Government Polytechnic Ahmedabad
Program: Diploma in Computer Engg
Computer and Network Security (3350704-C304)

UNIT_3
Cryptography and Public Key Infrastructure

BASIC TERMS

- **Plain Text(PT):** Data that can be read and understand without any special measure.
- **Cipher Text(CT):** Data that is transformed or converted by Encryption algorithm.
- **Encryption:** Algorithm for transforming plain text to cipher text.
- **Decryption:** Algorithm for transforming cipher text to plain text.

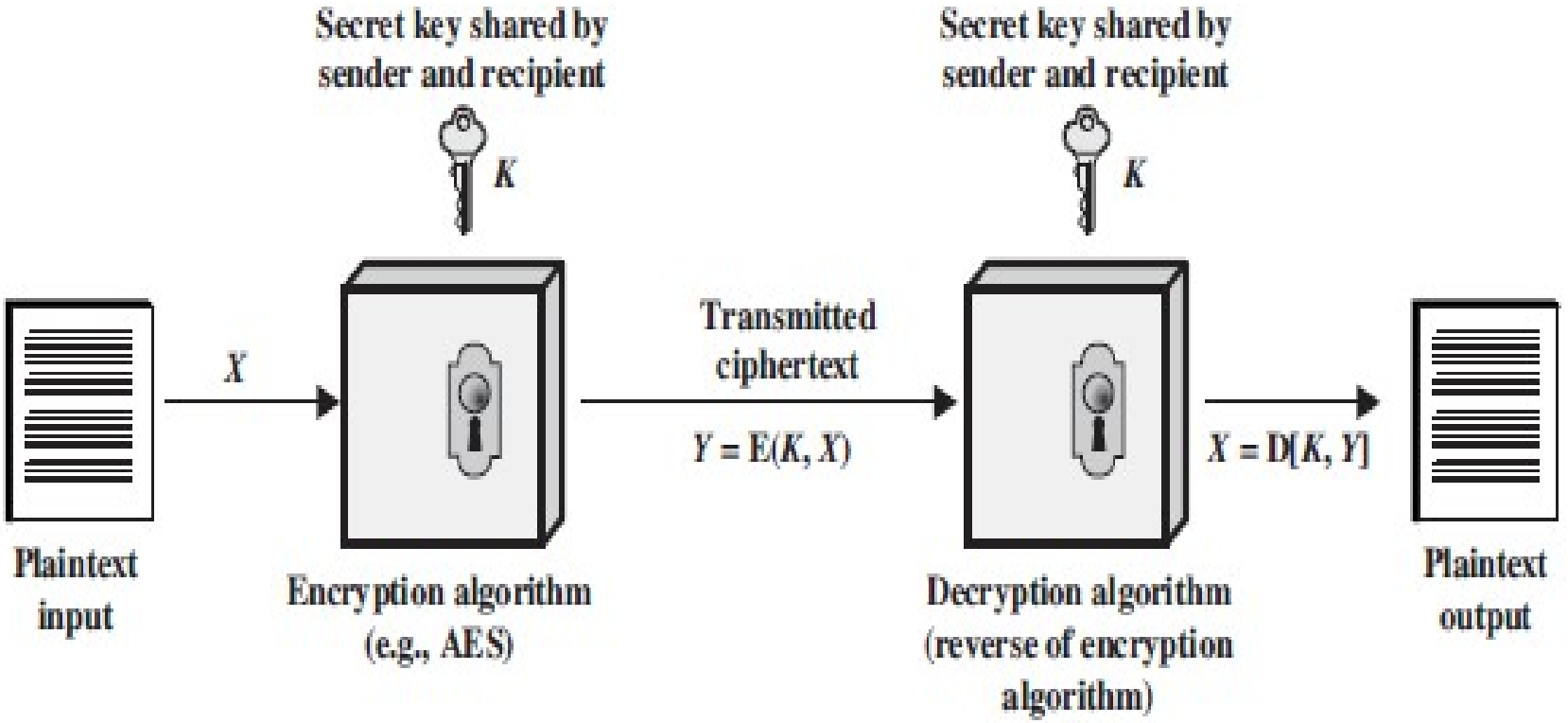
CONT..

- **Key:** It is used for encryption and decryption of message.
- **Cryptography:** It is the science of using mathematics to encrypt and decrypt data.
- **Objectives of Cryptography:**
  - 1.Confidentiality
  - 2. Integrity
  - 3. Non repudiation
  - 4. Authentication

INTRODUCTION ABOUT SYMMETRIC ENCRYPTION

- **Symmetric Encryption:**
- An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message.
- In other terms, Data is encrypted and decrypted using the same key.
- Symmetric-key cryptography is sometimes called secret key cryptography.

CONT….


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

CONT..

- Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Public-key encryption avoids this problem because the public key can be distributed in a non-secure way, and the private key is never transmitted.
- Examples of symmetric algorithms are DES, 3DES and AES

CONT..

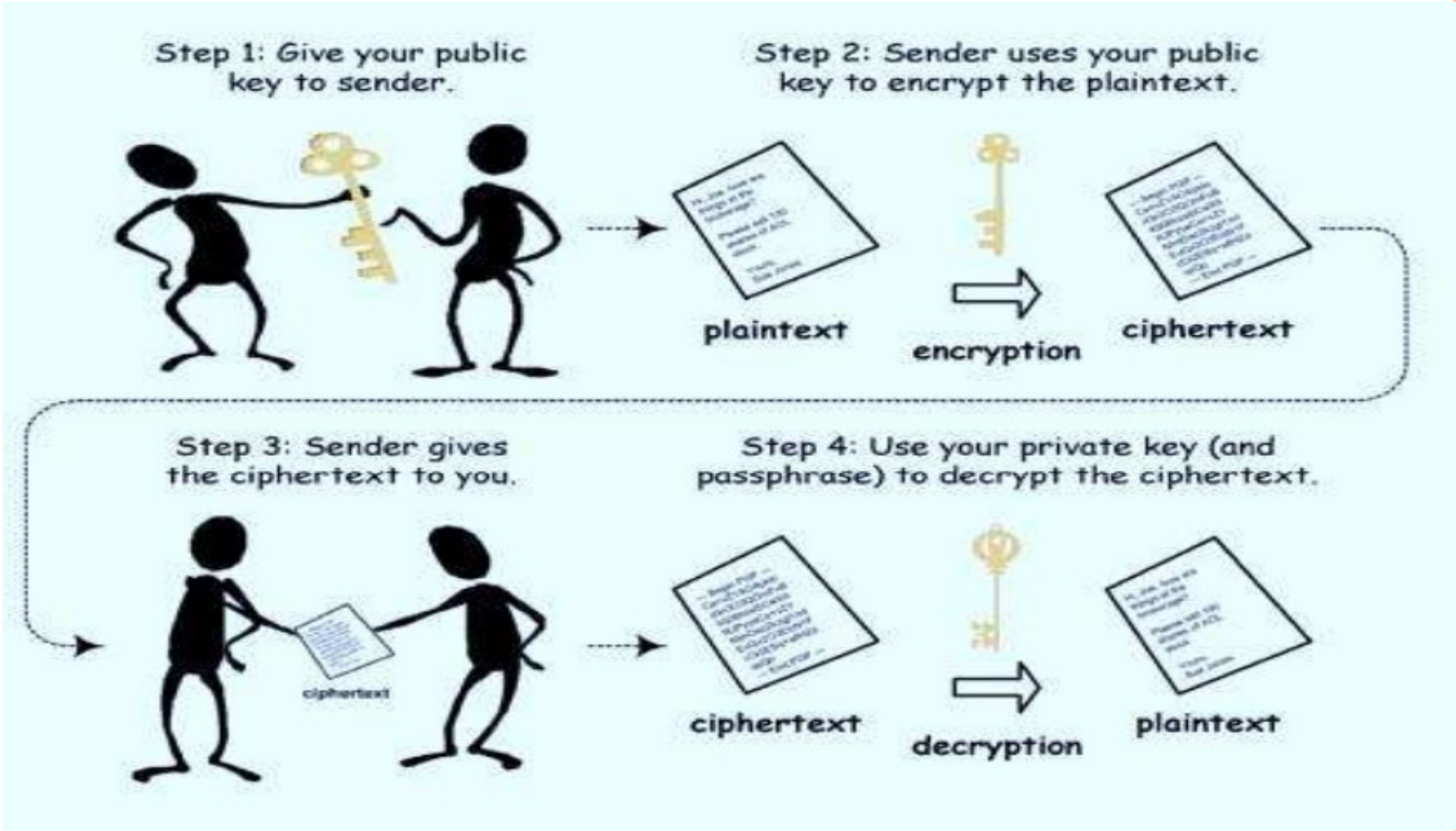
- The most popular symmetric-key system is the Data Encryption Standard (DES).
- DES uses 56-bit keys, they are short enough to be easily brute-forced by modern hardware and it is recommended that DES should not to be used.
- Triple DES (or 3DES) uses 128 bits key length, the same algorithm, applied three times to produce strong encryption.

CONT..

- Merits:
  - SIMPLER
  - FASTER
- De-Merits:
  - Two parties must somehow exchange the key in a secure way.
  - Public key is distributed in a non-secure way b/n Client/Server.
  - Easy for hackers to get the key as it is shared in unsecure way.

Asymmetric encryption

- Asymmetric encryption use two keys, one to encrypt the data, and another key to decrypt the data. These keys are generated together.
- One is named as Public key and is distributed freely. The other is named as Private Key and it is kept hidden.
- Both Sender & Recipient has to share their Public Keys for Encryption and has to use their Private Keys for Decryption.


Step 1: Give your public key to sender.
Step 2: Sender uses your public key to encrypt the plaintext.
plaintext
encryption
ciphertext
Step 3: Sender gives the ciphertext to you.
Step 4: Use your private key (and passphrase) to decrypt the ciphertext.
ciphertext
ciphertext
decryption
plaintext

Key Points in Asymmetric Encryption

- Asymmetric encryption use two keys:
- Public Key - to encrypt the data
- Private Key - to decrypt the data
- These keys are generated together.
- The Public key(s) is distributed freely between the sender and receiver.
- The other is named as Private Key and it is kept hidden.
- The Private Key is only used for Decryption and will not be shared between the sender and receiver.

CONT..

- RSA:
  - Rivest-Shamir-Adleman is the most commonly used asymmetric algorithm (public key algorithm). It can be used both for encryption and for digital signatures.
- Digital Signature Algorithm:
  - The standard defines DSS to use the SHA-1 hash function exclusively to compute message. The main problem with DSA is the fixed subgroup size (the order of the generator element), which limits the security to around only 80 bits. Hardware attacks can be menacing to some implementations of DSS. However, it is widely used and accepted as a good algorithm.

CONT..

- Diffie-Helman: Diffie-Hellman is the first asymmetric encryption algorithm, invented in 1976, using discrete logarithms in a finite field. Allows two users to exchange a secret key over an insecure medium without any prior secrets.
- ElGamal: The ElGamal is a public key cipher - an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key agreement. ElGamal is the predecessor of DSA.

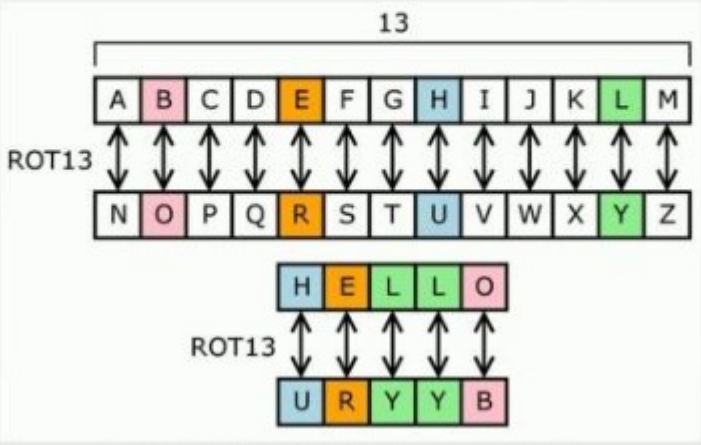
CONT..

- Merits:
  - Two parties don't need to have their private keys already shared in order to communicate using encryption.
  - Authentication and Non-Repudiation are possible. (Authentication means that you can encrypt the message with my public key and only I can decrypt it with my private key. Non-repudiation means that you can "sign" the message with your private key and I can verify that it came from you with your public key.)
- De-Merits:
  - Asymmetric Encryption algorithms are comparatively complex.
  - Time consuming process for Encryption and Decryption.

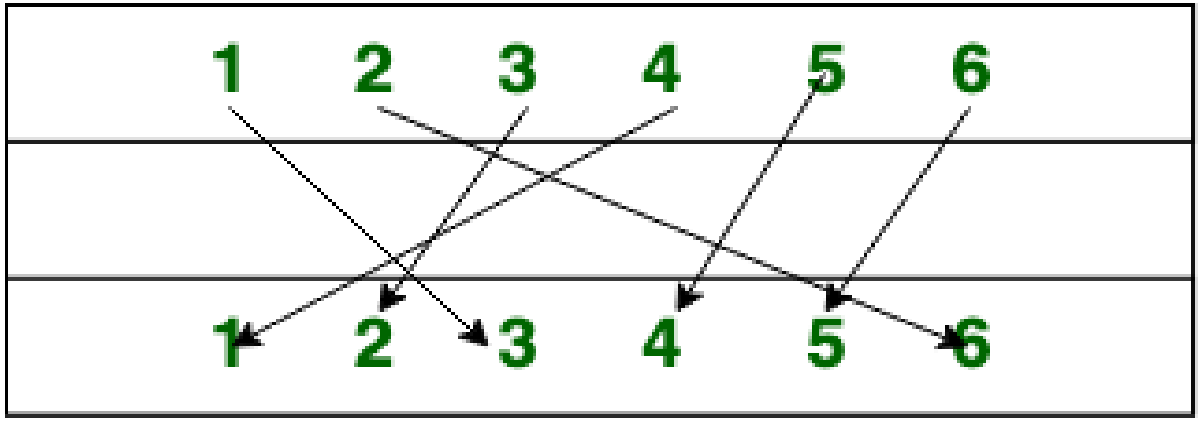
Difference between Substitution Cipher Technique and Transposition Cipher Technique

- **Substitution Cipher Technique:**
  - In Substitution Cipher Technique plain text characters are replaced with other characters, numbers and symbols as well as in substitution Cipher Technique, character's identity is changed while its position remains unchanged.
- **Transposition Cipher Technique:**
  - Transposition Cipher Technique rearranges the position of the plain text's characters. In transposition Cipher Technique, The position of the character is changed but character's identity is not changed.

Substitution cipher



https://en.wikipedia.org/wiki/File:ROT13.png

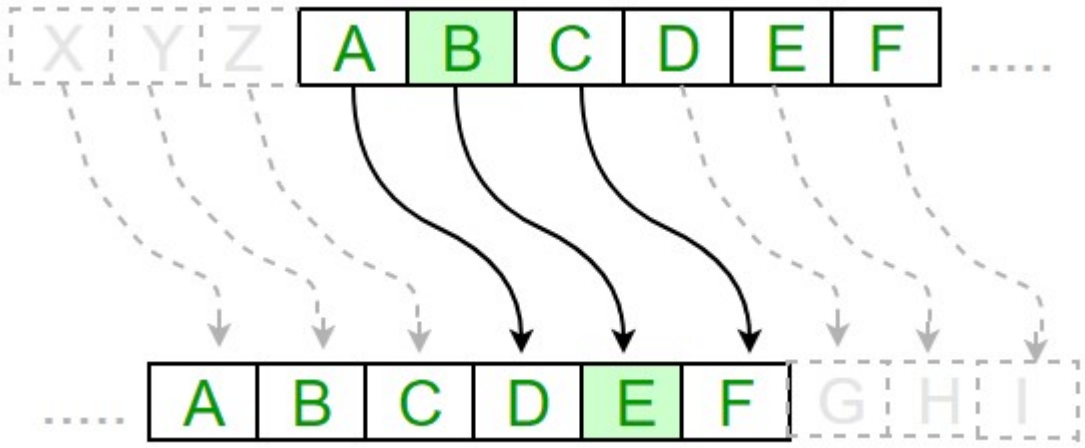


Transportation Cipher

SUBSTITUTION CIPHER TECHNIQUE	TRANSPOSITION CIPHER TECHNIQUE
In substitution Cipher Technique, plain text characters are replaced with other characters, numbers and symbols.	In transposition Cipher Technique, plain text characters are rearranged with respect to the position.
Substitution Cipher's forms are: Mono alphabetic substitution cipher and poly alphabetic substitution cipher.	Transposition Cipher's forms are: Key-less transposition cipher and keyed transposition cipher.
In substitution Cipher Technique, character's identity is changed while its position remains unchanged.	While in transposition Cipher Technique, The position of the character is changed but character's identity is not changed.
In substitution Cipher Technique, The letter with low frequency can detect plain text.	While in transposition Cipher Technique, The Keys which are nearer to correct key can disclose plain text.
The example of substitution Cipher is Caesar Cipher.	The example of transposition Cipher is Reil Fence Cipher.

ENCRYPTION ALGORITHM

- **CAESAR CIPHER**
- It is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet.
- For example, with a **shift of 1, A would be replaced** by **B, B would become C, and so on.**
- First translate all of characters to numbers, 'a'=0, 'b'=1, 'c'=2, ... , 'z'=25.
- For Encryption, C=E(P)=(P+3) mod 26
- For Decryption, P=D(C)=(C-3)mod 26



- Example:
  - Plain Text=HELLO
  - Key=3
- **Encryption:**
  - Cipher Text=KHOOR
- **Decryption:**
  - Plain Text=HELLO

PLAYFAIR CIPHER

- The Playfair cipher was the first practical digraph substitution cipher.
- The scheme was invented in 1854 by Charles Wheatstone, but was named after Lord Playfair who promoted the use of the cipher.
- The technique encrypts pairs of letters (digraphs), instead of single letters as in the simple substitution cipher.

The Playfair Cipher Encryption Algorithm:

- Any sequence of 25 letters can be used as a key, so long as all letters are in it and there are no repeats.
- there is no 'j', it is combined with 'i'.
- Remove any punctuation or symbols that are not present in the key square.
- Identify any double letters in the plaintext and replace the second occurrence with an 'x' e.g. 'hammer' -> 'hamxmer'.
- 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. 'hamxmer' -> 'ha mx me rx'
- The algorithm now works on each of the letter pairs.

- **For example:**
- The key is "**monarchy**"
- Thus the initial entires are **'m', 'o', 'n', 'a', 'r', 'c', 'h', 'y'** followed by remaining characters of **a-z(except 'j')** in that order.

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

- 1) If the letters are in different rows and columns, Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.
- **For example:**
- **Diagraph:**
- "nt" **Encrypted Text:** rq
- **Encryption:** n -> r t -> q
- EX-> PT=MH
- CT=OC
- HA->BO
- MX->AU
- ME->CL
- RX->AZ

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

- 2) 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).
- **Diagraph:** "st"
- **Encrypted Text:** tl
- **Encryption:** s -> t t -> l
- EX=>
- PT=YD
- CT=BC

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

- 3) 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).
- **Diagraph:** "me"
- **Encrypted Text:** cl
- **Encryption:** m -> c e -> l
- EX->
- PT=PV
- CT=VO

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

CONT..

- PT= GUJARAT
  PT= GU JA RA TX
  GU-> EW
  JA->NG->SB
  RA->MR
  TX->SZ

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

SHIFT CIPHER

- The Caesar Cipher is a type of **shift cipher**.
- **shift** Ciphers work by using the modulo operator to encrypt and decrypt messages. The **shift** Cipher has a **key K**, which is an **integer from 0 to 25**.
- We will only share this key with people that we want to see our message.

How to Encrypt:

- For every letter in the message **M** :

1. Convert the letter into the number that matches its order in the alphabet starting from 0, and call this number **X**. (A=0, B=1, C=2, …,Y=24, Z=25)

2. Calculate: **Y = (X + K)** mod **26**

3. Convert the number **Y** into a letter that matches its order in the alphabet starting from 0.

(A=0, B=1, C=2, …,Y=24, Z=25)

- **For Example:** We agree with our friend to use the Shift Cipher with **key K=19** for our message.
- We encrypt the message **"KHAN",** as follows:

ENCRYPTION

	K	H	A	N	
	10	7	0	13	
+	19	19	19	19	
(	29	26	19	32	) mod 26
	3	0	19	6	
	D	A	T	G	

- So, after applying the Shift Cipher with key K=19 our message text "**KHAN**" gave us **cipher text "DATG"**.
- We give the message "DATG" to our friend.

How to decrypt:

- For every letter in the cipher text **C** :

1. Convert the letter into the number that matches its order in the alphabet starting from 0, and call this number Y. (A=0, B=1, C=2, …, Y=24, Z=25)

2. Calculate: **X= (Y - K)** mod **26**

3. Convert the number **X** into a letter that matches its order in the alphabet starting from 0. (A=0, B=1, C=2, …, Y=24, Z=25)

- Our friend now decodes the message using our agreed upon **key K=19.** As follows:

DECRYPTION

	D	A	T	G	
	3	0	19	6	
-	19	19	19	19	
(	-16	-19	0	-13	) mod 26
	10	7	0	13	
	K	H	A	N	

SO, AFTER DECRYPTING THE SHIFT CIPHER WITH KEY K=19 OUR FRIEND DECIPHERS THE CIPHER TEXT "**DATG**" INTO THE MESSAGE TEXT "**KHAN**".

Why is the Shift Cipher insecure?

- A cipher should prevent an attacker, who has a copy of the cipher text but does not know the key, from discovering the contents of the message. Since **we only have 26 choices for the key**, someone can easily try all of the 26 keys, one by one, until they recover the message. This type of attack is called a **brute force attack**.

VIGENERE CIPHER

- It is a polyalphabetic cipher.
- For Vigenere Cipher, use Tabula Recta in which each row of the table corresponds to a Caesar Cipher. The first row is a shift of 0; the second is a shift of 1; and the last is a shift of 25.
- The Vigenere cipher uses this table together with a keyword to encipher a message.

CONT….

	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

CONT….

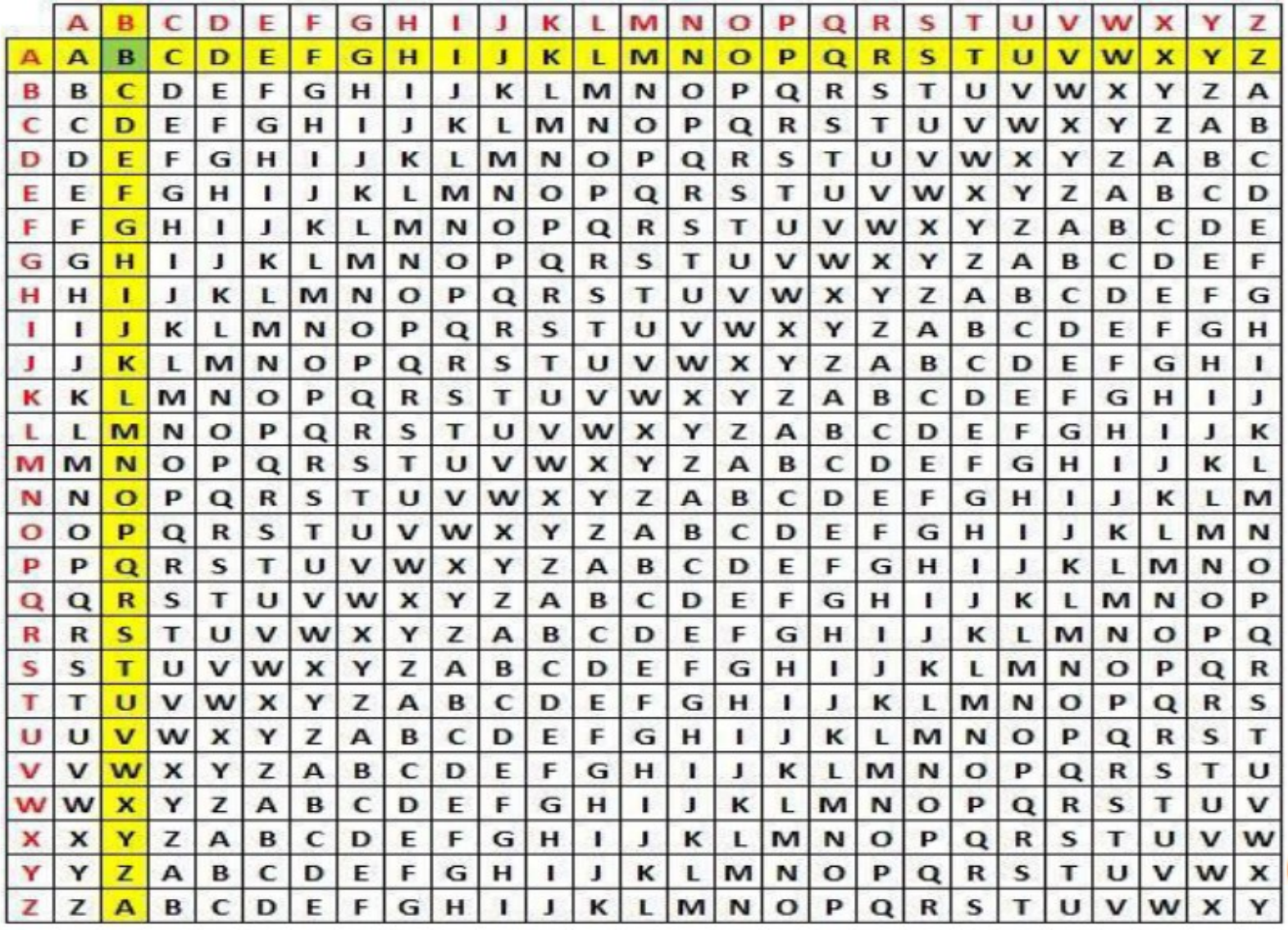
- To encrypt a message using the Vigenère Cipher you first need to choose a keyword
- for each plaintext letter, find the letter down the left hand side of the tabula recta. You take the corresponding letter from the key stream, and find this across the top of the tabula recta.
- Where these two lines cross in the table is the cipher text letter you use.

CONT..

Plaintext	a	s	i	m	p	l	e	e	x	a	m	p	l	e
Keystream	b	a	t	t	i	s	t	a	b	a	t	t	i	s

- Encrypt the plaintext "a simple example" using the keyword battista.
- First we must generate the keystream, by repeating the letters of the keyword until it is the same length as the plaintext.
- The keystream b means choose the column with B at the top, and the plaintext "a" means we choose the row with A at the left. We get the ciphertext "B".

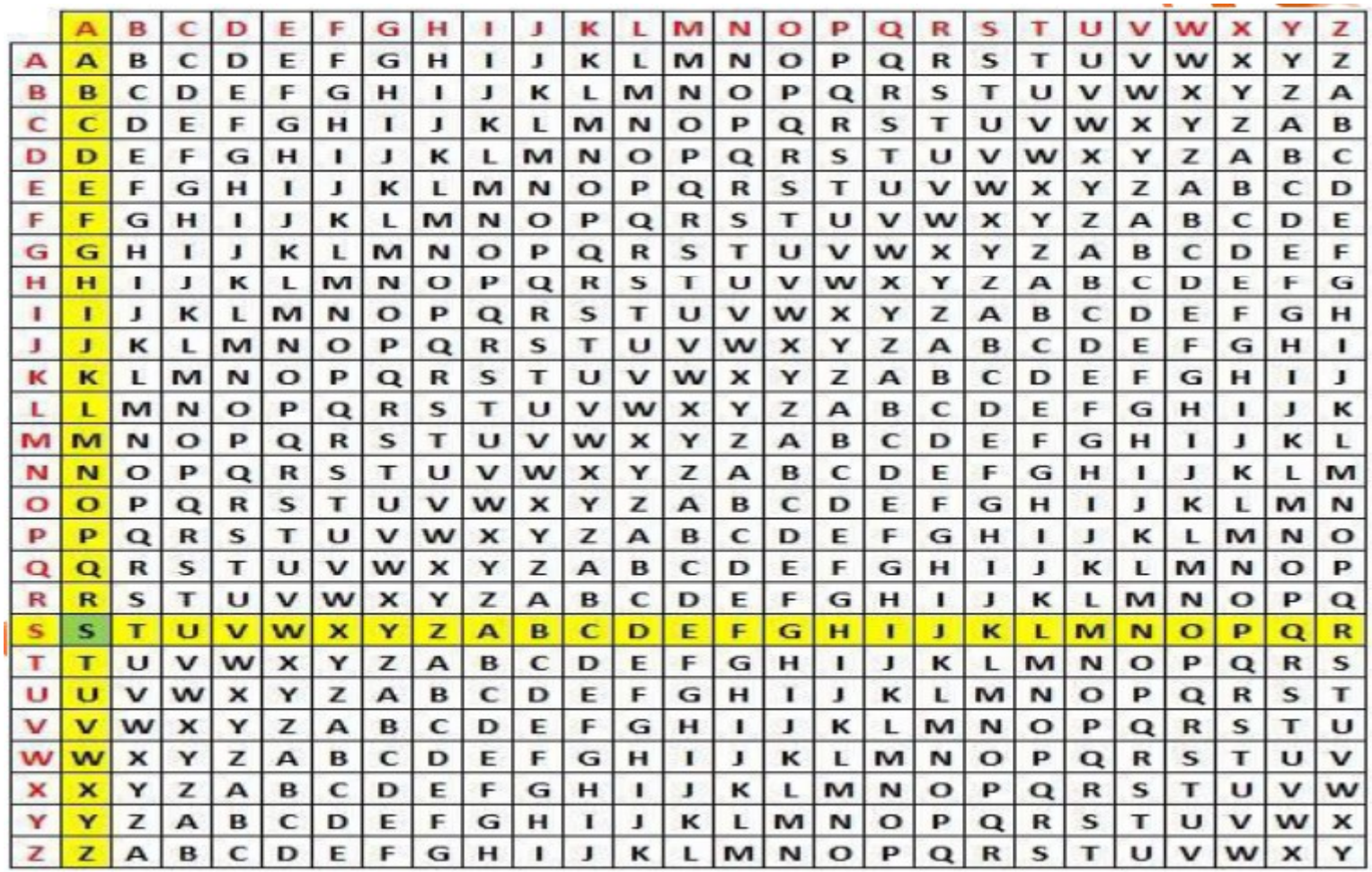
CONT..



	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

CONT….

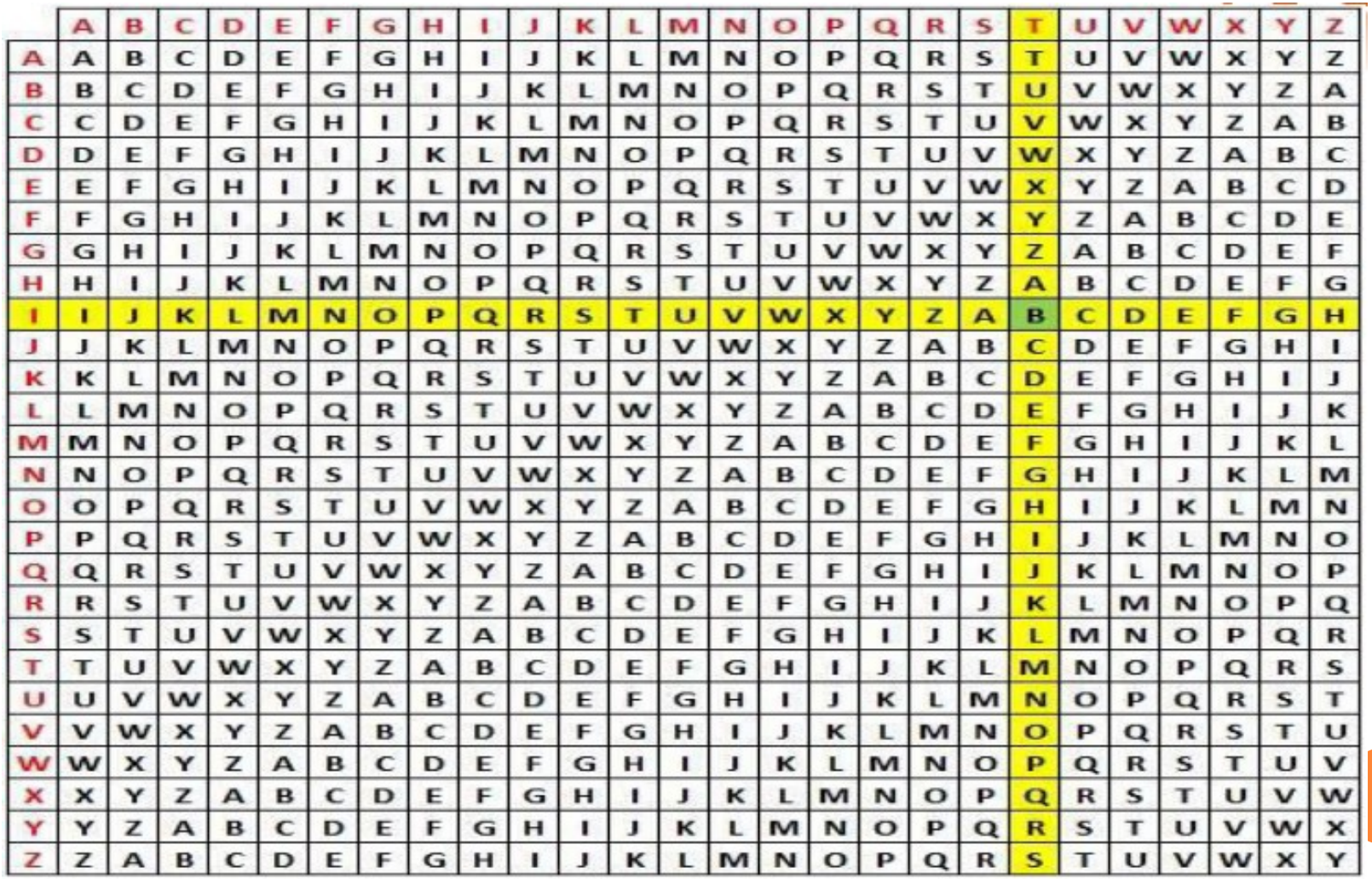
- For the second plaintext letter "s", we go down to S on the left, and use the keystream a to go to A along the top. We get the ciphertext letter "S".



	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

CONT….

- With the plaintext letter "i", we go down to I on the left, and the key stream letter t means we go to T across the top. We get the cipher text letter "B".



	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

CONT….

- Continuing in this way we get the final ciphertext "BSBF XDXEYA FITW".

VERNAM CIPHER

- It is also known as One Time Pad(OTP).
- It is unbreakable encryption technique.
- Vernam cipher is a stream cipher where the plain text is add with a random stream of data of the same length to generate the encrypted data.
- Key characteristics:
  - Key must truly random.
  - key must be as long as the plaintext, and not repeating
  - Key must be used once.
  - There should be two copies of the key: One for sender and other for receiver.

CONT…

- It is also known as One Time Pad(OTP).
- We shall encrypt the simple message "hello" using the random key stream “jqxyt”
- Cipher Text will be “QUIJH”

Plaintext	h	e	l	l	o
Keystream	J	Q	X	Y	T
Ciphertext	Q	U	I	J	H

HILL CIPHER

- The Hill Cipher was invented by Lester S. Hill in 1929.
- It can work on digraphs (2X2), trigraphs (3X3) or theoretically any sized blocks.
- The Hill Cipher uses an area of mathematics called Linear Algebra.
- It also makes use of Modulo Arithmetic.
- The cipher has a significantly more mathematical nature than some of the others ciphers.

HILL CIPHER

- Encryption :
- To encrypt a message using the Hill Cipher ,first turn keyword into a key matrix (either in 2x2 matrix or 3x3 matrix).
- Also turn the plaintext into digraphs (or trigraphs) and each of these into a column vector.
- We then perform matrix multiplication modulo the length of the alphabet (i.e. 26) on each vector

Hill Ciphers example

The *key* for a hill cipher is a matrix
e.g.

$$\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix}$$

- ✓ In the above case, we have taken the size to be 3×3
- ✓ Assume we want to encipher the message **ATTACK AT DAWN**.
- ✓ We now take the first 3 characters from our plaintext, **ATT** and create a vector that corresponds to the letters to get: `[0 19 19]`

$$\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \\ 19 \end{bmatrix} = \begin{bmatrix} 171 \\ 57 \\ 456 \end{bmatrix} \pmod{26} = \begin{bmatrix} 15 \\ 5 \\ 14 \end{bmatrix} = \text{'PFO'}$$

TRANSPOSITION TECHNIQUE

- Here, Plaintext symbols are rearranged to produce Cipher text.
- Example, Rail Fence Cipher

RAIL FENCE CIPHER

- Rail fence cipher is a type of transposition cipher.
- It involves rearranging of letters in plain text to encrypt the message.
- Example, Plain Text=THIS IS A SECRET MESSAGE
- Key(Rail)=3
- For Encryption, write message in zigzag(vertically)

T	S	A	C	T	S	G
H	I	S	R	M	S	E
I	S	E	E	E	A	

The message is read horizontally: TSACTSGHISRMSEISEEEAX
This is cipher text.

CONT…

- For Decryption, Total letter =21 Divided in to 3 groups of letter(bcz no. of rails=3)
- TSACTSG HISRMSE ISEEEAX
- Key(Rail)=3, so in each rail write 7 letters.
- The message is read vertically: THIS IS A SECRET MESSAGE

T	S	A	C	T	S	G
H	I	S	R	M	S	E
I	S	E	E	E	A	

STEGANOGRAPHY

- Steganography means hiding a message within another message or image.
- Steganography is an art of hiding a message, image, or file within another message,image, or file.
- The word steganography combines the Ancient Greek words steganos (ŭŪεγανόŬ), meaning "covered, concealed, or protected", and graphein (γŏάφειν) meaning "writing".
- For example, the hidden message may be in invisible ink between the visible lines of a private letter.

CONT…

- Examples of Steganography:
  - 1)Character Marking
  - 2)Invisible Ink
  - 3)Pin punctures

  Digital Stegnography:

  We can insert date or we can hide data in the image by replacing bits of image.

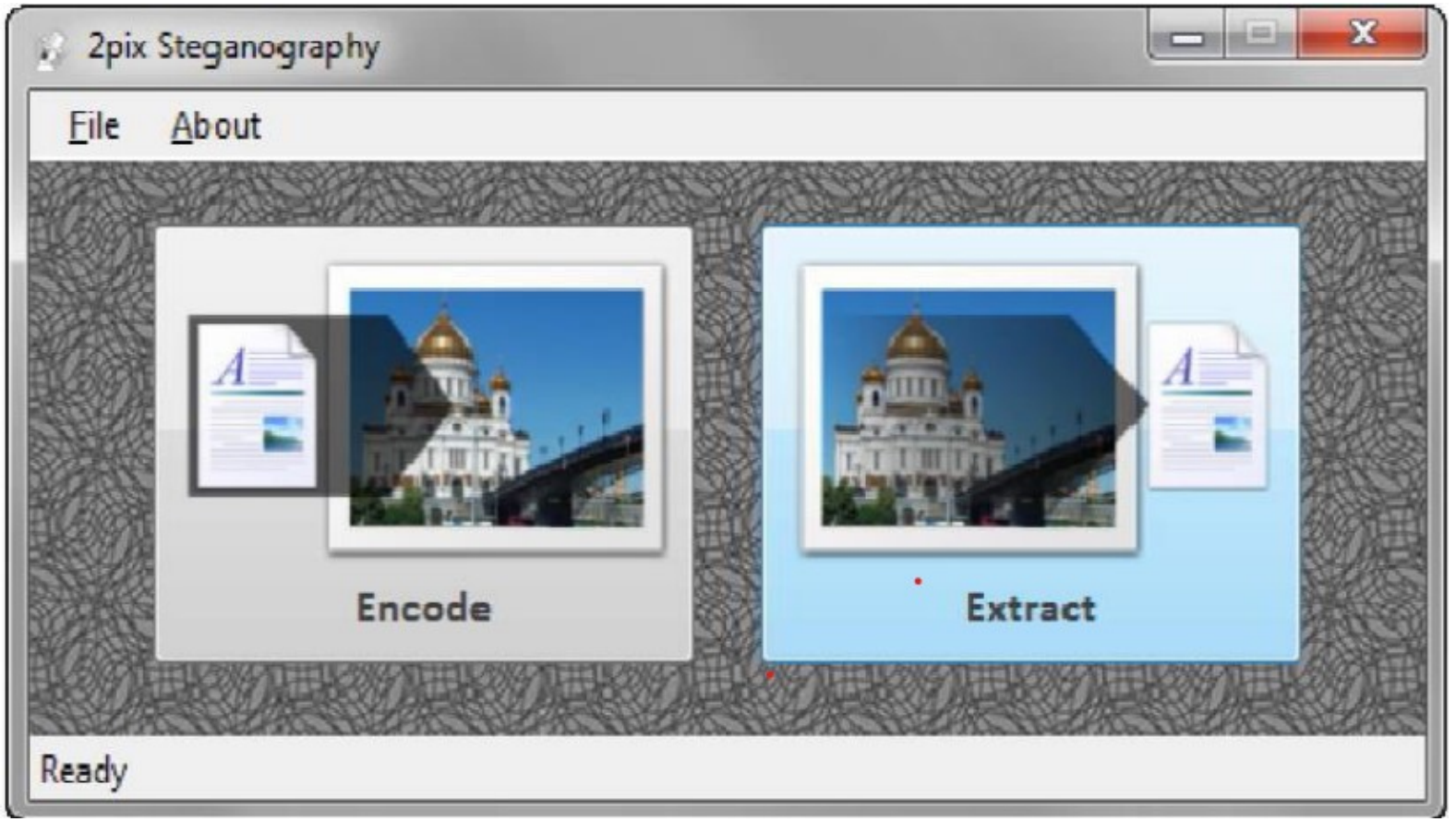
  Most common technique are:

  1)LSB,

  2)DCT and

  3)Append type.

CONT…



CONT…

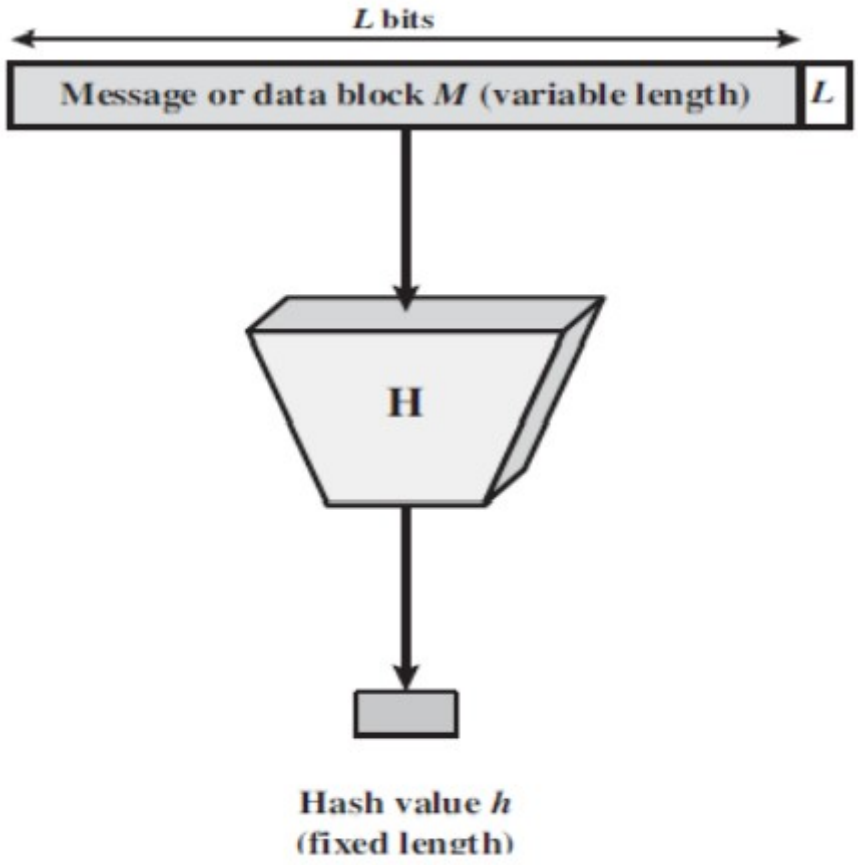
- LSB: Least Significant Bit
- Replace LSB bit with a bit from hidden data.
- LSB has smallest effect on the amount of color.
- Replacing LSB to hidden data will have small effect on the picture.

CONT…

- DCT stands for Discrete Cosine Transform
- It works by calculating the frequencies of the image then replace some of them.
- Append:
  - Instead of hide the data in the photo by manipulating the picture, Append algorithm appends the data to the end of the file as appending.
  - This algorithm will change the size of the file.

HASH FUNCTION

- Hash function H accepts a variable length block of data M as input and produces fixed sized hash value as output.
- h=H(M)



CONT…

- It is impossible to recreate the input data from its hash value.
- Input is called the Message.
- Hash value is called the Message Digest.
- It is infeasible to find two different messages with the same hash.

APPLICATION OF HASH FUNCTION

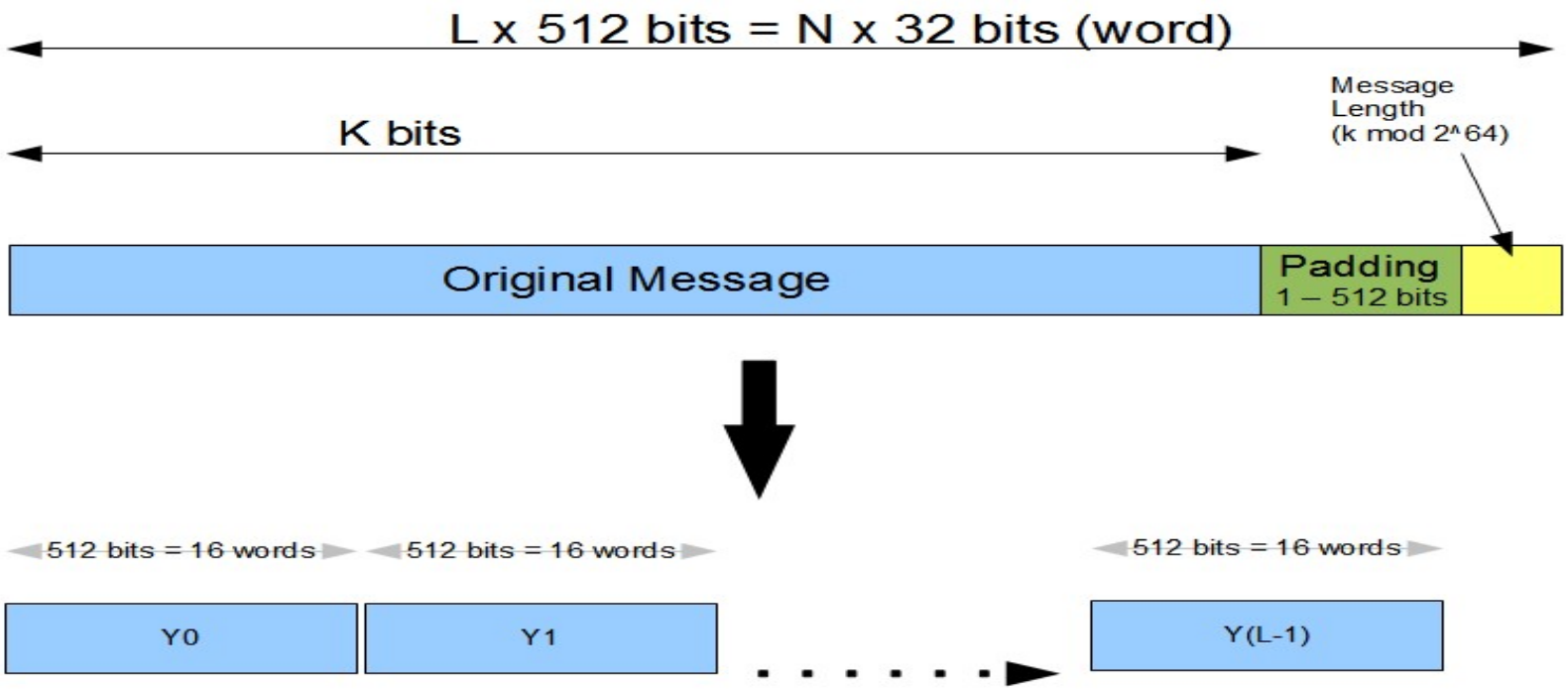
- Message Authentication
- Digital Signature
- File Integrity Verification
- Password Hashing
- Key Derivation

CONT..

- It works for any input message that is less than 264 bits.
- The output of SHA is a message digest of 160 bits in length. This is designed to be computationally infeasible to:
  - Obtain the original message , given its message digest.
  - Find two messages producing the same message digest

How SHA-1 works.?

- *Step 1: Padding of Bits*



CONT..

- *Step 2: Append Length*
- *Step 3: Divide the input into 512-bit blocks*
- *Step 4: Initialize chaining variables*

Chaining Variables	Hex values
A	01 23 45 67
B	89 AB CD EF
C	FE DC BA 98
D	76 54 32 10
E	C3 D2 E1 F0

- *Step 5: Process Blocks*- Now the actual algorithm
- begins….

CONT..

- *Step 5.1 :* Copy chaining variables A-E into variables a-e.
- *Step 5.2 :* Divide current 512-bit block into 16 sub blocks of 32-bits.
- *Step 5.3 :* SHA has 4 rounds, each consisting of 20 steps. Each round takes 3 inputs-
  - 512-bit block,
  - The register abcde
  - A constant K[t] (where t= 0 to 79)

CONT..

- *Step 5.4 :* SHA has a total of 80 iterations (4 rounds X 20 - iterations). Each iteration consists of following operations:-

abcde = (e +Process P + S5(a) + W[t] + K[t]), a, S30(b) , c , d

Where,

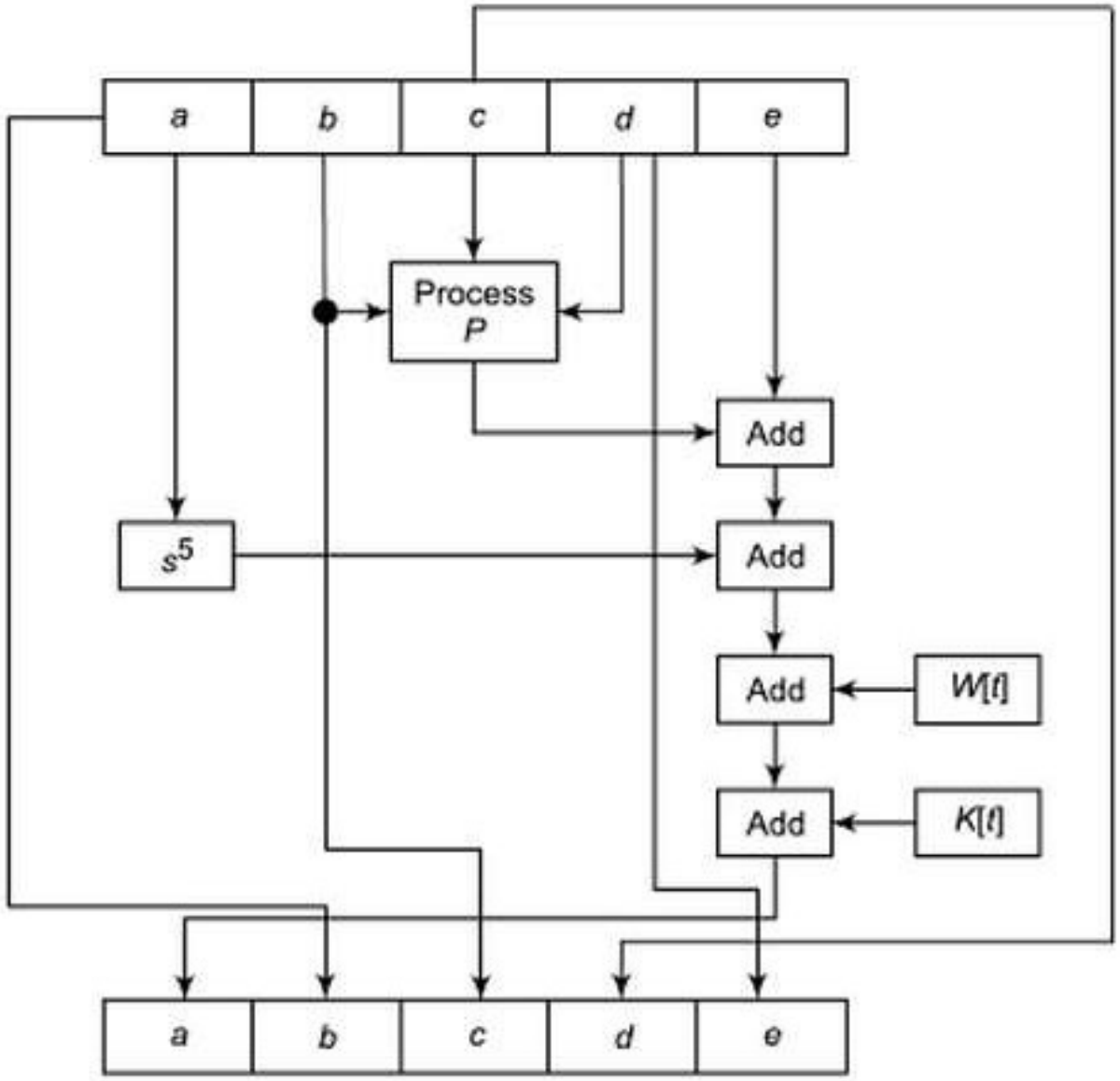
- abcde = The register made up of 5 variables a, b, c, d, e.
- Process P = The logic operation.
- St = Circular-left shift of 32-bit sub-block by t bits.
- W[t[= A 32-bit derived from the current 32-bit sub-block.
- K[t] = One of the five additive constants.

CONT..

- *Process P in each SHA round*

Round	Process P
1	(b AND c) OR ((NOT b) AND (d))
2	b XOR c XOR d
3	(b AND c) OR (b AND d) OR (c AND d)
4	b XOR c XOR d

SINGLE SHA-1 ITERATION



CONT..

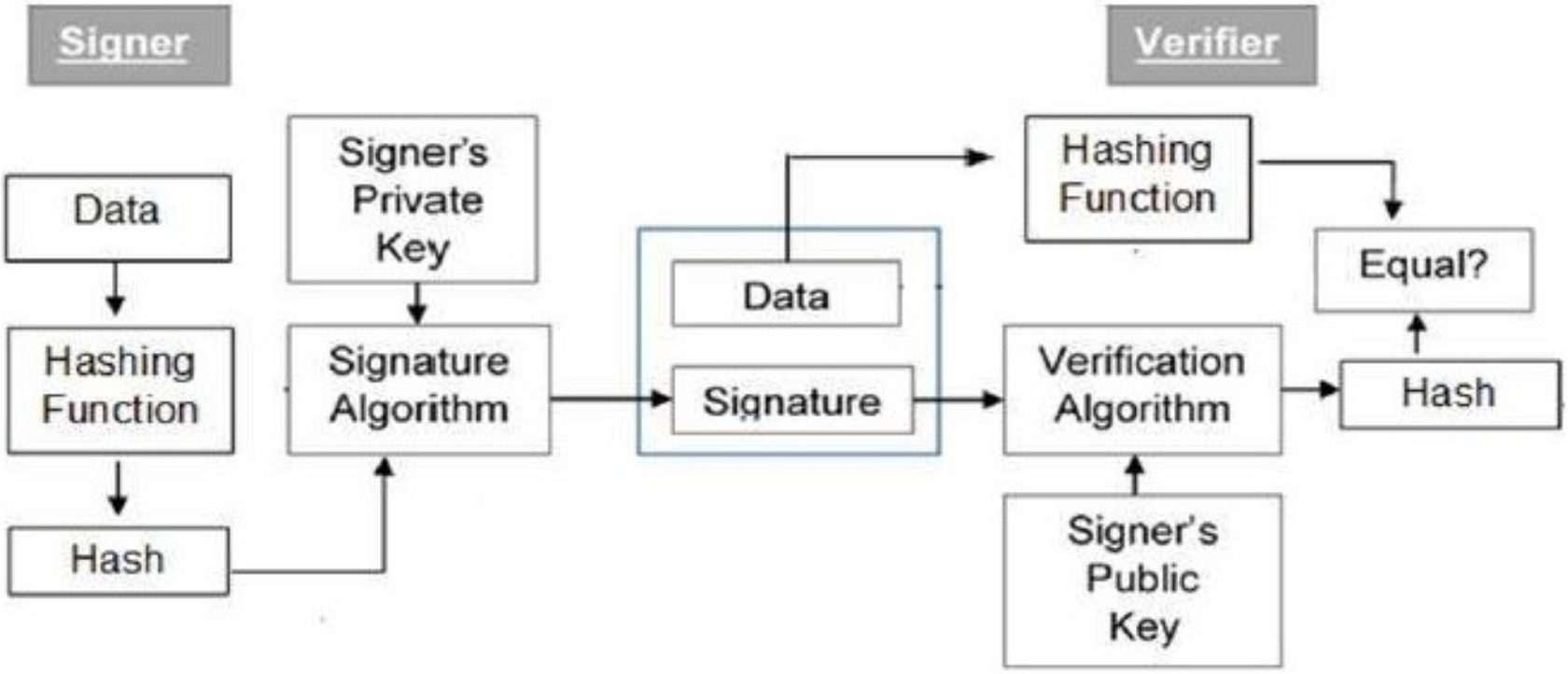
- *The values of W[t] are calculated as follows :*
  - For the first 16 words of W (i.e. t=0 to 15) , the contents of the input message sub-block M[t] become the contents of W[t].
  - For the remaining 64 values of W are derived using the equation

  - **W[t] = s1 (W[t-16] XOR W[t-14] XOR W[t-8] XOR W[t-3])**

ASYMMETRIC ENCRYPTION (DIGITAL SIGNATURE)

- When there is not complete trust between sender and receiver, Digital Signature is needed.
- Property of Digital Signature
  - It must verify the sender, date and time of signature
  - It must authenticate the content at the time of signature
  - It must be verifiable by third parties to resolve disputes.

CONT..


Signer
Verifier
Data
Signer's Private Key
Hashing Function
Signature Algorithm
Hash
Data
Signature
Hashing Function
Equal?
Verification Algorithm
Hash
Signer's Public Key

CONT..

- Digital Signature give two algorithm:
- One for sender which involve user's private key and one for verifying signature which involve user's public key.
- Digital Signature is an electronic signature that can be used to authenticate the identity of the sender of a message and ensure that content of the message that has been sent is unchanged.

KEY ESCROW

- It is a cryptographic key exchange process in which a key is held in escrow or stored by a third party.
- Key escrow provides a backup source for cryptographic keys.
- It is a risky because a third party is involved.
- Key Escrow is to serve as a backup if the parties with access to the cryptographic key lose the data, such as through some natural disaster or a crack attack.

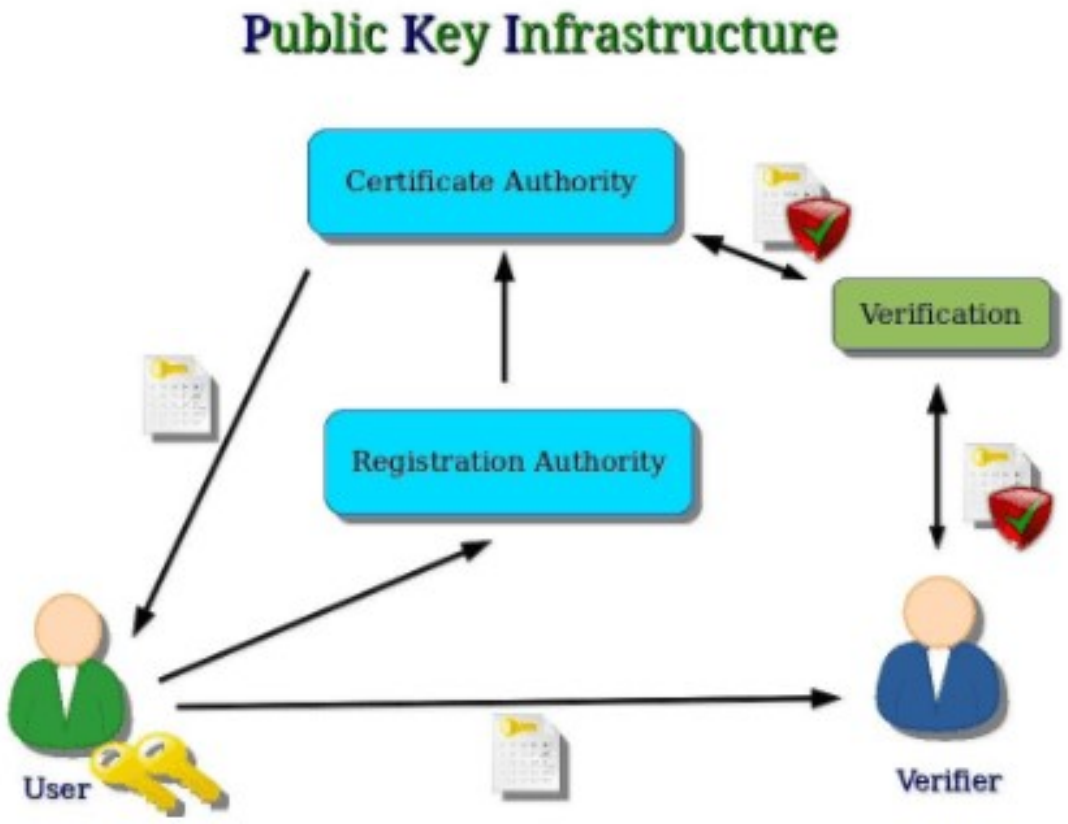
PKI (PUBLIC KEY INFRASTRUCTURE)

- PKI is also called asymmetric key Infrastructure, uses a key pair to encrypt and decrypt the data.
- A PKI enables users of a unsecure to securely and privately exchange data through the use of a private and public cryptography.
- The Key pair is consists of a private and public key.
- The Private key must be kept secret.
- Public key needs to be distributed.

Cont…

- Data encrypted by one of the two keys can be decrypted by the other.
- The key problem of PKI is to manage the public keys.
- Currently, PKI uses Digital Certificate mechanism to solve the problem.
- Digital Certificate binds public key to their owners, help to distribute public keys in large network securely.

Architecture of PKI



Public Key Infrastructure

CONT…

- Entity: End user of PKI services, such as person, an organization, a device like a router.
- Certificate Authority: CA issues certificates and specifies the validity periods of certificate.
- Registration Authority: RA implements functions like identity authentication, Key pair generation and key pair backup.
- PKI Repository: Server or common database. It stores and manage information like certificate request, certificates, keys.

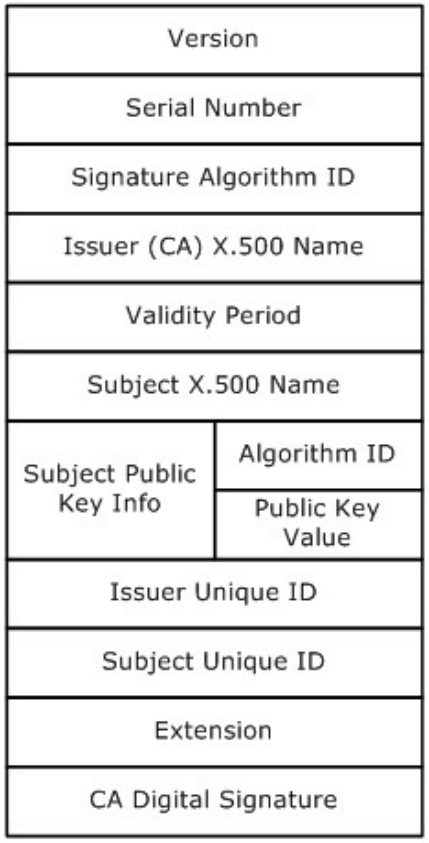
DC

- A certificate binds an identity to public key, with all contents signed by a trusted public-key or certificate authority(CA).
- A user can present his or her public key to the authority in a secure manner, and obtain a certificate. The user can then publish the certificate.
- X.509 certificates are used in most network security applications.
- In Understanding Digital Signatures article, it was assumed that the receiver knows the Public Key of the sender. In fact, the issue of distributing Public Key is massive, because the Public Key should be distributed in a scalable way as well as be trusted as the true Public Key of the sender. These problems are solved when a user obtains another user's Public Key from the digital certificate.

CONT..

- **Public Key Infrastructure (PKI)** consists of protocols, standards and services, that allows users to authenticate each other using digital certificates that are issued by CA. For a digital certificate to be useful, it has to be structured in a standard way so that information within the certificate can be retrieved and understood regardless of who issued the certificate.
  The ***X.509, PKI X.509*** and ***Public Key Cryptography Standards (PKCS)*** are the building blocks a PKI system that defines the standard formats for certificates and their use.

CONT..



Version of X.509 to which the Certificate conforms

A number that uniquely identifies the Certificate

The names of the specific Public Key algorithms that the CA has used to sign the Certificate (Ex.- RSA with SHA-1)

The identity of the CA Server who issued the Certificate

The period of time for which the Certificate is valid with start date and expiration date

The owner's identity with X.500 Directory format (Ex.- cn=auser, ou=SP, o=Alphawest)

The Public Key of the owner of the Certificate and the specific Public Key algorithms associated with the Public Key

Information used to identify the issuer of the Certificate

Information used to identify the Owner of the Certificate

Additional information like Alternate name, CRL Distribution Point (CDP)

The actual digital signature of the CA

CONT…

- Digital Certificate is a file signed by a CA for an entity.
- It includes identity information of the entity, Public key of the entity, name and signature of CA, validity period of the certificate where the signature of CA ensures the validity and authority of the certificate.
- Digital Certificate binds a public key to information about its owner.

CONT….

- Two types of certificate: Local and CA certificate.
- Local Certificate is a digital certificate signed by CA for entity.
- CA certificate is a certificate of a CA .
- Digital Certificate are issued by CA.
- CA is made of software ,hardware ,procedures, policies and people.

Steps for obtaining Digital Certificate

- When a user request a certificate, the registration process will require the user to enter specific information in to a web form.
- The web page accepts the user's public key or it will step the user to create a public/private key pair.
- Then public key and registration form are forwarded to the RA for processing.

CONT..

- Once the RA is finished processing the request and verify the individual's identity , the RA sends request to the CA.
- The CA uses the RA – provided information to generate a digital certificate and integrates necessary data into the certificate.

CENTRALIZED OR DECENTRALIZED INFRASTRUCTURE

- Centralized Approach:
- Keys are generated and stored in a central server, and transmitted to the individual systems as needed.
- Decentralized Approach:
- Software on individual computers generates and stored cryptographic keys local to the system

CONT…

- Benefits of Centralized Key generation :
- Only central computer need necessary resource power to produce the key
- Much easier to back up the keys and implement key recovery procedures with central storage
- Low risk factor(Only center computer maintain their own key pair)

CONT..

- Drawbacks of Centralized Key generation:
- Must be securely transmitted
- Key must be available
- Single point of failure
- Prime target for attacker
- If company wants to provide truly authenticity the key should not be generated at a centralized server.

PROTECTING PRIVATE KEY

- Private key Protection:
- Key must be stored for future use. This storage area is called Key Store.
- Transported Securely
- Stored Securely
- Minimize access to private key
- Minimize number of users
- Changed at the end of its life time
- Properly destroyed
- Never be exposed in clear text
- Should not be shared.

Trust Models

- Potential scenarios exist other than just having more than one CA—each of the companies or each department of an enterprise can actually represent a trust domain itself.
- A trust domain is a construct of systems, personnel, applications, protocols, technologies, and policies that work together to provide a certain level of protection.
- All of these components can work together seamlessly within the same trust domain because they are known to the other components within the domain and are trusted to some degree.
- Different trust domains are usually managed by different groups of administrators, have different security policies, and restrict outsiders from privileged access.

CONT..

- In the nondigital world, it is difficult to figure out who to trust, how to carry out legitimate business functions, and how to ensure that one is not being taken advantage of or lied to.
- Jump into the digital world and add protocols, services, encryption, CAs, RAs, CRLs, and differing technologies and applications, and the business risks can become overwhelming and confusing.
- So start with a basic question: What criteria will we use to determine who we trust and to what degree?

CONT..

- example of a trust anchor. If Joe and Stacy need to communicate through e-mail and would like to use encryption and digital signatures, they will not trust each other's certificate alone.
- But when each receives the other's certificate and sees that it has been digitally signed by an entity they both do trust—the CA—they have a deeper level of trust in each other.
- The trust anchor here is the CA. This is easy enough, but when we need to establish trust anchors between different CAs and PKI environments, it gets a little more complicated.

CONT..

- If two companies need to communicate using their individual PKIs, or if two departments within the same company use different CAs, two separate trust domains are involved.
- The users and devices from these different trust domains need to communicate with each other, and they need to exchange certificates and public keys, which means that trust anchors need to be identified and a communication channel must be constructed and maintained.

CONT..

- A trust relationship must be established between two issuing authorities (CAs). This happens when one or both of the CAs issue a certificate for the other CA's public key, as shown in Figure.
- This means that each CA registers for a certificate and public key from the other CA.
- Each CA validates the other CA's identification information and generates a certificate containing a public key for that CA to use.
- This establishes a trust path between the two entities that can then be used when users need to verify other users' certificates that fall within the different trust domains.
- The trust path can be unidirectional or bidirectional, so either the two CAs trust each other (bidirectional) or only one trusts the other (unidirectional).

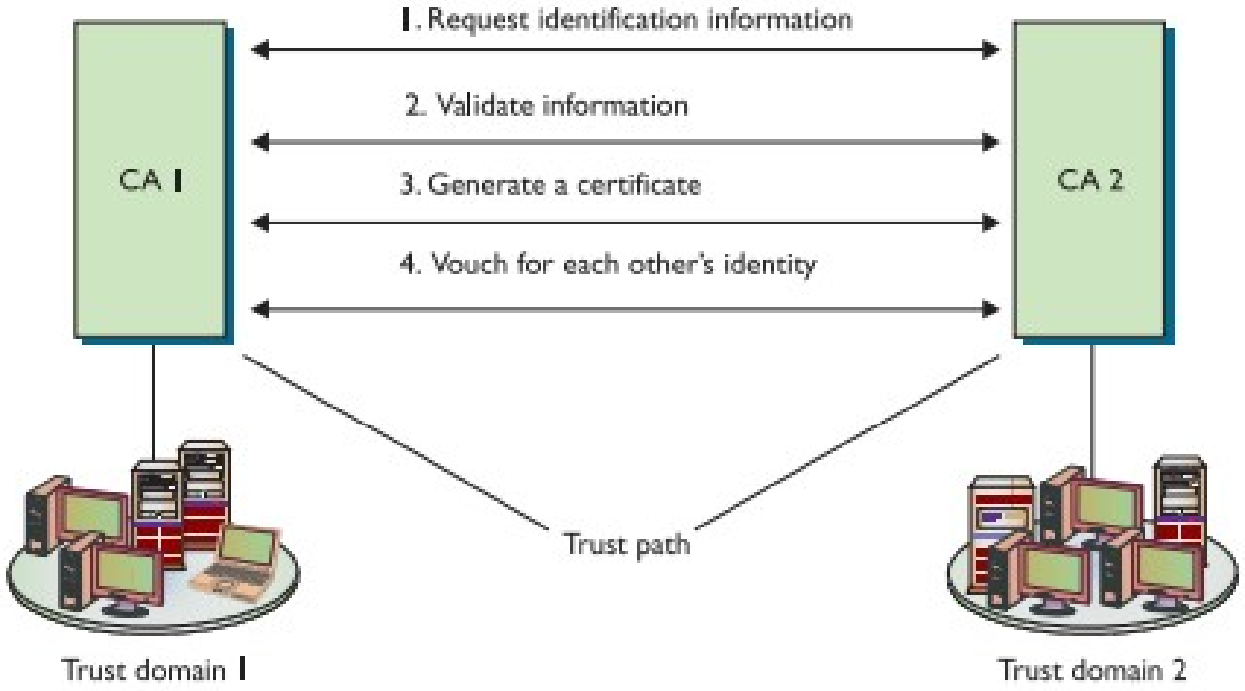


fig.:- a trust relationship can be built between two trust domains to set up a communication channel.

CONT..

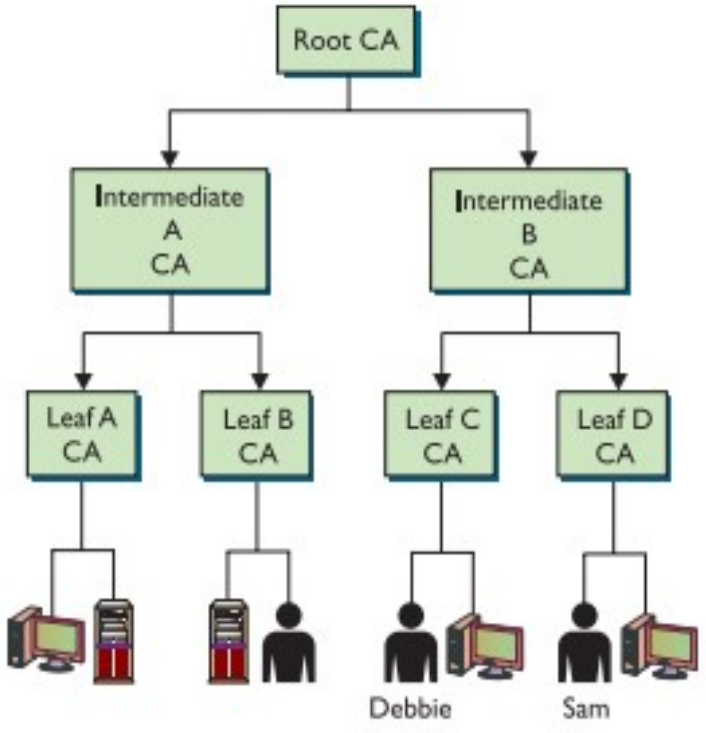
- As illustrated in Figure, all the users and devices in trust domain 1 trust their own CA, CA 1, which is their trust anchor.
- All users and devices in trust domain 2 have their own trust anchor, CA 2.
- The two CAs have exchanged certificates and trust each other, but they do not have a common trust anchor between them.

CONT…

- The trust models describe and outline the trust relationships between the different CAs and different environments, which will indicate where the trust paths reside.
- The trust models and paths need to be thought out before implementation to restrict and control access properly and to ensure that as few trust paths as possible are used.
- Several different trust models can be used:
  - The hierarchical models
  - The peer-to-peer models
  - The hybrid models

Hierarchical Trust Model

- The hierarchical trust model is a basic hierarchical structure that contains a root CA, intermediate CAs, leaf CAs, and end-entities.
- The configuration is that of an inverted tree, as shown in Figure.
- The root CA is the ultimate trust anchor for all other entities in this infrastructure, and it generates certificates for the intermediate CAs, which in turn generate certificates for the leaf CAs, and the leaf CAs generate certificates for the end-entities (users, network devices, and applications).



CONT..

- Intermediate CAs function to transfer trust between different CAs.
- These CAs are referred to as subordinate CAs because they are subordinate to the CA that they reference.
- The path of trust is walked up from the subordinate CA to the higher-level CA; in essence the subordinate CA is using the higher-level CA as a reference.

CONT..

- As shown in Fig., no bidirectional trusts exist—they are all unidirectional trusts, as indicated by the one-way arrows. Since no other entity can certify and generate certificates for the root CA, it creates a self-signed certificate.
- This means that the certificate's issuer and subject fields hold the same information, both representing the root CA, and the root CA's public key will be used to verify this certificate when that time comes.
- This root CA certificate and public key are distributed to all entities within this trust model.

Walking the Certificate Path

- When a user in one trust domain needs to communicate with a user in another trust domain, one user will need to validate the other's certificate.
- This sounds simple enough, but what it really means is that each certificate for each CA, all the way up to a shared trusted anchor, also must be validated.
- If Debbie needs to validate Sam's certificate, as shown in Figure, she actually also needs to validate the Leaf D CA and Intermediate B CA certificates, as well as Sam's.

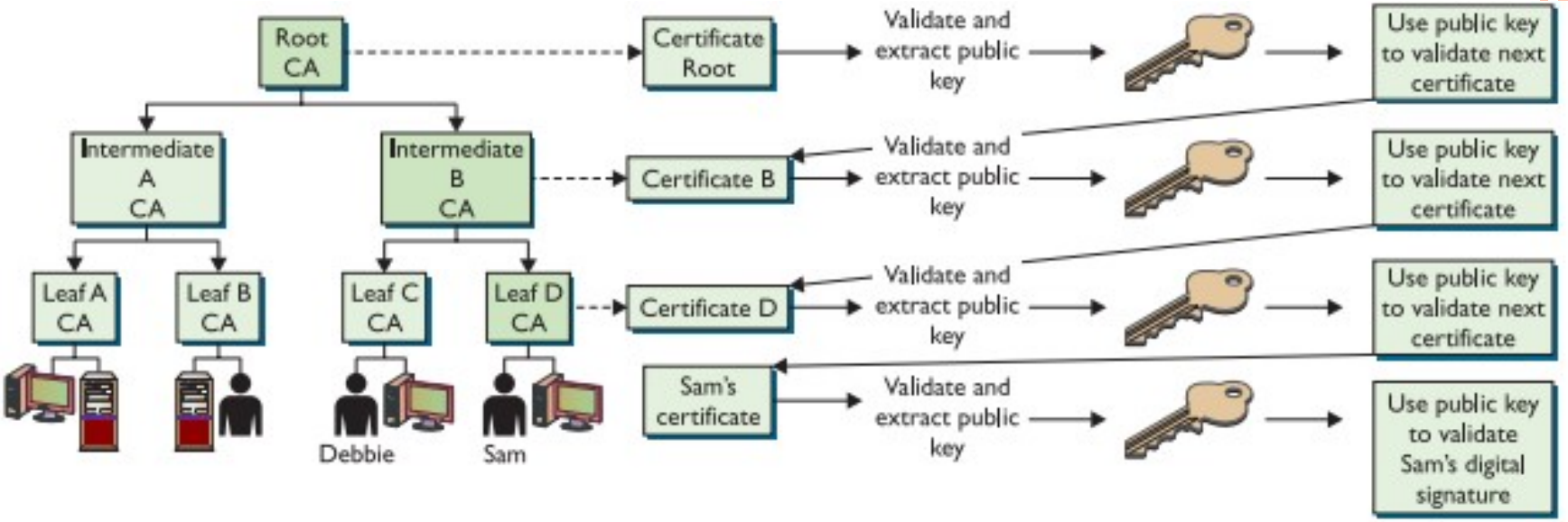
CONT..

- So in Figure, we have a user, Sam, who digitally signs a message and sends it and his certificate to Debbie.
- Debbie needs to validate this certificate before she can trust Sam's digital signature.
- Included in Sam's certificate is an issuer field, which indicates that the certificate was issued by Leaf D CA.
- Debbie has to obtain Leaf D CA's digital certificate and public key to validate Sam's certificate.
- Remember that Debbie validates the certificate by verifying its digital signature.
- The digital signature was created by the certificate issuer using its private key, so Debbie needs to verify the signature using the issuer's public key.

CONT..

- Debbie tracks down Leaf D CA's certificate and public key, but she now needs to verify this CA's certificate, so she looks at the issuer field, which indicates that Leaf D CA's certificate was issued by Intermediate B CA.
- Debbie now needs to get Intermediate B CA's certificate and public key.
- Debbie's client software tracks this down and sees that the issuer for Intermediate B CA is the root CA, for which she already has a certificate and public key. So Debbie's client software had to follow the certificate path, meaning it had to continue to track down and collect certificates until it came upon a self-signed certificate.
- A self-signed certificate indicates that it was signed by a root CA, and Debbie's software has been configured to trust this entity as her trust anchor, so she can stop there. Figure illustrates the steps Debbie's software had to carry out just to be able to verify Sam's certificate.

verifying each certificate in a certificate path



CONT..

- This type of simplistic trust model works well within an enterprise that easily follows a hierarchical organizational chart, but many companies can not use this type of trust model because different departments or offices require their own trust anchors.
- These demands can be derived from direct business needs or from inter organizational politics. This hierarchical model might not be possible when two or more companies need to communicate with each other.
- Neither company will let the other's CA be the root CA, because each does not necessarily trust the other entity to that degree.
- In these situations, the CAs will need to work in a peer-to-peer relationship instead of in a hierarchical relationship.

Peer-to-Peer Model

- In a peer-to-peer trust model, one CA is not subordinate to another CA, and no established trusted anchor between the CAs is involved.
- The end-entities will look to their issuing CA as their trusted anchor, but the different CAs will not have a common anchor.
- Figure illustrates this type of trust model. The two different CAs will certify the public key for each other, which creates a bidirectional trust.
- This is referred to as cross-certification, since the CAs are not receiving their certificates and public keys from a superior CA, but instead are creating them for each other.

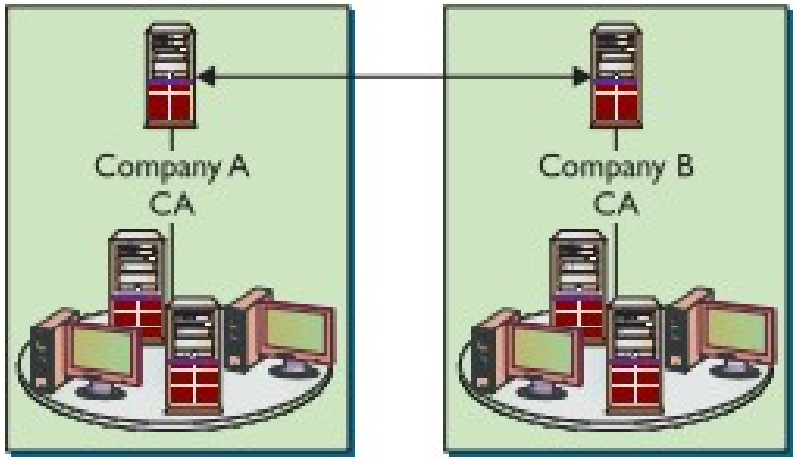
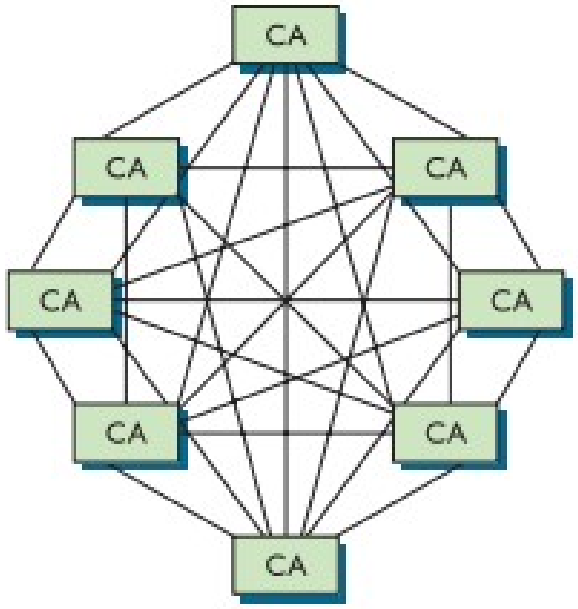


Fig.-Cross-certification creates a peer-to-peer PKI model

CONT..

- One of the main drawbacks to this model is scalability.
- Each CA must certify every other CA that is participating, and a bidirectional trust path must be implemented, as shown in Figure.
- If one root CA were certifying all the intermediate CAs, scalability would not be as much of an issue.
- Figure represents a fully connected mesh architecture, meaning that each CA is directly connected to and has a bidirectional trust relationship with every other CA.
- As you can see in this illustration, the complexity of this setup can become overwhelming.



Scalability is a drawback in cross-certification models.

Hybrid Trust Model

- A company can be internally complex, and when the need arises to communicate properly with outside partners, suppliers, and customers in an authorized and secured manner, this complexity can make sticking to either the hierarchical or peer-to-peer trust model difficult, if not impossible.
- In many implementations, the different model types have to be combined to provide the necessary communication lines and levels of trust.
- In a hybrid trust model, the two companies have their own internal hierarchical models and are connected through a peer-to-peer model using cross-certification.

CONT..

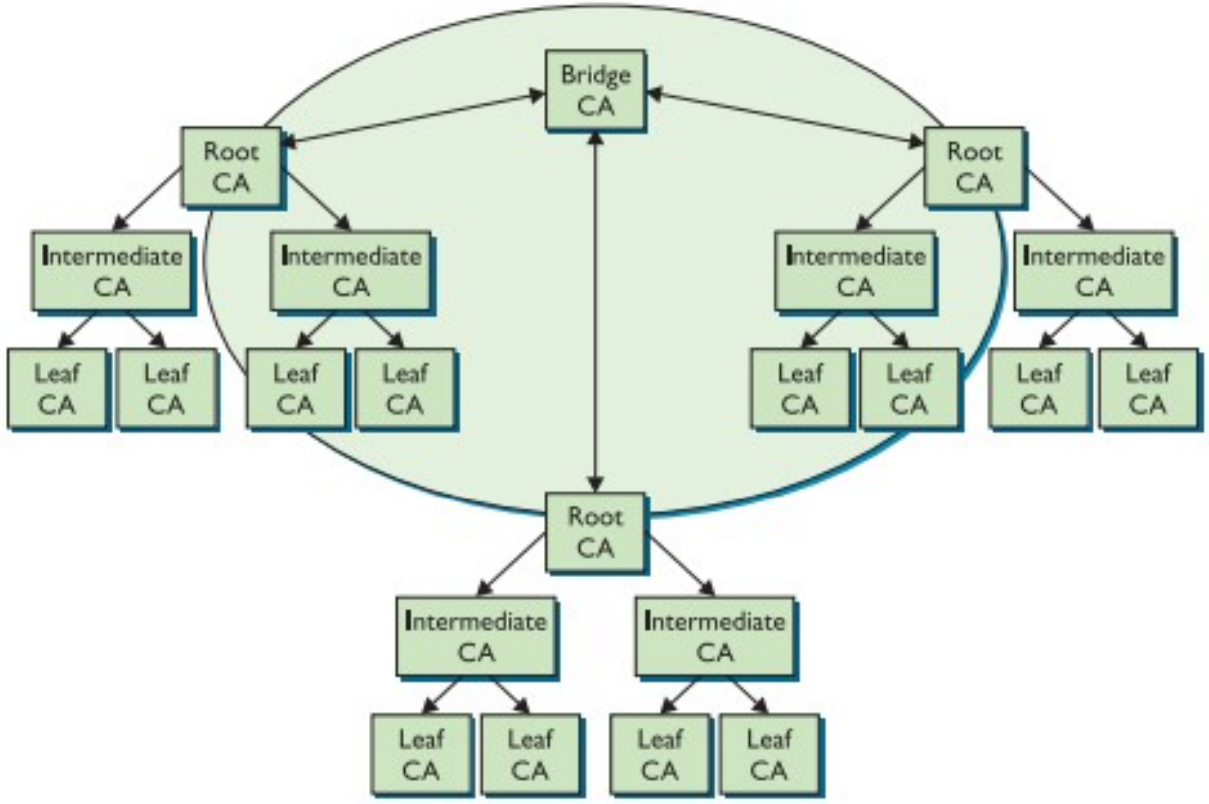


Fig.- A bridge CA can control the cross-certification procedures.

CONT..

- Another option in this hybrid configuration is to implement a bridge CA. Figure illustrates the role that a bridge CA could play—it is responsible for issuing cross-certificates for all connected CAs and trust domains. The bridge is not considered a root or trust anchor, but merely the entity that generates and maintains the cross-certification for the connected environments.