Chapter 3

Cryptography

Introduction:

Cryptography is an ancient art of keeping secrets. Cryptography ensures security of communication over insecure medium.

Terms used in Cryptography:

1) Plain text

Plain text signifies a message that can be understood by the sender, the recipient and also by anyone else who gets an access to the message.

2) Cipher text

When a plain text message is codified using any suitable scheme, the resulting message is called as cipher text.

3) Cryptography

Cryptography is the art and science of achieving security by encoding messages to make them non-readable.

4) Cryptanalysis

Cryptanalysis is the technique of decoding messages from a non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format.

5) Encryption: The process of encoding plain text into cipher text message is known as Encryption.

6) Decryption: The process of transforming cipher text message into plain text or original text is known as Decryption.

7) Cipher - algorithm for transforming plaintext to ciphertext

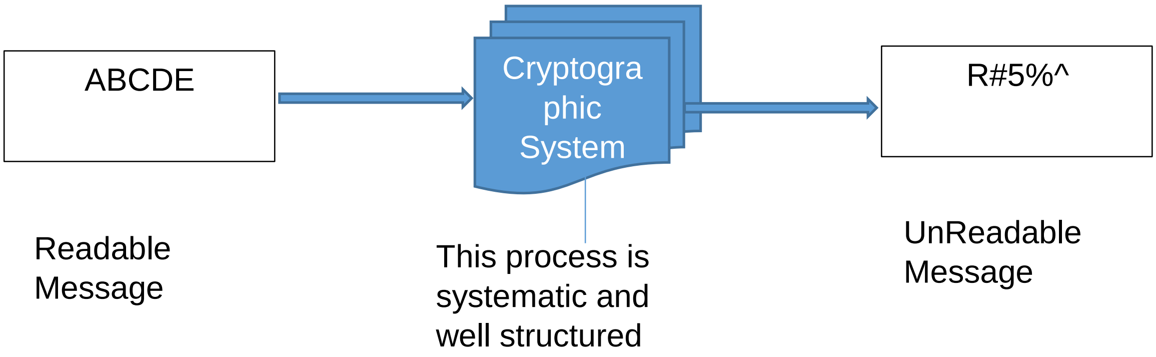
8) Cryptology: The combination of cryptography and cryptanalysis.

There are two kinds of cryptography:

a)Symmetric Cryptography: use the same key (the secret key) to encrypt and decrypt a message

b) Asymmetric Cryptography: use one key (the public key) to encrypt a message and a different key (the private key) to decrypt it. Asymmetric cryptography is also called public key cryptography.

Cryptographic System



ABCDE

Cryptographic System

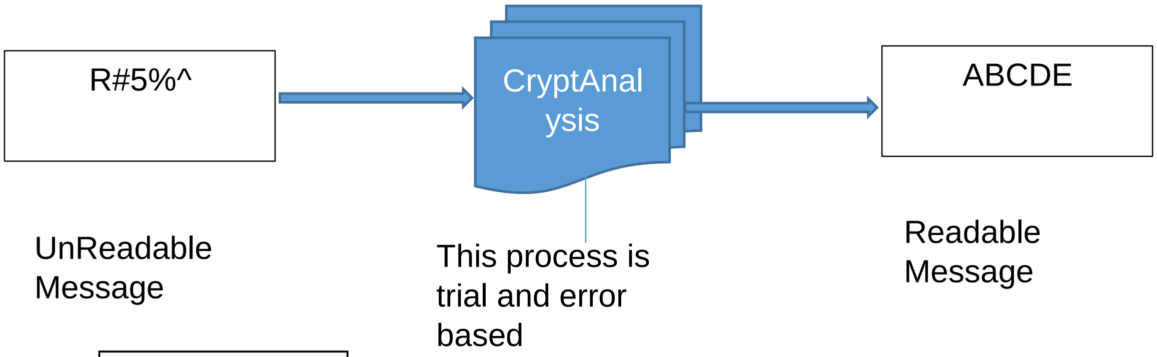
R#5%^

Readable Message

This process is systematic and well structured

UnReadable Message

CryptAnalysis



R#5%^

CryptAnalysis

ABCDE

UnReadable Message

This process is trial and error based

Readable Message

Cryptography

+

Cryptanalysis

=

Cryptology

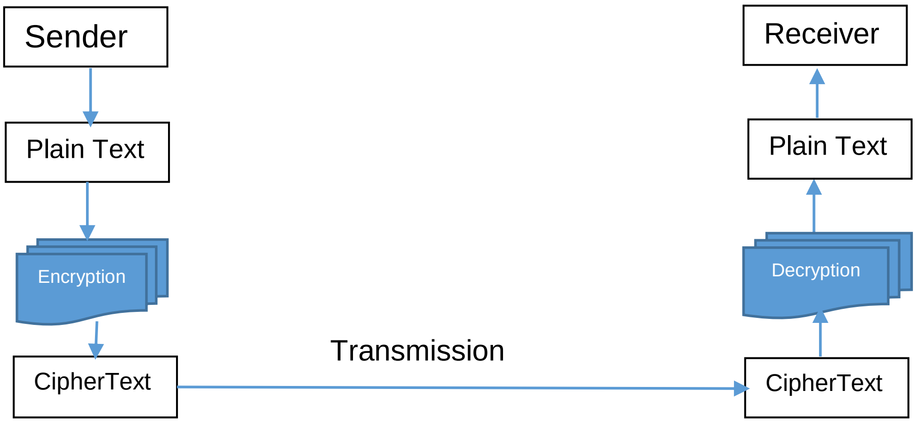
For any communication in applications following four security requirements are required:

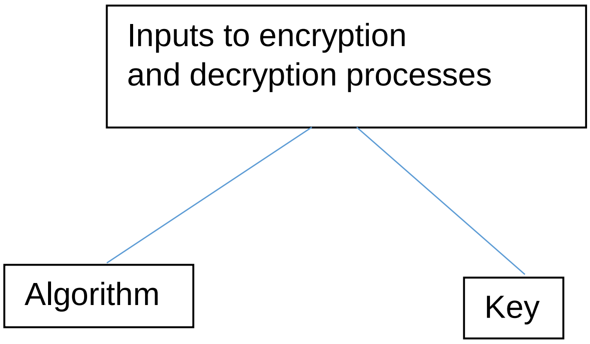
i) Authentication: It is the process of proving one's identity

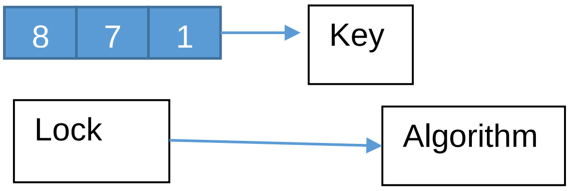
ii) Privacy /Confidentiality: It is the process of ensuring that no one can read the message except the intended receiver.

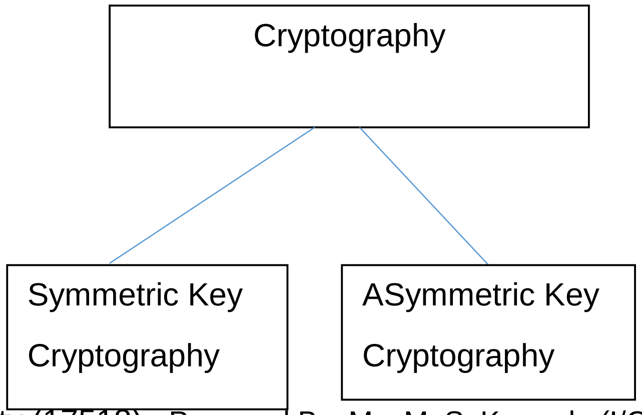
iii) Integrity: It is the process of assuring the receiver that the received message has not been changed in any way from the original.

iv) Non Repudiation: It is the process to prove that the sender has really sent this message and he cannot deny it.





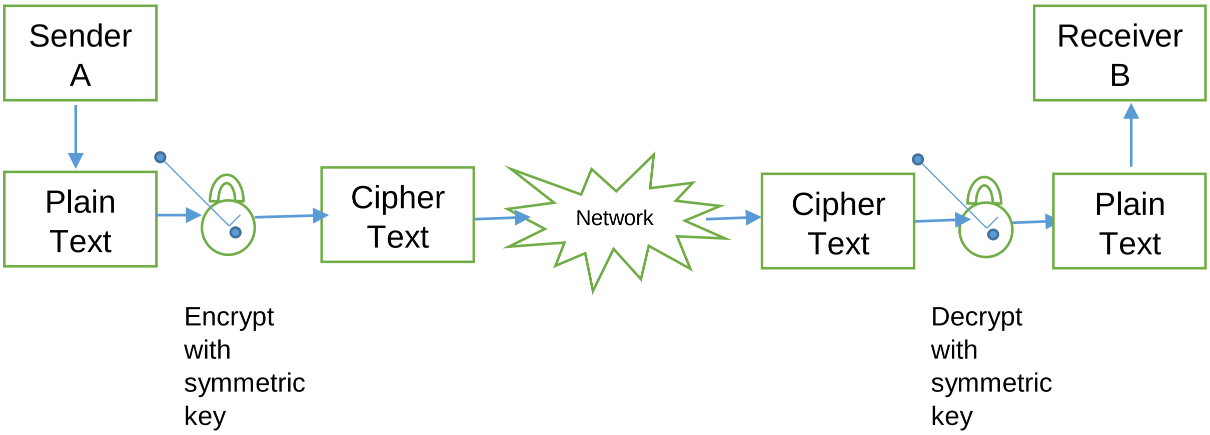




Applications of Cryptography

1. Data Hiding: The original use of cryptography is to hide something that has been written.
2. Digitally Code: Cryptography can also can be applied to software, graphics or voice that is, it can be applied to anything that can be digitally coded.
3. Electronic payments in Banking: When electronic payments are sent through a network, the biggest risk is that the payment message will alter or bogus messages introduced and the risk that someone reads the messages may be minor significance.
4. Message Authentication: One cannot entirely prevent someone from tampering with the network and changing the message, but if this happens it can certainly be detected. This process of checking the integrity of the transmitted message is often called message authentication. The most recent and useful development in the uses of cryptography is the **Digital Signature**
5. Mobile banking, ATM , Credit cards
6. Email, Ecommerce, Electronic payment gateways

1) Symmetric Key Cryptography

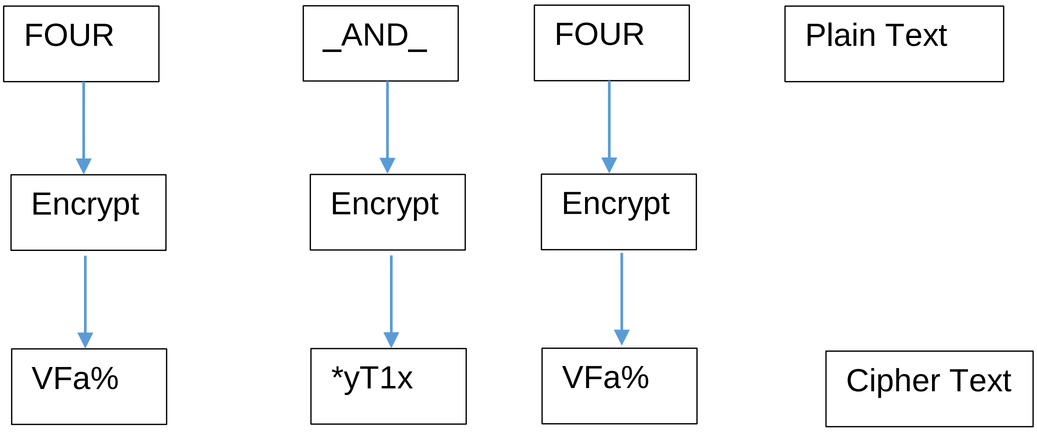


In symmetric cipher, the same key is used for encryption and decryption. Hence this is also known as single key or secret key or shared key algorithm.

The key has to be kept secret, sender and receiver uses the same key to read encrypted data. The key is only known to sender and receiver and no one else. There are two types of Algorithm Types.

1) Block Cipher:

Block Cipher technique involves encryption of one block of text at a time. Decryption also takes one block of encrypted text at a time.



Encryption Process

The blocks used in block ciphers generally contain 64 bits or more

2) Stream Cipher

Stream Cipher technique involves the encryption of one plain text byte at a time. The decryption also happens one byte at a time

In text format	In binary format	
Pay 100	010111001	Plain text
	100101011	XOR operation with key
ZTU91^%D	11001001	Cipher Text

Block Ciphers:

Advantages: Random Access, Potentially High Security

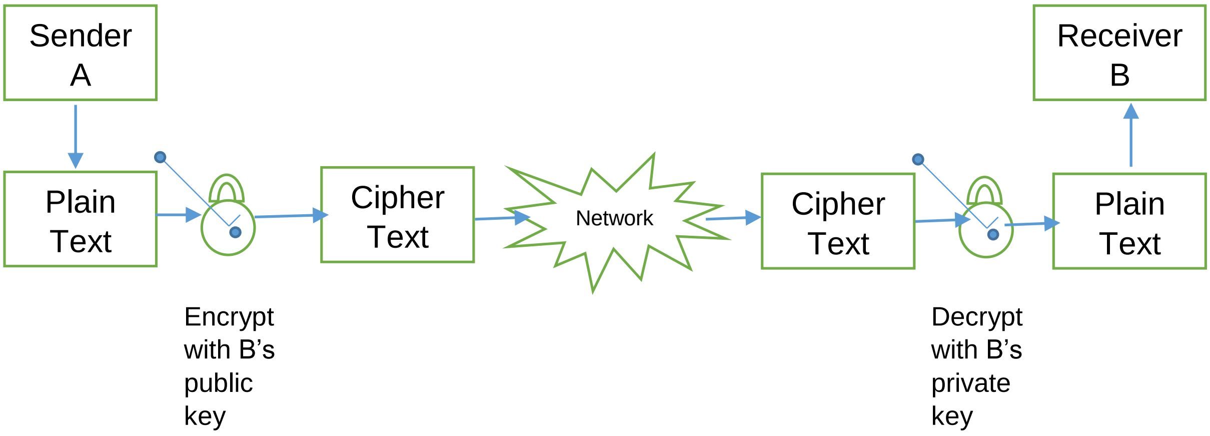
Disadvantages: Larger Block Size needed, Patterns retained throughout messages

Stream Ciphers:

Advantages: Can work on smaller Block series, Little memory/processing/Buffering Needed

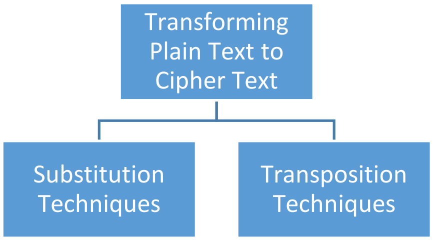
Disadvantages: Random Access Difficult, Hard to use large keys, sender and receiver must be synchronized, inserted bits can lead to errors.

2) Asymmetric Key Cryptography:



- Asymmetric Encryption is also known as Public Key Cryptography, since users typically create a matching key pair and make one public while keeping the other secret.
- Users can send secret messages by encrypting a message with the recipient's public key In this case, only the intended recipient can decrypt the message, since only that user should have access to the required key.
- The main advantage of asymmetric cryptography is the security of a key.

There are two types of techniques to transform plain text to cipher text.



Substitution Techniques

In substitution technique, letters of plaintext can be replaced by another letters or numbers/symbols to generate cipher text.

1) Caesar Cipher:

It was first proposed by Julius Caesar and is termed as Caesar Cipher. It was the first example of substitution cipher. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet

It is very simple to implement and easily get cracked

Example:

Plain Text : 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

Encryption Key=3

Cipher Text: 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

Plain Text: W E L C O M E

Encryption Key=3

Cipher Text: Z H O F R P H

Cipher Text: CK D S S B

Decryption Key =3

Plain Text: H A P P Y

2) Mono-alphabetic Ciphers:-

Major drawback of the Caesar cipher is its predictability. Once we decide to replace an alphabet in a plain-text message with an alphabet that is k positions up or down the order, one replace all other alphabets with same technique.

In mono alphabetic ciphers instead of using uniform scheme for all the alphabets in a given plain text messages, we decide to use random substitution. This means that in a given plain text message, each A can replace by any other alphabet (B through Z). The crucial difference being there is no relation between replacement of B and replacement of A.

Example:-

PLAIN	A	B	C	D	E	F	G	H	I	J	K	L	M
CIPHER	E	L	X	N	A	K	R	V	F	Z	O	Y	H

PLAIN	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CIPHER	C	M	Q	D	U	W	B	S	J	T	G	P	I

PLAIN TEXT: INFORMATION SECURITY

CIPHER TEXT: FCKMUHEBFMC WAXSUFBP

3) Homophonic Substitution Cipher

In this technique, one plain text alphabet can map to more than one cipher text alphabet.

For eg A can be replaced by [D, H, P, R]

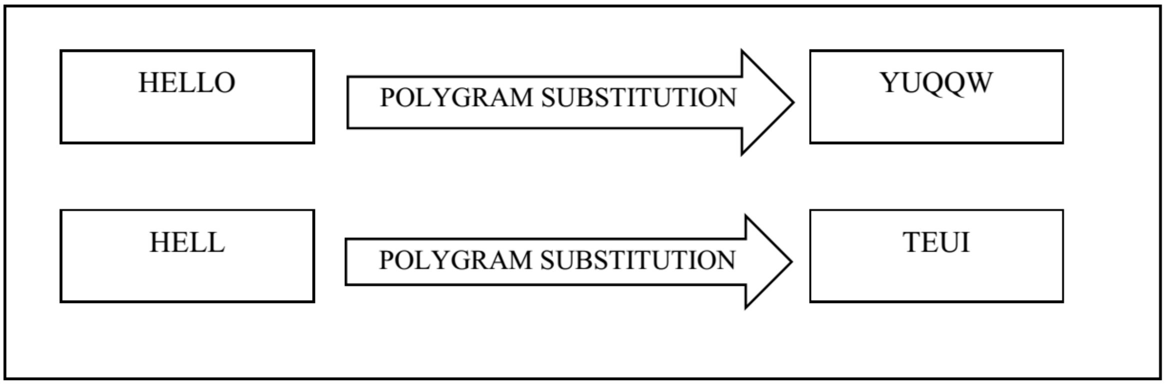
B can be replaced by [E, I, Q, S]

Homophonic Substitution Cipher also involves substitution of one plain text character with a cipher text character at a time, however the cipher text character can be any one of the chosen set.

4) Polygram Substitution Cipher

In Polygram Substitution cipher instead of replacing one plain text alphabet with one cipher text alphabet at a time, a block of alphabets are replaced with another block. This is done by replacing a block with completely different cipher text block.

Example:



1) Polyalphabetic Substitution Cipher

Leon Battista invented the Polyalphabetic Substitution Cipher in 1568 eg Vigenere Cipher, Beaufort Cipher

This cipher uses multiple one character keys. Each of the key encrypts one plain text character.

Vigenere Cipher

The logic for encryption is quite simple. For Key letter p and plain text letter q, the corresponding cipher text letter is at the intersection of row titled p and column titled q.

It should be clear that for encrypting a plain text message, we need a key whose length is equal to that of plain text message. Usually , a key that repeats itself is used.

Vigenere Table:

	PLAIN TEXT																										
		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
KEYWORD	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

Example:

Encryption

Keyword: Relations

Plain Text: TO BE OR NOT TO BE

Keyword: RE LA TI ONS RE LA

Cipher Text: KS ME HZ BBL KS ME

		PLAIN TEXT																									
		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
KEYWORD	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

Decryption:

Keyword: RE LA TI ONS RE LA

CipherText: KS ME HZ BBL KS ME

Plain Text: TO BE OR NOT TO BE

	PLAIN TEXT																										
		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
KEYWORD	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

2) PlayFair Cipher:
   Step 1:
- Creation and Population of Matrix
  Step 2:
- Encryption Process
  Step 1: Creation and Population of Matrix
  The Playfair Cipher makes use of a 5 x 5 Matrix (Table) which is used to store a keyword/ phrase that becomes the key for encryption and decryption.

1. Enter the keyword in the matrix row-wise: Left –to-Right and then top-to-bottom.
2. Drop duplicate letters

3. Fill the remaining spaces in the matrix with rest of the English alphabets (A-Z) that were not part of our keyword. While doing so, combine I and J in the same cell of the table. In other words, if I/J is a part of the keyword, disregard both I and J while filling the remaining slots.

   KeyWORD :

   PLAYFAIR EXAMPLE {A is duplicate hence dropped from the matrix}

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

5 x 5 Matrix

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

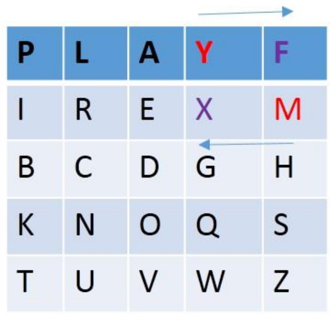
Generated 5 x 5 PlayFair Matrix

- **Step 2: Encryption Process**

1) The plaintext message that we want to encrypt needs to be broken down into groups of two alphabets For e.g. if our message is
   MY NAME IS ATUL it becomes
   MY NA ME IS AT UL
   2) If both alphabets are the same (and only one is left) add an X after the first alphabet. Encrypt the new pair and continue
   3) If both the alphabets in the pair appear in the same row of our matrix, replace them with alphabets to their immediate right respectively. If the original pair is on the right side of the row, then wrapping around to the left side of the row happens
   4) If both the alphabets in the pair appear in the same column of our matrix, replace them with alphabets immediately below them respectively. If the original pair is on the bottom side of the row, then wrapping around to the top side of the row happens
   5) If the alphabets are not in the same row or column, replace them with the alphabets in the same row resp. but at the other pair of corners of the rectangle defined by the original pair. The order is quite significant here. The first encrypted alphabet of the pair is the one that is present on the same row as the first plaintext alphabet.

- Encrypt the text MY NAME IS ATUL

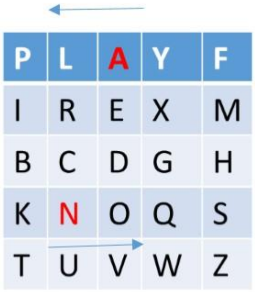
1) First Pair: MY



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

Apply Step #5
Plain Text: MY
Cipher text block: XF

2) Next Pair: NA

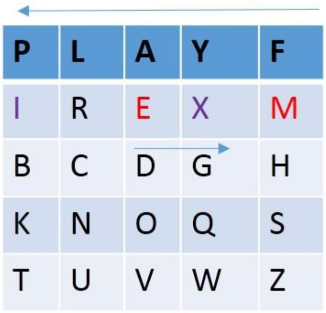


P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

Apply Step #5
Plain Text: NA
Cipher text block: OL

- Encrypt the text MY NAME IS ATUL

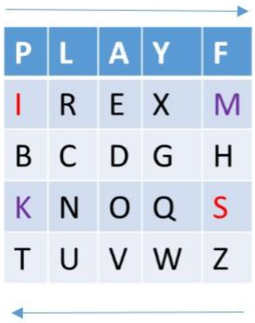
3) Next Pair: ME



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

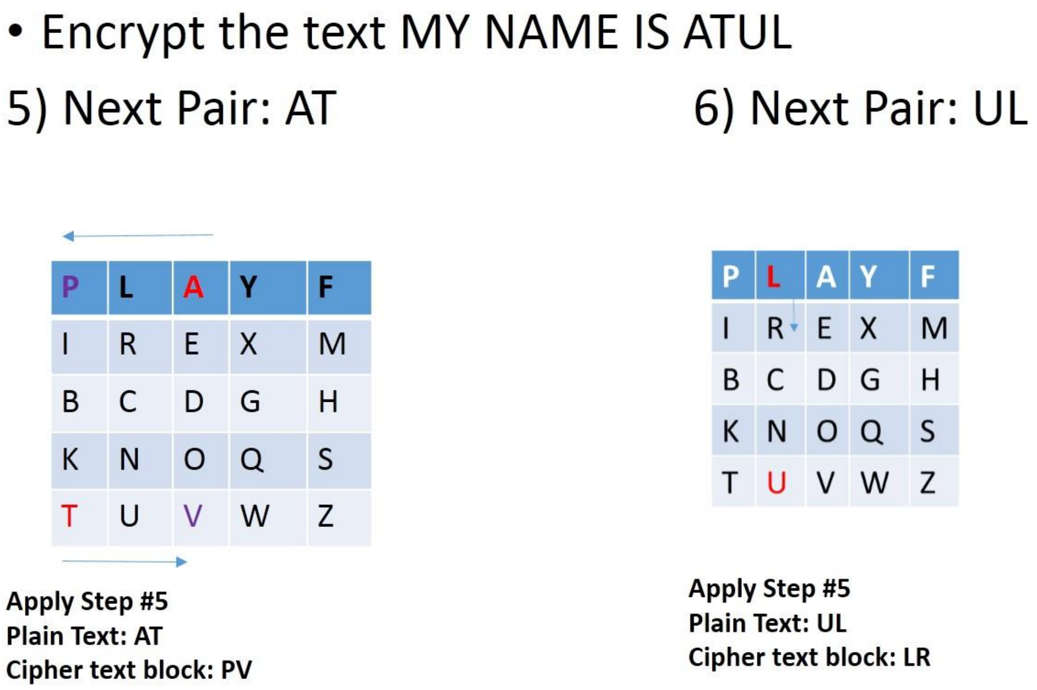
Apply Step #3
Plain Text: ME
Cipher text block: IX

4) Next Pair: IS



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

Apply Step #5
Plain Text: IS
Cipher text block: MK



- Encrypt the text MY NAME IS ATUL

5) Next Pair: AT

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

Apply Step #5
Plain Text: AT
Cipher text block: PV

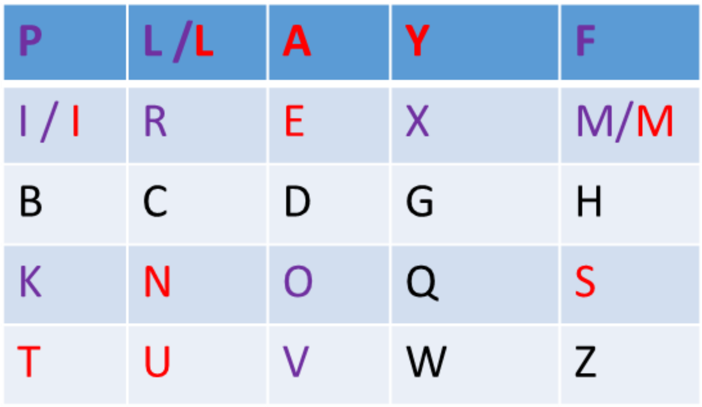
6) Next Pair: UL

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

Apply Step #5
Plain Text: UL
Cipher text block: LR

Plain Text: MY NAME IS ATUL
Cipher Text: XF OL IX MK PV LR

- Decryption
  Cipher Text: XF OL IX MK PV LR
  Plain Text: MY NAME IS ATUL
  KEY : PLAYFAIR EXAMPLE



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

3) Hill Cipher

Encryption

To encrypt a message using the Hill Cipher we must first turn our keyword into a key matrix (a 2 x 2 matrix for working with digraphs, a 3 x 3 matrix for working with trigraphs, etc). We 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. These vectors are then converted back into letters to produce the ciphertext.

2x2Example

We shall encrypt the plaintext message "PIET" using the keyword *hill* and a 2 x 2 matrix. The first step is to turn the keyword into a matrix. If the keyword was longer than the 4 letters needed, we would only take the first 4 letters, and if it was shorter, we would fill it up with the alphabet in order.

With the keyword in a matrix, we need to convert this into a key matrix. We do this by converting each letter into a number by its position in the alphabet (starting at 0). So, A = 0, B = 1, C= 2, D = 3, etc.

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix}$$

The keyword written as a matrix.

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$$

The key matrix (each letter of the keyword is converted to a number).

2) We now split the plaintext into digraphs, and write these as column vectors. That is, in the first column vector we write the first plaintext letter at the top, and the second letter at the bottom. Then we move to the next column vector, where the third plaintext letter goes at the top, and the fourth at the bottom. This continues for the whole plaintext.

$$\begin{pmatrix} P \\ I \end{pmatrix} \begin{pmatrix} E \\ T \end{pmatrix} \qquad \begin{pmatrix} 15 \\ 08 \end{pmatrix} \begin{pmatrix} 4 \\ 19 \end{pmatrix}$$

Now we must perform some matrix multiplication. We multiply the key matrix by each column vector in turn. We shall go through the first of these in detail, then the rest shall be presented in less detail. We write the key matrix first, followed by the column vector.

3) To perform matrix multiplication we "combine" the top row of the key matrix with the column vector to get the top element of the resulting column vector. We then "combine" the bottom row of the key matrix with the column vector to get the bottom element of the resulting column vector. The way we "combine" the four numbers to get a single number is that we multiply the first element of the key matrix row by the top element of the column vector, and multiply the second element of the key matrix row by the bottom element of the column vector. We then add together these two answers.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

The algebraic rules of matrix multiplication.

That is, we follow the rules given by the algebraic method shown to the left.

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 15 \\ 08 \end{pmatrix} = \begin{pmatrix} 7 * 15 + 8 * 8 \\ 11 * 15 + 11 * 8 \end{pmatrix} = \begin{pmatrix} 169 \\ 253 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} 13 \\ 19 \end{pmatrix} = \begin{pmatrix} N \\ T \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 4 \\ 19 \end{pmatrix} = \begin{pmatrix} 7 * 4 + 8 * 19 \\ 11 * 4 + 11 * 19 \end{pmatrix} = \begin{pmatrix} 180 \\ 253 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} 24 \\ 19 \end{pmatrix} = \begin{pmatrix} Y \\ T \end{pmatrix}$$

Plain Text : PIET

Cipher Text: NTYT

Decryption

To decrypt a ciphertext encoded using the Hill Cipher, we must find the inverse matrix. Once we have the inverse matrix, the process is the same as encrypting. That is we multiply the inverse key matrix by the column vectors that the ciphertext is split into, take the results modulo the length of the alphabet, and finally convert the numbers back to letters.

Since the majority of the process is the same as encryption, we are going to focus on finding the inverse key matrix (not an easy task), and will then skim quickly through the other steps (for more information see Encryption above).

In general, to find the inverse of the key matrix, we perform the calculation below, where *K* is the key matrix, *d* is the determinant of the key matrix and *adj*(*K*) is the adjugate matrix of K.

$$K^{-1} = d^{-1} \times adj(K)$$

General method to calculate the inverse key matrix.

2 x 2 Example

We shall decrypt the example above, so we are using the keyword *hill* and our ciphertext is "NTYT". We start by writing out the keyword as a matrix and converting this into a key matrix as for encryption. Now we must convert this to the inverse key matrix, for which there are several steps.

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix}$$

The keyword written as a matrix.

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$$

The key matrix (each letter of the keyword is converted to a number).

Step 1 - Find the Multiplicative Inverse of the Determinant

The determinant is a number that relates directly to the entries of the matrix. It is found by multiplying the top left number by the bottom right number and subtracting from this the product of the top right number and the bottom left number. This is shown algebraically below. Note that the notation for determinant has straight lines instead of brackets around our matrix.

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

Algebraic method to calculate the determinant of a 2 x 2 matrix.

Once we have found this value, we need to take the number modulo 26. Below is the way to calculate the determinant for our example.

$$\begin{vmatrix} 7 & 8 \\ 11 & 11 \end{vmatrix} = 7 \times 11 - 8 \times 11 = -11 = 15 \; mod \; 26$$

Calculating the determinant of our 2 x 2 key matrix.

We now have to find the multiplicative inverse of the determinant working modulo 26. That is, the number between 1 and 25 that gives an answer of 1 when we multiply it by the determinant. So, in this case, we are looking for the number that we need to multiply 15 by to get an answer of 1 modulo 26. There are algorithms

$$dd^{-1} = 1 \; mod \; 26$$

If d is the determinant, then we are looking for the inverse of d.

$$15 \times x = 1 \; mod \; 26$$

to calculate this, but it is often easiest to use trial and error to find the inverse.

The multiplicative inverse is the number we multiply 15 by to get 1 modulo 26.

$$15 \times 7 = 105 = 1 \; mod \; 26$$

This calculation gives us an answer of 1 modulo 26.

So the multiplicative inverse of the determinant modulo 26 is 7. We shall need this number later.

Step 2 - Find the Adjugate Matrix

The adjugate matrix is a matrix of the same size as the original. For a 2 x 2 matrix, this is fairly straightforward as it is just moving the elements to different positions and changing a couple of signs. That is, we swap the top left and bottom right numbers in the key matrix, and change the sign of the the top right and bottom left numbers. Algebraically this is given below.

$$adj\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

The adjugate matrix of a 2 x 2 matrix.

Again, once we have these values we will need to take each of them modulo 26 (in particular, we need to add 26 to the negative values to get a number between 0 and 25. For our example we get the matrix below.

$$adj\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} = \begin{pmatrix} 11 & -8 \\ -11 & 7 \end{pmatrix} = \begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix}$$

The adjugate matrix of the key matrix.

Step 3 - Multiply the Multiplicative Inverse of the Determinant by the Adjugate Matrix

To get the inverse key matrix, we now multiply the inverse determinant (that was 7 in our case) from step 1 by each of the elements of the adjugate matrix from step 2. Then we take each of these answers modulo 26.

$$7 \times \begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix} = \begin{pmatrix} 77 & 126 \\ 165 & 49 \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \; mod \; 26$$

Multiplying the multiplicative inverse of the determinant by the adjugate to get the inverse key matrix.

That is:

$$if \; K = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}, then \; K^{-1} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}$$

Now we have the inverse key matrix, we have to convert the ciphertext into column vectors and multiply the inverse matrix by each column vector in turn, take the results modulo 26 and convert these back into letters to get the plaintext.

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 13 \\ 19 \end{pmatrix} = \begin{pmatrix} 25 * 13 + 22 * 19 \\ 1 * 13 + 23 * 19 \end{pmatrix} = \begin{pmatrix} 743 \\ 450 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} 15 \\ 8 \end{pmatrix} = \begin{pmatrix} P \\ I \end{pmatrix}$$

$$\begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}24\\ 19\end{pmatrix}=\begin{pmatrix}25*24+22*19\\ 1*24+23*19\end{pmatrix}=\begin{pmatrix}1018\\ 461\end{pmatrix}\text{mod }26=\begin{pmatrix}4\\ 19\end{pmatrix}=\begin{pmatrix}E\\ T\end{pmatrix}$$

Transposition Techniques:

Transposition technique differ from substitution techniques in the way that they do not simply replace one alphabet with another. They also perform some permutation over the plain text alphabets.

E g In Harry Potter II (Harry Potter and the Chamber of Secrets)

“ TOM MARVOLO RIDDLE” becomes

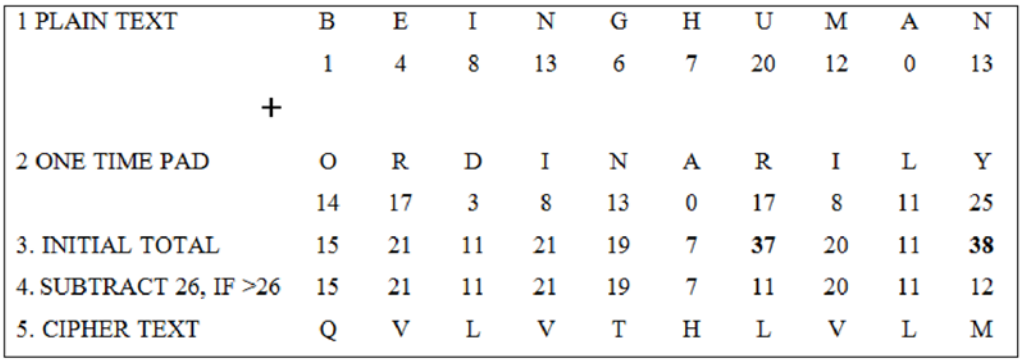
I AM LORD VOLDEMORT

1) Vernam Cipher(One Time Pad):

One time pad also known as Vernam Cipher, is implemented using random set of non-repeating characters as the input cipher text. The most significant point here is that once an input cipher text for transposition is used, it is never used again for any other message hence the name one time pad. The length of the input cipher text is equal to the length of the original plain text. The algorithm used in the Vernam cipher / one time pad is described as follows.

1. Treat each plain text alphabet as a number in an increasing sequence i.e. A = 0, B = 1, …Z = 25.
2. Do the same for each character of the input cipher text.
3. Add each number corresponding to the plain text alphabet to the corresponding input cipher text alphabet number.
4. If the sum thus produced is greater than 26, then subtract 26 from it.
5. Translate each number of the sum back to the corresponding alphabet. This gives the output cipher text.

Example: - Plain Text = ***“BEING HUMAN”***



1 PLAIN TEXT	B	E	I	N	G	H	U	M	A	N
	1	4	8	13	6	7	20	12	0	13
+										
2 ONE TIME PAD	O	R	D	I	N	A	R	I	L	Y
	14	17	3	8	13	0	17	8	11	25
3. INITIAL TOTAL	15	21	11	21	19	7	**37**	20	11	**38**
4. SUBTRACT 26, IF >26	15	21	11	21	19	7	11	20	11	12
5. CIPHER TEXT	Q	V	L	V	T	H	L	V	L	M

One time pad is discarded after single use and therefore is suitable only for short messages.

Row Transposition:-Variations of the basic transposition techniques such as rail fence technique exist. Such a scheme is given below which is known as

Simple columnar Transposition technique or Row Transposition technique.

Algorithm Steps:-

1. Write the plain text message row by row in a rectangle of a predefined size (keyword size)
2. Read the message column by column, however, it need not be in the order of columns, it can be any random order.
3. The message thus obtained is the cipher text message.

Example: Plain Text: —**Come Home Tomorrow"**
Keyword: ZEBRAS

Consider a rectangle with six column and. Therefore, when the message is written in the rectangle row by row it will look as follow

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6
C	O	M	E	H	O
M	E	T	O	M	O
R	R	O	W		

Now, decide the order of columns as some random order, say, 4, 6, 1, 2, 5, 3 Then read the text in the order of these columns.

The cipher text obtained from it would be :**EOW OO CMR OER HM MTO**

While Decryption phase the cipher is written back in same rectangle with same size and all ciphers are placed as per the key.

Double Columnar Transposition technique

Algorithm Steps:-

1. Write the plain text message row by row in a rectangle of a predefined size (keyword size)
2. Read the message column by column, however, it need not be in the order of columns, it can be any random order.
3. The message thus obtained is the cipher text message of round 1
4. Repeat steps 1 to 3 as many times as desired.

Example: Plain Text: —**Come Home Tomorrow"**
Keyword: ZEBRAS

Consider a rectangle with six column and. Therefore, when the message is written in the rectangle row by row it will look as follow

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6
C	O	M	E	H	O
M	E	T	O	M	O
R	R	O	W		

Now, decide the order of columns as some random order, say, 4, 6, 1, 2, 5, 3 Then read the text in the order of these columns.

The cipher text obtained from it would be :**EOW OO CMR OER HM MTO**

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6
E	O	W	O	O	C
M	R	O	E	R	H
M	M	T	O		

Now, decide the order of columns as some random order, say, 4, 6, 1, 2, 5, 3 Then read the text in the order of these columns.

The cipher text obtained from it would be : **OEO CH EMM ORMORWOT** in Round 2

Steganography

Steganography is the art and science of hiding information by embedding message within another message that is to be kept secret. It conceals the existence of the message.
Steganography works by replacing bits of useless /unused data in regular computer files (such as graphics, sound, text, html) with bits of different invisible information.
This hidden information can be plaintext, ciphertext or even image
The formula provides the description of stenographic process
Cover-Medium + Hidden-Data + Stego-Key = Stego-Medium

Here Cover-Medium – Data within which a message is to be hidden
Eg image file, audio file etc
Stego Key can be used to encrypt the hidden data.
Stego-Medium – Data within which a message has been hidden.

Uses of Steganography:

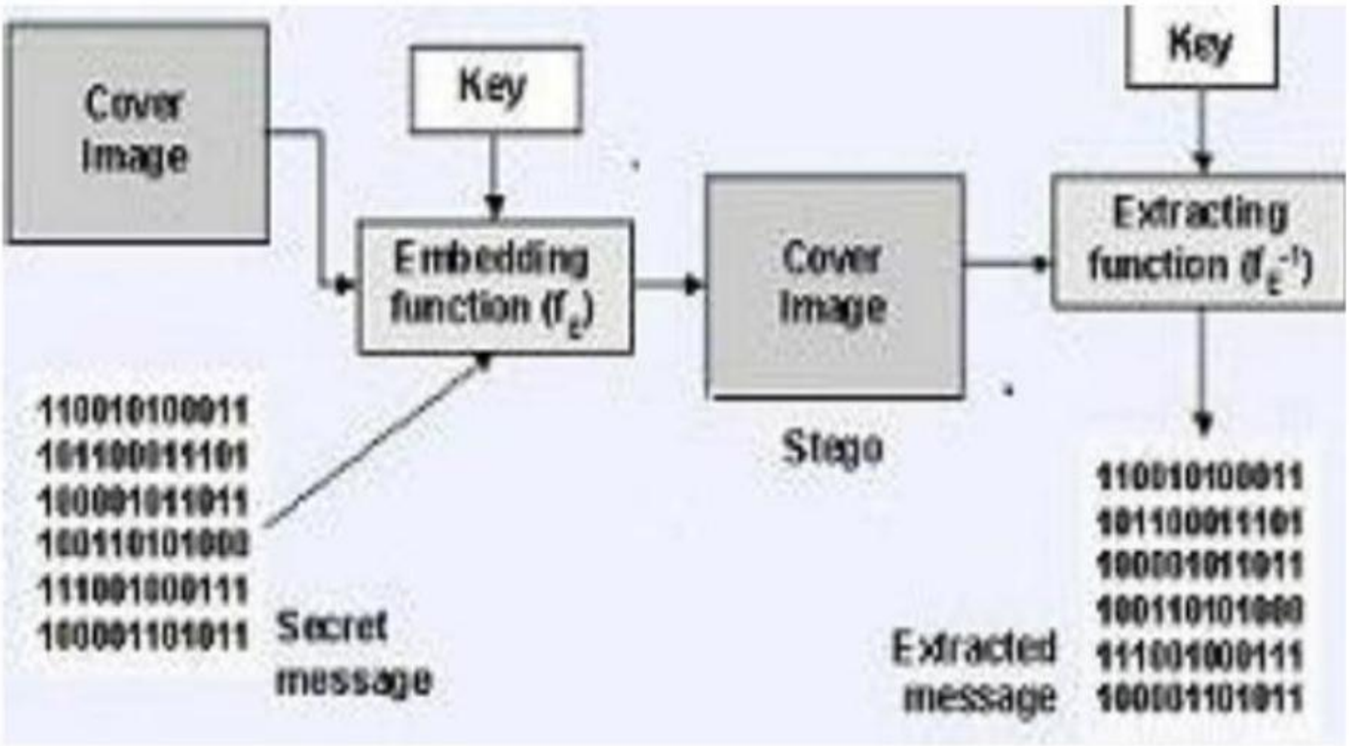
1) Legitimate purposes can include things such as watermarking images for copyright protection.

2) Steganography can also be used as a way to make a substitute for a one-way hash function
3) It can be used to tag notes to online images.
4) It can be used to maintain the confidentiality of valuable information to protect the data from possible sabotage, theft or unauthorized viewing.

DrawBacks:

It requires a lot of overhead to hide a relatively few bits of information.

Once the attacker knows the system, it becomes virtually worthless.



Authentication Protocols:

When designing a remote connection strategy it is critical to consider how remote users will be authenticated.

Authentication defines the way in which a remote client and server will negotiate on a user’s credentials when the user is trying to gain access to the network.

The following authentication protocols are listed

1) CHAP (Challenge Handshake Authentication Protocol)

This protocol is used by server to validate the identity of remote client CHAP verifies the identity by using 3-way handshaking and by using shared secrets.

After establishment of link, the server sends a challenge message to the client . Then client responds with a value obtained by using a one-way hash function.

Server compares the response i.e hash value with its own calculated hash value.

If the value matches, then the authentication is acknowledged or else the connection is terminated.

2) Extensible Authentication Protocol (EAP) is mostly used in wireless networks.
3) Password Authentication Protocol (PAP) is a two way handshake protocol for use with Point to Point (PPP) Protocol. It is not secure.
4) Shiva PAP (SPAP) : It is Shiva Password Authentication Protocol used by Shiva Remote Access servers. SPAP offers more security than PAP but not as secure as CHAP.
5) Data Encryption Standard (DES) It is used for older clients and servers.
6) Remote Authentication Dial –In-User Service RADIUS is used to authenticate users dialing in remotely to servers in a organizations network.
7) S/Key : One Time Password System developed for operating systems like UNIX
8) Terminal Access Controller Access Control System (TACACS) : It is an older authentication protocol used mainly in UNIX networks.
9) MS-CHAP (MD4): It is Microsoft Challenge Handshake Authentication Protocol. Uses a Microsoft version of RSA Message Digest for challenge and reply protocol. It only works on Microsoft systems and enables data encryption Selecting this authentication methods causes all data to be encrypted. It only works on Microsoft Systems.
10) SKID- SKID2 & SKID3 –Secret Key Identification Protocols

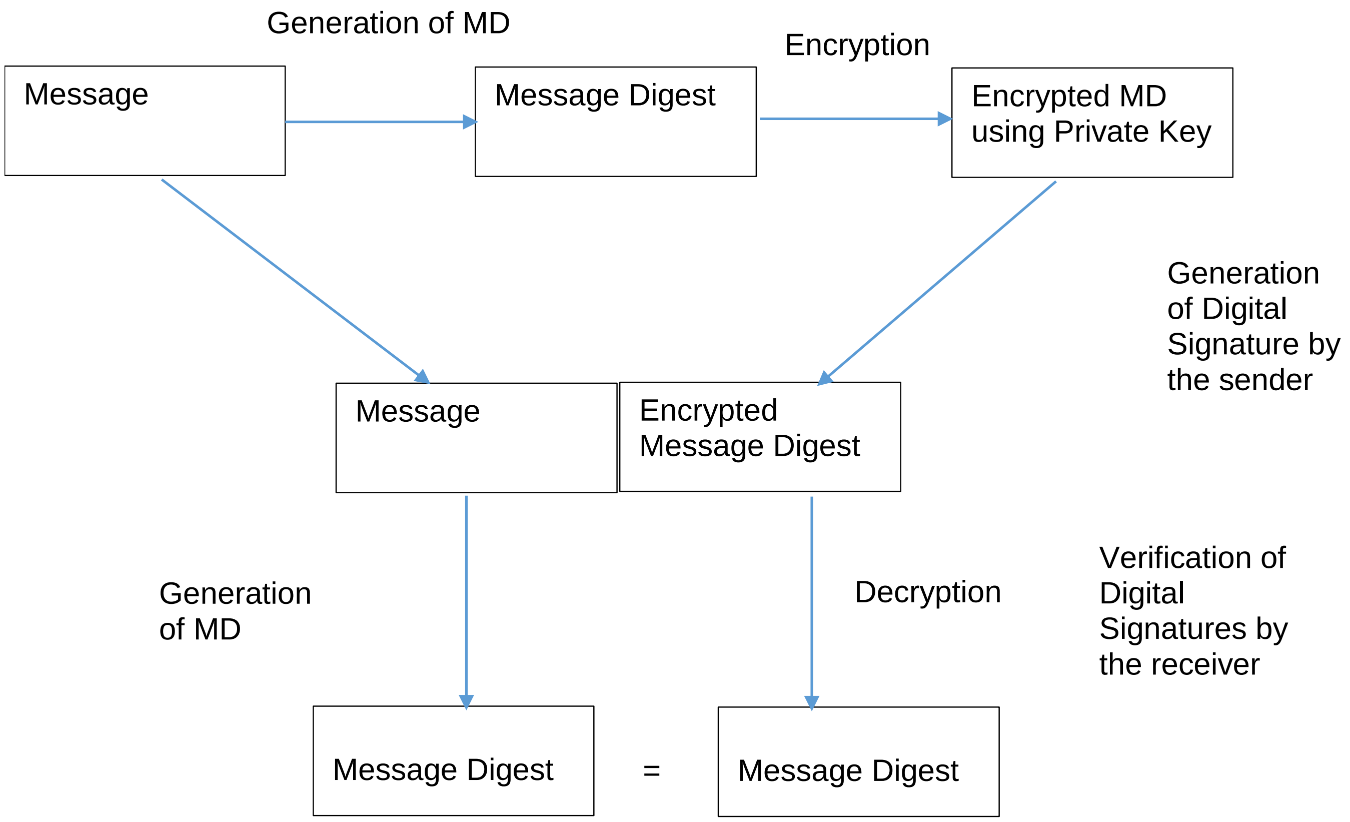
SKID2 provides unilateral entity authentication whereas SKID3 provides mutual entity authentication. These are vulnerable to a MAN-In the Middle Attack.

Digital Signatures:

Digital Signatures were created in response to the rising need to verify information transferred via electronic systems.

There are 3 common reasons for applying a Digital Signature to communications

1) Authentication 2) Integrity 3) Non-Repudiation



Generation and Verification of Digital Signatures

Digital Signature is an electronic signature that can be used to authentic the identity of the sender of a message or the signer of a document and possibly to ensure that the original content of the message or document that has been sent is unchanged.

Digital Signatures are easily transportable, cannot be imitated by someone else and can be automatically time-stamped.

The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later. It can be used with any type of message whether it is encrypted or not.

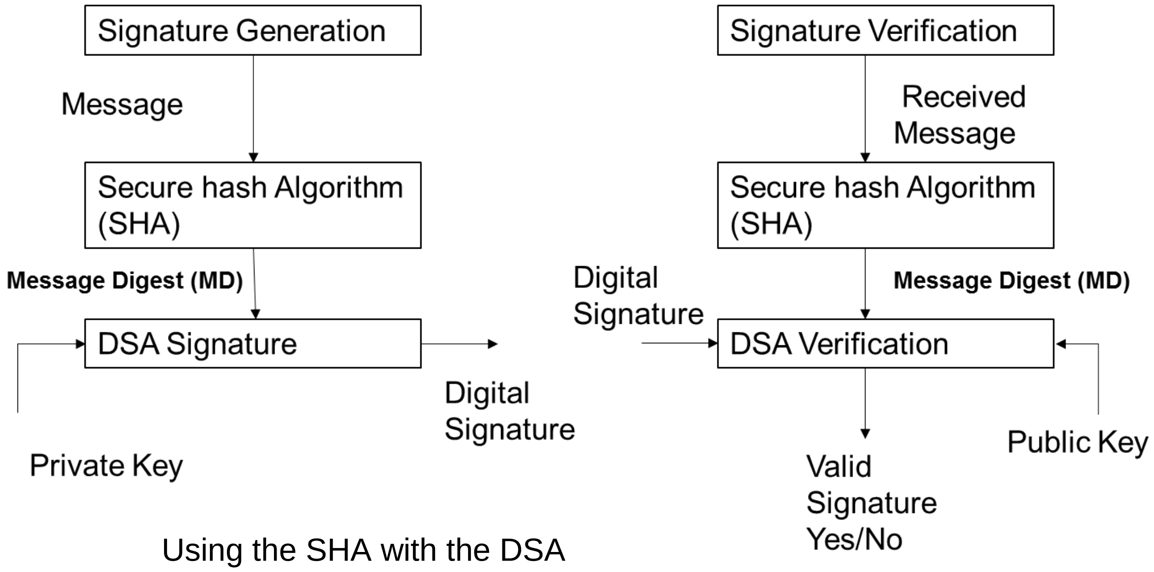
At the Sender's Side:

The message digest (MD) is calculated from the plaintext or message and then the private key of the sender is used to encrypt this message digest and then send this encrypted MD with the plaintext /message to the receiver.

At the Receiver's Side:

1) The receiver again calculates the MD from the plaintext or message and decrypts the encrypted MD received with the message with the sender's public key.
2) If both the MD is not the same, then the plaintext /message was changed after signing as shown in the figure above.

Digital Signature Standard (DSS)



Using the SHA with the DSA

- The digital signature standard was developed for performing digital signatures.
- It specifies a Digital Signature Algorithm (DSA) appropriate for Digital applications.
- National Institute of Standards and Technology (NIST) published DSA in 1991
- DSS makes use of SHA-1 algorithm for calculating message Digest.
- DSS is a standard whereas DSA is the actual algorithm
- DSA digital signature is a pair of large numbers represented in a computer as strings of binary digits.
- The digital signature is computed using a set of rules(i.e DSA) and a set of parameters such that the identity of the signatory and integrity of the data can be verified.
- The DSA provides the capability to generate and verify signatures.
- Signature Verification makes use of a public key Each user possess a private and public key pair.
- Anyone can verify the signature of a user by employing that user's public key.
- Signature generation can be performed only by the possessor of the user's private key.
- A hash function is used in the signature generation process to obtain a condensed version of data called a Message Digest (MD).
- The message digest is then input to the DSA to generate the Digital Signature.
- The Digital Signature is sent to the intended verifier along with the signed data (often called the message).
- The verifier of the message and signature verifies the signature key using the sender's public key. The same has in function must also be used in the verification process.

MSBTE Questions:

Summer 2016

1. List any four authentication protocols. Explain any one authentication protocol.
2. Consider a plain text "My name is Atul" convert given plain text into cipher text using "Playfair" cipher cryptography using Key-Playfair cipher example.

3. Explain in detail biometric authentication.
4. Consider a Plain Text “INFORMATION SECURITY” convert given plain text into cipher text using single columnar transposition cryptography using following data:
   No. of columns = 6
   Encryption Key = 326154
5. Differentiate between symmetric and asymmetric key cryptography.
6. Define the following terms:
   a. Plain text
   b. Cipher text
   c. Cryptography
   d. Cryptanalysis
7. Explain one time PAD cryptography for encryption

Winter 2015

8. Explain Ceaser cipher with example
9. What is cryptography ? Mention any three application of it.
10. What is digital signatures ? State digital signature standards
11. Describe play fair cipher.
12. Explain classical encryption techniques of cryptography.
13. Explain how to encrypt and decrypt message using transposition method. (6M)
14. What is steganography? Describe authentication protocols (6M)

Summer 2015

15. Define following with diagram:
    1) Encryption
    2) Decryption
    3) Cipher text
16. Consider plain text “Team” and key as “HILL”. Convert given plain text into cipher text using Hill cipher. Write step by step procedure.(Procedure-3M, Correct Answer-3M).
17. Describe then term digital steganography with neat diagram. (Diagram 1 Mark; Explanation 3 Marks).
18. Describe classical encryption techniques. (Any two encryption methods are expected 3 Marks each).
19. Describe play fair cipher and describe step by step encryption of plain with example. (Description 2 Marks; Encryption 2 Marks; Decryption 2 Marks).
20. Explain transposition cipher techniques with example. (Explanation 4m, Example-4M)
21. Describe double columnar transposition cipher technique with example. Also state criteria for selecting keyword. (Explanation -1M, Example-2Marks, Criteria-1Marks)

Winter 2014

22. Define cryptography. Explain application of cryptography. (Any three points) (Definition-1 Mark, Application-1 Mark each (any 3)).
23. Explain any two substitution cipher you have studied. (Any 2 Techniques are expected - 4 Marks each, for Description - 2 Marks, for example - 2 Marks (any relevant example shall be consider)).
24. Mention and explain any two classical encryption techniques.(List - 2 Marks, Explanation - 1 Mark each (Any technique shall be considered).

25. Explain row transposition cipher with example.(Description - 2 Marks, Example - 2 Marks).
26. Explain the meaning of Stegnography and Digital signature. Give example. (Stegnography - 2 Marks, Digital Signature - 2 Marks, Any relevant example shall be consider).
27. Explain one time Pad cipher and Hill cipher with example. (One time pad -2 Marks, Hill cipher - 2 Marks, 1 Mark for each example).
28. Describe Symmetric and Asymmetric Cipher: Give example. (Symmetric Cipher - 1 Mark, Asymmetric Cipher - 1 Mark, Example - 1 Mark each)