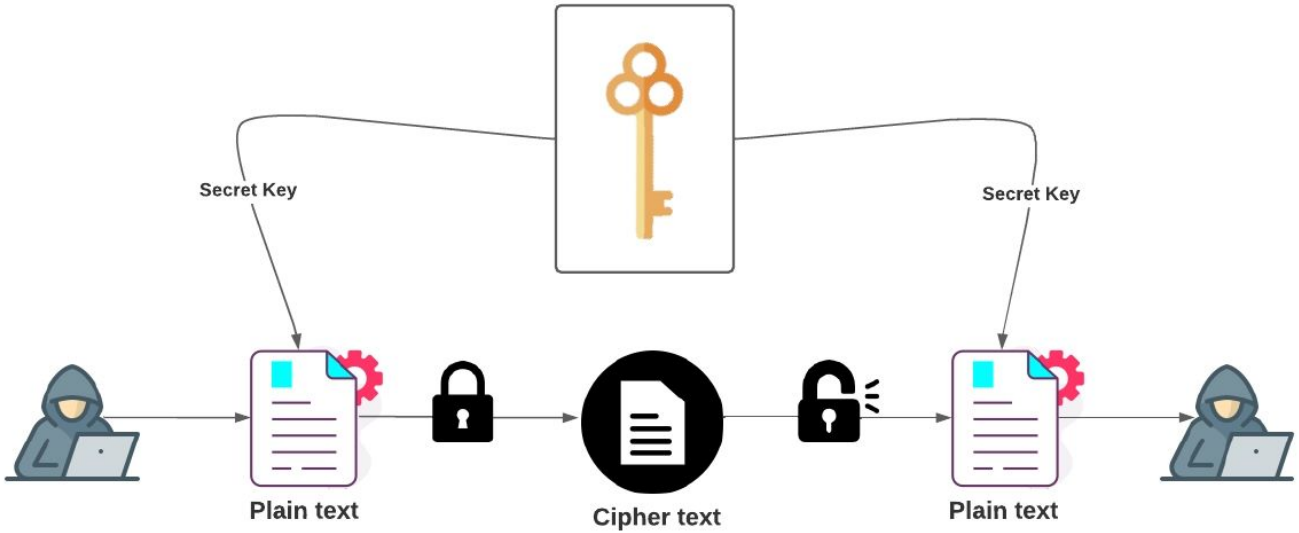
Unit 2 Cryptography



Cryptography & Network Security

- Cryptography
- Cryptography & Cryptanalysis
- Encryption Techniques
- Types of Cryptography
- Symmetric Encryption Algorithms

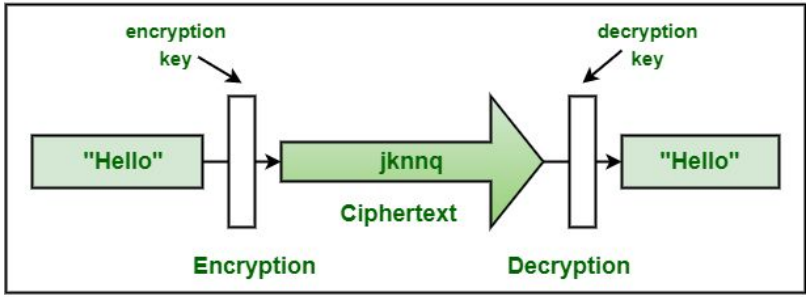
Cryptography

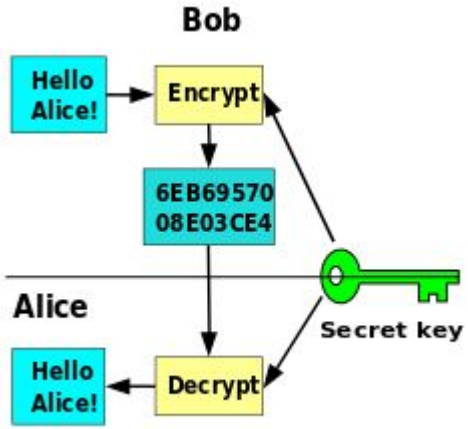
Cryptography

- Cryptography is the science, as well as art which focuses on encryption of communication and information by using cipher codes.

Cryptography Terminologies

- **Plaintext**: The medium, the non-encrypted source data, and the clear message.
- **Ciphertext**: The ciphertext is the form of incomprehensible plaintext. Only the encryption key can open the cipher and let the message be read.
- **Encryption**: The process of applying cryptographic algorithms and keys to convert the plaintext into ciphertext.
- **Decryption**: The process that is equivalent to encryption does decryption by way of converting ciphertext to plaintext with the aid of decryption keys.

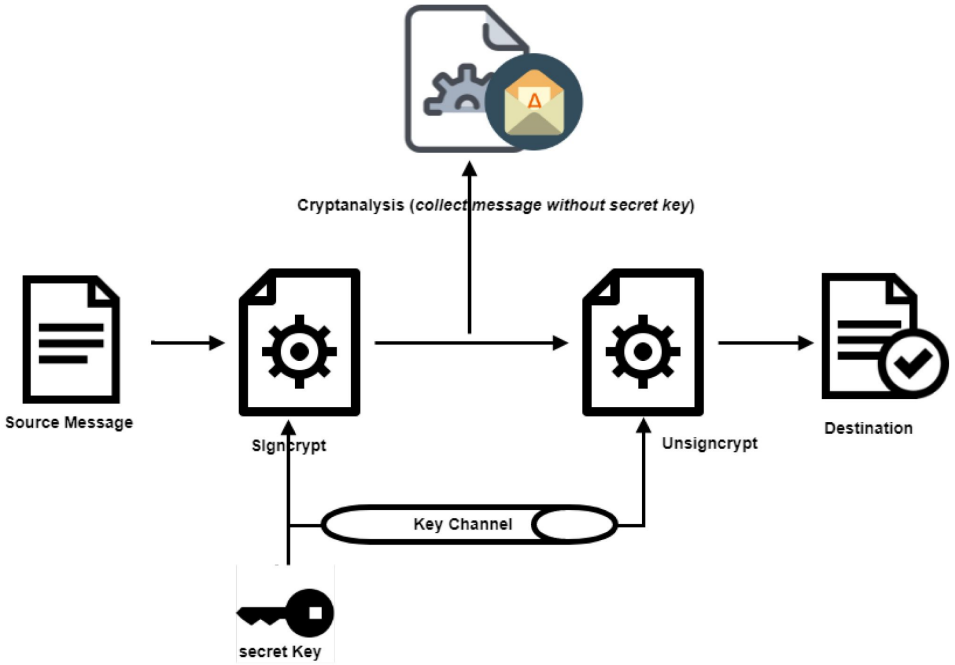




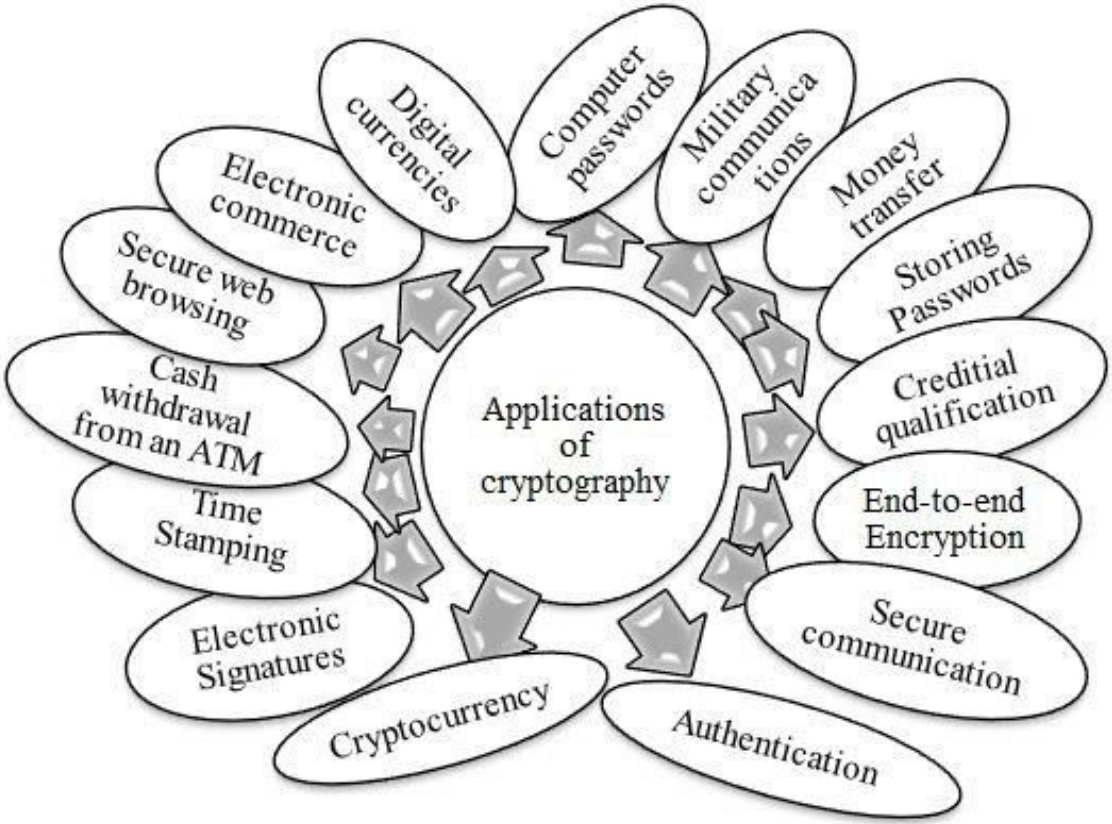
Cryptanalysis

What is Cryptanalysis?

- Cryptanalysis is a unique science, which, among other things, solves the task of breaking the encrypted information and such cryptosystems as well.
- Decryption is doing what encryption is doing in reverse to face ciphertext, making clear patterns that lead to the original keys that can be employed to unravel the intention message.
- Cryptanalysts use different tools to accomplish their task from mathematical algorithms and statistical analysis to test-all keys, substitution, and frequency analysis.
- The very goal of cryptanalysis is to delay the decoding of the coded text and ensure the process of evolution of even more advanced cryptographic algorithms in the attempts to divert new cryptanalytic techniques.

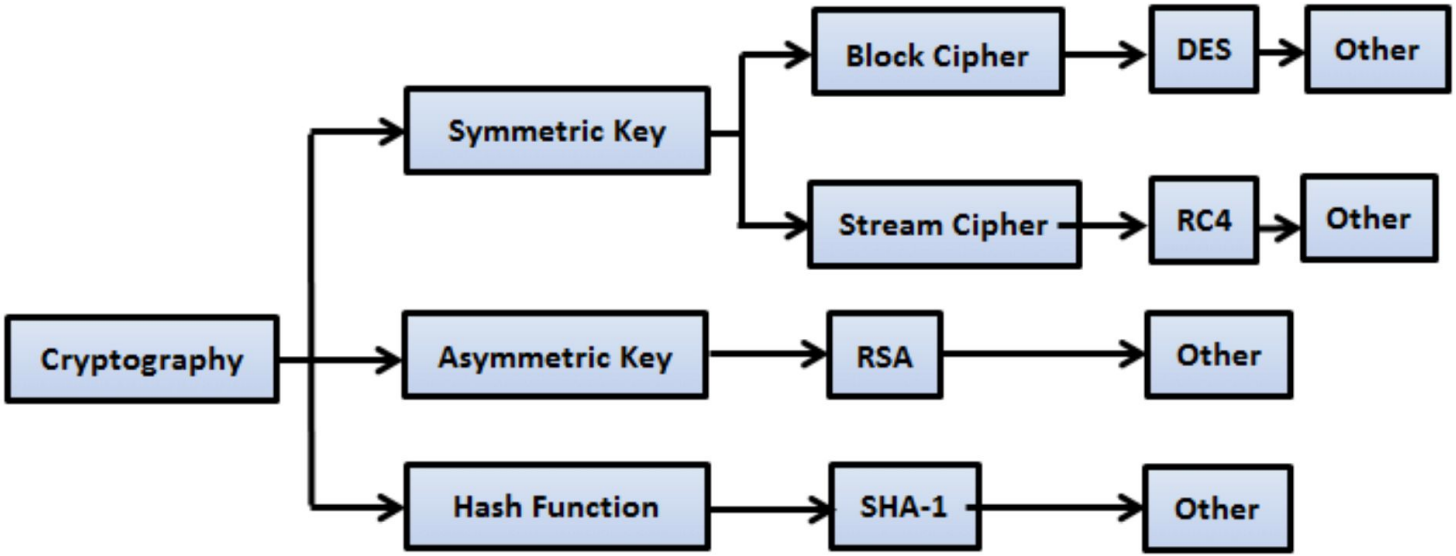


Application of Cryptography



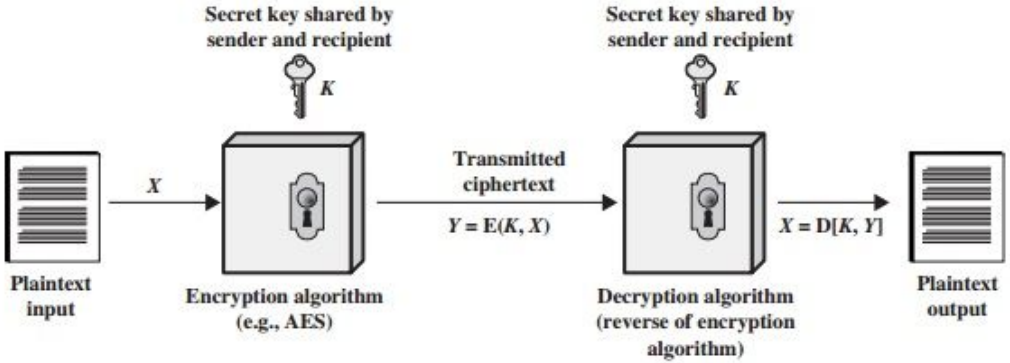
Types of Cryptography

- There are three types of cryptography
  - Symmetric key cryptography
  - Asymmetric key cryptography
  - Hash Function



Symmetric Key Cryptography

- Symmetric cipher model consists of five elements:
- 1. Plain Text
- 2. Encryption algorithm
- 3. Secret key
- 4. Cipher text
- 5. Decryption algorithm



Symmetric Key Cryptography

- Symmetric key cryptography is also known as **secret-key cryptography**, and in this type of cryptography, you can use only a **single key**.
- The sender and the receiver can use that single key to encrypt and decrypt a message.
- Because there is only one key for encryption and decryption, the symmetric key system has one major disadvantage: the two parties must exchange the **key in a secure** manner.
- Note that original encryption and decryption process uses well known symmetric key algorithm called as Data Encryption Standard (DES).
- Mathematically it is represented as **C = E(K, P)**, where C = cipher text, E= encryption, K = Secret shared key, P = Plain Text.
- Same as **P = D(K, C)**, where D = Decryption.
- For Example, Data Encryption Standard (DES), Advanced Encryption Standard (AES) and BLOFISH.

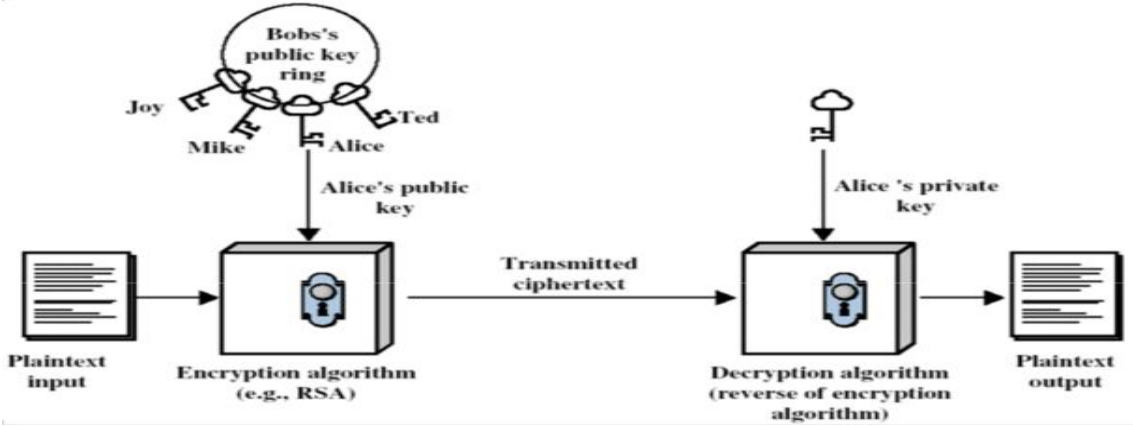
Symmetric Key Cryptography

- Advantages:
  - Symmetric key is **faster** than asymmetric key cryptography.
  - Same key is used for encryption and decryption, receiver cannot decrypt data without key (without sender permission).
  - Symmetric key achieves the authentication principle because it checks receiver's identity.
  - System resources are less utilized in this cryptography.
- Disadvantages:
  - Once key is **stolen** while transmitted data can easily decrypt.
  - In symmetric key cryptography, key is transmitted first and then message is transfer to the receiver. If attacker intercept the communication, he can easily decrypt the message.

Questions
1. What are the essential ingredients of a symmetric cipher?
2. List and explain components of symmetric cipher.

Asymmetric Key Cryptography

- Asymmetric key cryptography is also known as **public-key cryptography**, and it employs the use of two keys. This cryptography differs from and is more secure than symmetric key cryptography.
- In asymmetric key cryptography two keys are used, one for encryption and other for decryption.
- As mentioned asymmetric key cryptography involves use of **two keys** one is public key that many know to everyone and can be used to encrypt messages and verify signature.
- Other is private key known only to the receiver of the message, used to decrypt message, and create signature for verification.
- It is also called asymmetric key cryptography because one key is used for encryption and its corresponding key is used for decryption. No other key can decrypt the message.
- Mathematically, it is represented **C = E(Pu(A), P)** and **P = D(Pr(A), C)**. Where, Pu(A) = Alice public key and Pr(A) = Alice private key.



Asymmetric Key Cryptography

- Advantages:
  - If data is transmitting on insecure channel, but key cannot distributing among sender and receiver.
  - Separate key is used for encryption and decryption, even if encrypted message is stolen by attacker he/she cannot decrypt the message.
  - Easy to use for user.
- Disadvantages:
  - Asymmetric key use more resource in compare to symmetric key cryptography.
  - More mathematical calculation required.
  - Slower in compare to symmetric key cryptography.

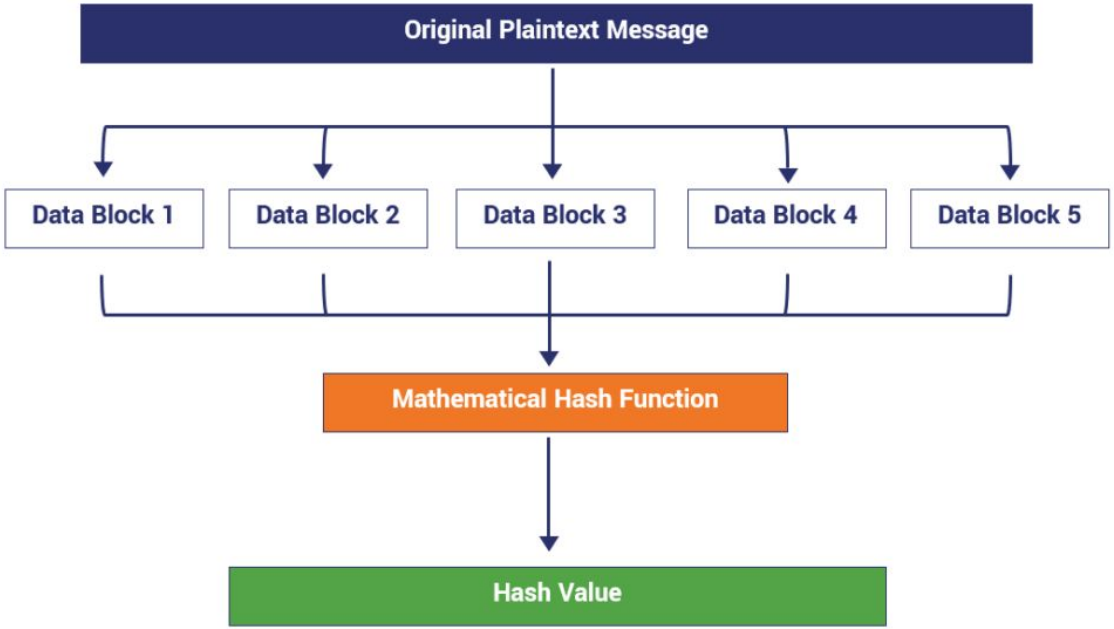
Questions
1. Explain asymmetric key cryptography.
2. Write short note on asymmetric cipher model.

Difference between Symmetric and Asymmetric key Cryptography

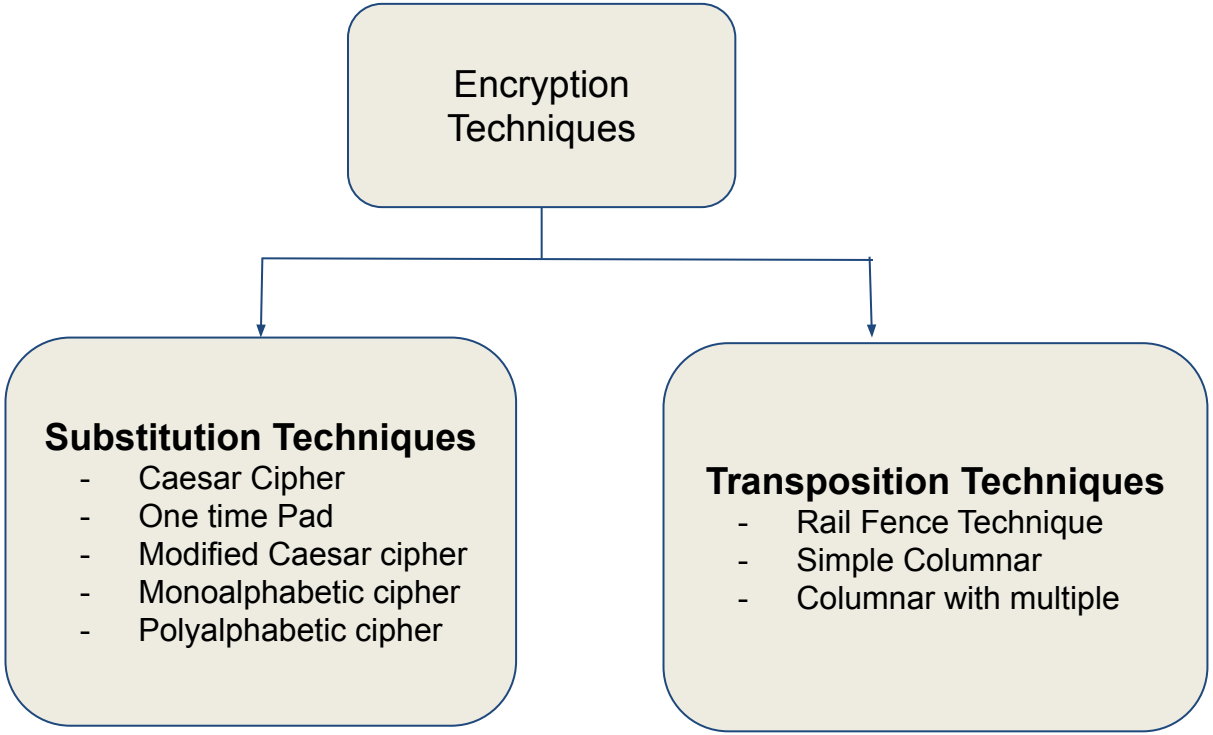
No	Symmetric Key Cryptography	Asymmetric Key Cryptography
1	Single key is used for encryption and decryption.	Two different key is used, one for encryption and other for decryption.
2	It is also called secret key or private key cryptography.	It is also called public key cryptography or conventional cryptographic system.
3	It is faster than asymmetric key cryptography.	It is slower than symmetric key cryptography.
4	It uses less resource in compare to asymmetric key cryptography.	It uses more resource in compare to symmetric key cryptography.
5	For encryption of large message symmetric key cryptography is used.	In asymmetric key cryptography plain text and cipher text treated as integer number.
6	For example: DES, AES and BLOWFISH	For example, RSA and Diffie-Hellman Key exchange.
7	Mathematically it is represented as $C = E(K, P)$ and $P = D(K, C)$ i.e., C = Cipher text, E = Encryption, D = Decryption, P = Plain text, K =Secret Key	Mathematically it is represented as $C = E(Pu(R), P)$ and $P = D(Pr(R), C)$ i.e., C = Cipher text, E = Encryption, D = Decryption, P = Plain text, Pr(R) =Private Key of receiver, Pu(R) = Public key of receiver.

Hash Functions

- There is no usage of any key in this algorithm.
- A hash value with a fixed length is calculated as per the plain text which makes it impossible for the contents of plain text to be recovered.
- Many operating systems use hash functions to encrypt passwords.

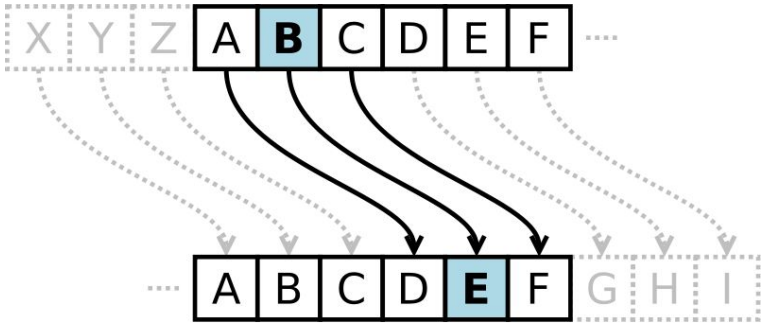


Encryption Techniques



Caesar cipher

- This technique was found by Julius Caesar. This technique is very simple and easy to generate cipher of given plain text.
- In Caesar cipher techniques each letter is replaced by the letter/alphabet which is three place next to the letter which is to be substituted.
- Caesar ciphers use a substitution method where letters in the alphabet are shifted by some fixed number of spaces to yield an encoding alphabet.
- A Caesar cipher with a shift of 3.
- 3 would encode an A as a D, an M as an P, and a Z as an C, and so on.
- For example, The algorithm can be expressed also as follow:
  - C=E(k,p)
- In general,
  - C=E(k,p)=(p+k) mod 26
  - P=D(k,c)=(c-k)mod 26



Caesar cipher

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
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

Fig. 2.5 A scheme for codifying messages by replacing each alphabet with an alphabet three places down the line

G	L	S		U	N	I	V	E	R	S	I	T	Y
J	O	V		X	Q	L	Y	H	U	V	L	W	B

Caesar cipher

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

- **Example 1:**

Plain text:- meet me after toga party
Key:-3
Cipher text:- phhw ph diwhnu wrjd sduwb

- **Example 2:**

Plain text:- india is my country
Key:- 5
Cipher text:- nsinf nx rd htzsywd

ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[END OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

One Time Pad Cipher

- One time pad also called as **Vernam cipher** that improves the security over substitution and transposition techniques.
- The one time pad technique uses a random key of the same length of the message (as long as the message), so that the key is not repeated.
- The case happens here is sender is generating new key for every new message while sending the message to the receiver called as one-time pad.
- The key is used to encrypt and decrypt a single message.
- Each new message requires a new key of the same length as the new message.
- This method is unbreakable. It produces random output with no relationship to the plain text.

One Time Pad Cipher

- The algorithm are as follows:

1. Each plain text alphabets as a number in increasing sequence.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

2. Do the same for each character of the input plain text.
3. Add each number corresponding to the plain text alphabet to the corresponding input one-time pad alphabet number.
4. If the sum produced greater than 26, subtract from it.
5. Translate each number of the sum back to corresponding alphabet. It gives the output cipher text.

One Time Pad Cipher

- The best example of one time pad is recharge voucher of any mobile company.
- All recharge voucher having different key or code printed on it. Once that code entered into mobile, customer will get talk time according to the voucher cost.
- If any customer trying to use same code of voucher he/she will get failure message.
- The company is regenerating all keys or code in such a way that every recharge voucher having new and unique code on it called one-time pad.
- Disadvantages:
  - Large random key cannot be generated.
  - Key distribution and generation of keys can be problematic.

1. Explain one time Pad in detail. What are the practical issues of this algorithm?
2. Explain one time pad cipher with example.

One Time Pad Cipher

Example 1:

PLAIN -TEXT: HOW ARE YOU

ONE TIME PAD: NCBTZQARX

P.T.:	H	O	W	A	R	E	Y	O	U
	7	14	22	0	17	4	24	14	20
O.T.P.:	N	C	B	T	Z	Q	A	R	X
	13	2	1	19	25	16	0	17	23
SUM:	20	16	23	19	42	20	24	31	43
SUB-26 (IF>26):	20	16	23	19	16	20	24	5	17
C.T.:	U	Q	X	T	Q	U	Y	F	R

CIPHER -TEXT: UQX TQU YFR

Example 2:

PLAIN -TEXT: COMPUTER

ONE TIME PAD: SECURITY

P.T.:	C	O	M	P	U	T	E	R
	2	14	12	15	20	19	4	17
O.T.P.:	S	E	C	U	R	I	T	Y
	18	4	2	20	17	8	19	17
SUM:	20	18	14	35	37	27	23	34
SUB-26 (IF>26):	20	18	14	9	11	1	23	8
C.T.:	U	S	O	J	L	B	X	I

CIPHER -TEXT: USOJLBXI

THANK YOU