Cryptography Algorithm

Marwadi University

Department of CE

Unit title :
Cryptography
Algorithm

Asst. Prof. Krupali Gosai

Cryptography

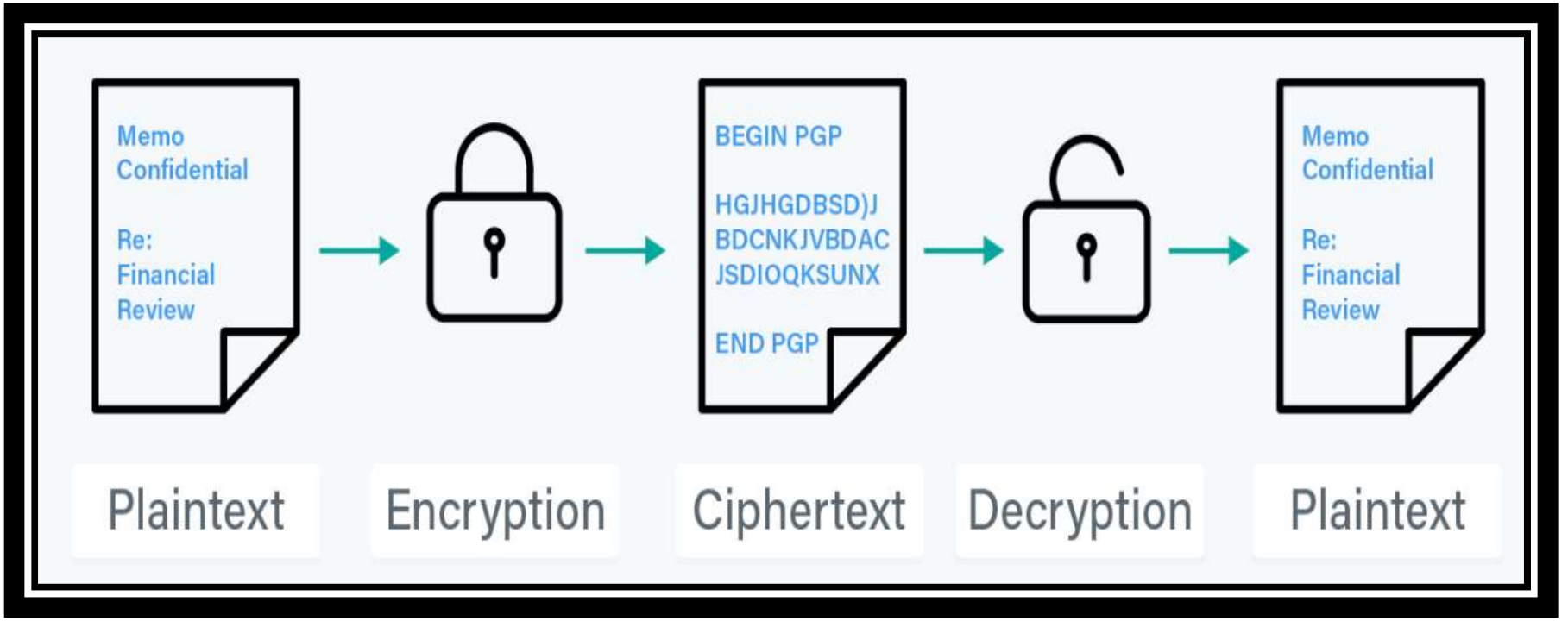
- Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.
- The term is derived from the Greek word *kryptos*, which means hidden.
- It is closely associated to encryption, which is the act of scrambling ordinary text into what's known as cipher text and then back again upon arrival.

Some Basic Terminology

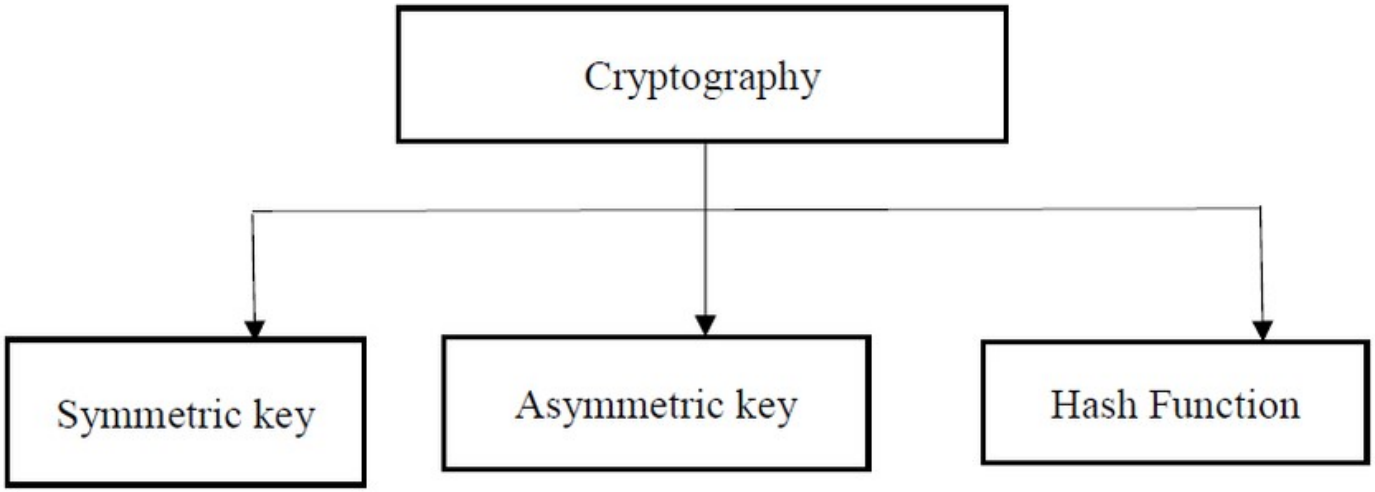
- **Plaintext** - original message
- **Cipher text** - coded message

- **Cipher** - algorithm for transforming plaintext to cipher text
- **Key** - info used in cipher known only to sender/receiver
- **Encipher (encrypt)** - converting plaintext to cipher text
- **Decipher (decrypt)** - recovering cipher text from plaintext

- **Cryptography** - study of encryption principles/methods
- **Cryptanalysis (codebreaking)** –it is the science of attacking cryptosystems(deduce the key and/or recover the plaintext)
- **Cryptology** - field of both cryptography and cryptanalysis


Memo
Confidential
Re:
Financial
Review
BEGIN PGP
HGJHGDBSD)J
BDCNKJVBDAC
JSDIOQKSUNX
END PGP
Memo
Confidential
Re:
Financial
Review
Plaintext
Encryption
Ciphertext
Decryption
Plaintext

Types of Cryptography

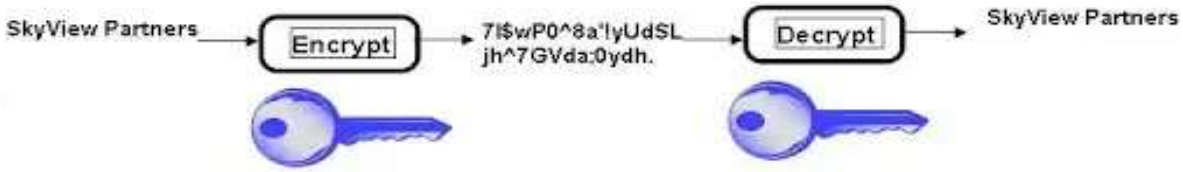


Types of Encryption

DES
TripleDES
AES
RC5

Symmetric Keys

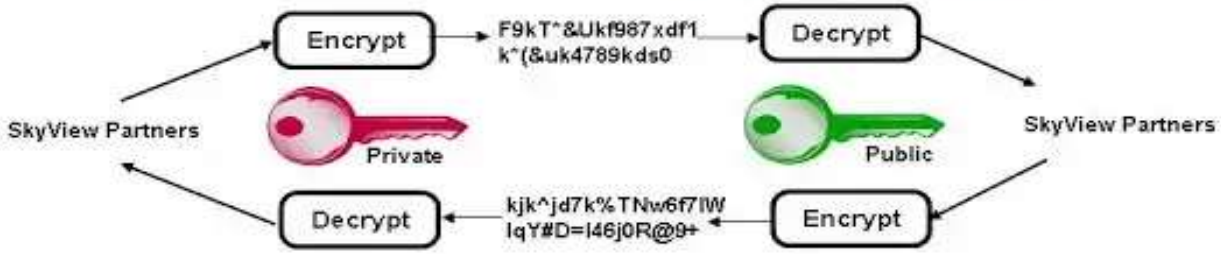
- Encryption and decryption use the **same key**.



RSA
Elliptic Curve

Asymmetric keys

- Encryption and decryption use different keys, a **public key** and a **private key**.



MD5
SHA-1

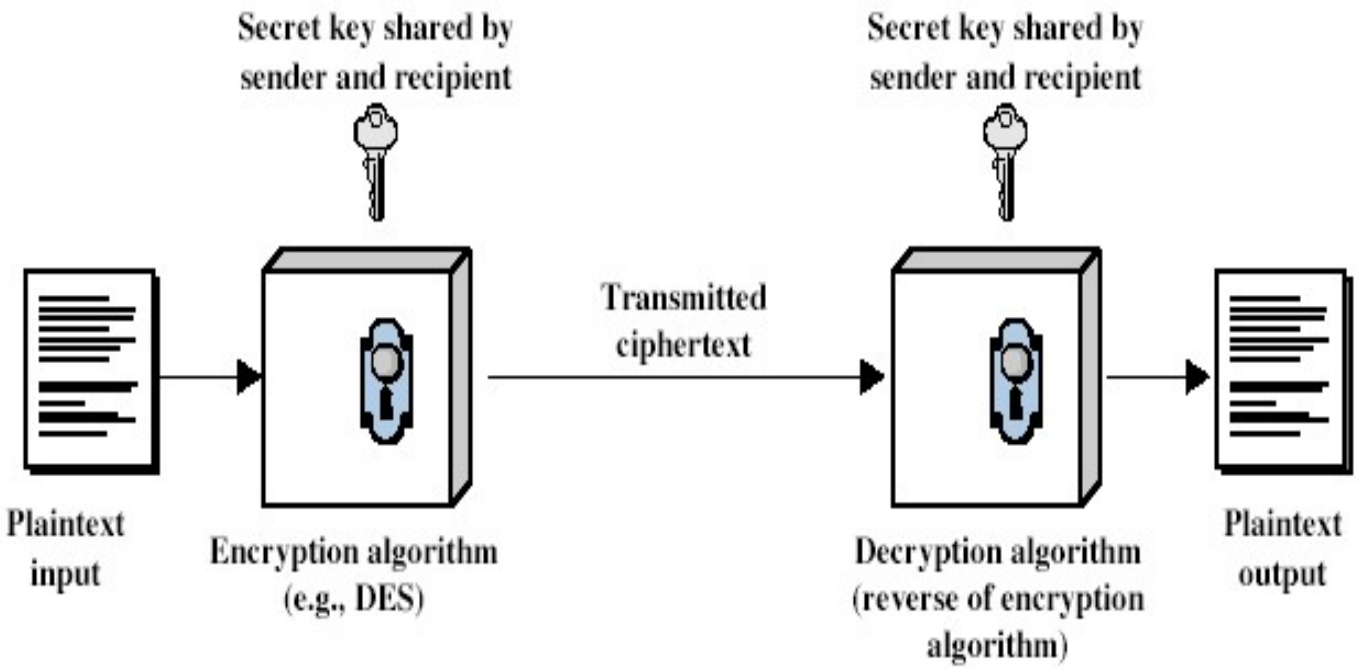
One-way hash

Symmetric Encryption

- Conventional / private-key / single-key
- sender and recipient share a common key
- all classical encryption algorithms are private-key.

- It was only type prior to invention of public-key in
- 1970's and by far most widely used

Symmetric Cipher Model



Requirements

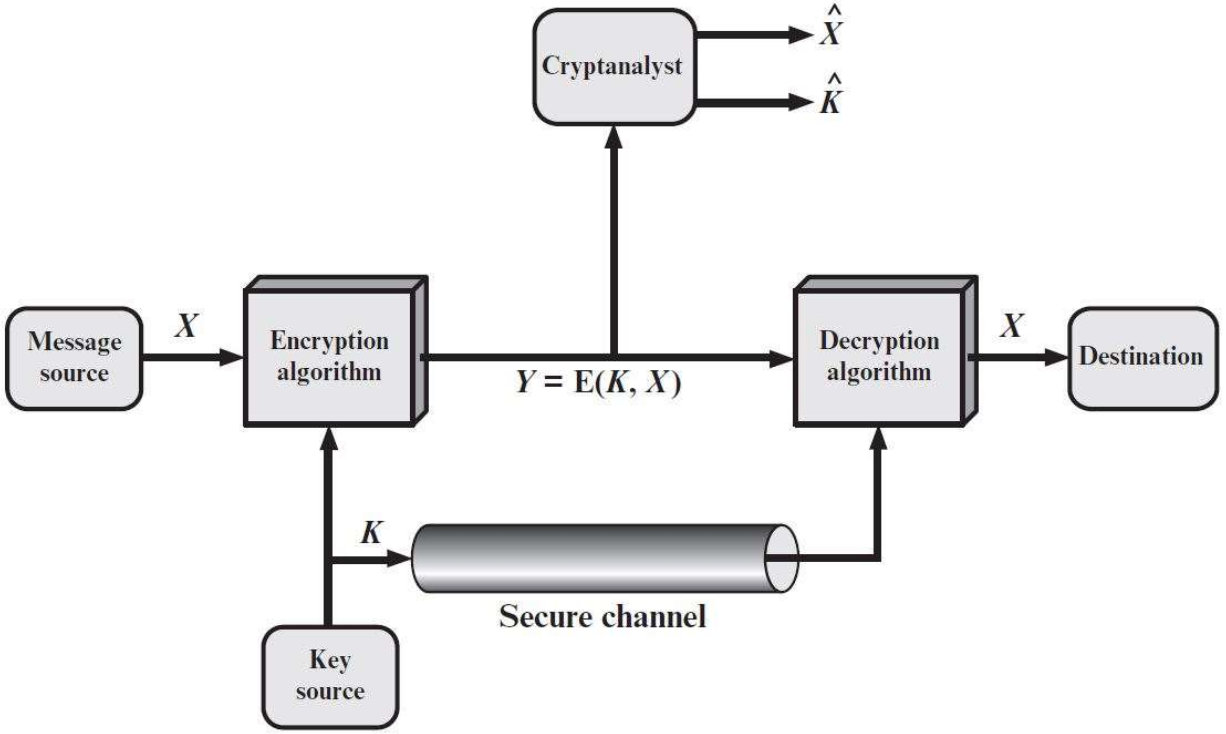
- Two Requirements for secure use of symmetric encryption:
  - 1. a strong encryption algorithm
  - 2. a secret key known only to sender / receiver
  - mathematically have:

    $Y = E_K(X)$

    $X = D_K(Y)$

- X = plaintext
- Y = ciphertext
- K = secret key
- E = encryption algorithm
- D = decryption algorithm
- Both E and D are known to public

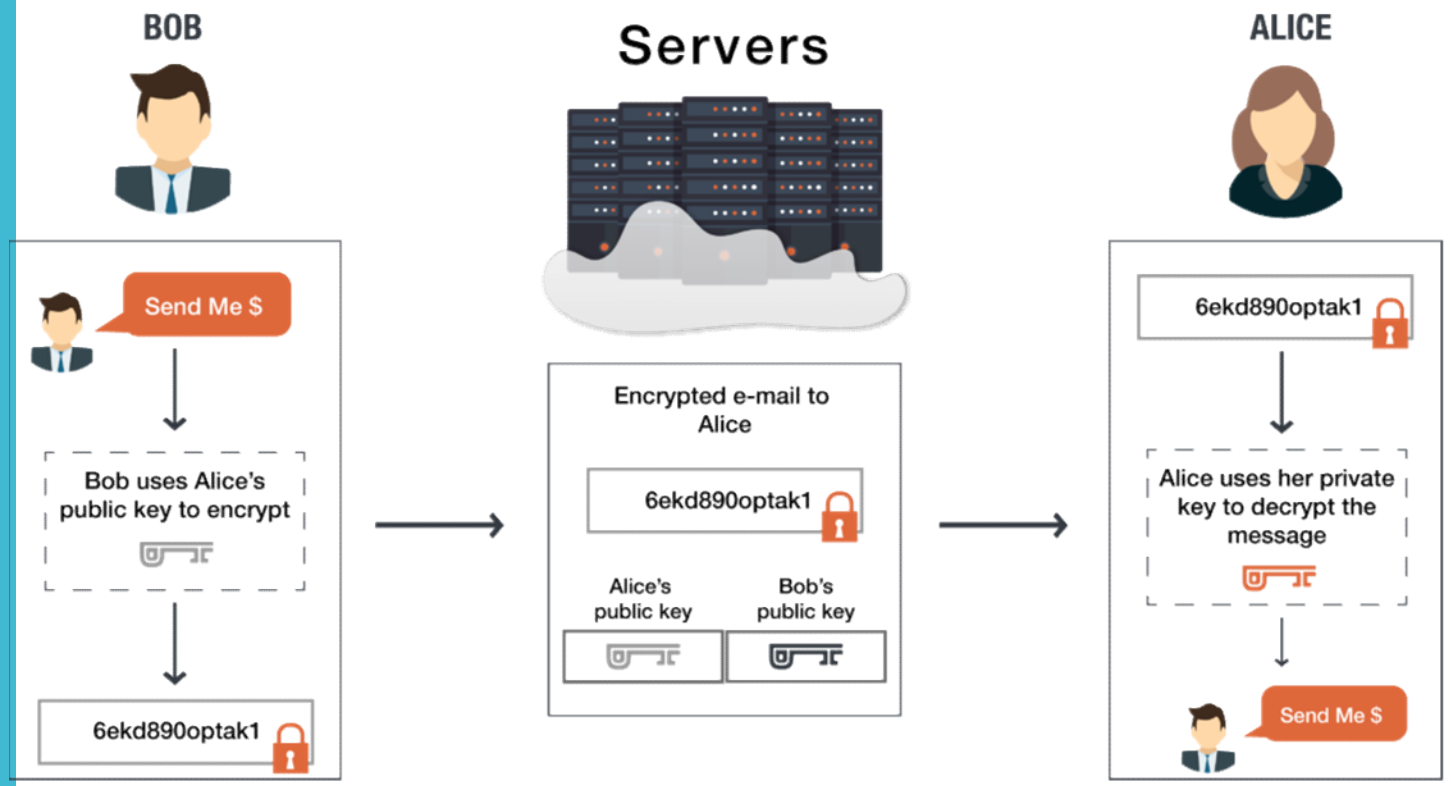
Symmetric Cipher Model



Best Uses

- 1)In services that store encrypted data on **behalf of a user** (like cloud backup services)
- 2)To encrypt computer or **device storage**(Computer password)
- 3)To create a secure channel between **two network endpoints**, provided there's a separate scheme for securely exchanging the key

Asymmetric key cryptography



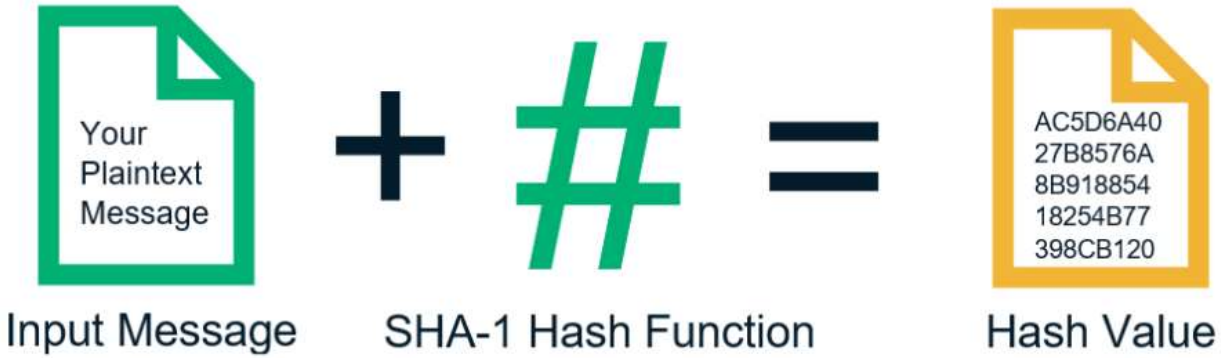
Symmetric Key Cryptography & Asymmetric Key Cryptography

Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two key one to encrypt and the other one to decrypt.
The size of cipher text is same or smaller than the original plain text.	The size of cipher text is same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amount of data.
It only provides confidentiality.	It provides confidentiality, authenticity and non-repudiation.
Examples: 3DES, AES, DES and RC4	Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA

Hash

- Hashing is used ***only to verify data***
- the **same input** will always produce the **same output**
- it's **impossible to reverse** it back to the original data
- given knowledge of only the hash, it's **infeasible** to create another string of data that will create the same hash (called a "collision" in crypto parlance)

An Example of a Hash Function

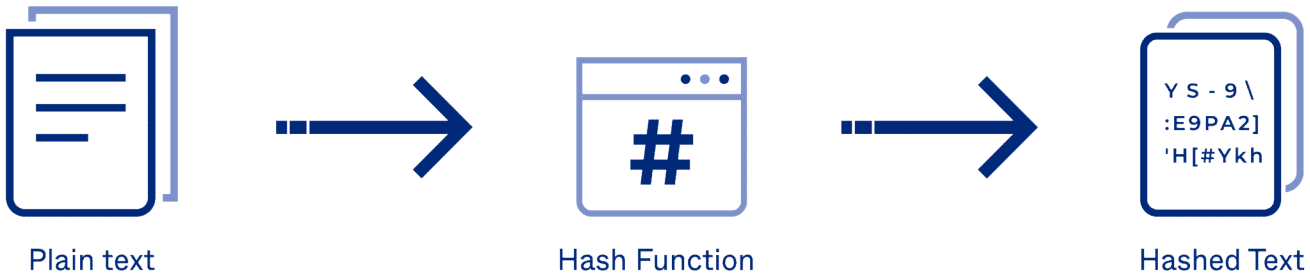


Encryption

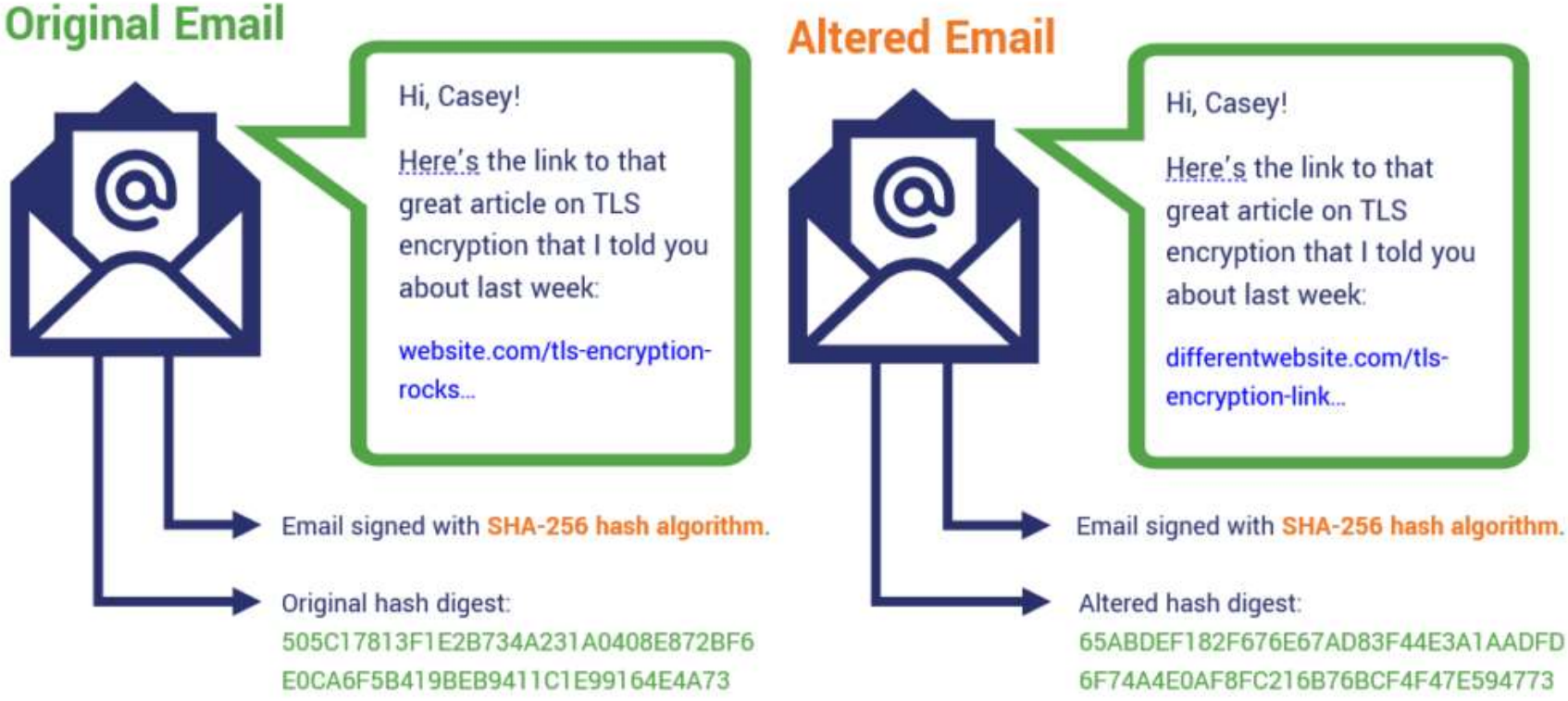
(used to protect sensitive information)

Hashing

(used to validate information)



How Hashing Ensures Data Integrity



Substitution Ciphers

- where letters of plaintext are replaced by other letters or by numbers or symbols.
- if plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns
- 1. Caesar cipher
- 2. Monoalphabetic cipher
- 3. Play fair cipher
- 4. Hill cipher
- 5. Polyalphabetic ciphers
- 6. OTP(One time pad)

Caesar Cipher

- Can define transformation as:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
D	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**

s	t	u	v	w	x	y	z
V	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**

- Mathematically give each letter a number

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**

p	q	r	s	t	u	v	w	x	y	z
15	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**

- then have Caesar cipher as:

  $c = E(p) = (p + k) \bmod (26)$

  $p = D(c) = (c - k) \bmod (26)$

Caesar Cipher

- Earliest known substitution cipher by Julius Caesar
- First attested use in military affairs replaces each letter by 3rd letter on example:

```
meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB
```

Caesar Cipher

- Can define transformation as:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
D	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**

s	t	u	v	w	x	y	z
V	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**

- Mathematically give each letter a number

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**

p	q	r	s	t	u	v	w	x	y	z
15	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**

- then have Caesar cipher as:

  $c = E(p) = (p + k) \bmod (26)$

  $p = D(c) = (c - k) \bmod (26)$

Cryptanalysis of Caesar Cipher

- Only have 26 possible ciphers
- A maps to A,B,..Z
- Could simply try each in turn
- a brute force search
- given ciphertext, just try all shifts of letters do need to recognize when have plaintext
- eg. break ciphertext "GCUA VQ DTGCM"

Playfair Cipher

- One approach to improving security is to encrypt multiple letters at a time.
- The Playfair Cipher is the best known such cipher.
- Invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair.

Playfair Key Matrix

- a 5X5 matrix of letters based on a keyword
- fill in letters of keyword (sans duplicates)
- fill rest of matrix with other letters
- eg. using the keyword MONARCHY
- Plain Text = BALLOON

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

Encrypting and Decrypting

- Plaintext is encrypted two letters at a time
- 1. if a pair is a repeated letter, insert filler like 'X'
- 2. if both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
- 3. if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom)
- 4. otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair.

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

- 1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that **balloon** would be treated as **ba lx lo on**
- 2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, **ar** is encrypted as **RM**.
- 3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, **mu** is encrypted as **CM**.
- 4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, **hs** becomes **BP** and **ea** becomes **IM** (or **JM**, as the encipherer wishes).

Playfair Cipher Example

- Key = MONARCHY
- Plain-Text= BALLOON

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

Playfair Cipher Example

- Plain-Text= BALLOON
- **After Split : BA LL OO N**
- **Rule 1.** if a pair is a repeated letter, insert filler like 'X'
- Now New Pair : **BA LX LO ON**
- **New Generate Cipher-Text.**
- **BA =**
- **LX =**
- **LO =**
- **ON =**

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

Playfair Cipher Example 1

- Key = MONARCHY
- Plain-Text= INSTRUMENT
- Cipher-Text =

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

Playfair

- If there is an odd number of letters, a X is added to the last letter. Let's say we want to encrypt the message "hide the gold".

- **HI DE TH EG OL DX**

Playfair Cipher Example 2

- Key = MONARCHY
- Plain-Text= HIDE THE GOLD
- Cipher-Text =

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

Security of Playfair Cipher

- Equivalent to a monoalphabetic cipher with an alphabet of 26 x 26 = 676 characters.
- Security is much improved over the simple monoalphabetic cipher.
- Was widely used for many decades
- eg. by US & British military in WW1 and early WW2
- Once thought to be unbreakable.
- Actually, it can be broken, because it still leaves some structure of plaintext intact.

Transposition Ciphers

- now consider classical transposition or permutation ciphers these hide the message by rearranging the letter order without altering the actual letters used can recognize these since have the same frequency distribution as the original text.

Rail Fence cipher

- Write message letters out diagonally over a number of rows then read off cipher row by row
- eg. write message out as:

```
m e m a t r h t g p r y
  e t e f e t e o a a t
```

- giving ciphertext

```
MEMATRHTGPRYETEFETEOAAT
```

Row Transposition Ciphers

- A more complex transposition
- Write letters of message out in rows over a specified number of columns
- then reorder the columns according to some key before reading off the rows

```
Key:          4 3 1 2 5 6 7
Plaintext: a t t a c k p
           o s t p o n e

Ciphertext: TT AP TS AO CO KN PE
```

Steganography

- An alternative to encryption hides existence of message using only a subset of letters/words in a longer message marked in some way using invisible ink hiding in LSB in graphic image or sound file has drawbacks high overhead to hide relatively few info bits.

Thank You!

Any Question…