Scan or click here for more resources

UNIT-4 (EC)

Need of Security: Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings. Once the data is out of hand, people with bad intention could modify or forge your data, either for amusement or for their own benefit.

Cryptography can reformat and transform our data, making it safer on its trip between computers. The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.

- **Computer Security** - generic name for the collection of tools designed to protect data
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

Security Attacks, Services and Mechanisms

To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements. One approach is to consider three aspects of information security:

Security attack – Any action that compromises the security of information owned by an organization.

Security mechanism – A mechanism that is designed to detect, prevent or recover from a security attack.

Security service – A service that enhances the security of the data processing systems and the information transfers of an **organization**. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

What is Cryptography?

Cryptography is the science of using mathematics to encrypt and decrypt data.

Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

"The Art of Hiding of Information"

"The practice and study of techniques for secure communication in the presence of third parties"

Cryptography is the science of securing data.

Cryptanalysis is the science of analyzing and breaking secure communication.

Cryptanalysts are also called attackers.

How does cryptography work?

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process.

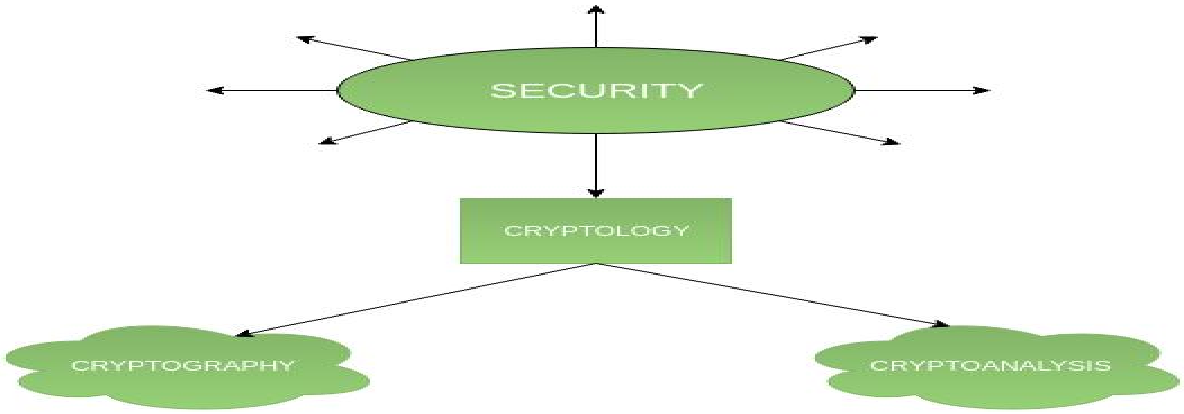
A cryptographic algorithm works in combination with a key—a word, number, or phrase—to encrypt the plaintext. The same plaintext encrypts to different ciphertext with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.

Cryptography is an important aspect when we deal with network security. 'Crypto' means secret or hidden. Cryptography is the science of secret writing with the intention of keeping the data secret.

Cryptanalysis, on the other hand, is the science or sometimes the art of breaking cryptosystems. These both terms are a subset of what is called as Cryptology.

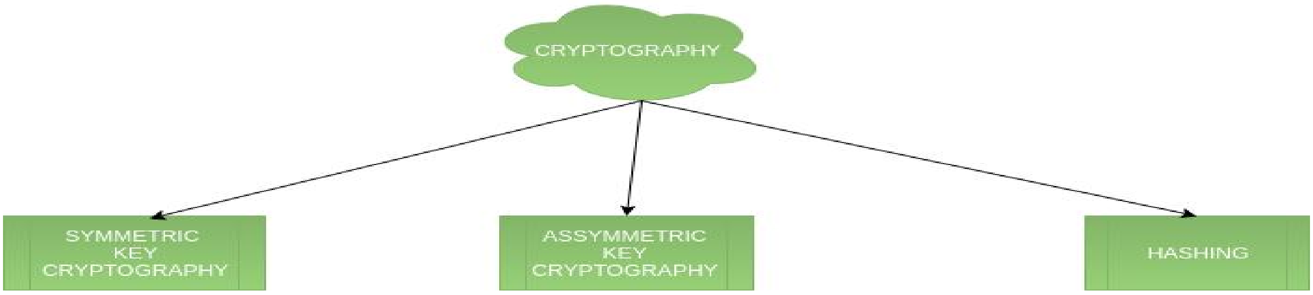
Classification –

The flowchart depicts that cryptology is only one of the factors involved in securing networks. Cryptology refers to study of codes, which involves both writing (cryptography) and solving (cryptanalysis) them. Below is a classification of the crypto-terminologies and their various types.



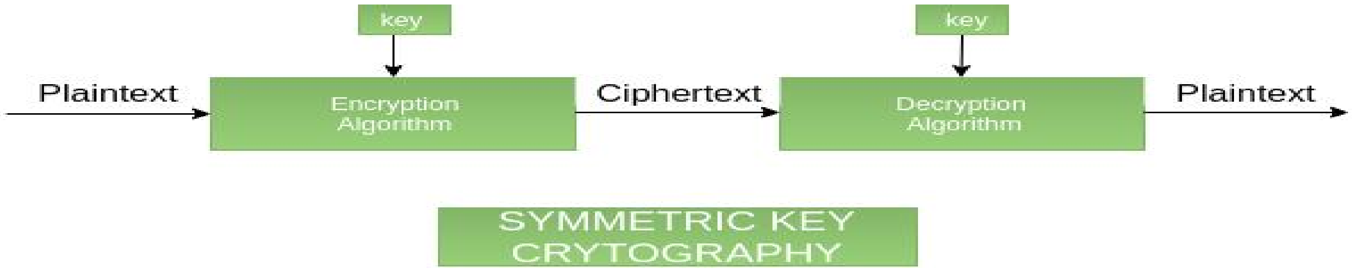
1. Cryptography –

Cryptography is classified into symmetric cryptography, asymmetric cryptography and hashing. Below are the description of these types.



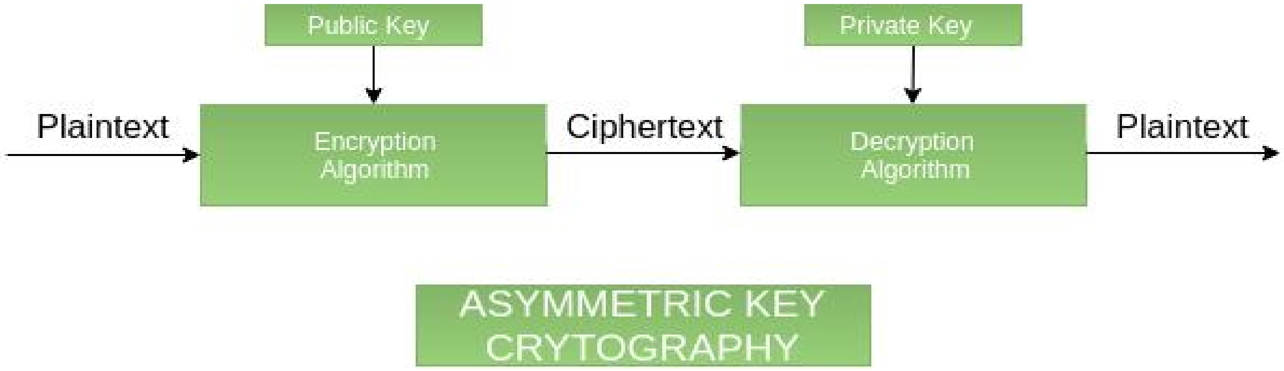
1. ***Symmetric key cryptography –***

   It involves usage of one secret key along with encryption and decryption algorithms which help in securing the contents of the message. The strength of symmetric key cryptography depends upon the number of key bits. It is relatively faster than asymmetric key cryptography. There arises a key distribution problem as the key has to be transferred from the sender to receiver through a secure channel.



2 Asymmetric key cryptography –

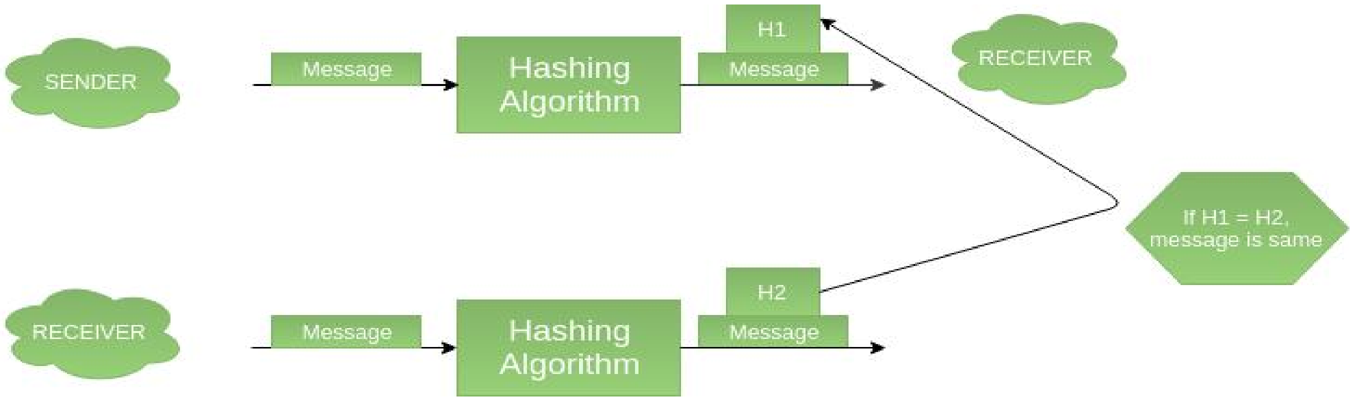
It is also known as public key cryptography because it involves usage of a public key along with secret key. It solves the problem of key distribution as both parties uses different keys for encryption/decryption. It is not feasible to use for decrypting bulk messages as it is very slow compared to symmetric key cryptography.



2.

3. ***Hashing –***

It involves taking the plain-text and converting it to a hash value of fixed size by a hash function. This process ensures integrity of the message as the hash value on both, sender\'s and receiver\'s side should match if the message is unaltered.

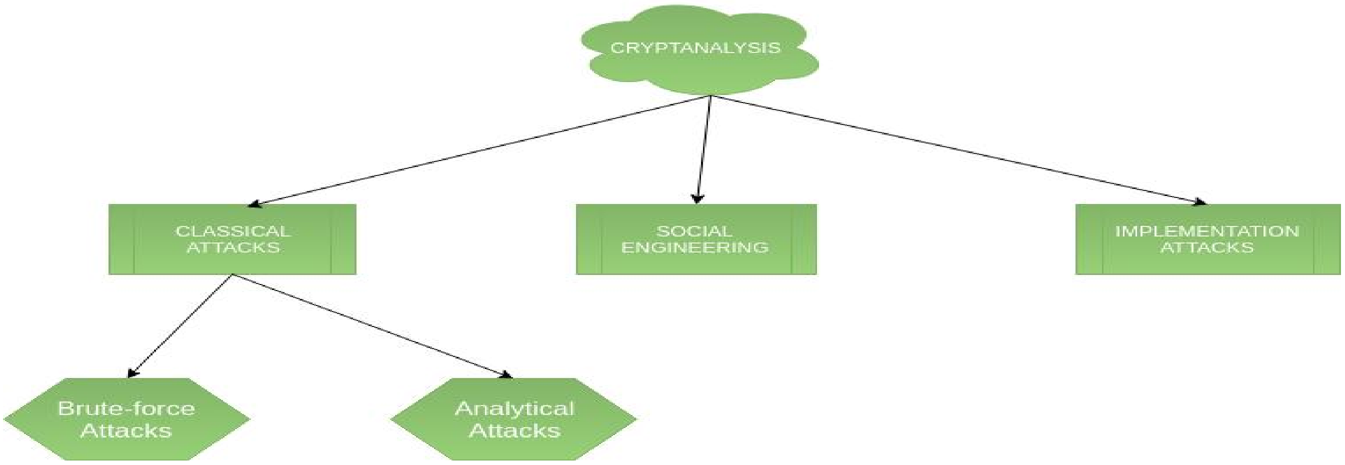


4.

2. Cryptanalysis –

1. ***Classical attacks –***

It can be divided into a)Mathematical analysis and b) Brute-force attacks. Brute-force attacks runs the encryption algorithm for all possible cases of the keys until a match is found. Encryption algorithm is treated as a black box. Analytical attacks are those attacks which focuses on breaking the cryptosystem by analysing the internal structure of the encryption algorithm.



2. *Social Engineering attack –*

   It is something which is dependent on the human factor. Tricking someone to reveal their passwords to the attacker or allowing access to the restricted area comes under this attack. People should be cautious when revealing their passwords to any third party which is not trusted.

3. *Implementation attacks –*

   Implementation attacks such as side-channel analysis can be used to obtain a secret key. They are relevant in cases where the attacker can obtain physical access to the cryptosystem.

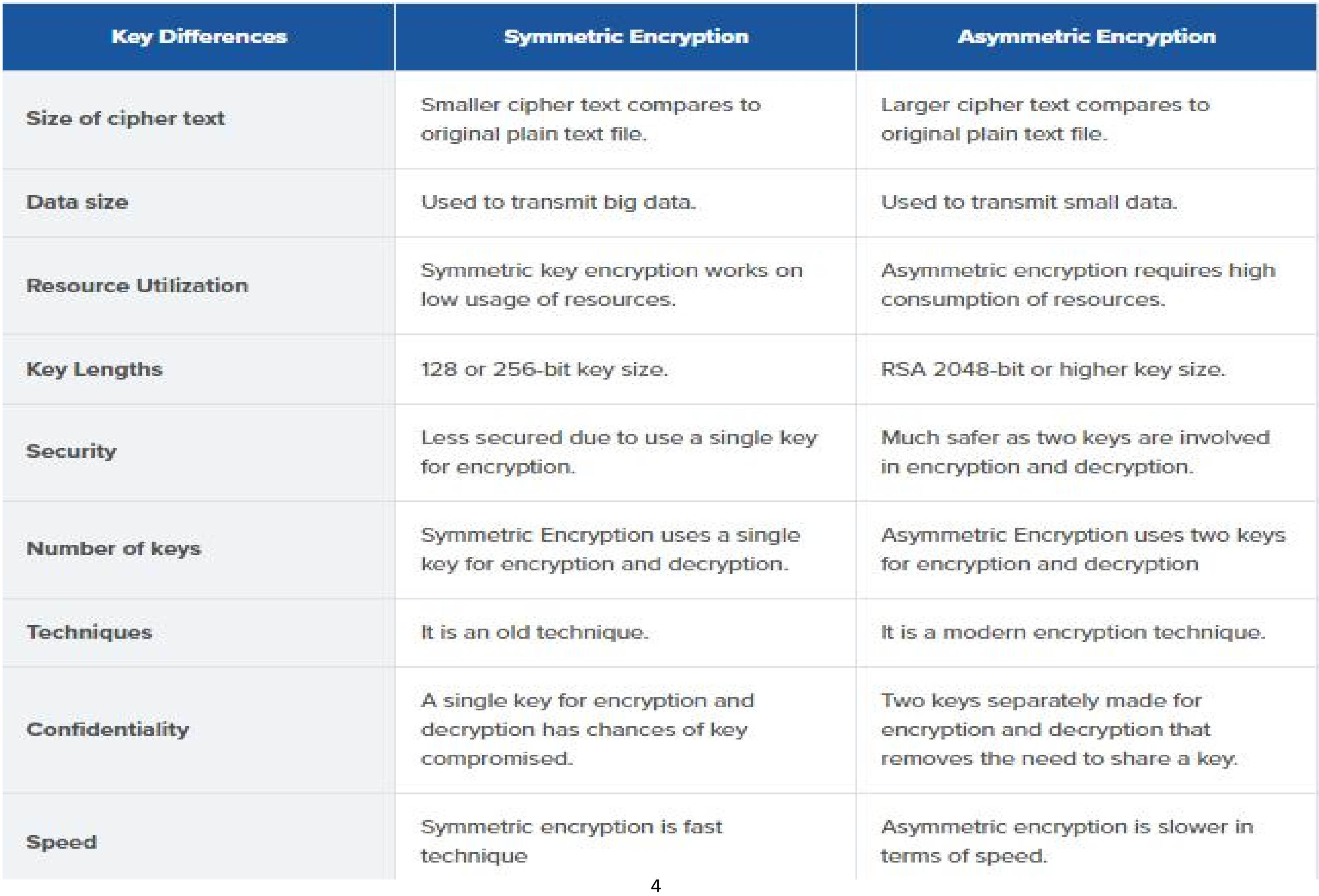
RSA Algorithm in Cryptography: *RSA algorithm is asymmetric cryptography algorithm.*

Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private.

What is Encryption

Data encryption translates data into another form, or code. so that only people with access to a secret key (formally called a decryption key) or password can read it.
Encrypted data is commonly referred to as ciphertext, while unencrypted data is called plaintext.
Encryption is one of the most popular and effective data security methods used by organizations.
Two main types of data encryption exist –
Asymmetric Encryption, also known as public-key encryption,
Symmetric encryption.

- **Symmetric**: the same key is used for both encryption and decryption
- **Asymmetric**: different keys for encryption and decryption, e.g. public-key encryption such as RSA.



Key Differences	Symmetric Encryption	Asymmetric Encryption
Size of cipher text	Smaller cipher text compares to original plain text file.	Larger cipher text compares to original plain text file.
Data size	Used to transmit big data.	Used to transmit small data.
Resource Utilization	Symmetric key encryption works on low usage of resources.	Asymmetric encryption requires high consumption of resources.
Key Lengths	128 or 256-bit key size.	RSA 2048-bit or higher key size.
Security	Less secured due to use a single key for encryption.	Much safer as two keys are involved in encryption and decryption.
Number of keys	Symmetric Encryption uses a single key for encryption and decryption.	Asymmetric Encryption uses two keys for encryption and decryption
Techniques	It is an old technique.	It is a modern encryption technique.
Confidentiality	A single key for encryption and decryption has chances of key compromised.	Two keys separately made for encryption and decryption that removes the need to share a key.
Speed	Symmetric encryption is fast technique	Asymmetric encryption is slower in terms of speed.

Encryption:-

The process of converting plain text to ciphertext.

Decryption:-

The process of converting cipher text to plaintext

Text Encryption:-

Encryption is a process whereby plaintext is converted into or ciphertext.

Decryption is the reverse process of encryption or encipherment, which is to convert ciphertext back to its original form of plaintext.

Symmetric key Encryption

- Encryption and decryption keys are same
- Conventional / private-key / single-key
- Sender and recipient share a common key
- All classical encryption algorithms are private key
- First prior to invention of public-key in 1970's
- Most widely used

Asymmetric cryptography

- Asymmetric cryptography, also known as public-key cryptography
- A process that uses a pair of related keys -- one public key and one private key -- to encrypt and decrypt a message and protect it from unauthorized access or use.
- A public key is a cryptographic key that can be used by any person to encrypt a message so that it can only be deciphered by the intended recipient with their private key. A private key -- also known as a secret key -- is shared only with key's

Some Basic Terminology

- **plaintext -** original message
- **ciphertext -** coded message
- **cipher - a**lgorithm for transforming plaintext to cip**hertext**
- **key -** info used in cipher known only **to sender/receiver**
- **encipher (encrypt) - c**onverting plaintext to ci**phertext**
- **decipher (decrypt) - r**ecovering ciphertext from **plaintext**
- **cryptography -** study of encryption pri**nciples/methods**
- **cryptanalysis (codebreaking) -** study of principles/ **methods of deciphering ciphertext without knowing key**
- **cryptology -** field of both cryptography an**d cryptanalysis**

# Substitution Cipher Techniques

It is a technics in which each latter or bit of the plaintext is substituted or replaced by some other latter, number or symbol to produce cipher text.

Types:

1. Caesar cipher
2. Mono alphabetic cipher
3. Polyalphabetic cipher
4. Play fair cipher
5. One time pad
6. Hill cipher

Hiding some data is known as encryption. When plain text is encrypted it becomes unreadable and is known as ciphertext. In a Substitution cipher, any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending on a key. For example with a shift of 1, A would be replaced by B, B would become C, and so on.

Note: Special case of Substitution cipher is known as Caesar cipher where the key is taken as 3.

Mathematical representation

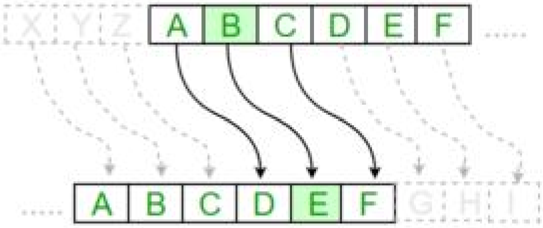
The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25. Encryption of a letter by a shift n can be described mathematically as.

$$E_n(x) = (x + n) mod\ 26$$

(Encryption Phase with shift n)

$$D_n(x) = (x - n) mod\ 26$$

(Decryption Phase with shift n)



Examples:

Plain Text: I am studying Data Encryption

Key: 4

Output: M eq wxyhCmrk Hexe IrgvCtxmsr

Plain Text: ABCDEFGHIJKLMNOPQRSTUVWXYZ **,Key:** 4 **,Output:** EFGHIJKLMNOPQRSTUVWXYZabcd

Algorithm for Substitution Cipher:

Input:

- A String of both lower and upper case letters, called PlainText.
- An Integer denoting the required key.

Procedure:

- Create a list of all the characters.
- Create a dictionary to store the substitution for all characters.
- For each character, transform the given character as per the rule, depending on whether we're encrypting or decrypting the text.
- Print the new string generated.

1. Monoalphabetic Cipher :
A monoalphabetic cipher is any cipher in which the letters of the plain text are mapped to cipher text letters based on a single alphabetic key. Examples of monoalphabetic ciphers would include the Caesar-shift cipher, where each letter is shifted based on a numeric key, and the atbash cipher, where each letter is mapped to the letter symmetric to it about the center of the alphabet.

2. Polyalphabetic Cipher :
A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The Vigenère cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.

Difference Between Monoalphabetic Cipher and Polyalphabetic Cipher :

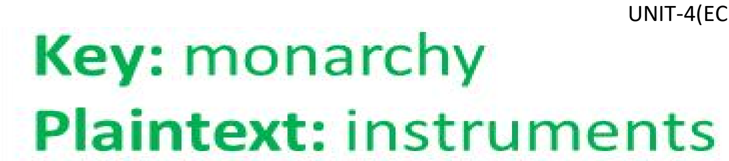
SR.NO	Monoalphabetic Cipher	Polyalphabetic Cipher
1	Monoalphabetic cipher is one where each symbol in plain text is mapped to a fixed symbol in cipher text.	Polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.
2	The relationship between a character in the plain text and the characters in the cipher text is one-to-one.	The relationship between a character in the plain text and the characters in the cipher text is one-to-many.
3	Each alphabetic character of plain text is mapped onto a unique alphabetic character of a cipher text.	Each alphabetic character of plain text can be mapped onto 'm' alphabetic characters of a cipher text.
4	A stream cipher is a monoalphabetic cipher if the value of key does not depend on the position of the plain text character in the plain text stream.	A stream cipher is a polyalphabetic cipher if the value of key does depend on the position of the plain text character in the plain text stream.
5	It includes additive, multiplicative, affine and monoalphabetic substitution cipher.	It includes autokey, Playfair, Vigenere, Hill, one-time pad, rotor, and Enigma cipher.
6	It is a simple substitution cipher.	It is multiple substitutions cipher.
7	Monoalphabetic Cipher is described as a substitution cipher in which the same fixed mappings from plain text to cipher letters across the entire text are used.	Polyalphabetic Cipher is described as substitution cipher in which plain text letters in different positions are enciphered using different cryptoalphabets.
8	Monoalphabetic ciphers are not that strong as compared to polyalphabetic cipher.	Polyalphabetic ciphers are much stronger.

Playfair Cipher with Examples

The **Playfair cipher** was the first practical digraph substitution cipher.

<u>Encryption Technique</u>

For the encryption process let us consider the following example:



Key: monarchy

Plaintext: instruments

The Playfair Cipher Encryption Algorithm:

The Algorithm consists of 2 steps:

1. ***Generate the key Square(5×5):***

- *The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.*
  The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

2. ***Algorithm to encrypt the plain text:*** *The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.*
   For example:

PlainText: "instruments" **After Split:** 'in' 'st' 'ru' 'me' 'nt' 'sz'

1. *Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter.*

Plain Text: *"hello"*

After Split: *'he' 'lx' 'lo'*

*Here **'x'** is the bogus letter.*

2. *If the letter is standing alone in the process of pairing, then add an extra bogus letter with the alone letter*

Plain Text: *"helloe"*

AfterSplit: *'he' 'lx' 'lo' 'ez'*

*Here **'z'** is the bogus letter.*

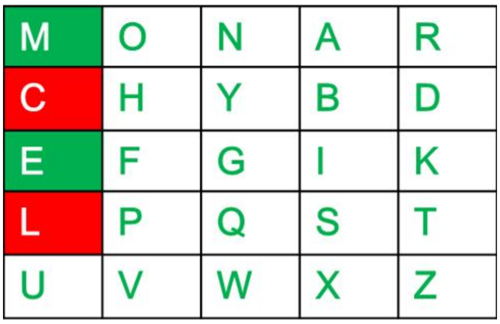
Rules for Encryption:

- ***If both the letters are in the same column:*** *Take the letter below each one (going back to the top if at the bottom).*
  For example:

Diagraph: "me"**Encrypted Text:** cl**Encryption:**

```
m -> c
e -> l
```

-



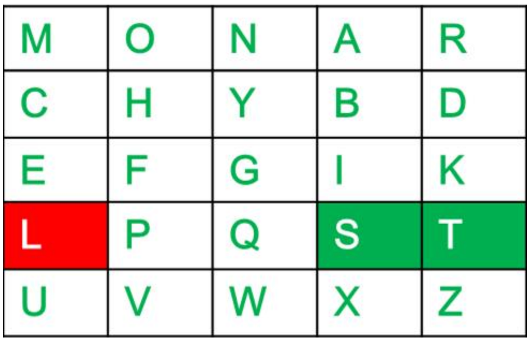
M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

- ***If both the letters are in the same row***: *Take the letter to the right of each one (going back to the leftmost if at the rightmost position).*

  For example:

Diagraph: "st"**Encrypted Text:** tl**Encryption:**

```
s -> t
t -> l
```



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

- ***If neither of the above rules is true***: *Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.*

  For example:

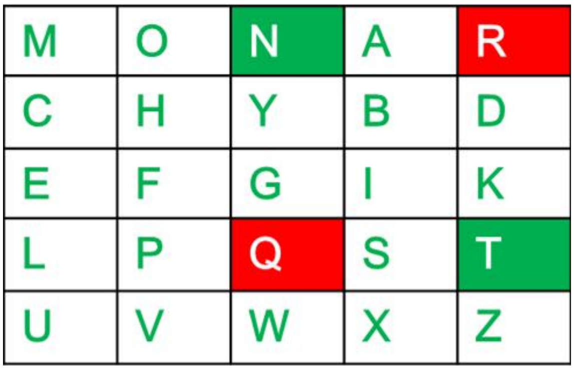
Diagraph: "nt"**Encrypted Text:** rq**Encryption:**

```
n -> r
t -> q
```

For example:

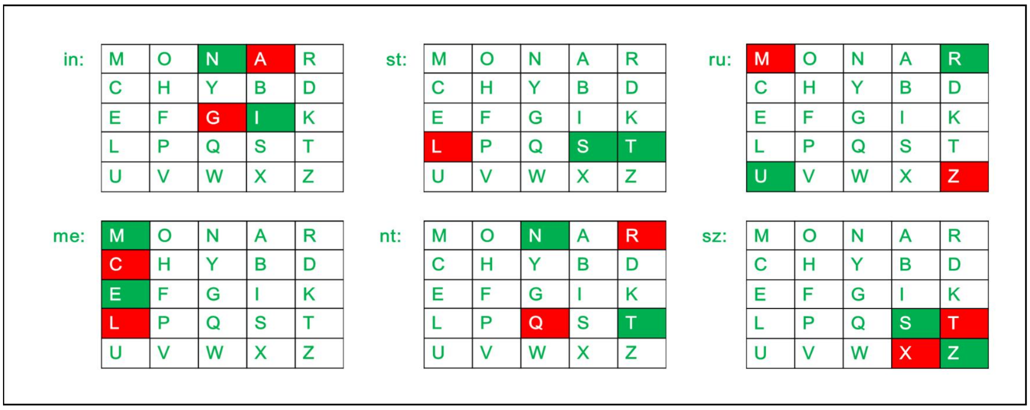
Plain Text: "instrumentsz"**Encrypted Text:** gatlmzclrqtx**Encryption:**

```
i -> g
n -> a
s -> t
t -> l
r -> m
u -> z
m -> c
```



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

```
e -> l
n -> r
t -> q
s -> t
z -> x
```



in:

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

st:

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

ru:

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

me:

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

nt:

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

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

Decryption Technique

Decrypting the Playfair cipher is as simple as doing the same process in reverse. The receiver has the same key and can create the same key table, and then decrypt any messages made using that key.

Key: monarchy

ciphertext: gatlmzclrqtx

The Playfair Cipher Decryption Algorithm:

The Algorithm consistes of 2 steps:

1. **Generate the key Square(5×5) at the receiver's end:**

- The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.
  The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

2. **Algorithm to decrypt the ciphertext**: The ciphertext is split into pairs of two letters (digraphs).

*Note: The **ciphertext** always have **even** number of characters.*

1. **For example:**

```
CipherText: "gatlmzclrqtx" After Split: 'ga' 'tl' 'mz' 'cl' 'rq' 'tx'
```

1. **Rules for Decryption:**

- **If both the letters are in the same column**: Take the letter above each one (going back to the bottom if at the top).
  For example:

```
Diagraph: "cl" Decrypted Text: meDecryption:
  c -> m
```

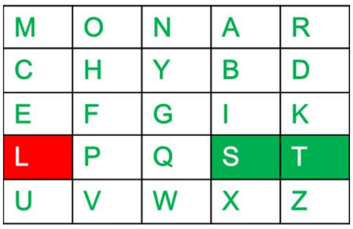
M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

```
l -> e
```

-
- ***If both the letters are in the same row***: *Take the letter to the left of each one (going back to the rightmost if at the leftmost position).*

  For example:

```
Diagraph: "tl" Decrypted Text: st Decryption:
  t -> s
  l -> t
```



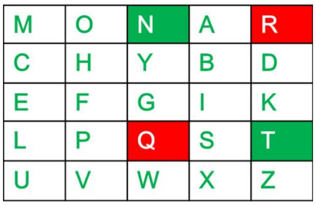
M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

If neither of the above rules is true: *Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.*

For example:

```
Diagraph: "rq" Decrypted Text: nt Decryption:
  r -> n
  q -> t
```

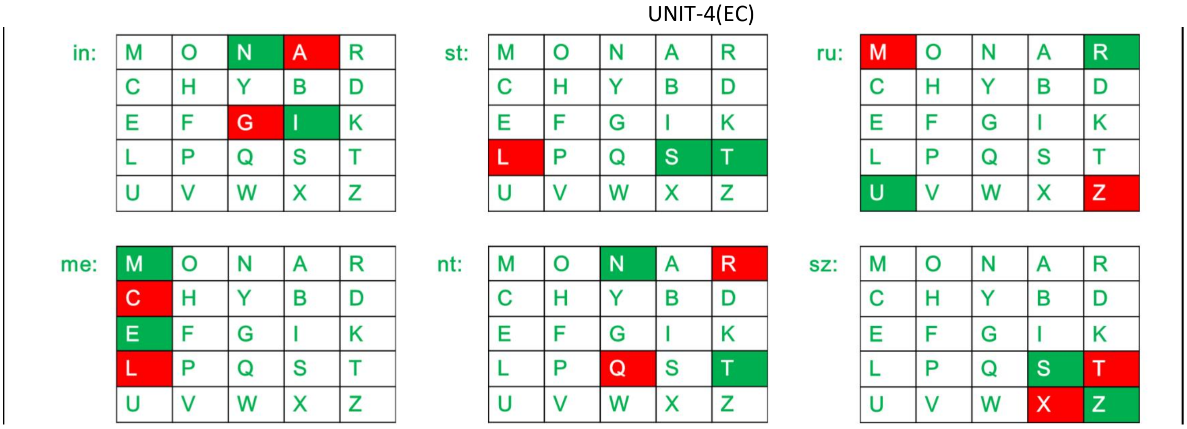
-



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

For example:

```
Plain Text: "gatlmzclrqtx"Decrypted Text: instrumentszDecryption:
(red)-> (green)
  ga -> in
  tl -> st
  mz -> ru
  cl -> me
  rq -> nt
  tx -> sz
```



in:

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

st:

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

ru:

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

me:

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

nt:

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

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

Vigenère Cipher/One time pad

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the Vigenère square or Vigenère table.

- The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.
- At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
- The alphabet used at each point depends on a repeating keyword.

Example:

```
Input : Plaintext :   GEEKSFORGEEKS
            Keyword :  AYUSH
Output : Ciphertext :  GCYCZFMLYLEIM
For generating key, the given keyword is repeated
in a circular manner until it matches the length of
the plain text.
The keyword "AYUSH" generates the key "AYUSHAYUSHAYU"
The plain text is then encrypted using the process
explained below.
```

Encryption

The first letter of the plaintext, G is paired with A, the first letter of the key. So use row G and column A of the Vigenère square, namely G. Similarly, for the second letter of the plaintext, the second letter of the key is used, the letter at row E, and column Y is C. The rest of the plaintext is enciphered in a similar fashion.

Decryption

Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column's label as the plaintext. For example, in row A (from AYUSH), the ciphertext G appears in column G, which is the first plaintext

letter. Next, we go to row Y (from AYUSH), locate the ciphertext C which is found in column E, thus E is the second plaintext letter.
A more **easy implementation** could be to visualize Vigenère algebraically by converting [A-Z] into numbers [0–25].

Encryption

The plaintext(P) and key(K) are added modulo 26.

$E_i = (P_i + K_i) \bmod 26$

Decryption

$D_i = (E_i - K_i + 26) \bmod 26$

Note: D_i denotes the offset of the i-th character of the plaintext. Like offset of **A** is 0 and of **B** is 1 and so on.

Hill Cipher

Hill cipher is a polygraphic substitution cipher based on linear algebra.Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, …, Z = 25 is used, but this is not an essential feature of the cipher. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.
The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26).

Examples:

```
Input  : Plaintext: ACT
         Key: GYBNQKURP
Output : Ciphertext: POH

Input  : Plaintext: GFG
         Key: HILLMAGIC
Output : Ciphertext: SWK
```

Encryption

We have to encrypt the message 'ACT' (n=3).The key is 'GYBNQKURP' which can be written as the nxn matrix:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

The message 'ACT' is written as vector:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

The enciphered vector is given as:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

which corresponds to ciphertext of 'POH'

Decryption

To decrypt the message, we turn the ciphertext back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters).The inverse of the matrix used in the previous example is:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \pmod{26}$$

For the previous Ciphertext 'POH':

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \pmod{26}$$

which gives us back 'ACT'.
Assume that all the alphabets are in upper case.

DIGITAL SIGNATURE

MAC(Message Authentication Code) was used to provide Message Integrity and Message Authentication but it needs symmetric key established between sender and receiver. A digital signature on other hand uses pair of asymmetric keys.

A valid digital signature helps the receiver to know the message comes from the authentic sender and is not altered in between.

What is a Signature?

We sign a document to show that is approved by us or created by us. The signature is proof to the recipient that this document is coming from the correct source. The signature on the document simply means the document is authentic.

When A sends a message to B, B needs to check the authenticity of the message and confirm it comes from A and not C. So B can ask A to sign the message electronically. The electronic signature proves the identity of A is also called a digital signature.

A digital signature is a mathematically generated code that validates the authenticity of a software, message, or digital file. It uses encryption techniques that are secure enough to be considered legal and binding in some countries. It guarantees that the file has not been altered during transmission, providing a layer of security against cyber threats and attacks .

Class 1: These digital signatures are "basic," and so are only acceptable in instances with low levels of risk for data compromise. They are not acceptable when signing legal documents since their validation only requires a check for an email address and a username.

Class 2: These digital signatures apply to instances where there is a moderate risk for data compromise. Some of their applications include electronic filing of income tax returns, company registrations, and goods and services tax (GST) documents.

Class 3: These digital signatures are of the highest level. They require the user, whether an individual or a company, to prove their identity before a certifying authority before they can use them for signing. These can help when downloading contracts, participating in electronic auctions, electronic tendering, submitting bidding documents, or any circumstance where there is a high risk for data compromise.

Who Uses Digital Signatures?

1. Government Institutions

Different government institutions use digital signatures to process tax returns, verify transactions, ratify laws, and manage contracts.

2. Financial Service Providers

Another industry that highly benefits from using digital signatures is the financial services sector. Digital signatures allow them to increase the security of transactions, enable faster turnaround times for loan processing**, automate processes to eliminate paperwork and reduce risks of fraud.**

3.Healthcare Providers

The use of digital signatures in healthcare helped the industry to streamline not only administrative processes but also diagnostic efficiency. However, the use of digital signatures in healthcare must still comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Virtual Private Network

VPN stands for the virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. A Virtual

Private Network is a way to extend a private network using a public network such as the internet. The name only suggests that it is a Virtual "private network" i.e. user can be part of a local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection.

Virtual. Virtual means not real or in a different state of being. In a VPN, private communication between two or more devices is achieved through a public network the Internet. Therefore, the communication is virtually but not physically there.

Private. Private means to keep something a secret from the general public. Although those two devices are communicating with each other in a public environment, there is no third party who can interrupt this communication or receive any data that is exchanged between them.

Network. A network consists of two or more devices that can freely and electronically communicate with each other via cables and wire. A VPN is a network. It can transmit information over long distances effectively.

Lets understand VPN by an example:

Think of a situation where corporate office of a bank is situated in Washington, USA. This office has a local network consisting of say 100 computers. Suppose other branches of the bank are in Mumbai, India, and Tokyo, Japan. The traditional method of establishing a secure connection between head office and branch was to have a leased line between the branches and head office which was a very costly as well as troublesome job. VPN lets us overcome this issue in an effective manner.

Types of VPNs

Remote access VPN

Intranet VPN

Extranet VPN

Remote access VPNs – Enable remote connectivity using any Internet access technology. The remote user launches the VPN client to create a VPN tunnel to the gateway.

Intranet VPNs - If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect LAN to LAN.

Extranet VPNs – When a company has a close relationship with another company (for example, a partner, supplier or customer), they can build an extranet VPN that connects LAN to LAN, and that allows all of the various companies to work in a shared environment.

Types of VPN protocols

- PPTP--Point-to-Point Tunneling Protocol
- L2TP -- Layer 2 Tunneling Protocol
- IPsec-- Internet Protocol Security
- SSL -- Secure Socket Layer

1. **Point-to-Point Tunneling Protocol(PPTP):** PPTP (Point-to-Point Tunneling Protocol) it's the most widely supported VPN method among Windows users and it was created by Microsoft in association with other technology companies. The disadvantage of PPTP is that it does not provide encryption and it relies on the PPP (Point-to-Point Protocol) protocol to implement security measures. But compared to other methods, PPTP is faster and it is also available for Linux and Mac users.

2. **Layer 2 Tunneling Protocol(L2TP)L2TP (Layer 2 Tunneling Proto**col) it's another tunneling protocol that supports VPNs. Like PPTP, L2TP does not provide encryption and it relies on PPP protocol to do this. The difference between PPTP and L2TP is that the second one provides not only data confidentiality but also data integrity. L2TP was developed by Microsoft and Cisco as a combination between PPTP and L2F(Layer 2 Forwarding).

3. **.Internet Protocol Security(IPsec) IPsec** protocol can be used for encryption in correlation with L2TP tunneling protocol. It is used as a "protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream". IPSec requires expensive, time consuming client installations and this can be considered an important disadvantage.

4. **Secure Socket Layer(SSL)** SSL (Secure Socket Layer) is a VPN accessible via https over web browser. The advantage of this SSL VPN is that it doesn't need any software installed because it uses the web browser as the client application. Through SSL VPNs the user's access can be restrict to specific applications instead of allowing access to the whole network.

VPNs - Advantages

- Eliminate the need for expensive private or leased lines
- Reduce the long-distance telephone charges
- Reduced equipment costs (modem banks, CSU/DSUs)
- Reduced technical support
- Scalability – easy adding of new locations to the VPN
- Security
- Simple Management
- Lower Cost

VPNs - Disadvantages

1. Require an in-depth understanding of public network security issues and taking proper precautions in VPN deployment.
2. The availability and performance of a corporate VPN (over the Internet) depends on uncontrollable external factors.
3. Shortage of standardization. The products from different vendors may not work well together.
4. VPNs need to accommodate complicated protocols other than IP.