Cryptography and PKI

DITISS– 2014

October, 2014

Agenda

- **Introduction to Cryptography**
  - Substitution Ciphers
  - Transposition Ciphers
  - Block and Stream Ciphers
  - DES
- **Hash Functions**
- **Symmetric Key Cryptography**
- **Asymmetric key Cryptography**

Introduction

Why information security?

What is an Incident ??

What is Information security?

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

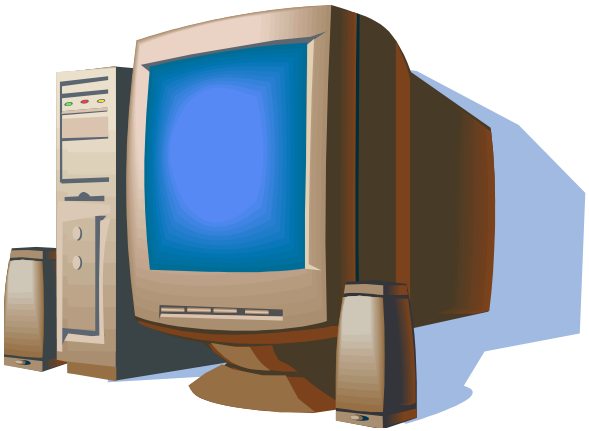
Privacy/Confidentiality: preventing disclosure of information to unauthorized individuals or systems

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

What defines an incident?



- ☑ A computer security incident covers a large range of violations, including:
  - ☞ Denial/Interruption of Service,
  - ☞ Malware Infection (worm, virus),
  - ☞ Unauthorized Access,
  - ☞ Misuse of Data or Services,
  - ☞ Copyright Infringement,
  - ☞ Spam etc.

Why Incidents Occur ??

Common Myths

- "Why should I care, I have nothing to hide."
- "Why does anyone care about my computer?"
- "It's too difficult to get access to my computer or personal information…"
- "If someone tries to insert malicious activity here, I will notice!"

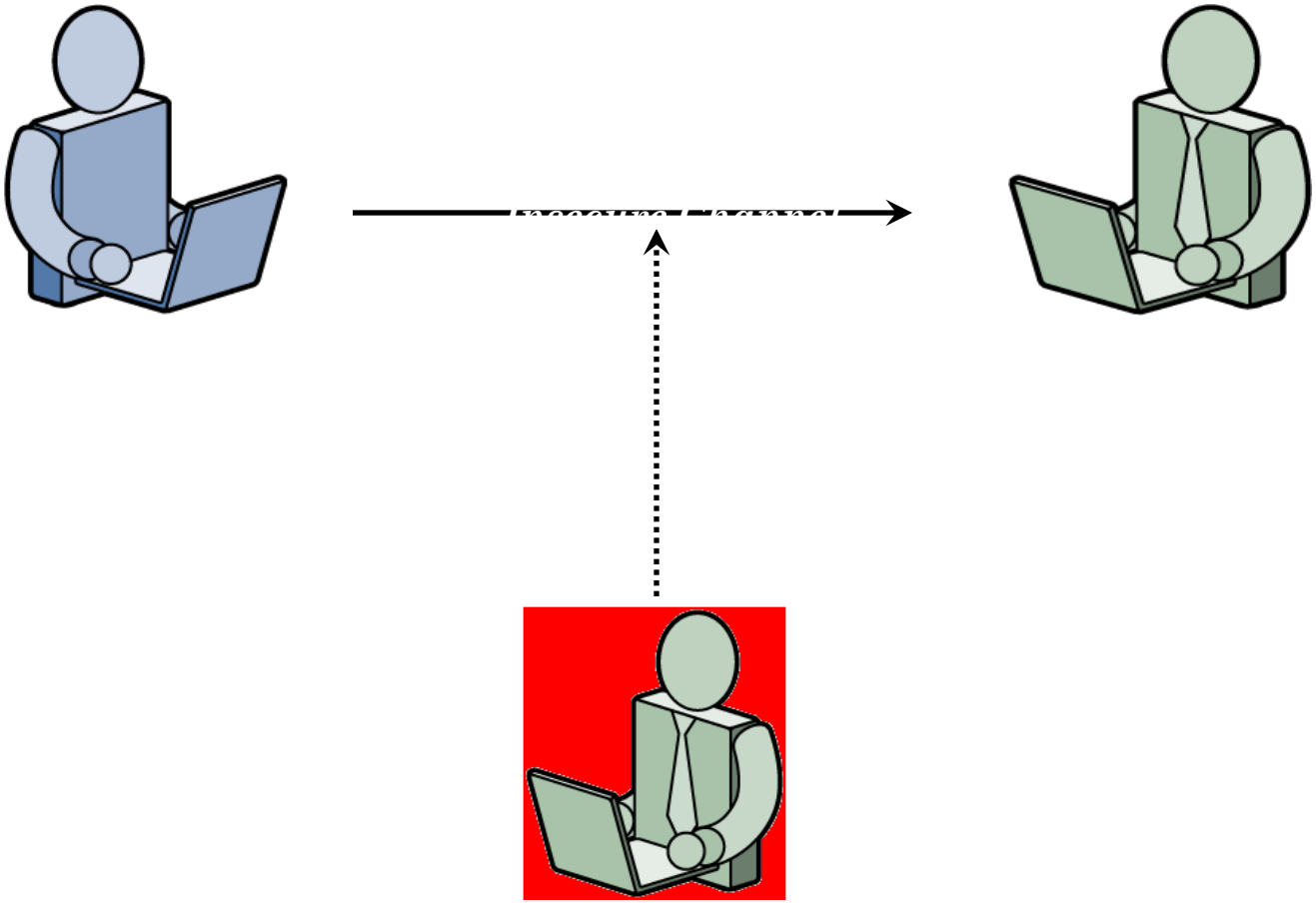
Are you at risk?

Using the following puts you at risk:

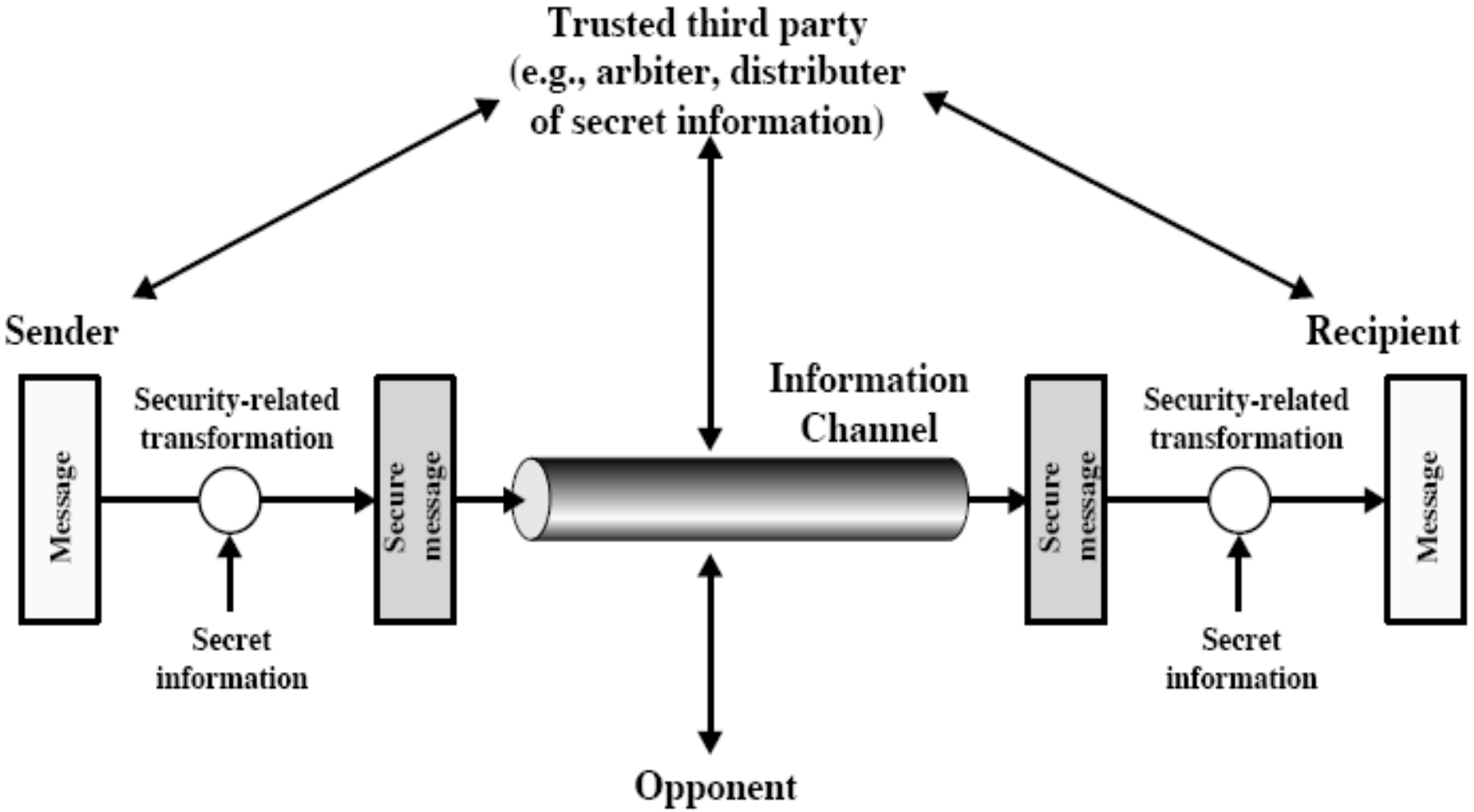
- ✓ Computers
- ✓ Credit Cards
- ✓ Mobile Devices
- ✓ Banks
- ✓ Automobiles
- ✓ …many more…

If you are using any of these then
you need to take security measures

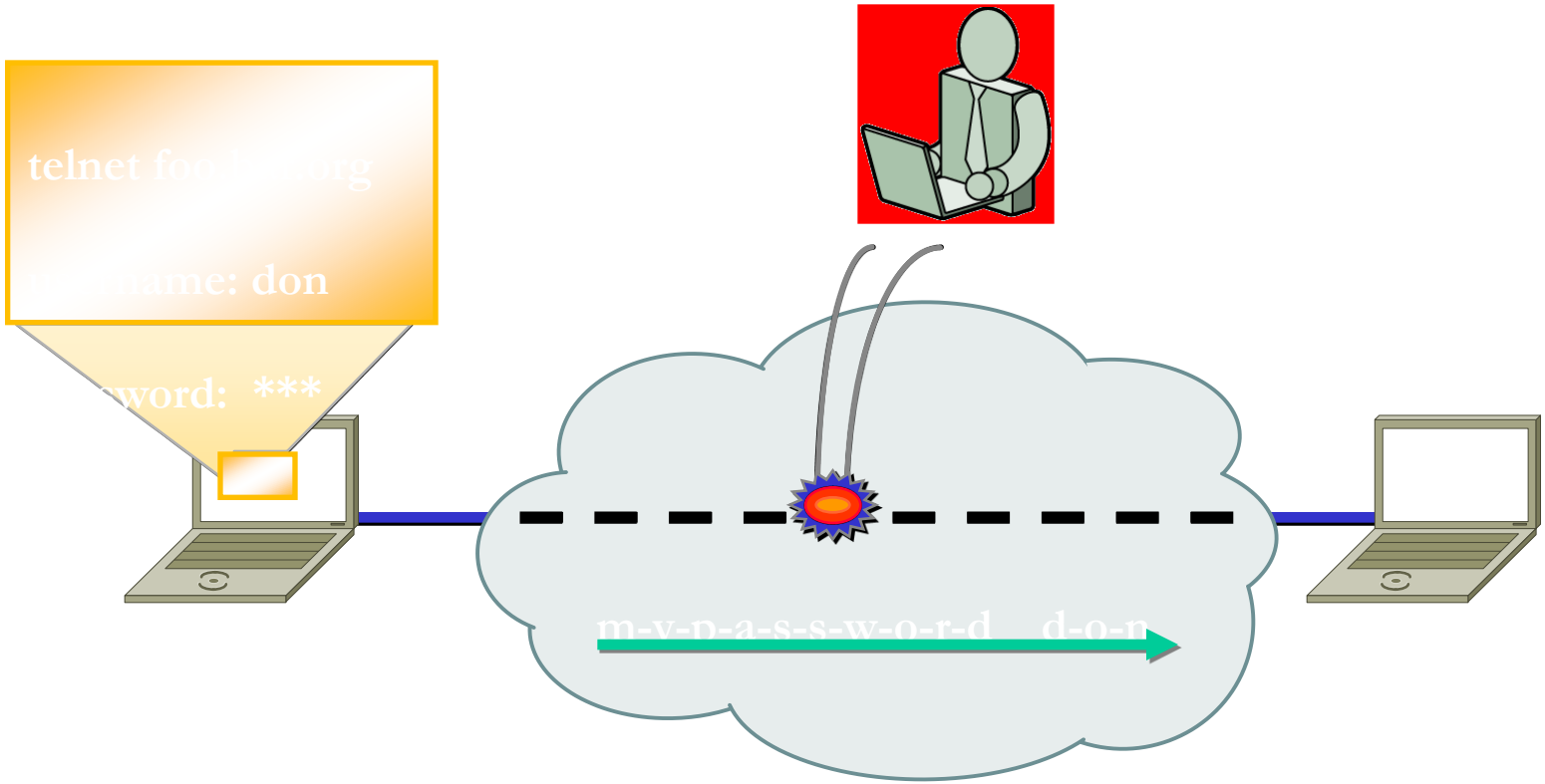
The Scenario



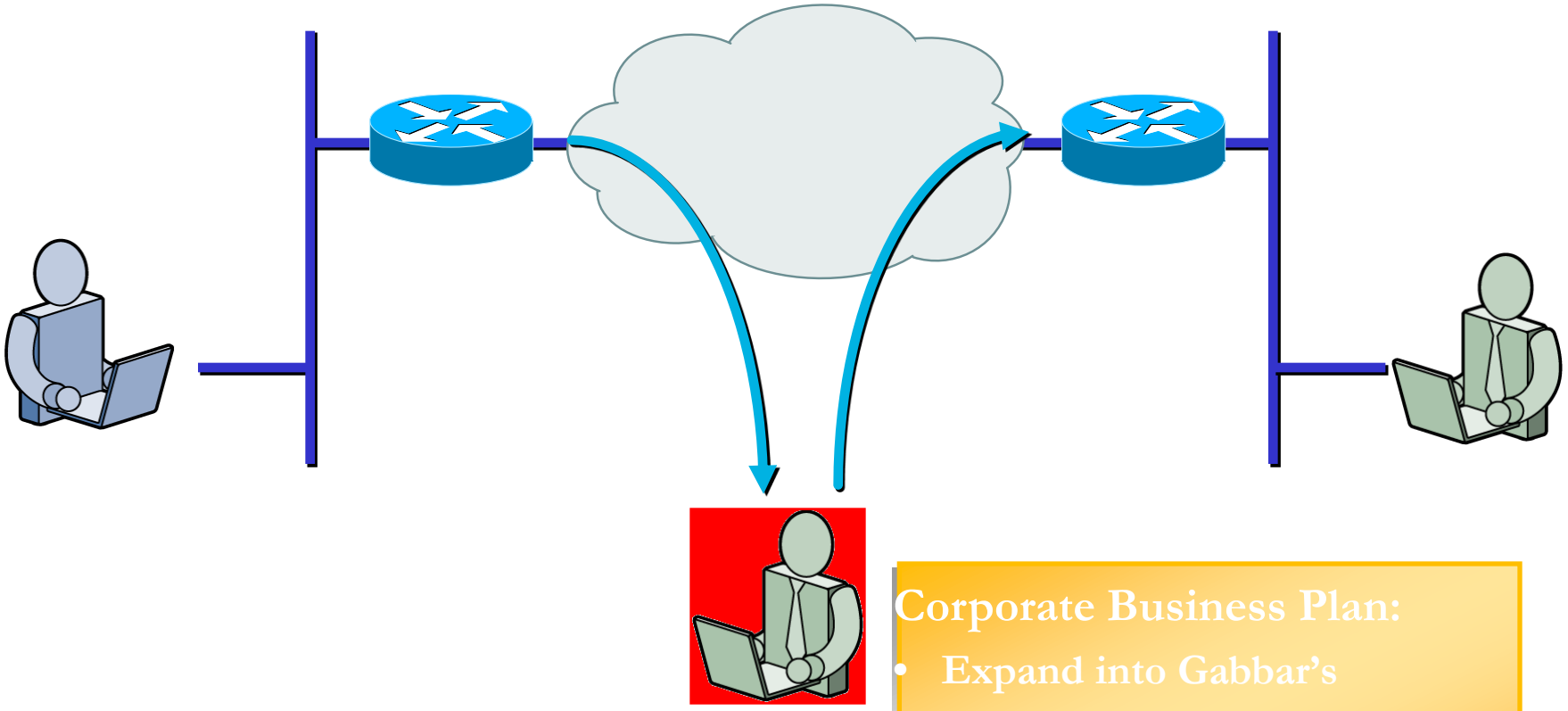
Model for Network Security



Threats: Packet Sniffing



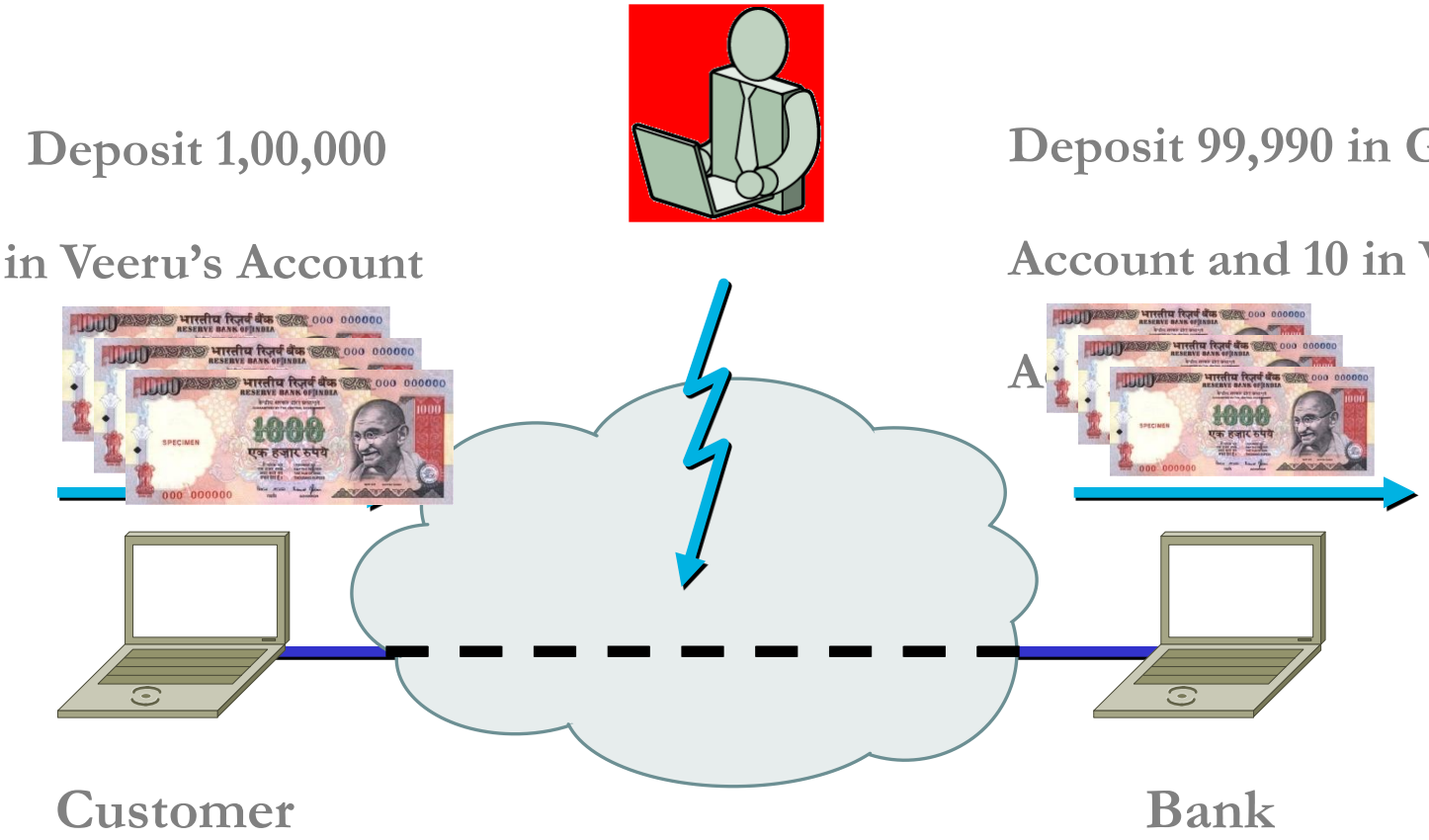
Threats: Data Theft



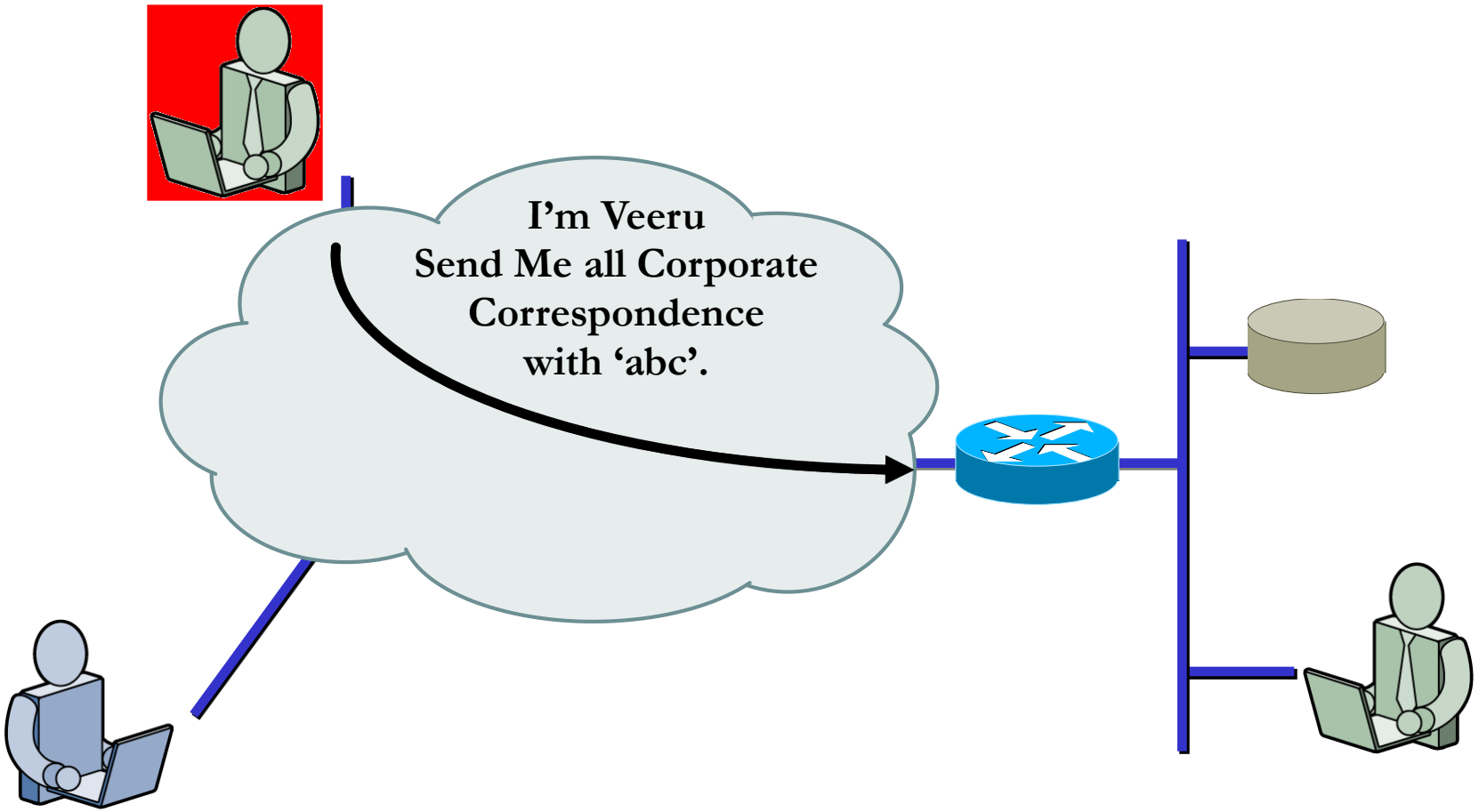
Corporate Business Plan:

- **Expand into Gabbar's core area**
- **Massively discount our products for next quarter**

Threats: Data Alteration



Threats: Spoofing



Security Threats

- Threats can come from a range of sources
- Various surveys, with results of order:
  - 55% human error
  - 10% disgruntled employees
  - 10% dishonest employees
  - 10% outsider access
  - also have "acts of god" (fire, flood etc)

List of some common attacks:

- Replay Attack
- Insider Attack
- Stolen Verifier Attack
- Shoulder surfing
- Server Spoofing
- Guessing Attack
- Dictionary Attack
- Brute-force Attack
- Man-In-The-Middle (MITM)
- Phishing Attack

Classification of Cryptographic

- Steganography
- 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
- Hash Functions

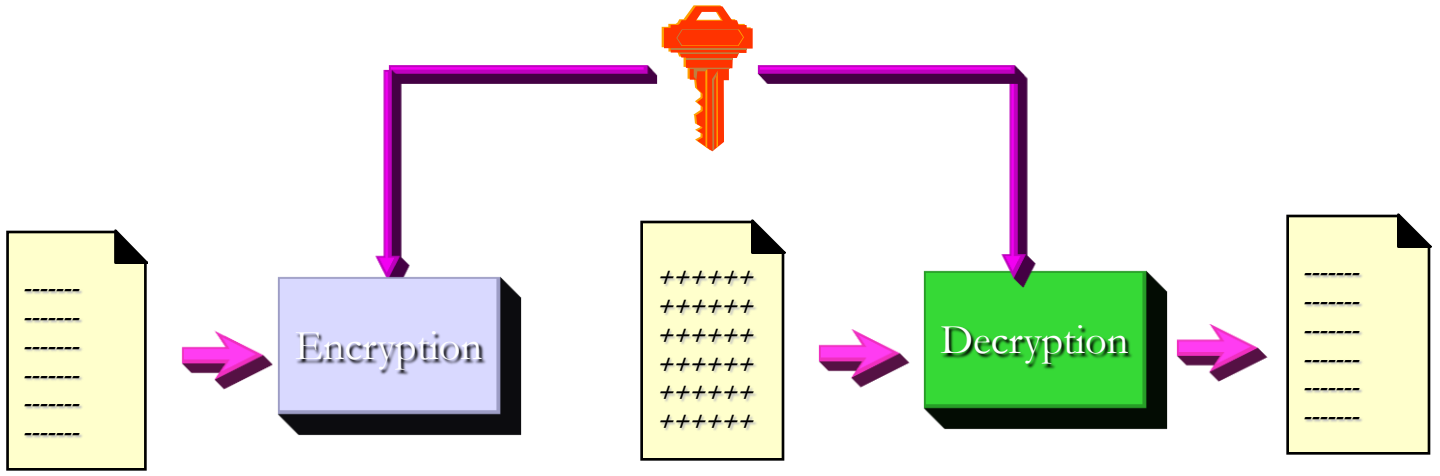
Cryptography

- 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…

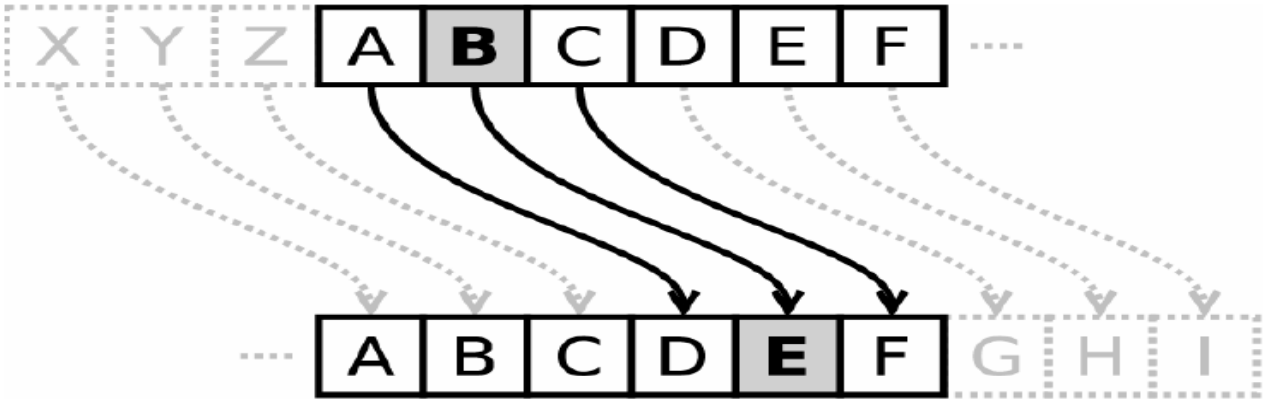
- In 50 BC, Julius Caesar used an alphabet with a shift of three and hence named as Caesar cipher.
- Blaise de Vigenère discussed Vigenere cipher in 1585 AD
- 1917 AD American, Gilbert S. Vernam, develops the One-time-pad
- 1976 AD Diffie-Hellman key exchange protocol is developed
- 1977 AD DES is developed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

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

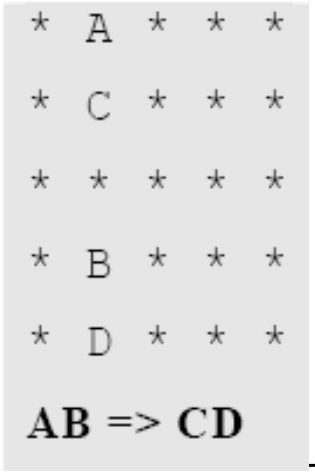
- Makes use of diagraphs and comprises of several small steps
  - **Key:** Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months
    - TREAYOUPSWDLIKHBNGVXMCFQZ

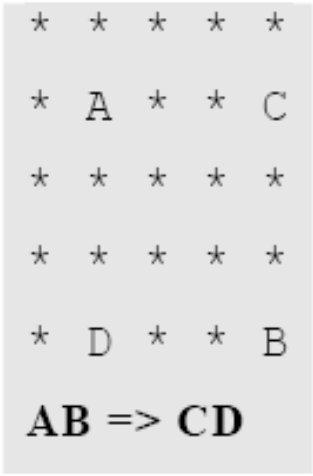
T	R	E	A	Y
O	U	P	S	W
D	L	I	K	H
B	N	G	V	X
M	C	F	Q	Z

- Plain Text: "Information is not knowledge"

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

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





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

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

Block Ciphers

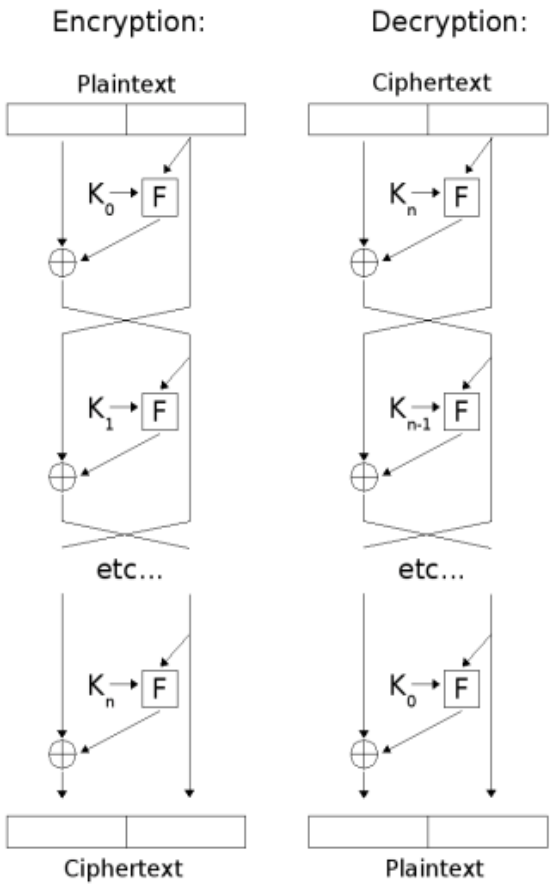
- A symmetric key cipher which operates on fixed-length groups of bits, termed *blocks*, with an unvarying transformation.
- When encrypting, a block cipher might take (for example) a 128-bit block of plaintext as input, and output a corresponding 128-bit block of ciphertext. But 64 bit is common.
- The exact transformation is controlled using a second input "the secret key."
- Decryption is similar

Iterated block ciphers

- Most block ciphers are constructed by repeatedly applying a simpler function. This approach is known as *iterated block cipher*
- Each iteration is termed a round, and the repeated function is termed the round function; anywhere between 4 to 32 rounds are typical.

Feistal Cipher

- Describes the structure of a cipher
- A block cipher with a symmetric structure it is also commonly known as a **Feistel network**.
- A large proportion of block ciphers use the scheme, including the DES.
- It has the advantage that encryption and decryption operations are very similar, even identical in some cases, requiring only a reversal of the key .
- The size of the code or circuitry required to implement such a cipher is nearly halved.



Feistel Cipher

Stream Ciphers (State Cipher)

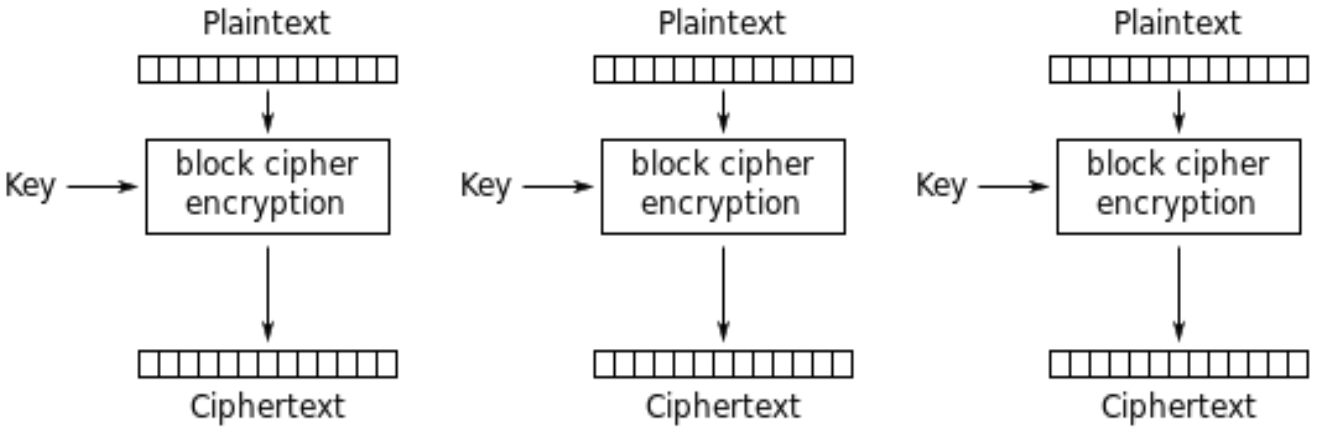
- A stream cipher is a symmetric key cipher where plaintext bits are combined with a pseudorandom cipher bit key stream, typically by an exclusive-or (xor) operation.
- In a stream cipher the plaintext digits are encrypted one at a time, and the transformation of successive digits varies during the encryption.
- An **alternative name** is a **state cipher**, as the encryption of each digit is dependent on the current state.

Block Ciphers

- Basis:
  - Take blocks of input and encrypt entire block
  - Reusable keys
  - Different modes
- Keep in mind potential problem areas:
  - Block padding
  - Initialization vectors
  - Codebook attacks, use the right modes

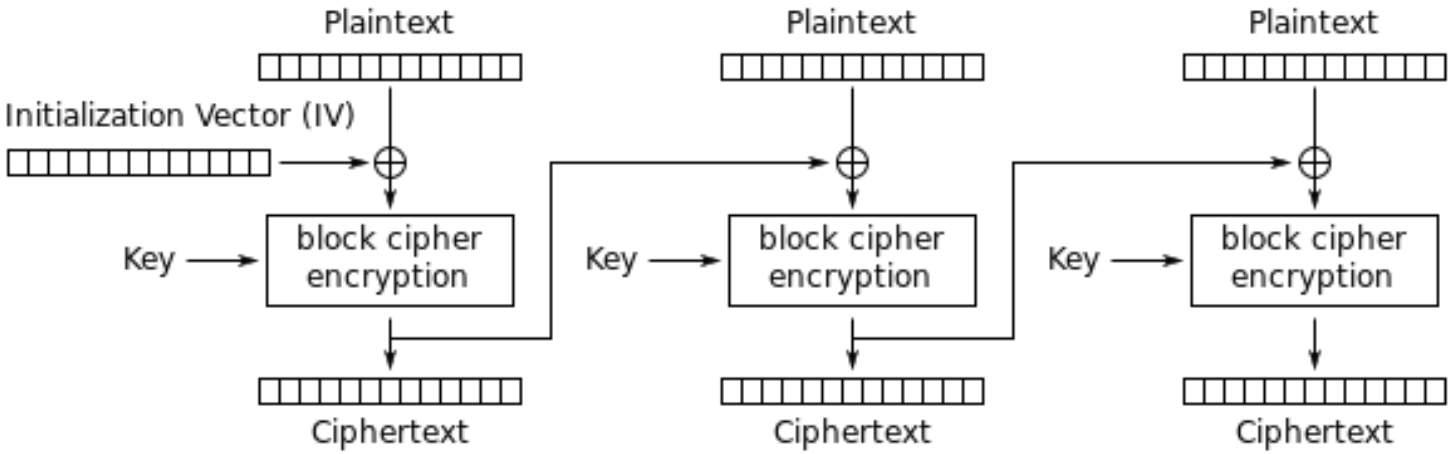
Block Ciphers

- Modes of Operation:
  - 4 Modes defined in FIPS
- **Electronic Code Book** – separately encrypt each block, patterns recognizable, "codebook" can be built up



Electronic Codebook (ECB) mode encryption

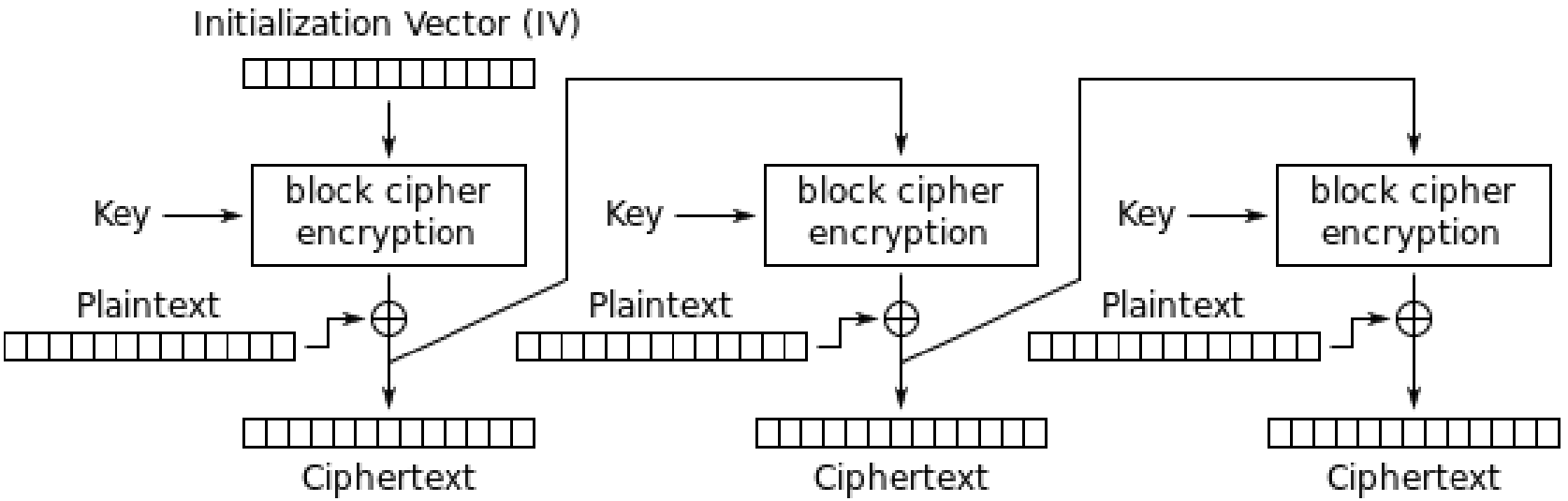
Cipher Block Chaining – XOR plaintext with previous cipher text block, then encrypt, use initialization vector for first block, makes identical inputs look different



Cipher Block Chaining (CBC) mode encryption

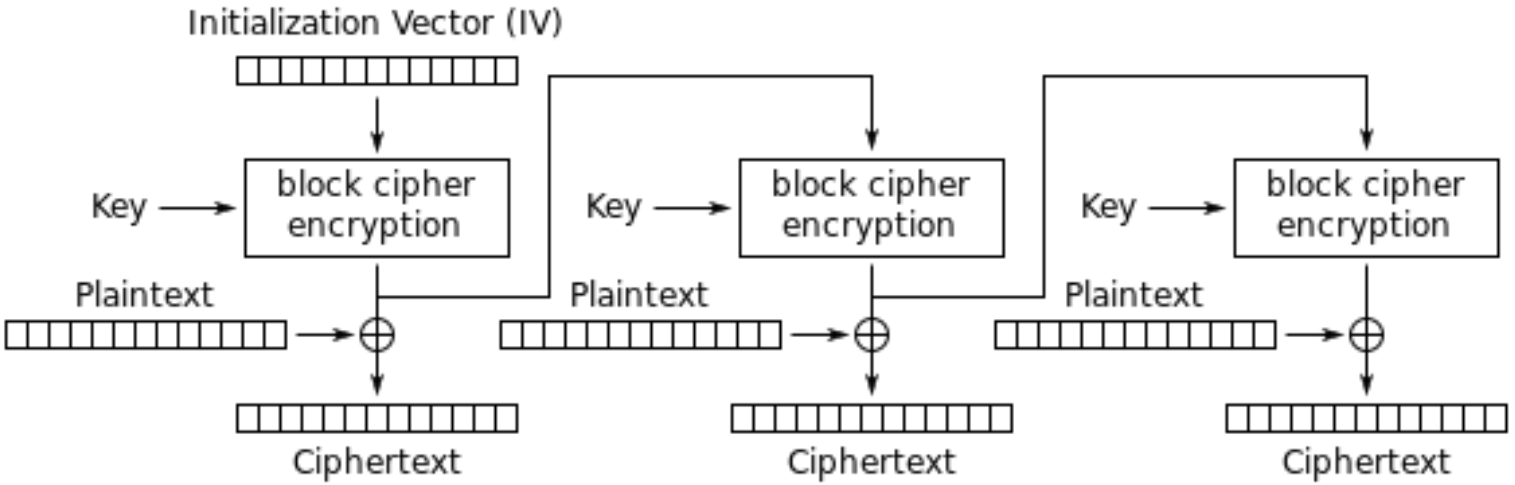
Block Ciphers

- **Cipher text Feedback** – take previous cipher text, encrypt, then XOR with plaintext



Cipher Feedback (CFB) mode encryption

- **Output Feedback** – encrypt previous output, then XOR with plaintext to get cipher text, uses counters to determine where to take from output



Output Feedback (OFB) mode encryption

Block Ciphers

- Basic Construction:
  - Generate key pair
  - Encrypt plaintext
    - Break message into consecutive blocks of length *l* (possibly have to augment the last block with some padding)
    - Encrypt each block with encryption key *r*
  - Decrypt ciphertext
    - Decrypt each block with decryption key *d* and concatenate blocks less padding to get plaintext

Block Ciphers

- The Basic Construction results in ciphertexts that reveal the exact length of the original plaintext
  - This is acceptable and completely hiding the length is futile
  - Encryption schemes that hide some information about the length of the plaintext can easily be constructed

Ciphers

- **Block Ciphers**
  - DES
  - AES
  - IDEA
  - Blowfish
  - RC5
  - GOST
  - CAST
  - SAFER etc…
- **Stream Ciphers**
  - RC4
  - SEAL
  - SNOW
  - FISH
  - Trivium
  - VEST etc…

Ex:

- **Block Ciphers** :

  128-bit block ciphers

  – Twofish
  – Serpent
  – Rijndael

  64-bit block ciphers

  – IDEA
  – Blowfish
  – DES

- **Stream Ciphers**

  – RC4
  – SEAL
  – SNOW

S-Box

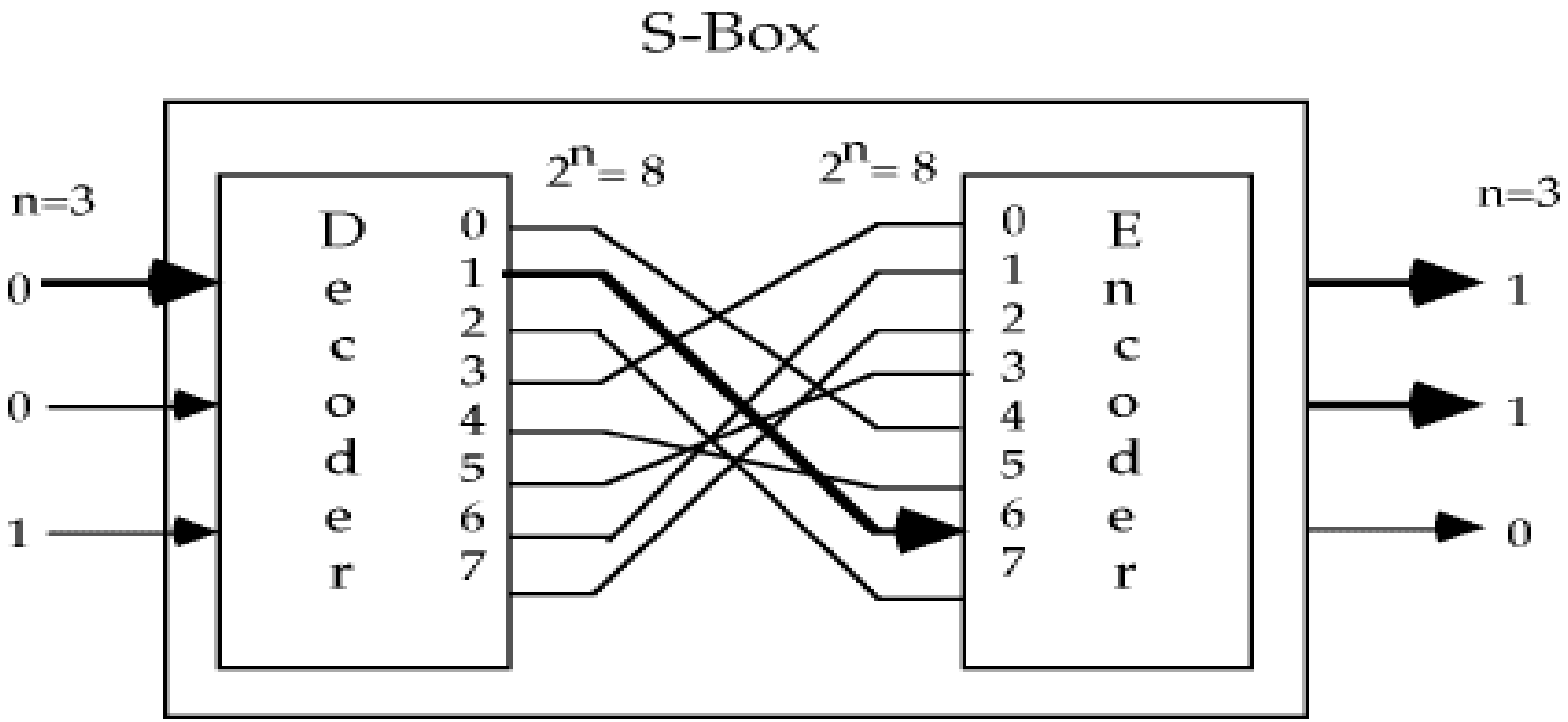


Fig 2.1 Substitution Operation

P-Box

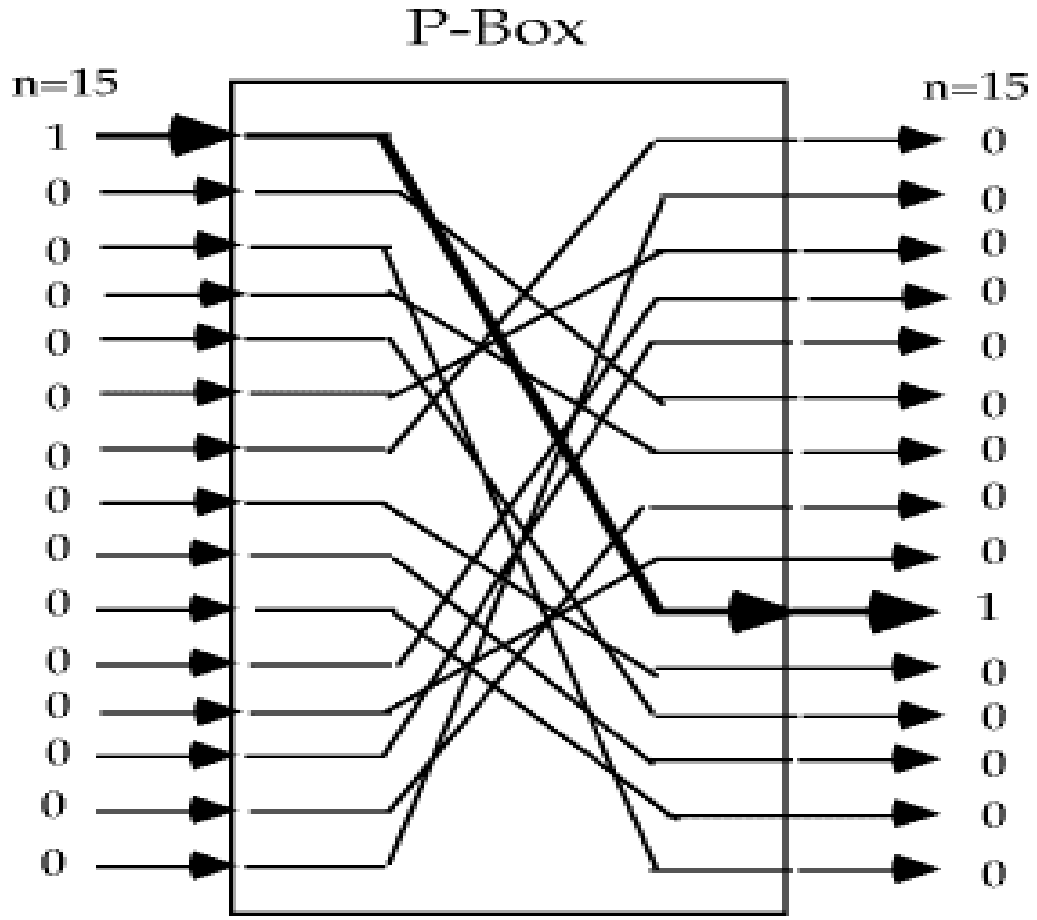


Fig 2.2 - Permutation or Transposition Function

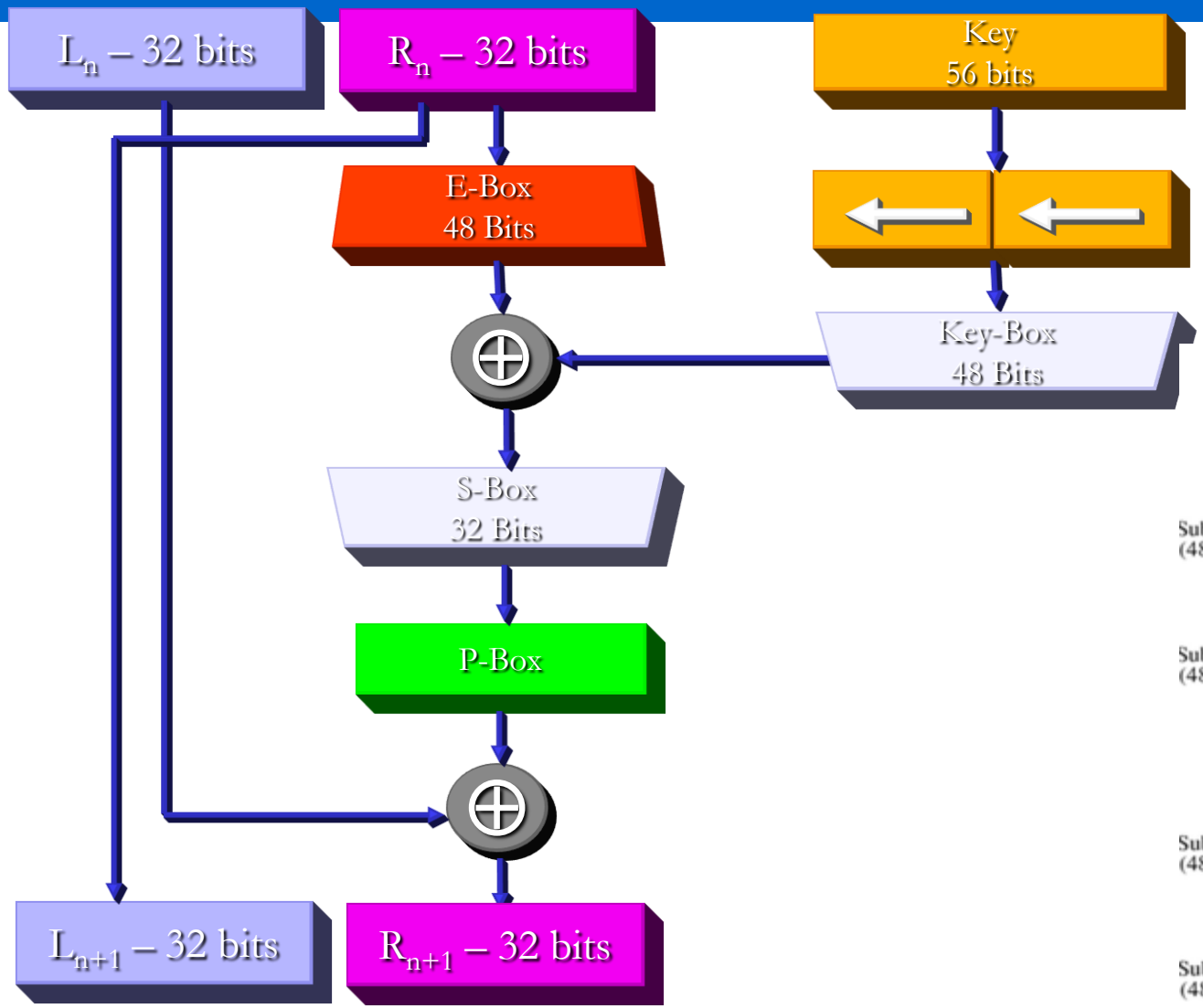
Choice of Crypto Algorithm

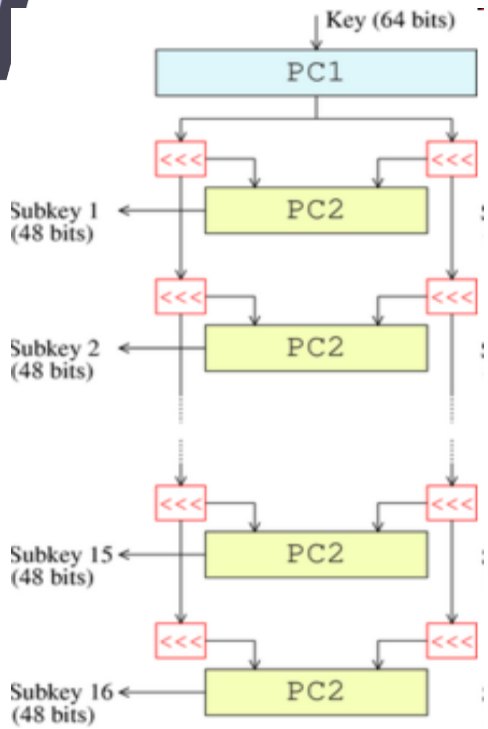
- No. of Rounds
- Combination of S & P Boxes
- Who has implemented the Algorithm
- Whether it is Open Source or Proprietary

Data Encryption Standard

- **DES** (Data Encryption Standard)
  - a very popular encryption scheme
  - Processes blocks of data at a time.
  - A simplified version of DES, i.e S-DES is used for educational purposes.
- Created by IBM called LUCIFER
- Adopted in 1977 by National Bureau of Standards (now NIST)
- 56 bit key to encrypt 64 bit blocks
- Consists of 16 stages plus initial/final permutations

DES – One Round





Attacks on DES

- Weak key size
  - Originally used a 128 bit key
  - Shortened to 56 bits to fit on 1 chip
- Brute force attacks
  - Deep Crack– EFF built $210K system
  - Distributed.Net– 1000s of Internet connected systems working together

Hash Function

- A hash function is a cryptographic mechanism that operates as one-way function

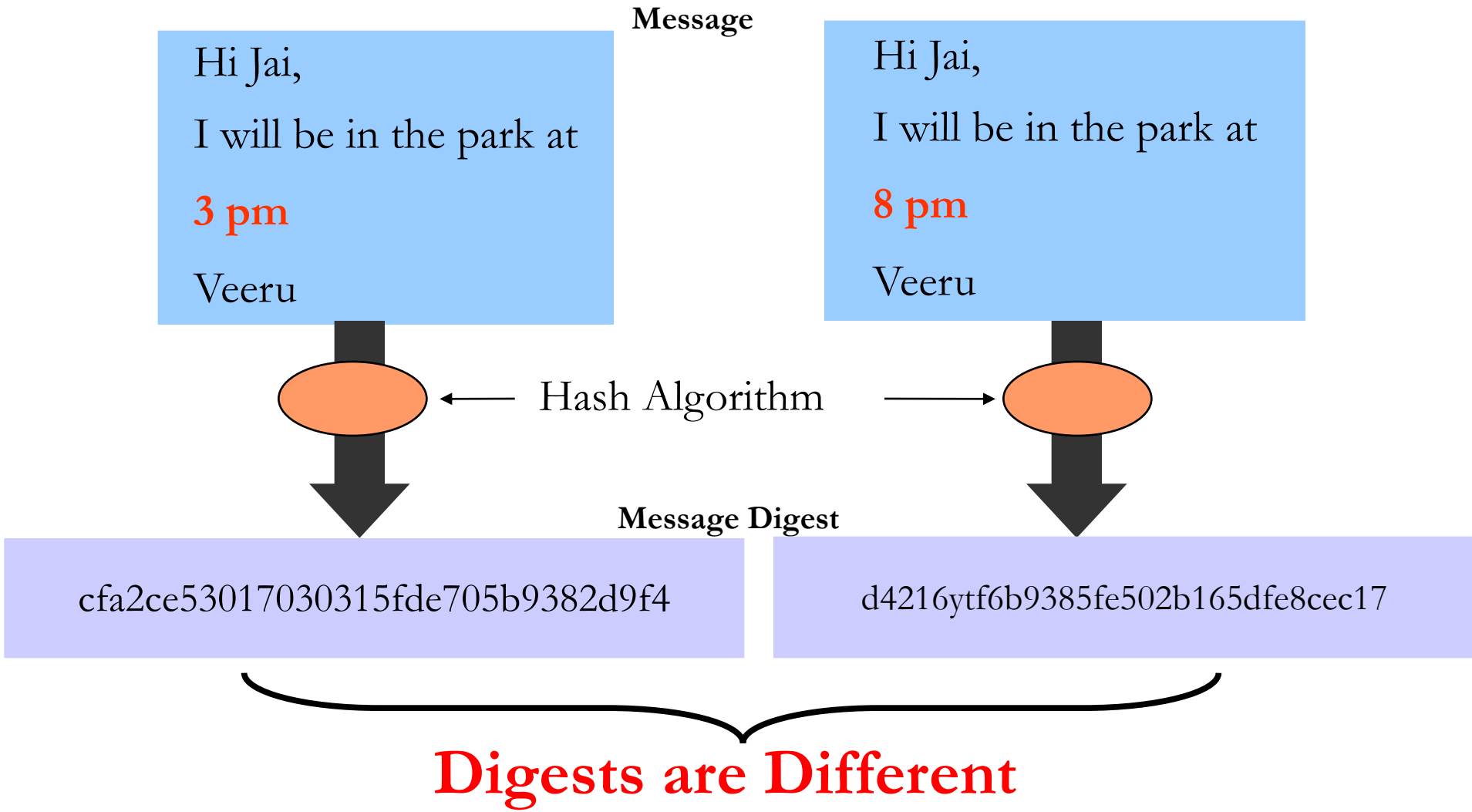
  - Creates a digital representation or "fingerprint“ (Message Digest)
  - Fixed size output
  - Change to a message produces different digest

  Examples : MD5 , Secure Hashing Algorithm (SHA)

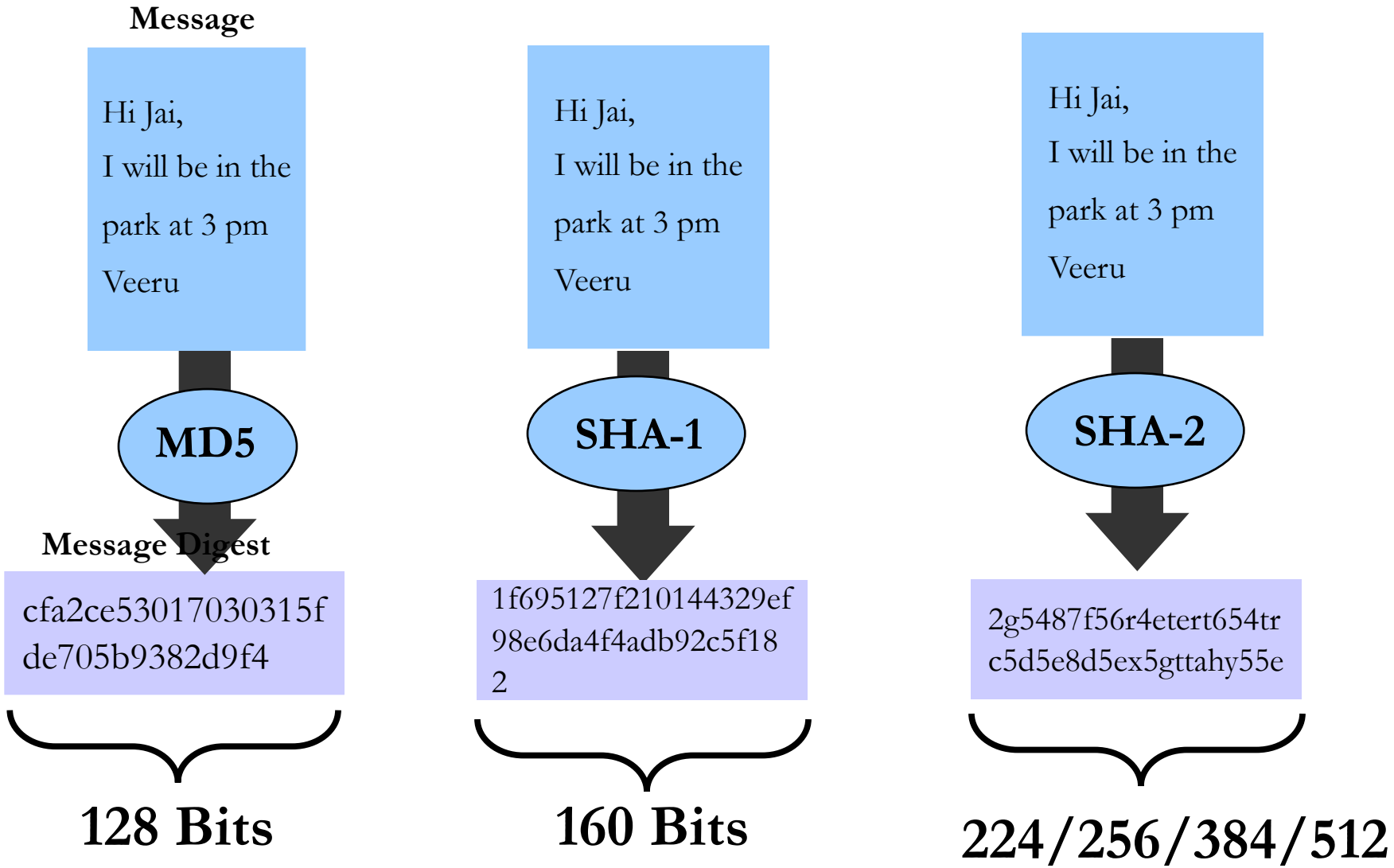
Hash function -Properties

- **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

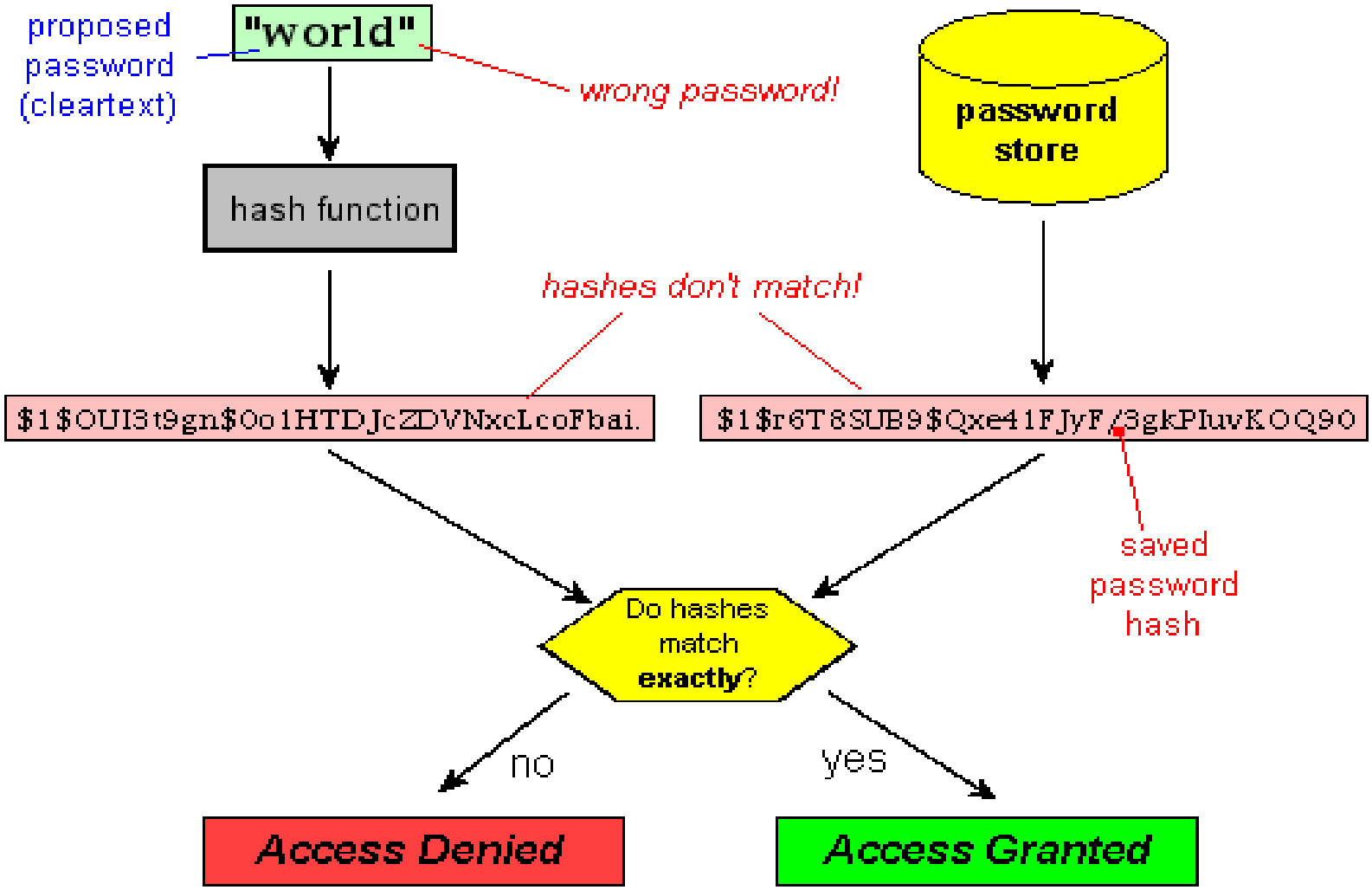
Hash - Example



MD5 and SHA



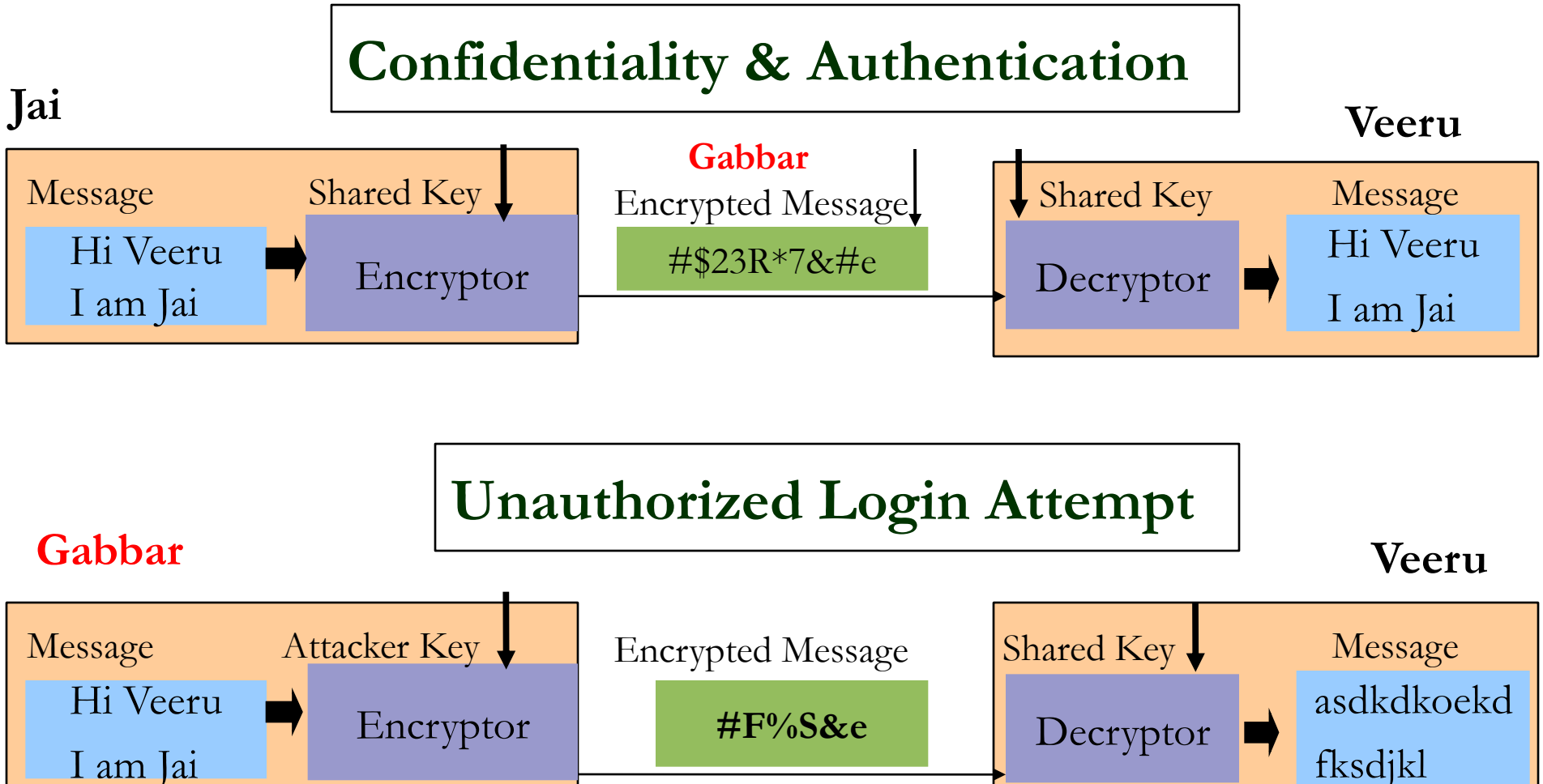
Example of Hash functions



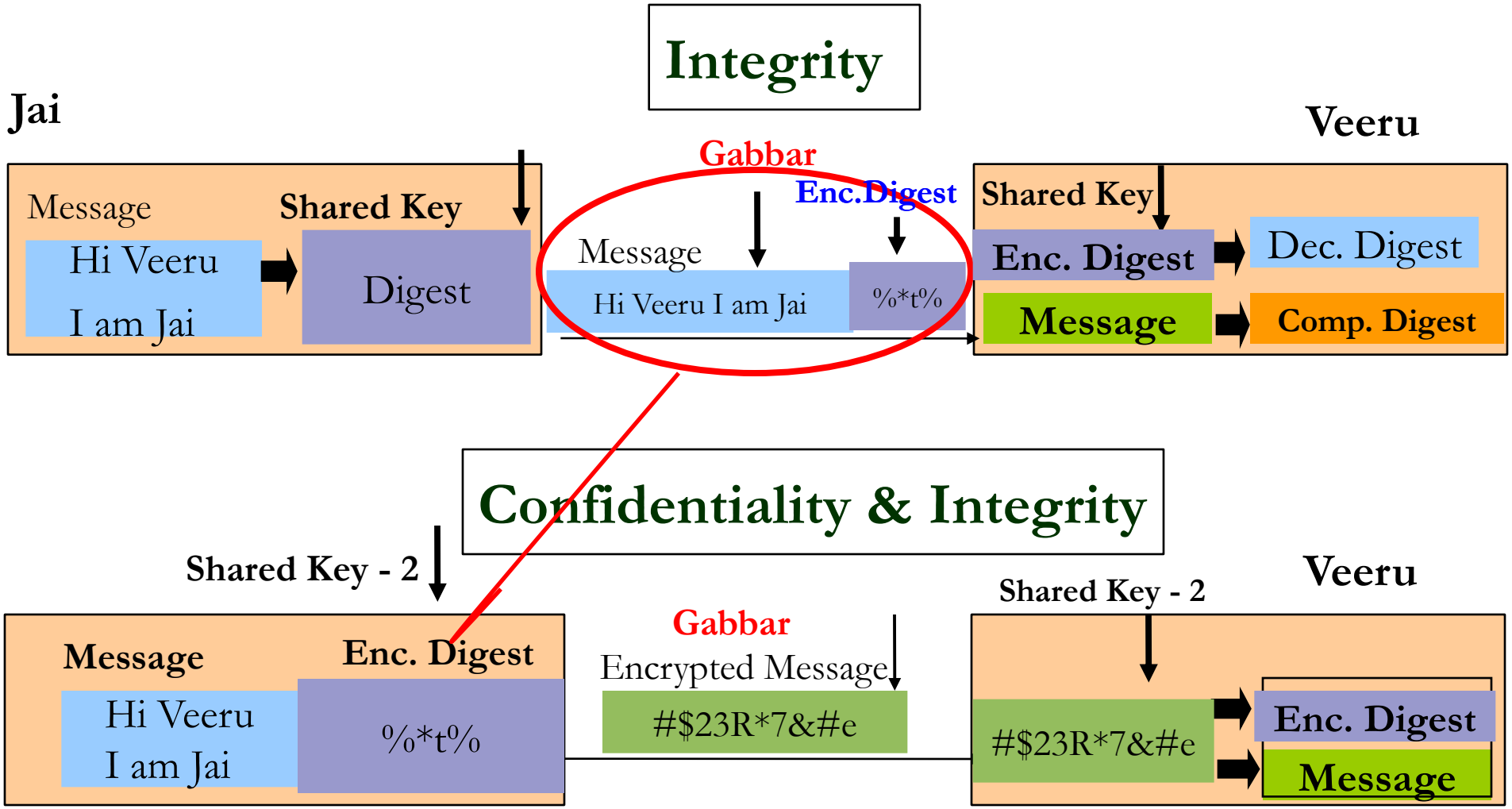
Symmetric Key Cryptography

- 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



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

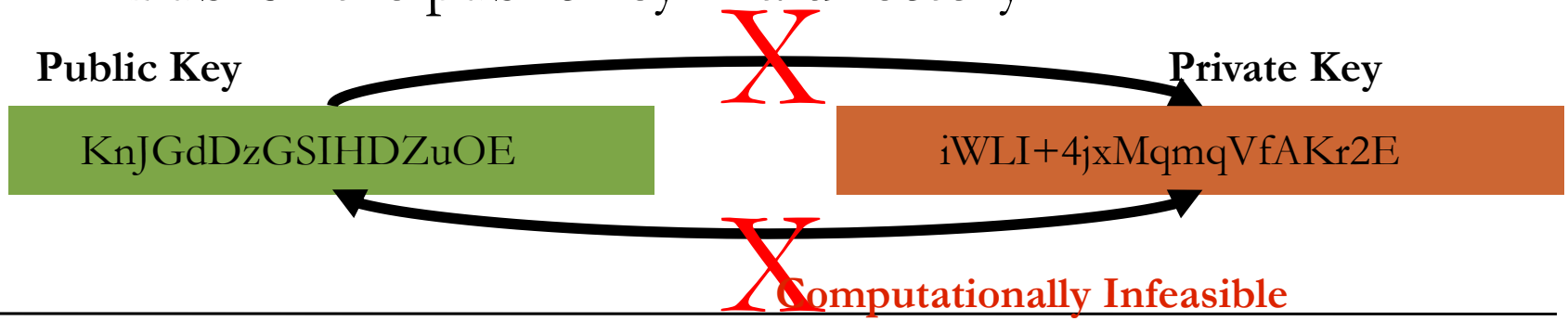
What can be achieved using Symmetric Key ?

- 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 Encryption

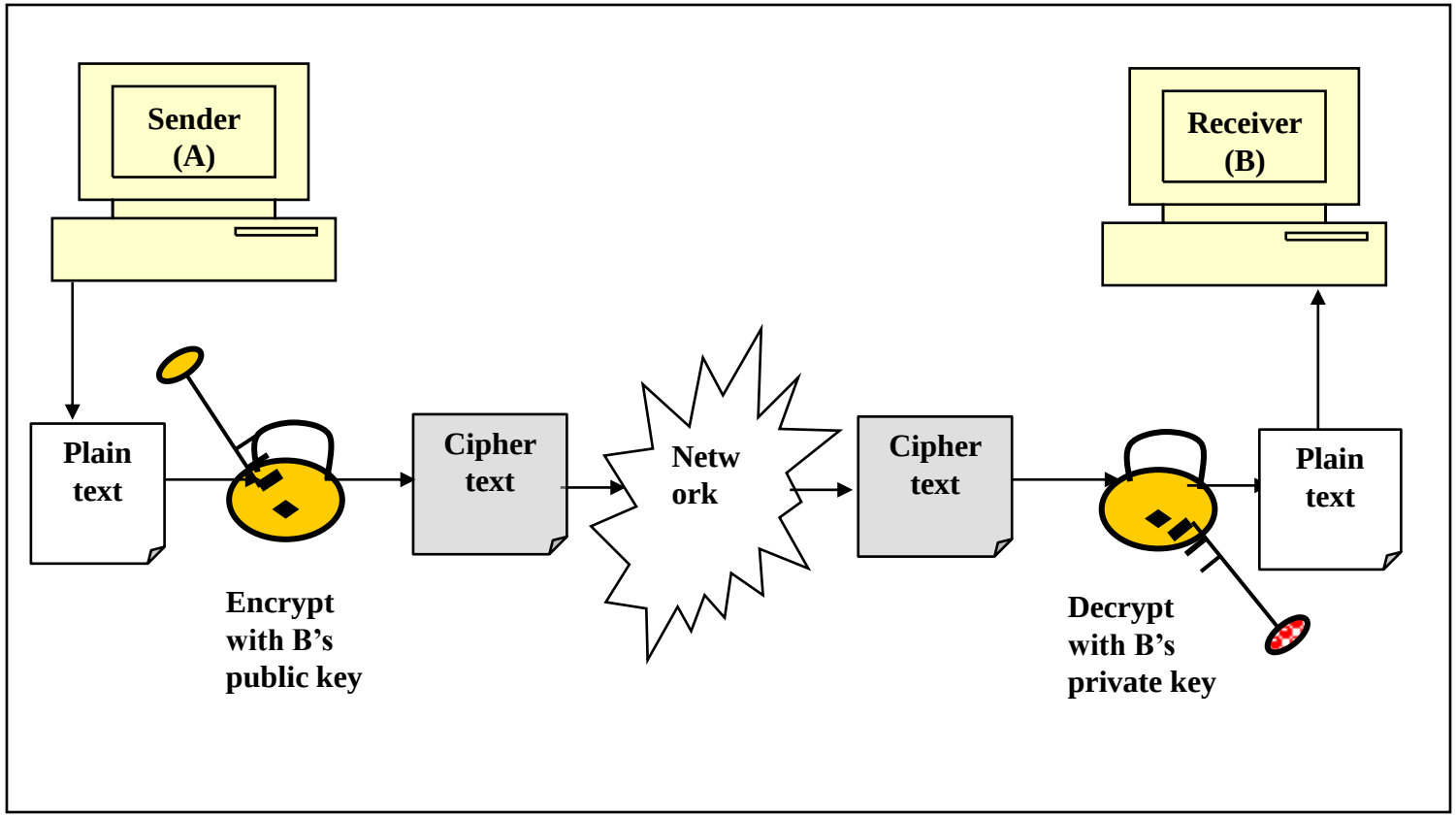
- Important to know who should know which key(s)

- In general:
  - Sender encrypts with recipient's public key
  - Recipient decrypts with its private key

Matrix of Keys

Key details	*A* should know	*B* should know
A's private key	Yes	No
A's public key	Yes	Yes
B's private key	No	Yes
B's public key	Yes	Yes

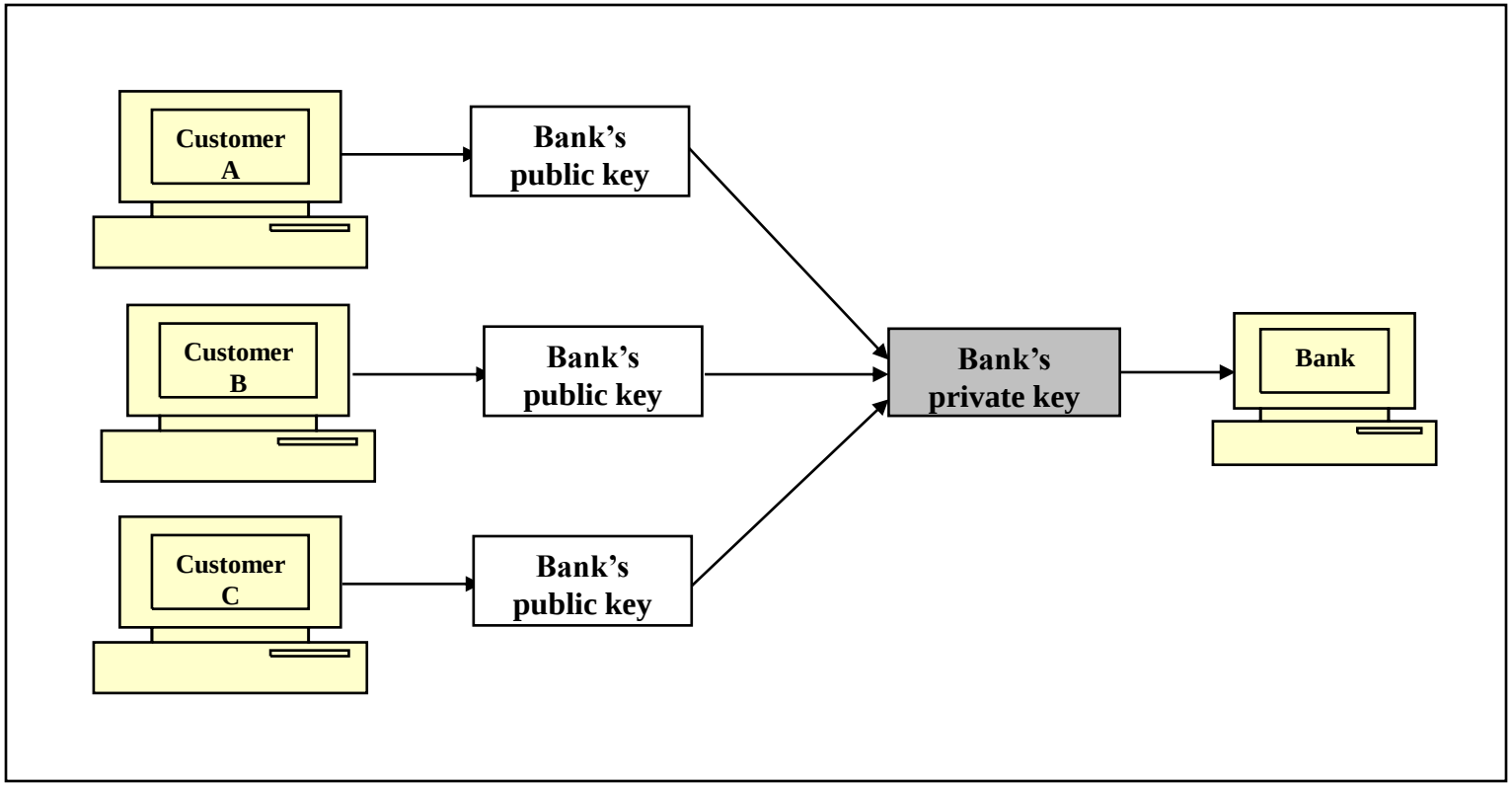
Asymmetric Key Cryptography



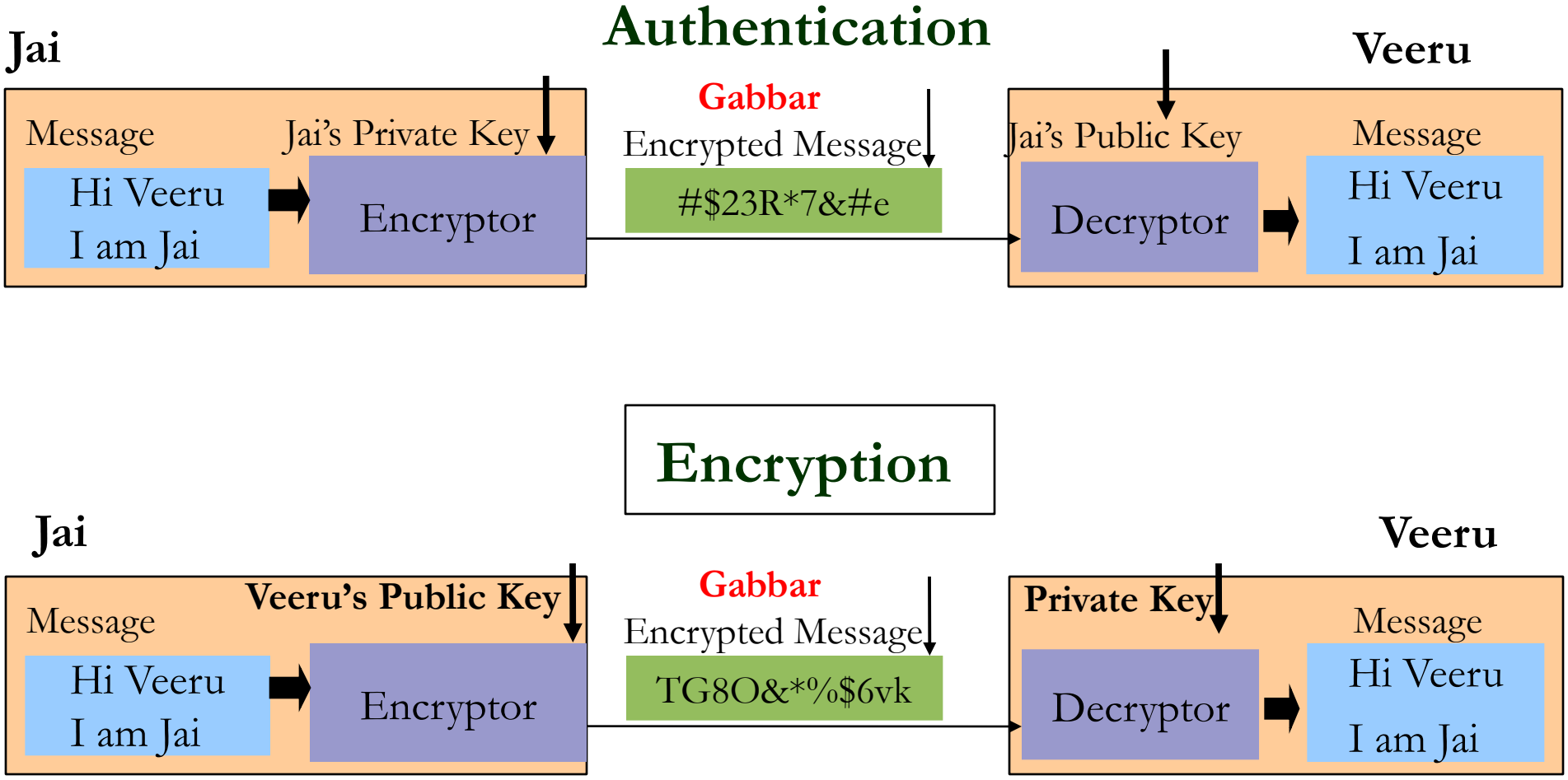
Asymmetric Key Example

- Consider a bank and its customers
- Customers encrypt their messages with bank's public key
- Bank decrypts messages with its private key

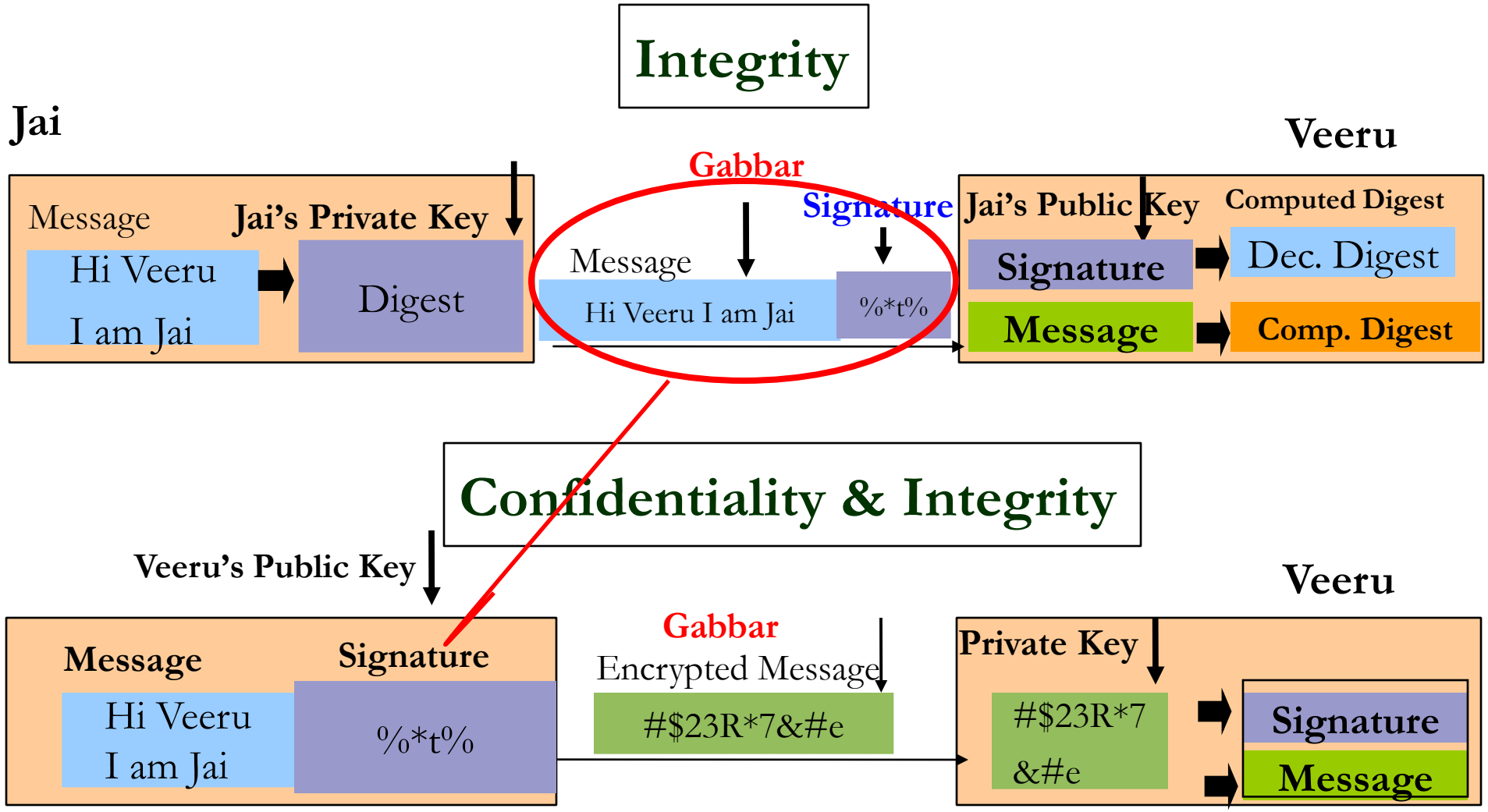
Asymmetric Key Cryptography -- Example



Asymmetric Key Cryptography



Asymmetric Key



Public Key Pros and Cons

Weakness

- Extremely slow

Strength

- Solves problem of passing the key

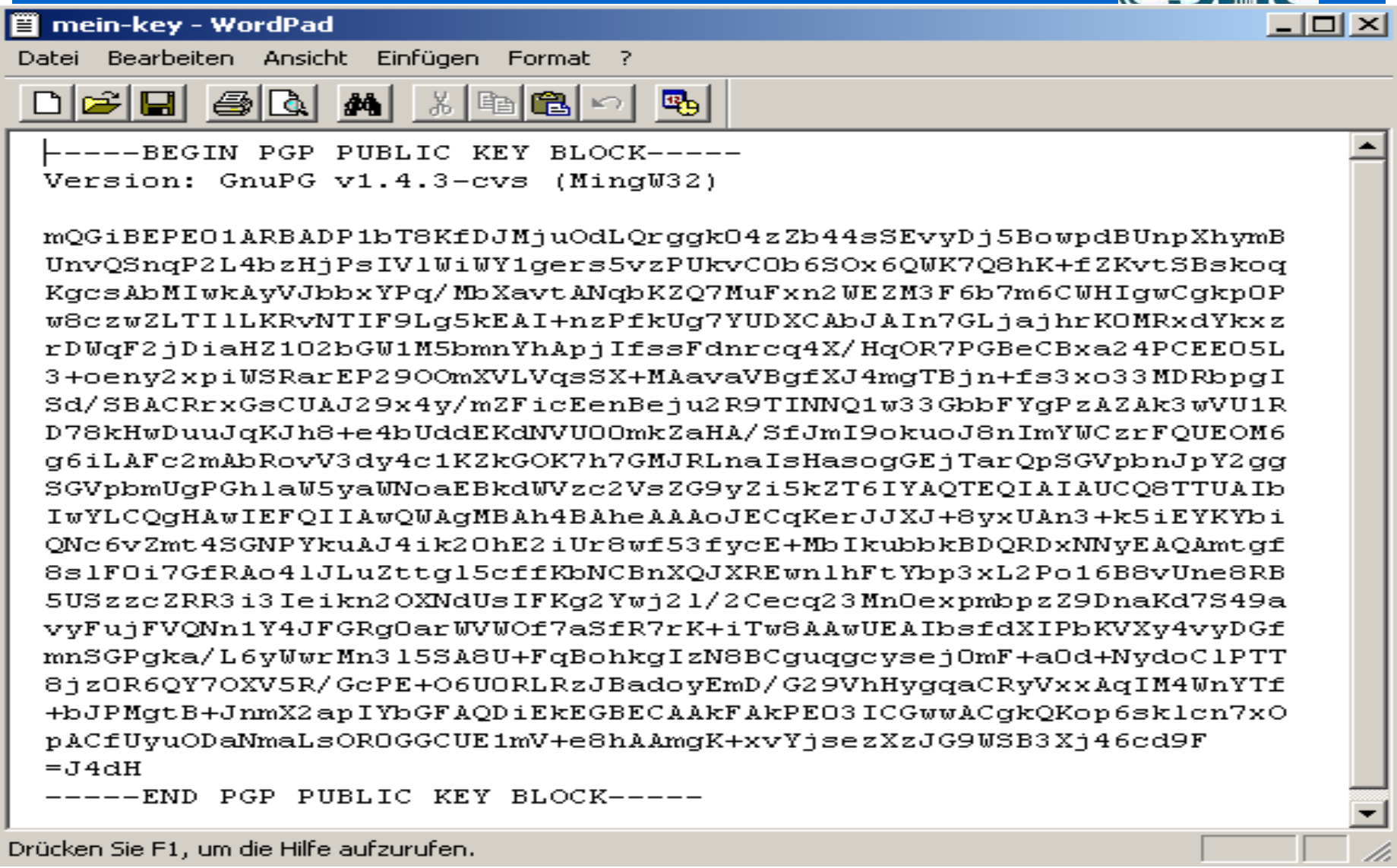
Key Aspects

- Public key encryption; RSA

Misconceptions

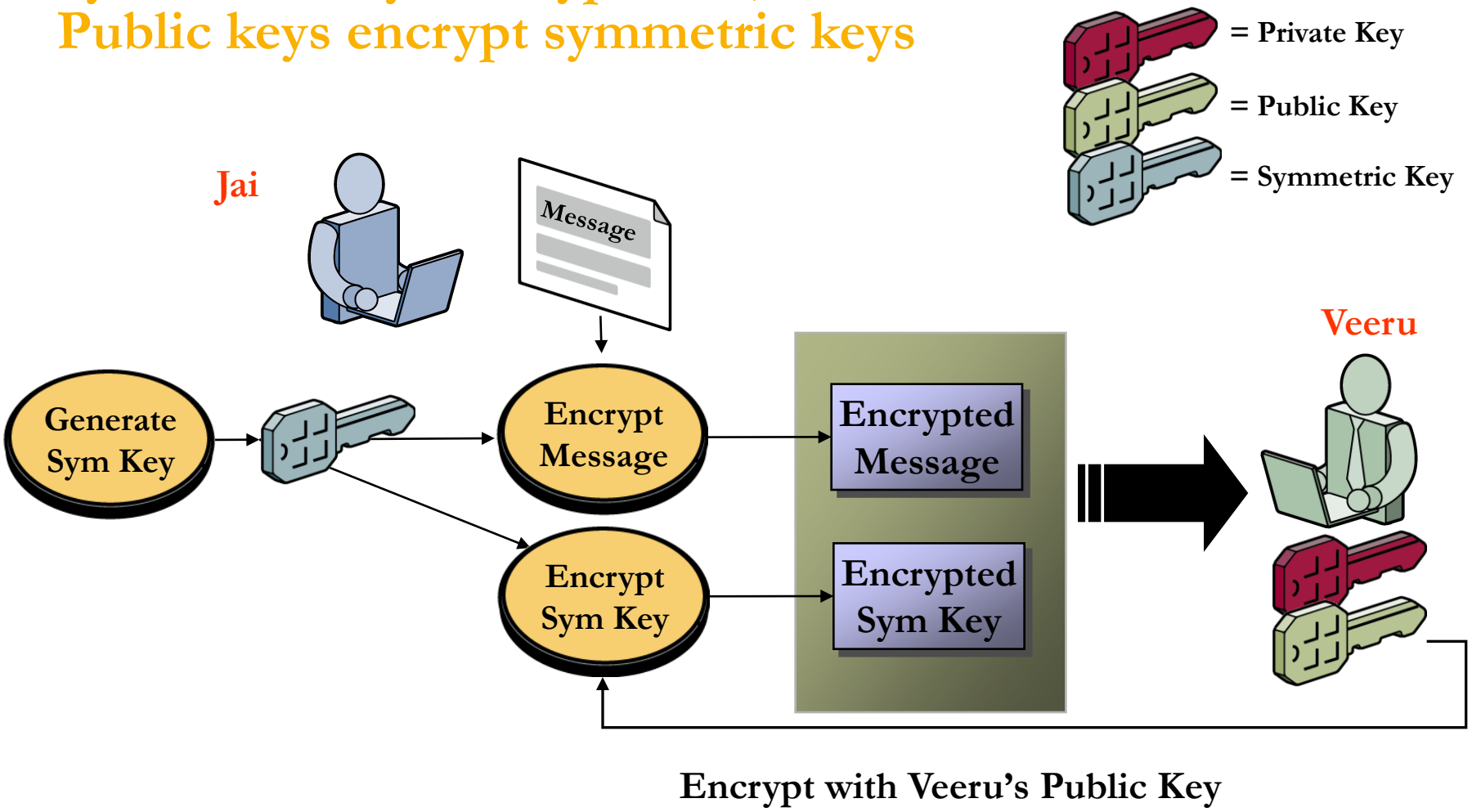
- More secure
- Has made Symmetric encryption obsolete

Example Public Key

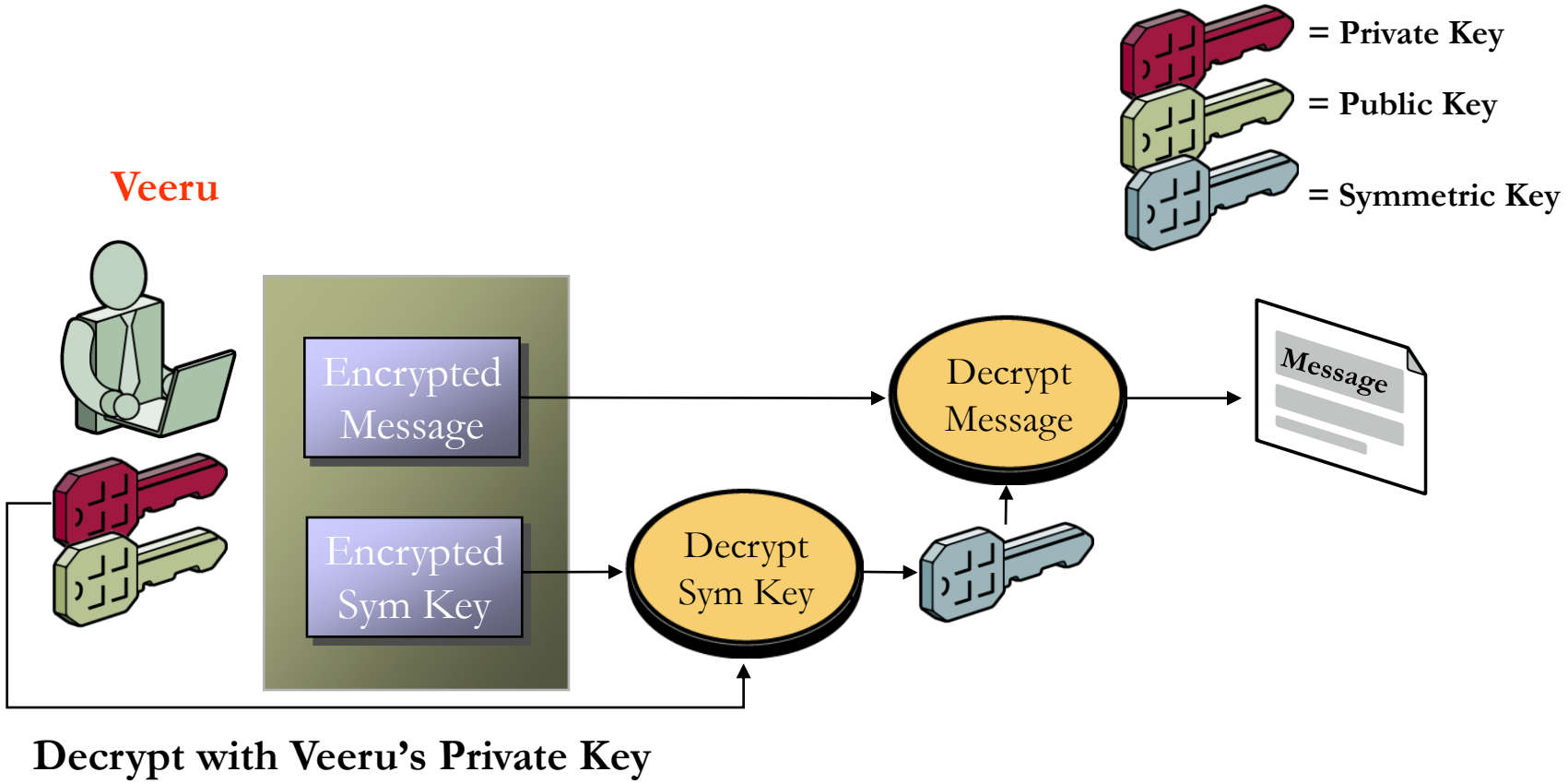


Public Key Encryption

Symmetric keys encrypt data;
Public keys encrypt symmetric keys



Public-Key – Decryption



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-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