E-Business Issues In Cyberspace

Presented By:-

Rahul Kumar

Preeti Sachdeva

Security

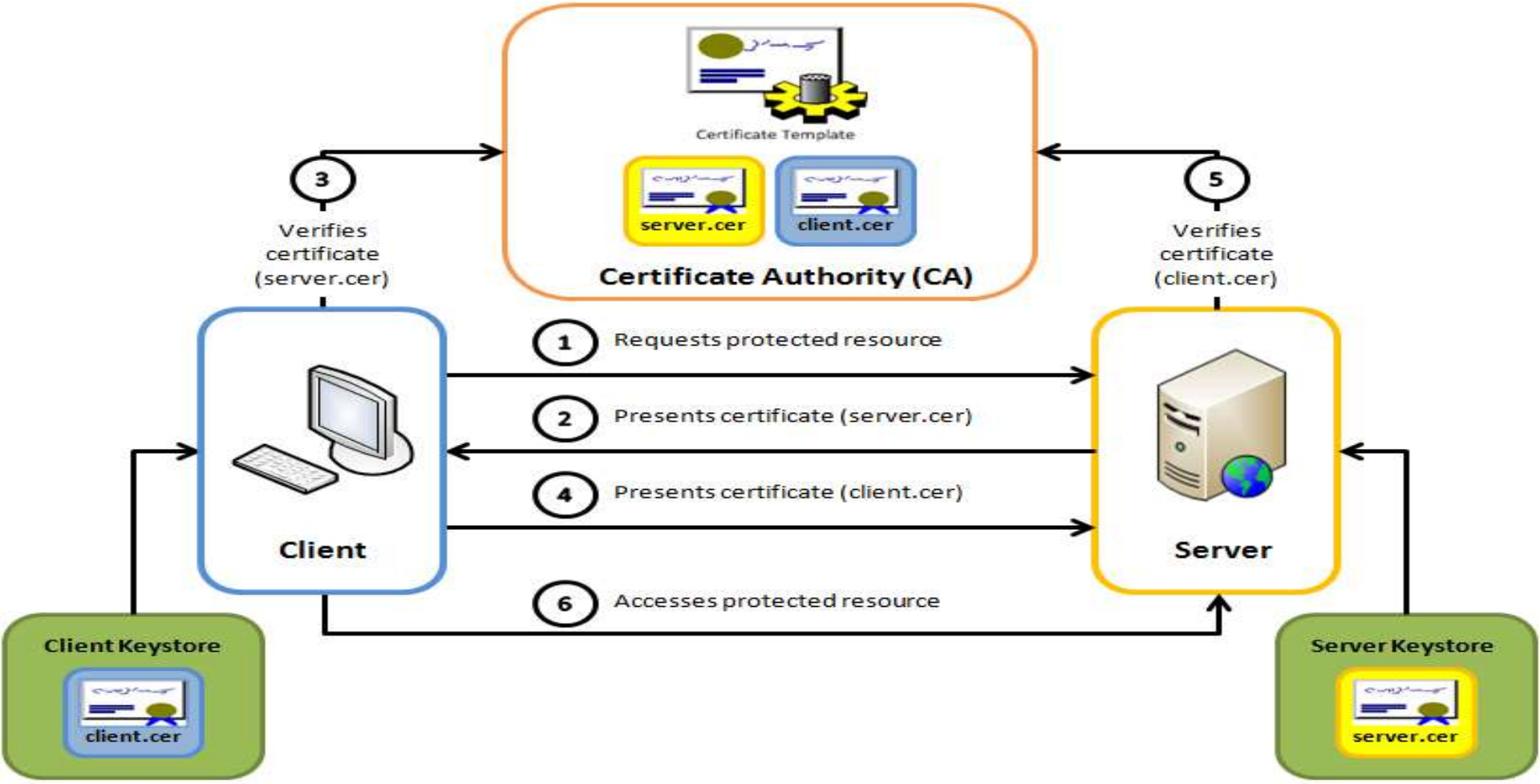
- To protect data from unauthorised access and virus (malicious code & trojan horse).

Basic Security Issues

- Authentication
- Authorisation
- Confidentiality
- Integrity
- Non repudiation

Authentication

- The process by which one entity can verifies that another entity is who.



Authorisation

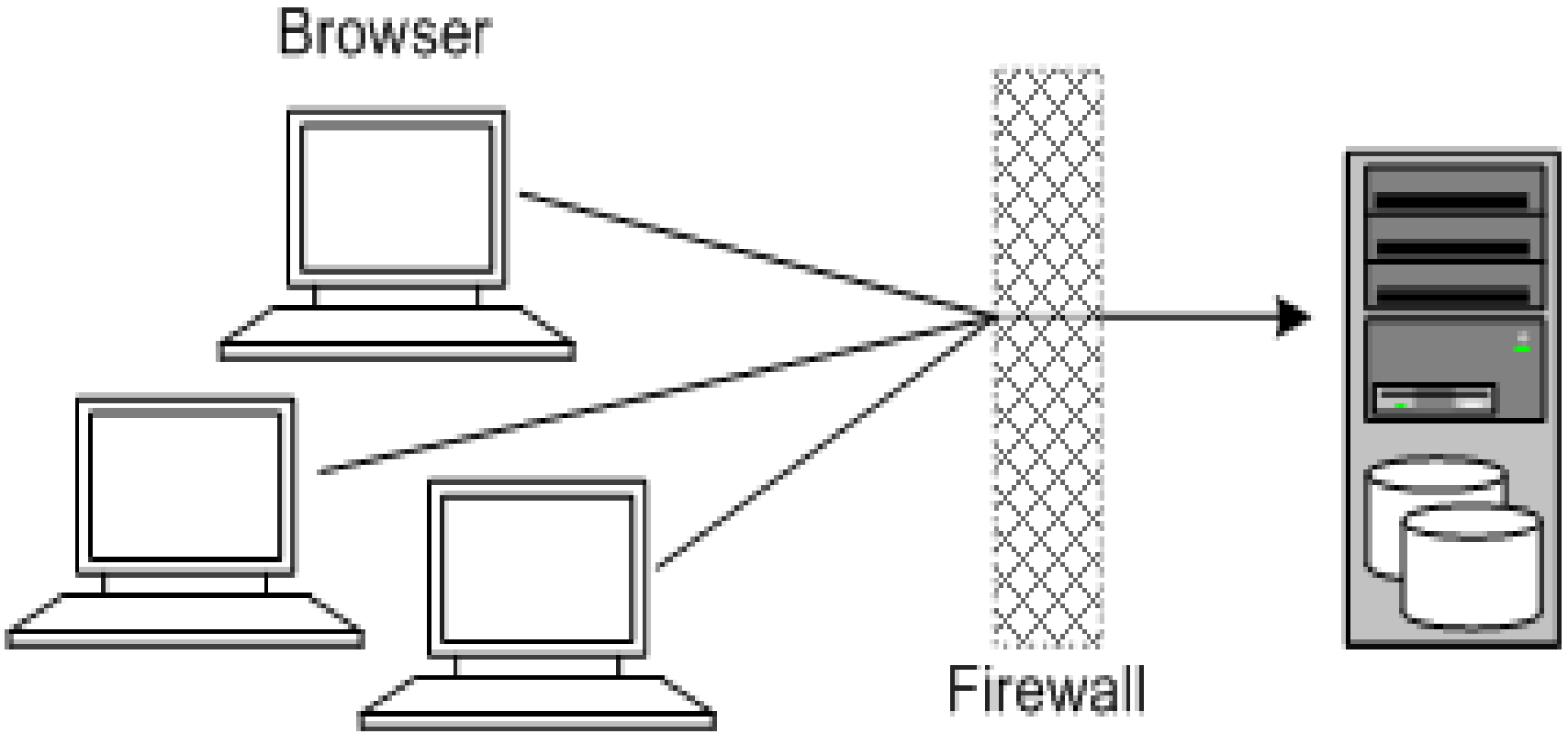
- The process that ensures that the person has the right to access certain resources.

Confidentiality

- Keeping private or sensitive information from being disclosed to unauthorised individuals, entities or processes.

Integrity

- The ability to protect data from being altered or destroyed by unauthorised access or accidental manner.



Non Repudiation

- The ability to limit parties from refusing that legitimate transaction took place, usually by means of a signature.

Types of Security Threats

- Denial of Service
- Unauthorized Access
- Theft and Fraud

Denial of Service

Two primary types of DOS attacks:

- Spamming
- Viruses

Spamming

- Sending unsolicited commercial emails to individuals
- E-mail bombing caused by a hacker targeting one computer or network, and sending thousands of email messages to it.
- Surfing involves hackers placing software agents onto a third-party system and setting it off to send requests to an intended target.
- DDOS (distributed denial of service attacks) involves hackers placing software agents onto a number of third-party systems and setting them off to simultaneously send requests to an intended target

Viruses

- Self-replicating computer programs designed to perform unwanted events.

Unauthorized Access

- Illegal access to systems, applications or data
- Passive unauthorized access –listening to communications channel for finding secrets. May use content for damaging purposes
- Active unauthorized access
  - Modifying system or data
  - Message stream modification
- Changes intent of messages, e.g., to abort or delay a negotiation on a contract
- Masquerading or spoofing –sending a message that appears to be from someone else.
- Impersonating another user at the ―name‖(changing the From field) or IP levels (changing the source and/or destination IP address of packets in the network)
- Sniffers–software that illegally access data traversing across the network.
- Software and operating systems‘ security holes

Theft and Fraud

- Fraud occurs when the stolen data is used or modified.
- Theft of software via illegal copying from company‘s servers.
- Theft of hardware, specifically laptops.

Types Security

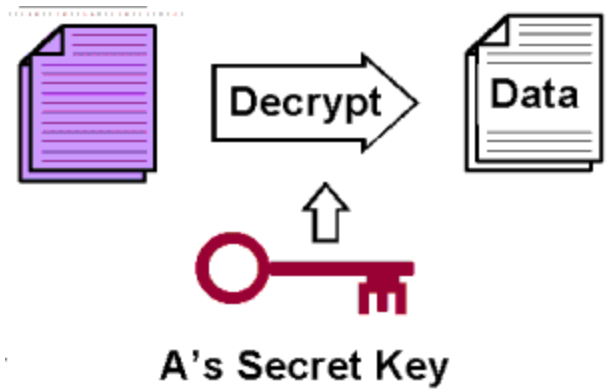
- Encryption
- Decryption
- Cryptography
- Virtual Private Network
- Gate
- Biometric Systems
- Digital Signature
- Digital Certificate
- Secure Socket Layer
- Transaction Layer Security

Encryption

- The process of scrambling a message in such a way that it is difficult, expecting or time consuming for an unauthorised person to unscramble (decrypt) it.

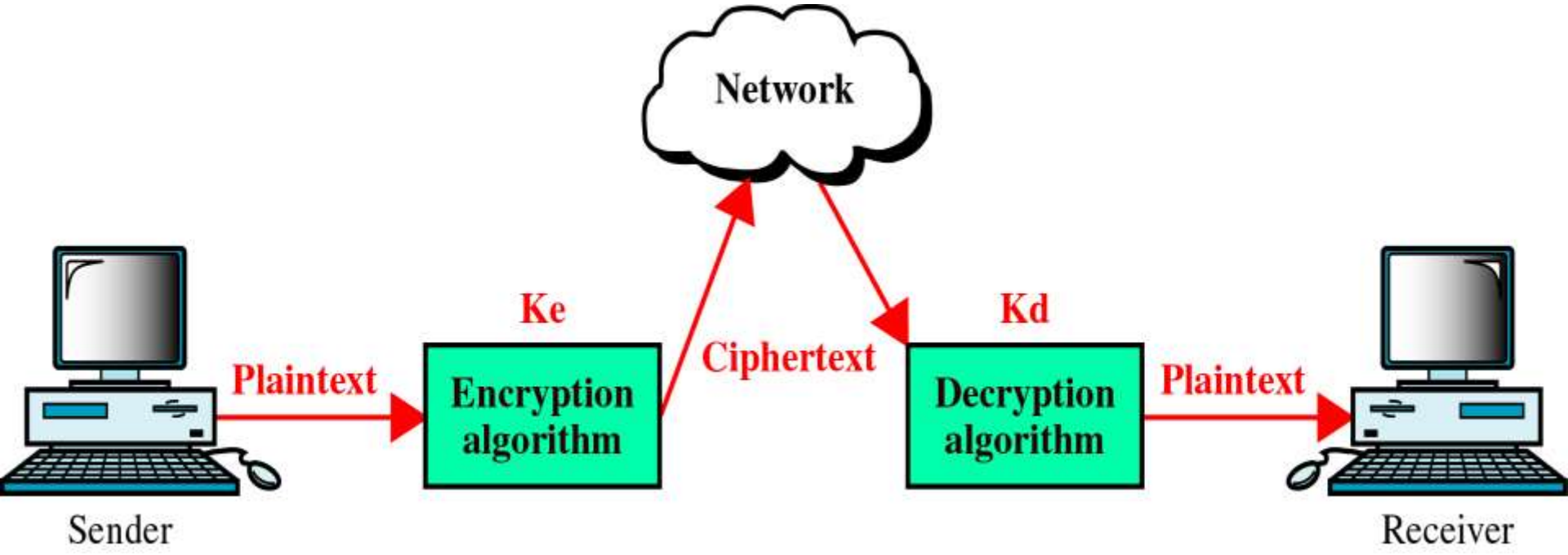
Decryption

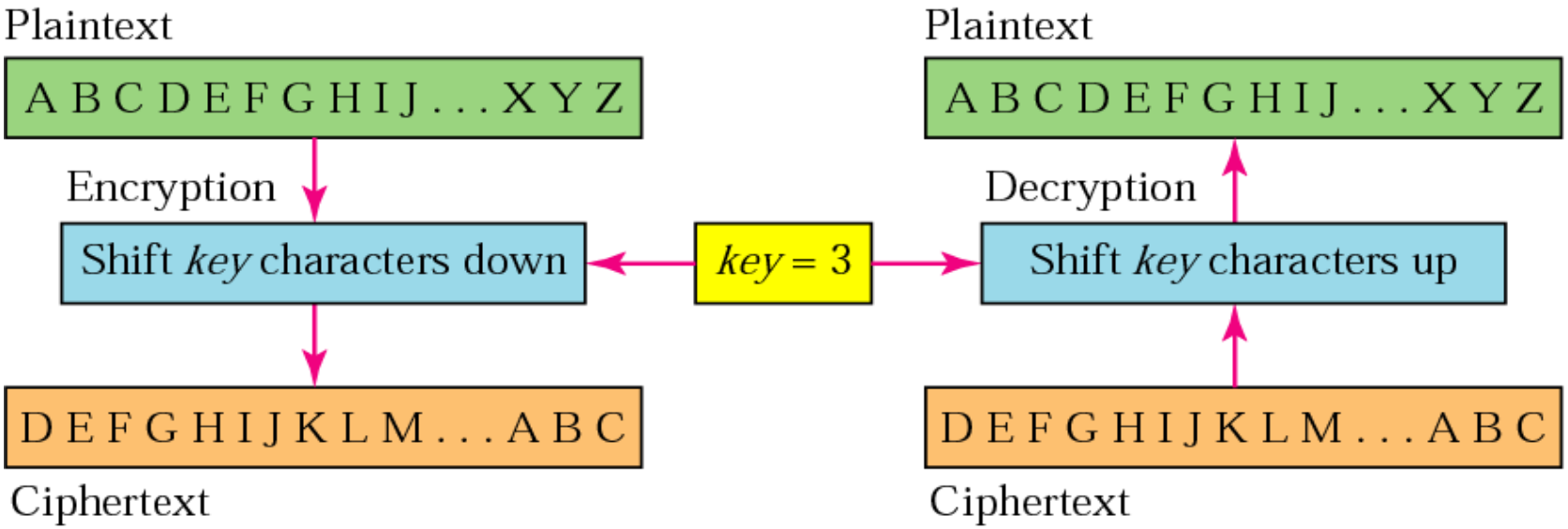
- The process of unscrambling a message in such a way that it is understand by authorised person.



Cryptography

- It is the process of encryption and decryption of message or data by using different algorithms or software's.

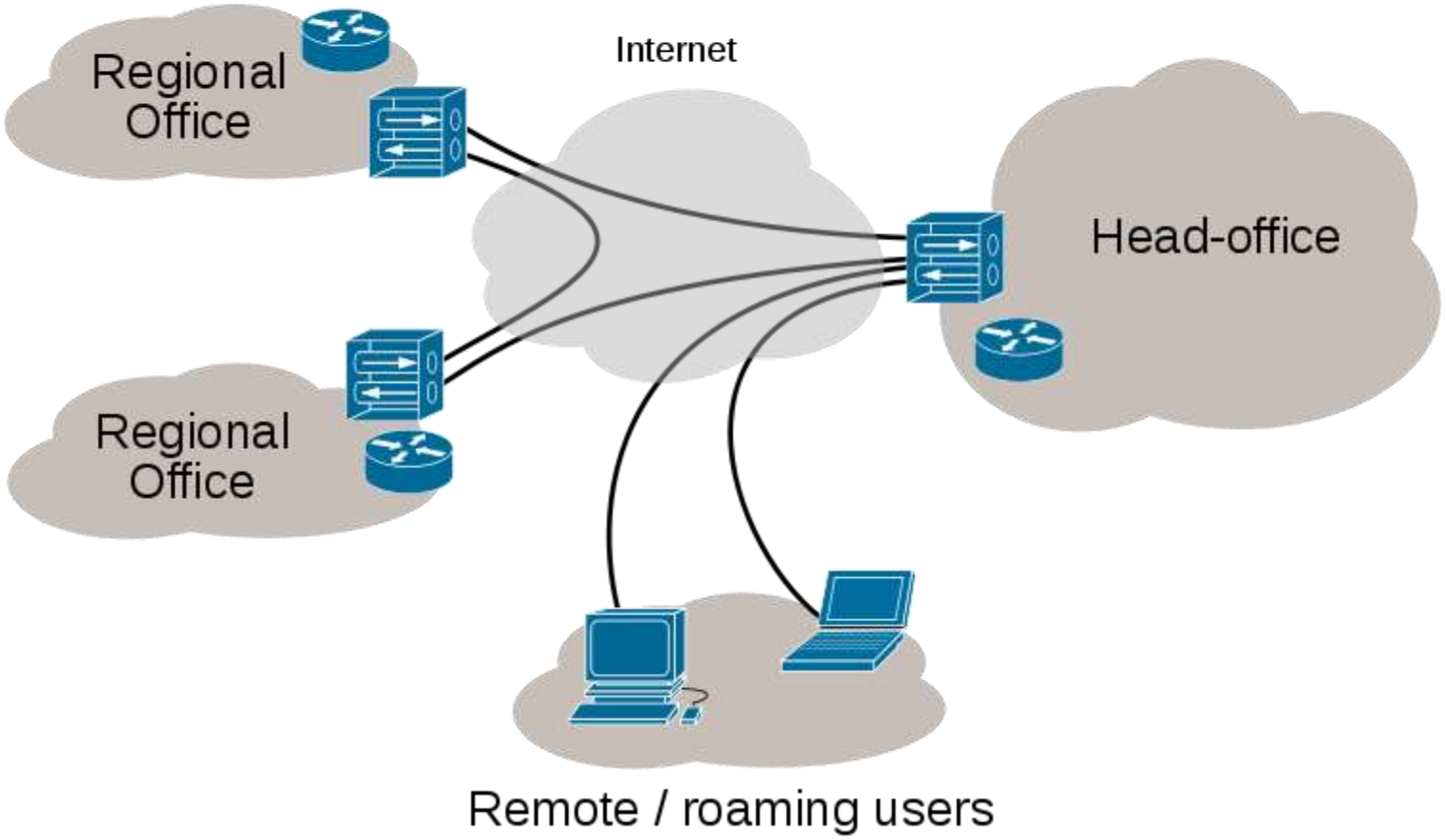



Plaintext
A B C D E F G H I J . . . X Y Z
Encryption
Shift key characters down
key = 3
D E F G H I J K L M . . . A B C
Ciphertext
Plaintext
A B C D E F G H I J . . . X Y Z
Decryption
Shift key characters up
D E F G H I J K L M . . . A B C
Ciphertext

Virtual Private Network

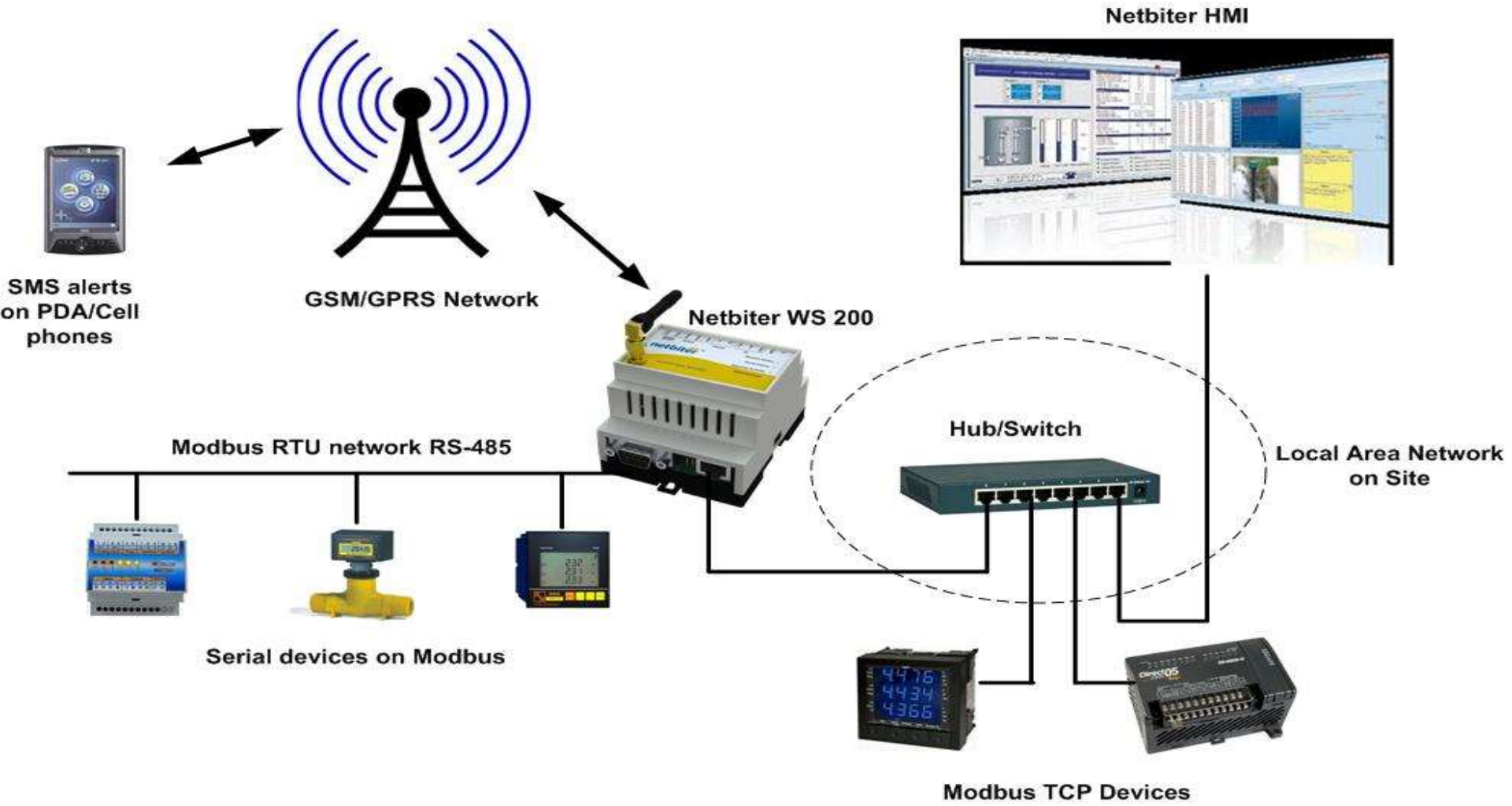
- A network that uses the public internet to carry information but remains private by using encryption to scramble the communications, authentication to ensure that information has not to been tampered with, and access control to verify the identity of anyone using the network.

Internet VPN



Gateway

- Gateway provide a secure way to do online transactions i.e. payment of various orders.



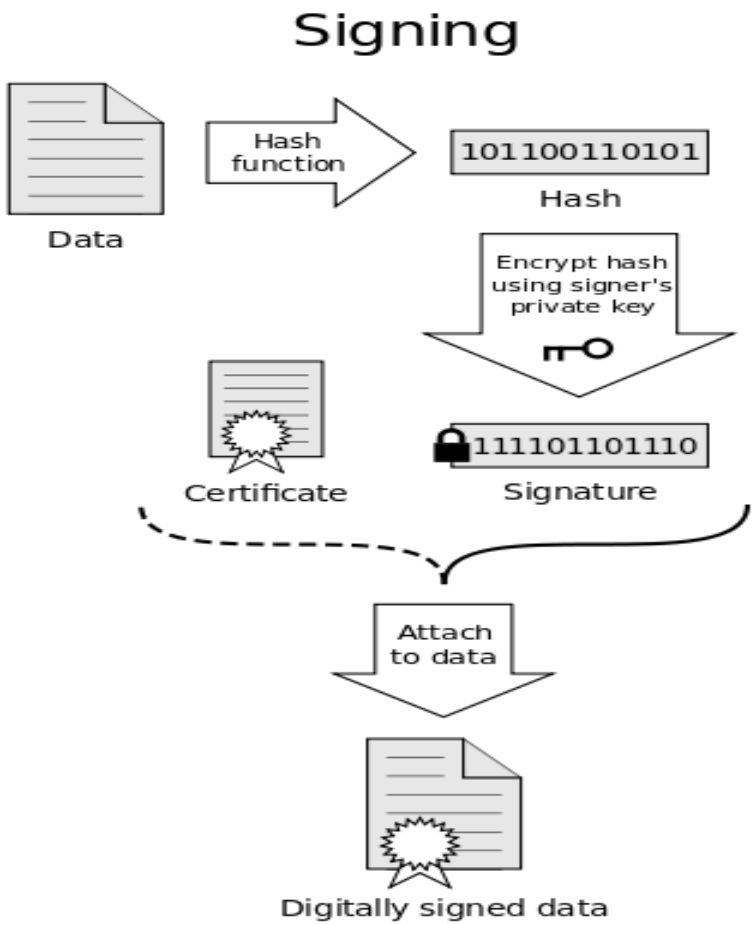
Biometric System

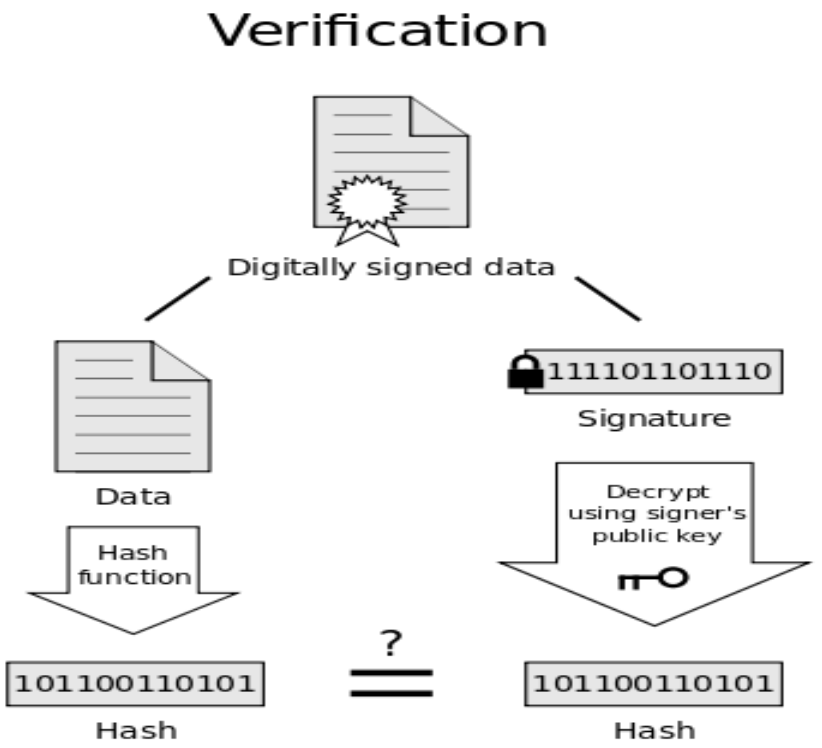
- Authentication systems that identify a person by measurement of a biological characteristics.
- There are various types of biometrics systems:-

1. Physiological Biometrics
2. Behavioural Biometrics
3. Fingerprint Scanning
4. Iris Scanning
5. Voice Scanning
6. Keystroke Monitoring

Digital Signature

- An identifying code that can be used to authenticate the identity of the sender of a document.





Digital Certificate

- A method for verification that the holder of a public or a private key is who he or she claim to be.

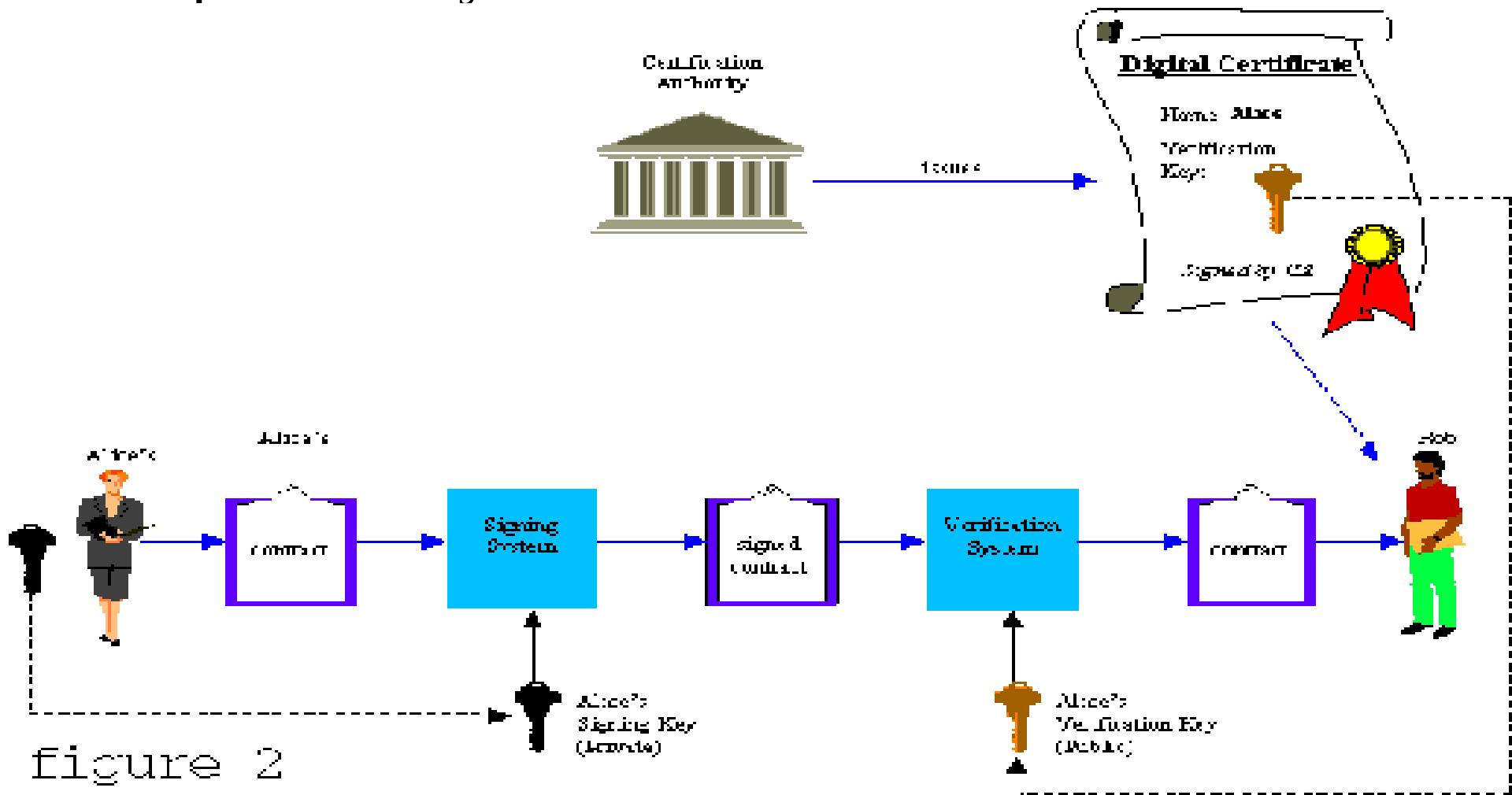
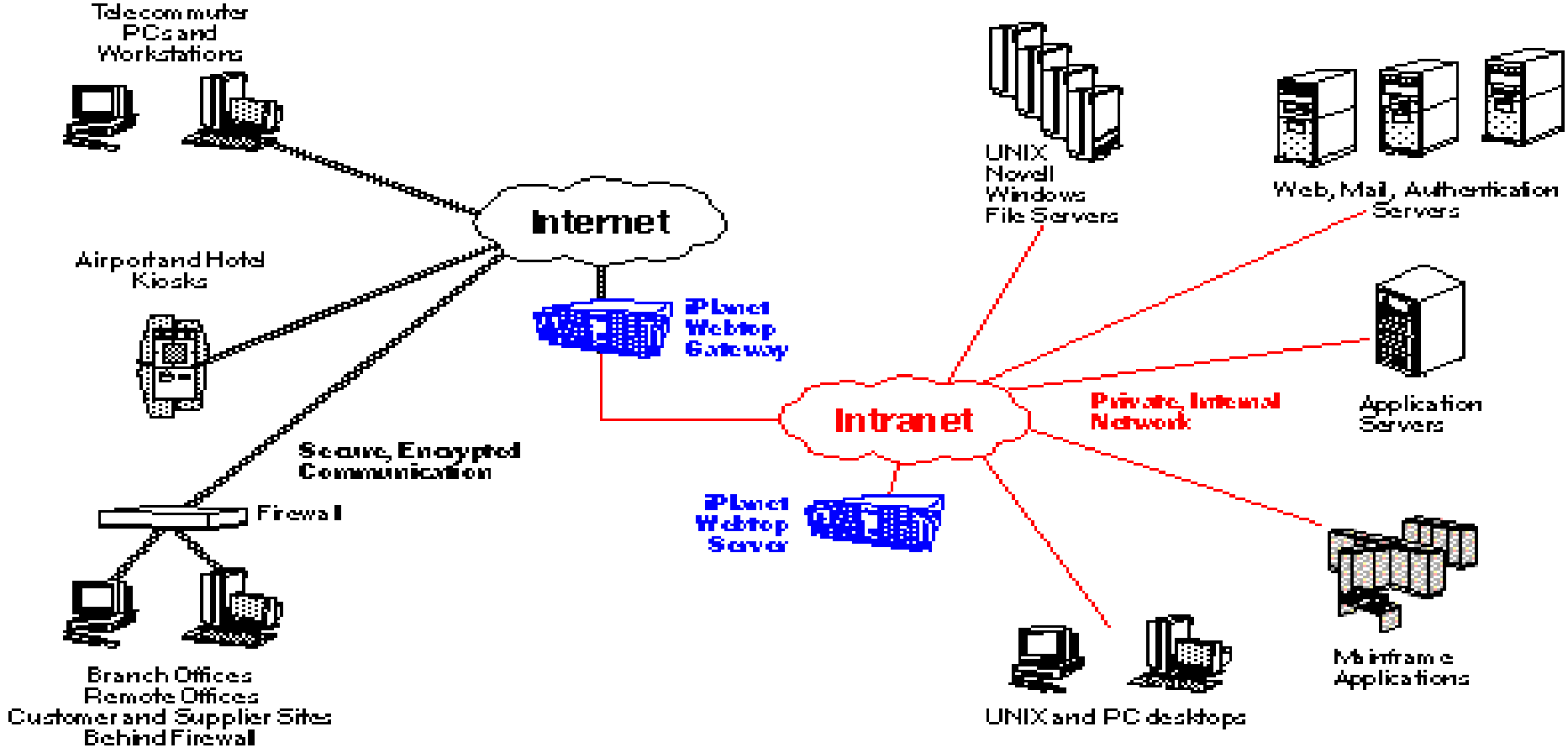


figure 2

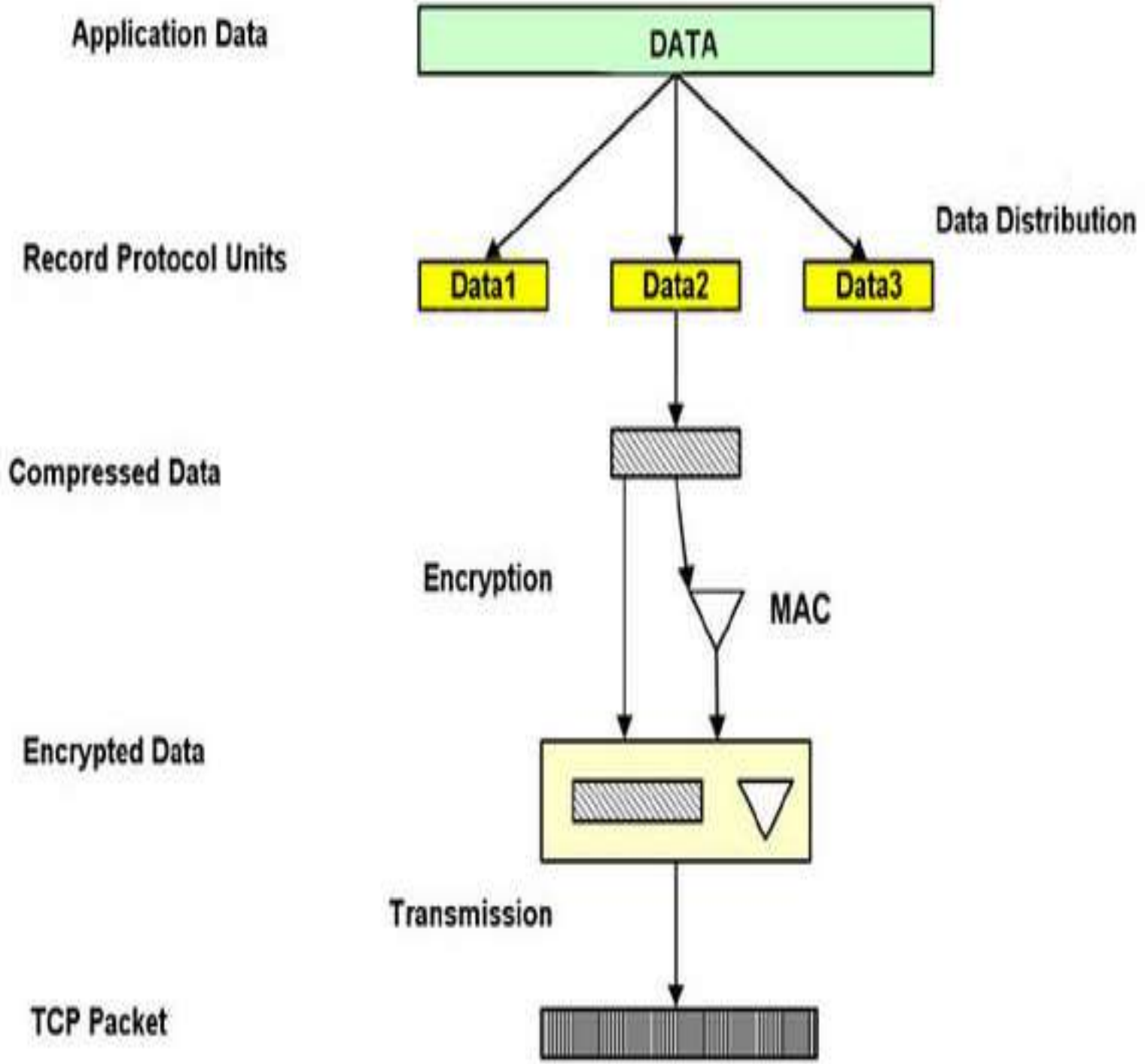
Secure Socket Layer

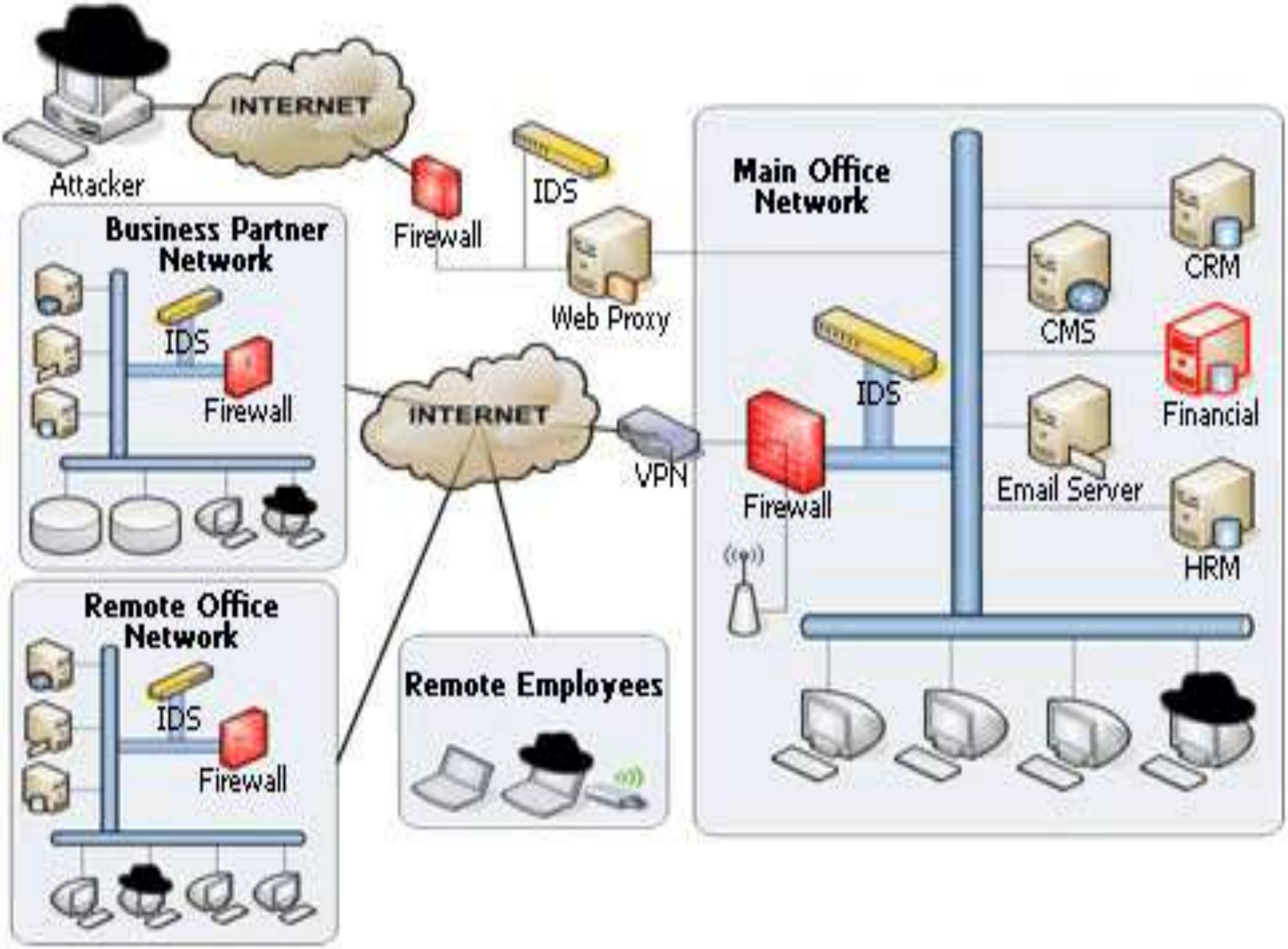
- Protocol that utilizes standard certificate for authentication and data encryption to ensyre privacy or confidentiality.



Transaction Layer Security

- It work same as Secure Socket Layer (SSL) and it is another name of SSL after 1996.


Application Data
DATA
Data Distribution
Record Protocol Units
Data1
Data2
Data3
Compressed Data
Encryption
MAC
Encrypted Data
Transmission
TCP Packet


Attacker
INTERNET
Firewall
IDS
Web Proxy
Main Office Network
CRM
CMS
Financial
IDS
Email Server
HRM
Firewall
VPN
INTERNET
Business Partner Network
IDS
Firewall
Remote Office Network
IDS
Firewall
Remote Employees

Thank You