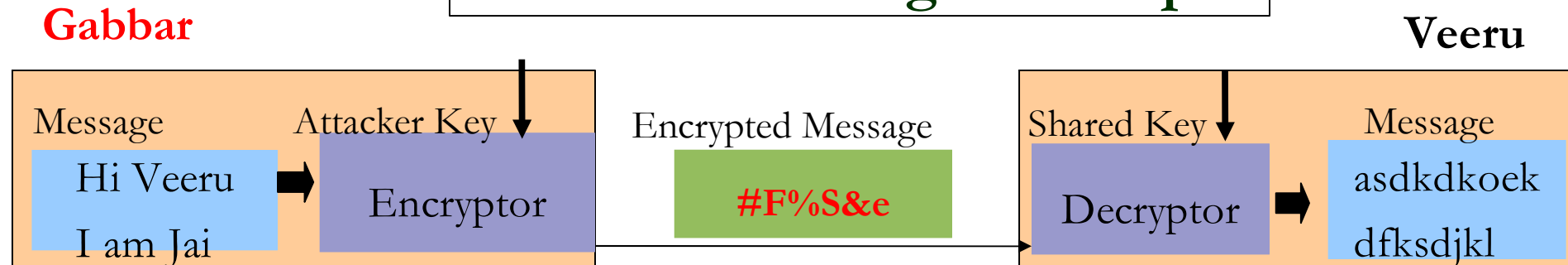
- Problems:
 - Jai and Veeru must agree on the secret key without anyone else finding out
 - Anyone who intercepts the key in transit can later read, modify, and forge all messages encrypted using that key
 - Doesn't Scale

Symmetric Key Cryptography

Confidentiality & Authentication

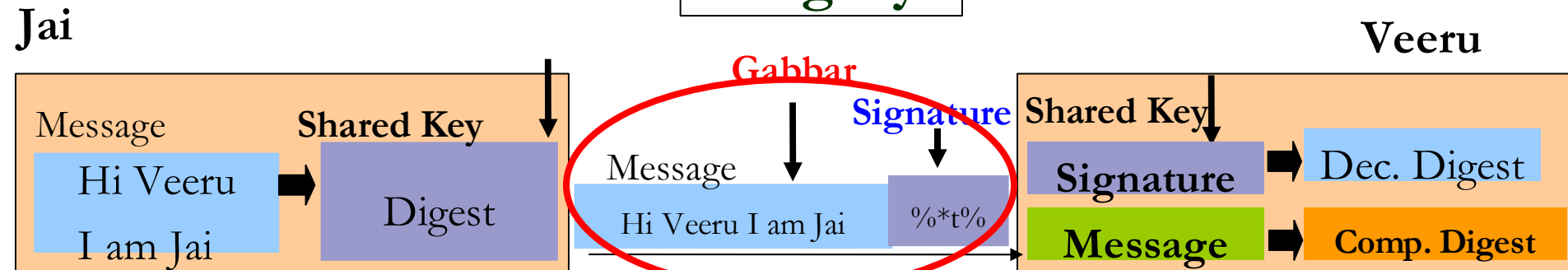


Unauthorized Login Attempt

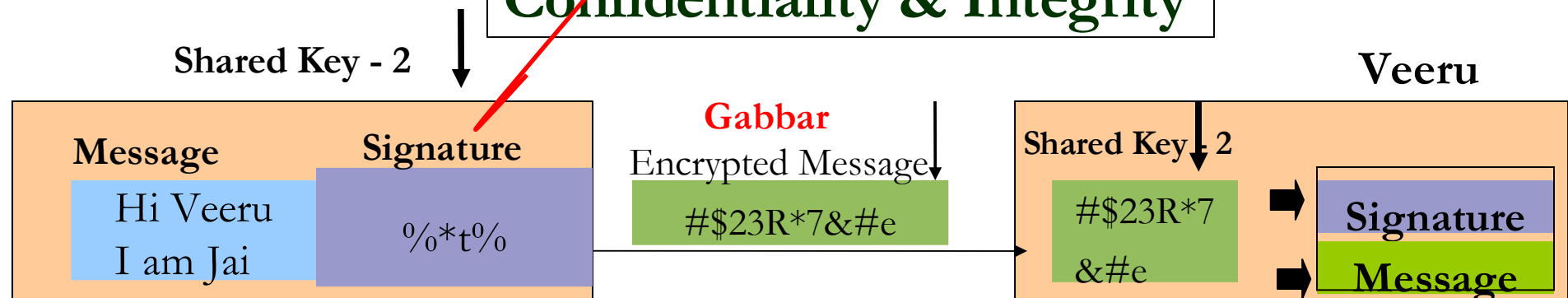


Symmetric Key Cryptography



Integrity





Confidentiality & Integrity



Weakness:

-  Must agree the key beforehand
-  Securely pass the key to the other party

Strength:

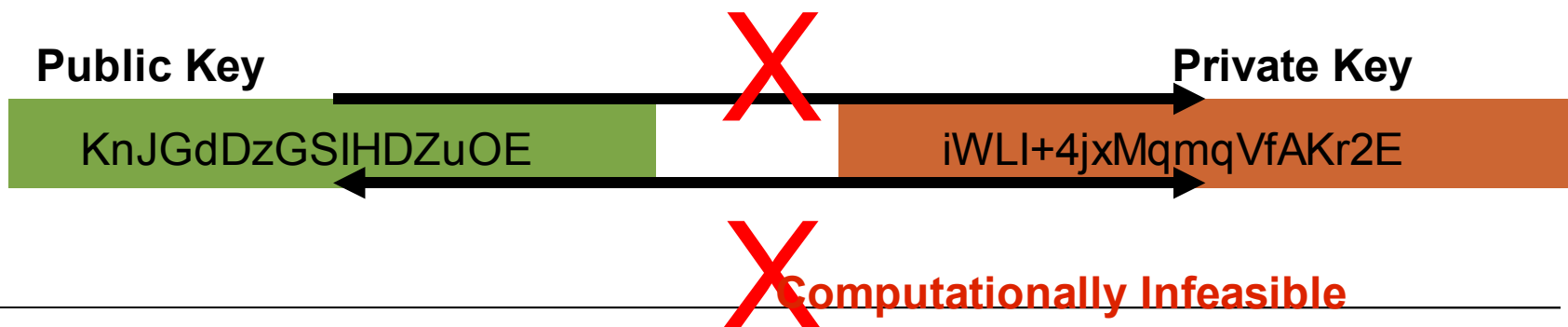
-  Simple and really very fast (order of 1000 to 10000 times faster than asymmetric mechanisms)
 -  Super-fast if done in hardware

Symmetric Key - issues

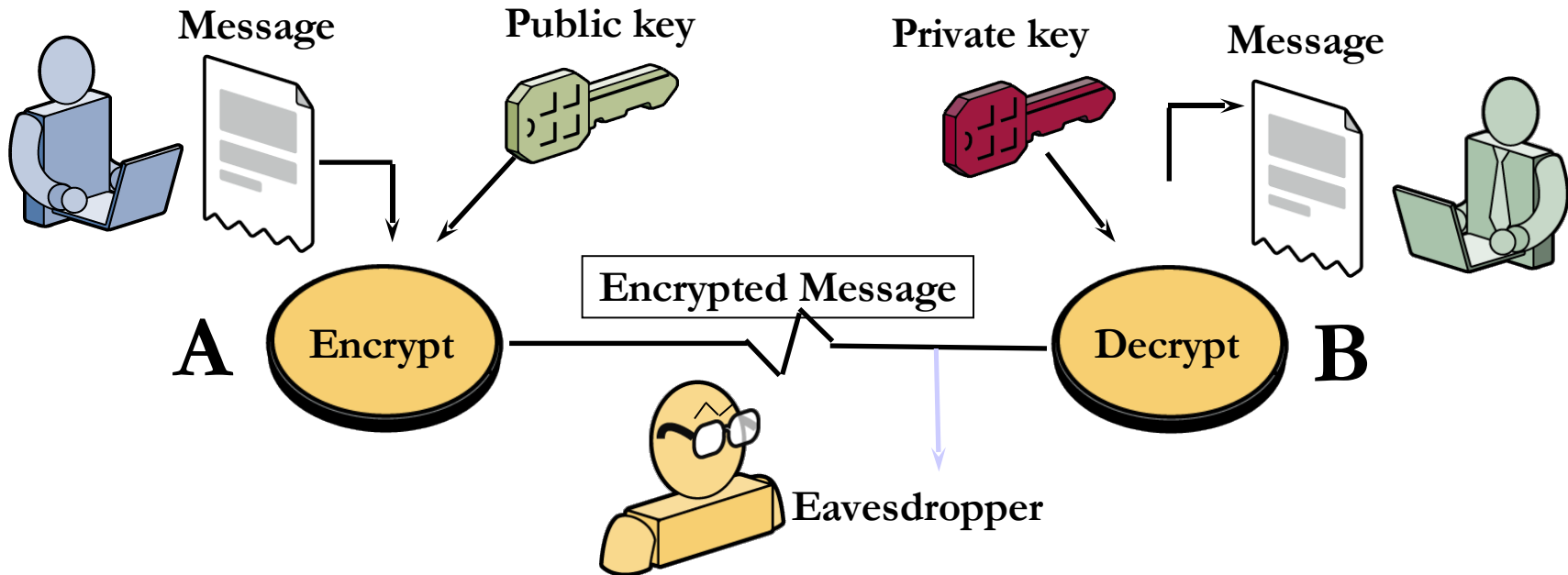
- What is achieved by symmetric key ?
 - Confidentiality
 - Integrity
 - Authentication
- What about Non-repudiation ?

Public Key Cryptography

- A related Key Pair
 - Private key, 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 Encryption



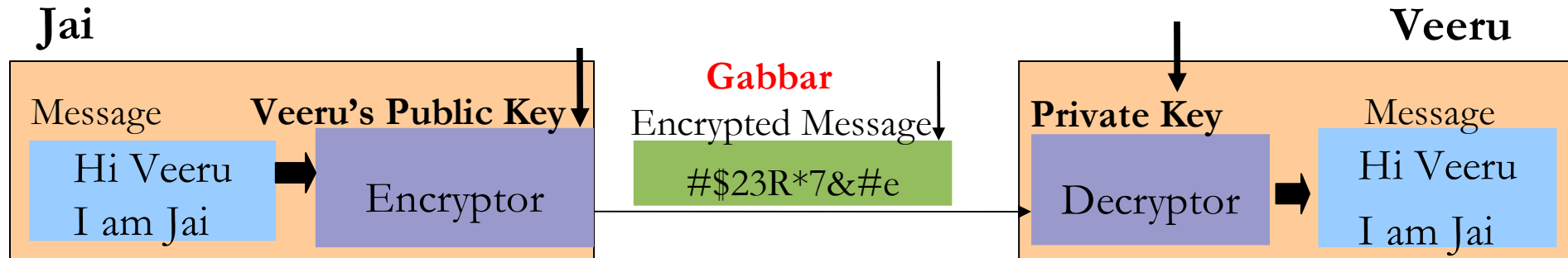
- Problems:
 - Encryption and decryption are extremely SLOW

Asymmetric Key Cryptography

Authentication

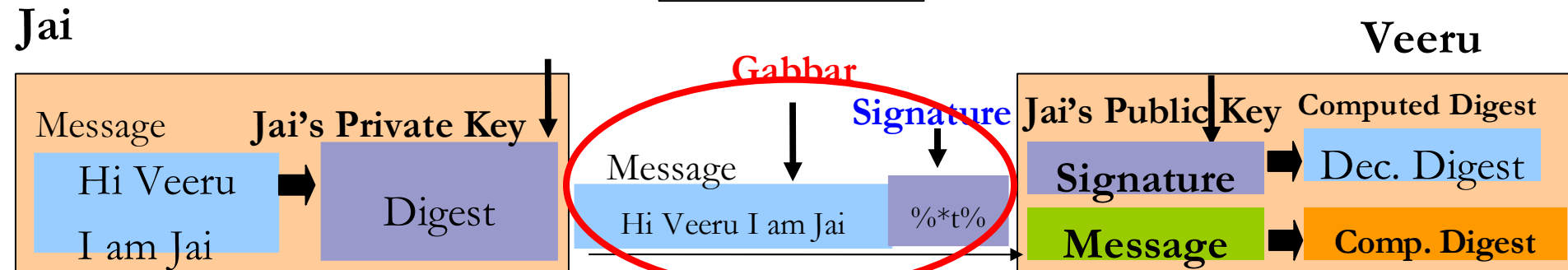


Encryption

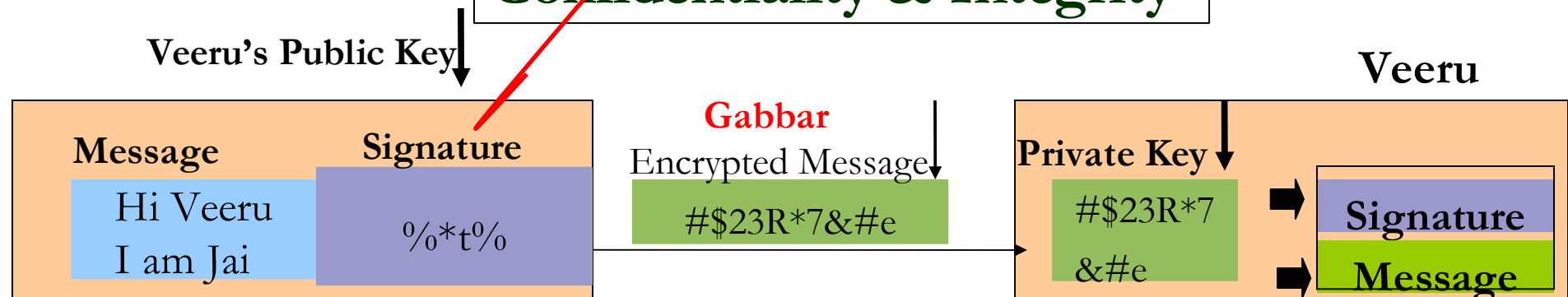


Asymmetric Key

Integrity



Confidentiality & Integrity



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

```
mein-key - WordPad
Datei Bearbeiten Ansicht Einfügen Format ?

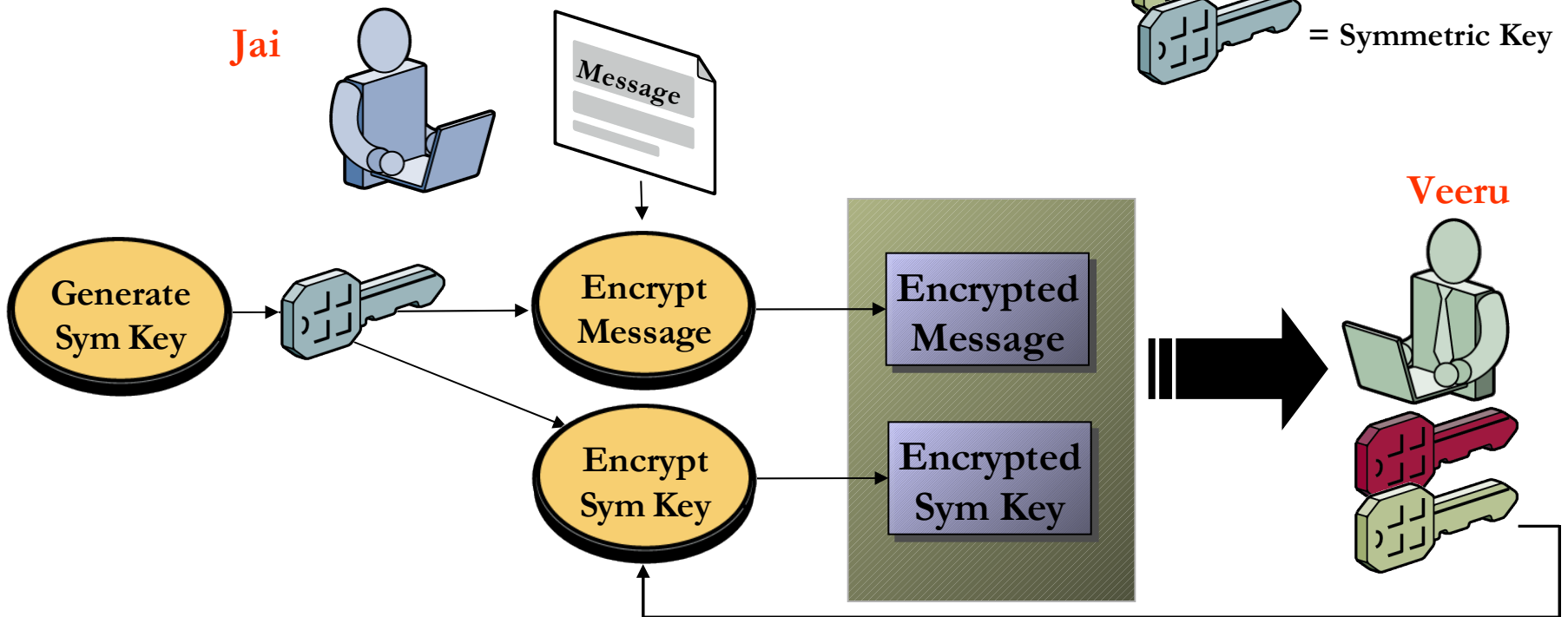
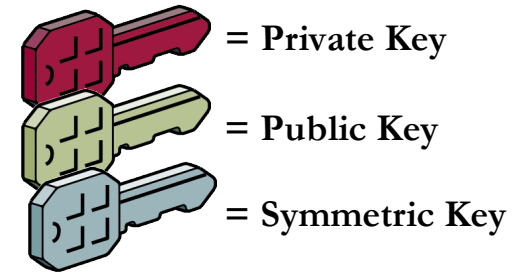
|-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.3-cvs (MingW32)

mQGIBEPEO1ARBADP1bT8KfDJMjuOdLQrggk04zZb44sSEvyDj5BowpdBUnpXhymB
UnvQSnqP2L4bzHjPsIV1WiWY1gers5vzPUkvCOb6SOx6QWK7Q8hK+fZKvtSBskoq
KgcsAbMIwkAyVJbbxYPq/ MbXavtANqbKZQ7MuFxn2WEZM3F6b7m6CWHIgwCgkpOP
w8czwZLTI1LKRVNTIF9Lg5kEAI+nzPfkUg7YUDXCABJAIn7GLjaJhrKOMRxdYkxz
rDWqF2jDiaHZ102bGW1M5bmnYhApjIfssFdnrcq4X/HqOR7PGBECBxa24PCEE05L
3+oeny2xpiWSRarEP290OmXVLVqsSX+MAavaVBgfXJ4mgTBjn+fs3xo33MDRbpgI
Sd/SBACRrxGsCUAJ29x4y/mZFicEenBeju2R9TINNQ1w33GbbFYgPzAZAk3wVU1R
D78kHwDuuJqKJh8+e4bUddeEKdNVU00mkZaHA/SfJmI9okuoJ8nImYWCzrFQUEOM6
g6iLAFc2mAbRovV3dy4c1KZkGOK7h7GMJRLnaIsHasogGEjTarQpSGVpbnJpY2gg
SGVpbmUgPGhlaW5yaWNoaEBkdWVzc2VsZG9yZi5kZT6IYAQTEQIAIAUCQ8TTUAib
IwYLCQgHAwIEFQIIAwQWAgMBAh4BAheAAAoJECqKerJJXJ+8yxUAN3+k5iEYKYbi
QNC6vZmt4SGNPYkuAJ4ik2OhE2iUr8wf53fycE+MbIkubbkBDQRDXNNyEAQAmtgf
8s1FOi7GfRAo41JLuZttg15cffKbNCBnXQJXREwnlhFtYbp3xL2Po16B8vUne8RB
5USzZcZRR3i3Ieikn2OXNdUsIFKg2Ywj2l/2Cecq23MnOexpmbpzZ9DnaKd7S49a
vyFujFVQNN1Y4JFGRgOarWVWOf7aSfR7rK+iTw8AAwUEAIBsfdXIPbKVXy4vyDGf
mnSGPgka/L6yWwrMn3l5SA8U+FqBohkgIzn8BCguqgcycysejOmF+aOd+NydoC1PTT
8jzOR6QY7OXV5R/GcPE+O6UORLRzJBadoyEmD/G29VhHygqaCRyVxxAqIM4WnYTF
+bJPMgtB+JnmX2apIYbGFAQDiEkEGBECAAKFAkPEO3ICGwwACgkQKop6sklcn7xo
pACfUyuODaNmaLsOROGGCUE1mV+e8hAAmgK+xvYjsezXzJG9WSB3Xj46cd9F
=J4dH
-----END PGP PUBLIC KEY BLOCK-----

Drücken Sie F1, um die Hilfe aufzurufen.
```

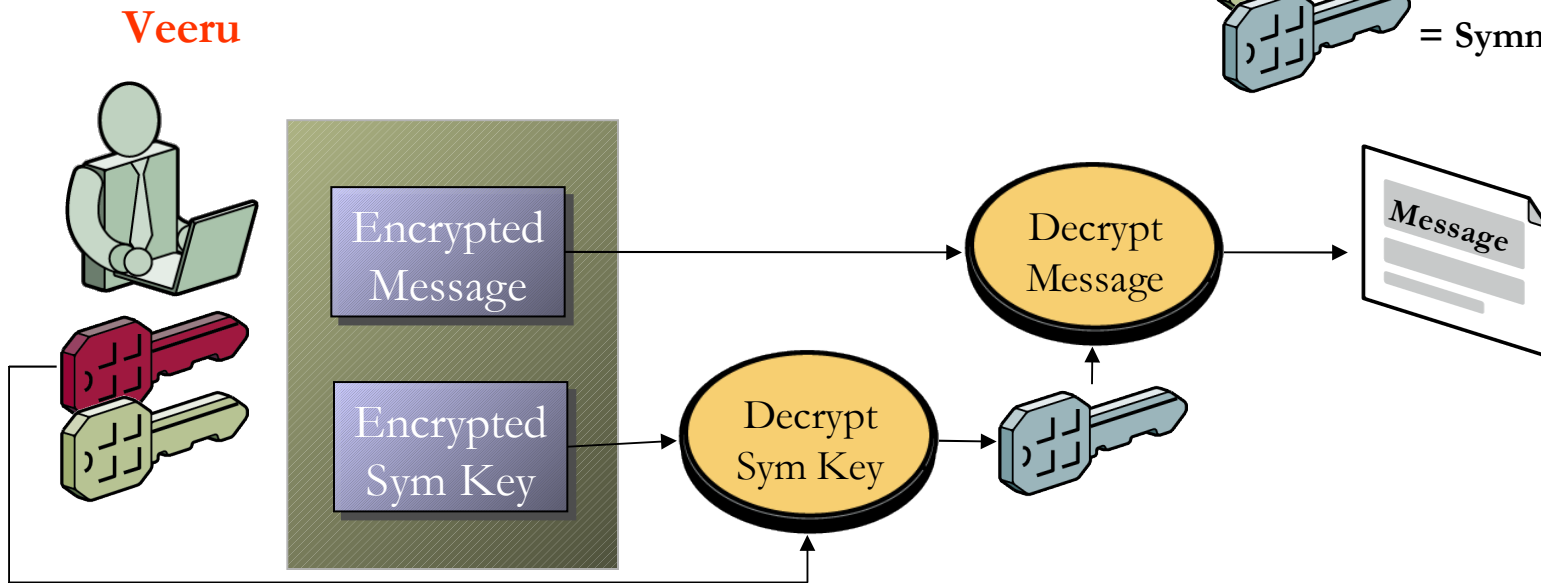
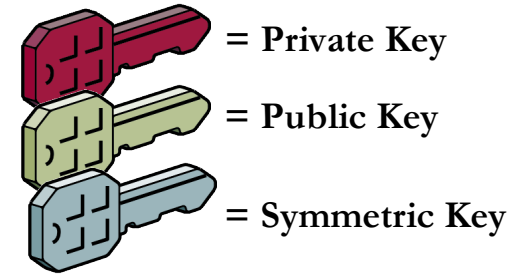
Public Key Encryption

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**

References

- Cryptography and Network security – principles and practice :
William Stallings
- Applied Cryptography, Second Edition: Bruce Schneier
- www.certicom.com/index.php/ecc-tutorial
- 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