Troubleshooting Methodologies

A General Approach to Troubleshooting

Rocket Scientist Approach

(Theorist)

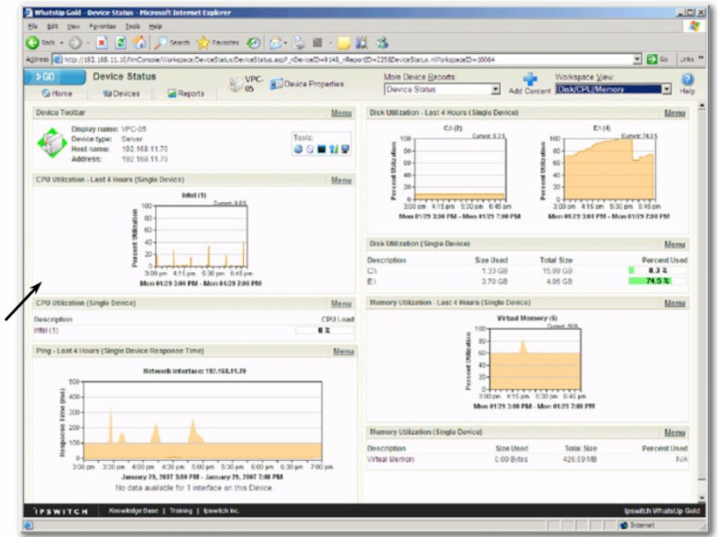
Caveman Approach

(Brute Force)

A Systematic Approach is Best

Troubleshooting Tools : Hardware & Software

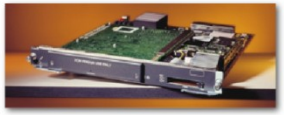
Software Troubleshooting Tools



WhatsUp Gold NMS Device Status display

Hardware Troubleshooting Tools

Web-based application displays NAM Traffic Analyzer Data



NAM module for a Catalyst 6500

Network Management: What it is ??

- 100s or 1000s of Interacting Hardware/Software Components.
- Complex System Requires Network Monitoring.
- Complex Systems => Jet Airplanes, Nuclear Plants etc.
- "Network Management includes the deployment, integration and coordination of the hardware, software and human elements to monitor, test, poll, configure, analyze, evaluate and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost"
- Example : LAN Management System (LMS)

Areas of Network Management

1. Performance Management
   - Quantify, measure, report, analyze and control the performance. (Utilization and Throughput)

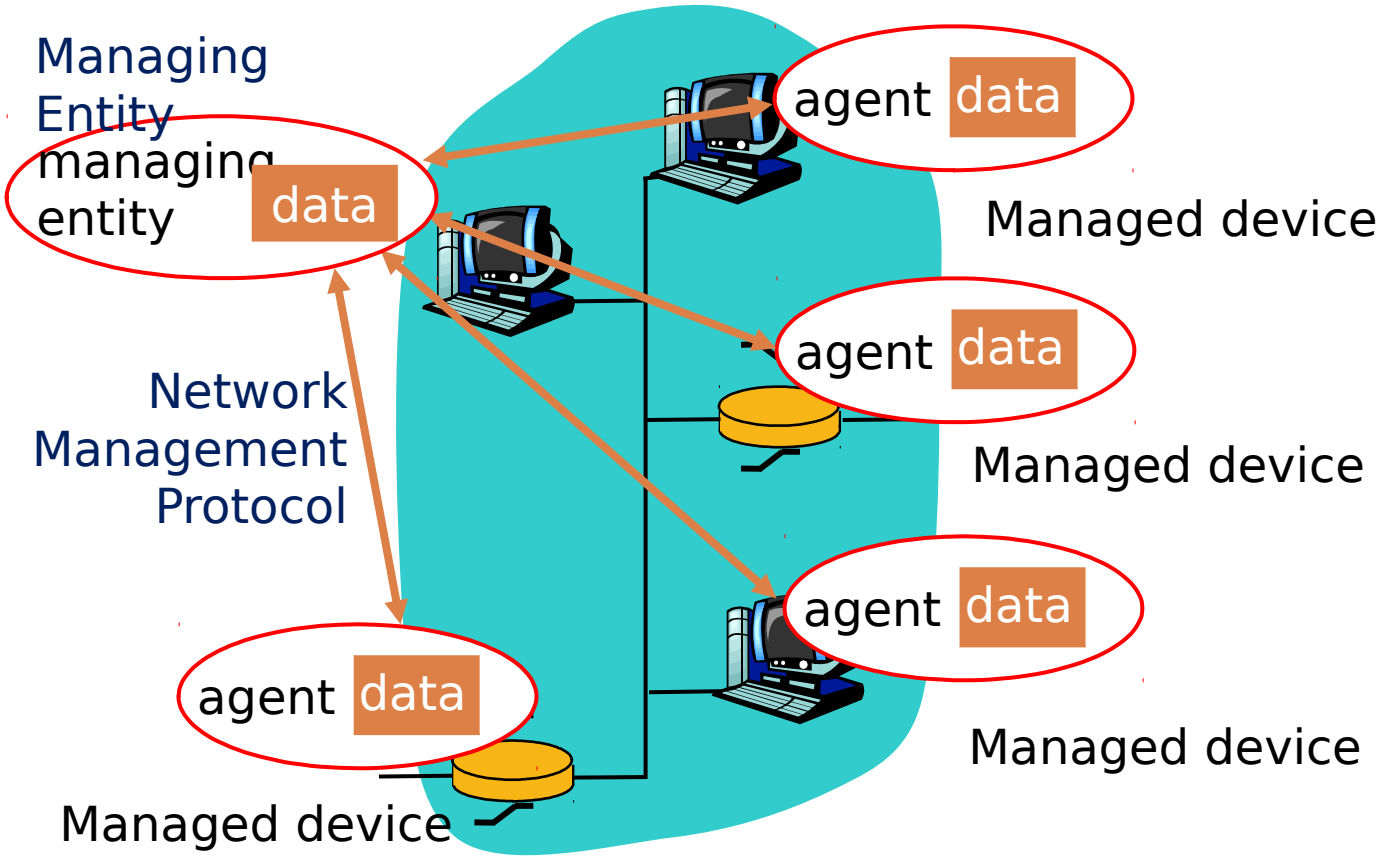
2. Fault Management
   - To log, detect and respond to fault conditions in the network.

3. Configuration Management
   - To manage configuration of device easily

4. Accounting Management
   - To enable accounting of user and their policy management.

5. Security Management
   - To control access to network resources according to defined policy.

Infrastructure of Network Management



Infrastructure of Network Management

- The Managing Entity is an application running in a centralized network management station in Network Operation Center.
- It controls the collection, processing, analysis and display of Network Management Information.

- A Managed Device is a piece of network equipment that resides on a managed network.
- It might be host, router, bridge, hub or printer.
- Managed Device contains several Managed Objects.
- Managed Object => E.g. NIC Card
- Managed Object => Have Piece of Information.
- Collection of Managed Object => Management Information Base.

- Network Management Protocol runs between Managing Entity and Managed Device. (SNMP)

Internet Standard Management Framework

- Root of Internet Standard Management Framework => SGMP.
- SGMP => Simple Gateway Management Protocol.
- It was designed by group of University network researchers.
- Four Components of Internet Standard Management Framework:
  1. Network Management Objects
  2. Data Definition Language
  3. A Protocol
  4. Security and Administration Capabilities

Network Management Objects : MIB

- It is also known as Management Information Base Objects.
- Management Information is represented as a collection of Managed Objects.
- MIB objects define the management information maintained by a Managed Device.
- Related MIB objects are gathered into MIB modules.

Data Definition Language : SMI

- It is also known as SMI.
- SMI => Structure of Management Information.
- It defines data type, an object model and rules for writing management information.
- SMI Data Types :
  - IPADDRESS => 32 bit Internet Address.
  - Integer32 => Integer 32 bit.
  - Unsigned32 => Unsigned Integer 32 bit.

A Protocol : SNMP

- SNMP => Simple Network Management Protocol.
- It Convey information and commands between Managing Entity and Managed Devices.
- Most common usage of SNMP is in a request/response mode.

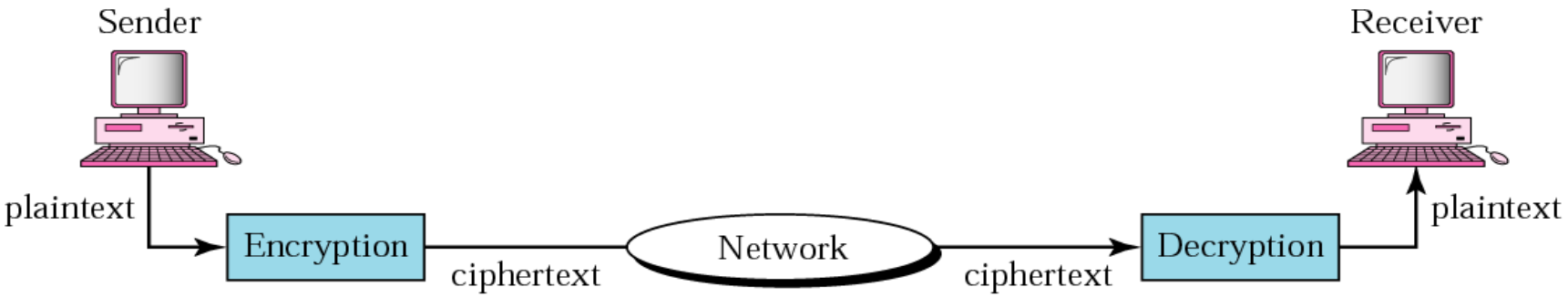
- SNMPv2 managing entity sends a requests to SNMPv2 agent of Managed Device.
- The SNMPv2 receives the request, perform actions and sends a reply.
- Typically request => To query of modify MIB object values.

- Trap messages are used to notify Managing Entity of an Exceptional Situation.

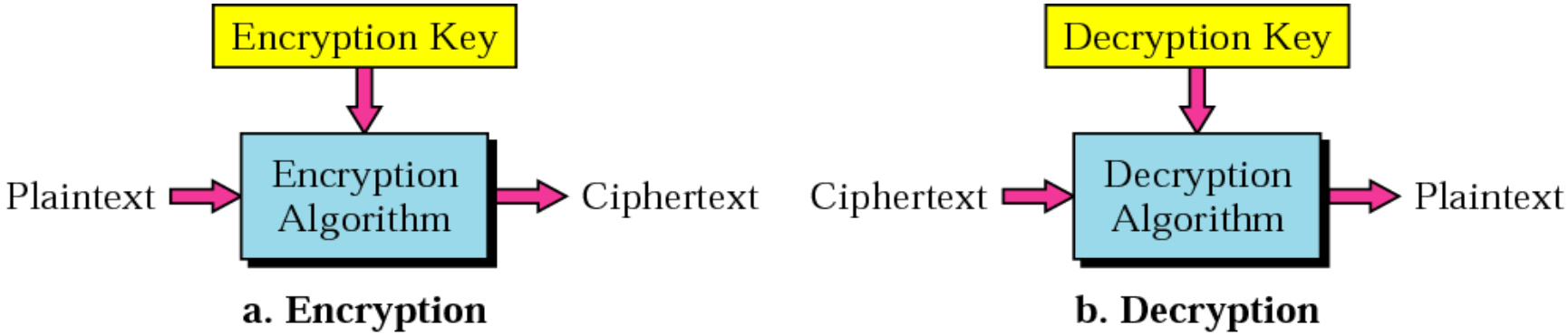
Cryptography : What it is ??

- Cryptography in Greek means “Secret Writing”
- Science and Art of transforming message to make them secure and immune to attack.
- Original message before transformation => Plaintext.
- An Encryption algorithm transforms => Plaintext to Ciphertext.
- Decryption algorithm transforms => Ciphertext to Plaintext
- Cipher refers to different categories of algorithm in Cryptography.

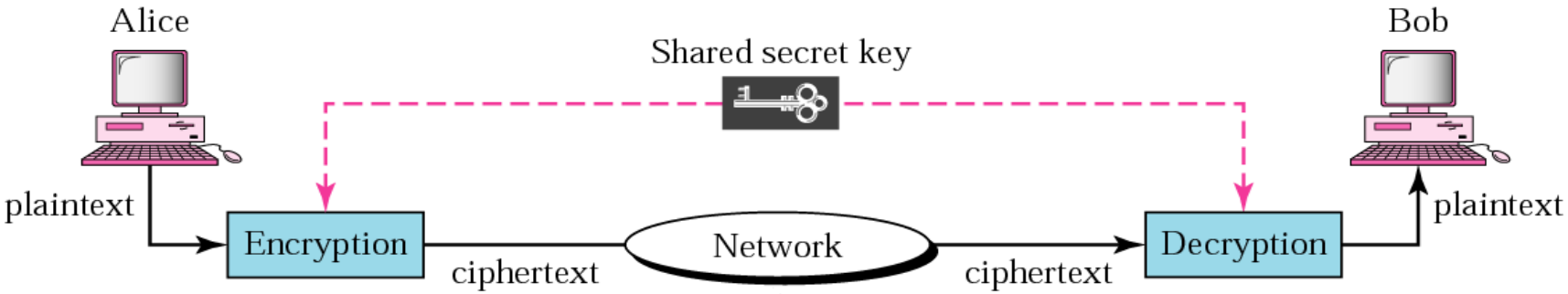
Cryptography : Components



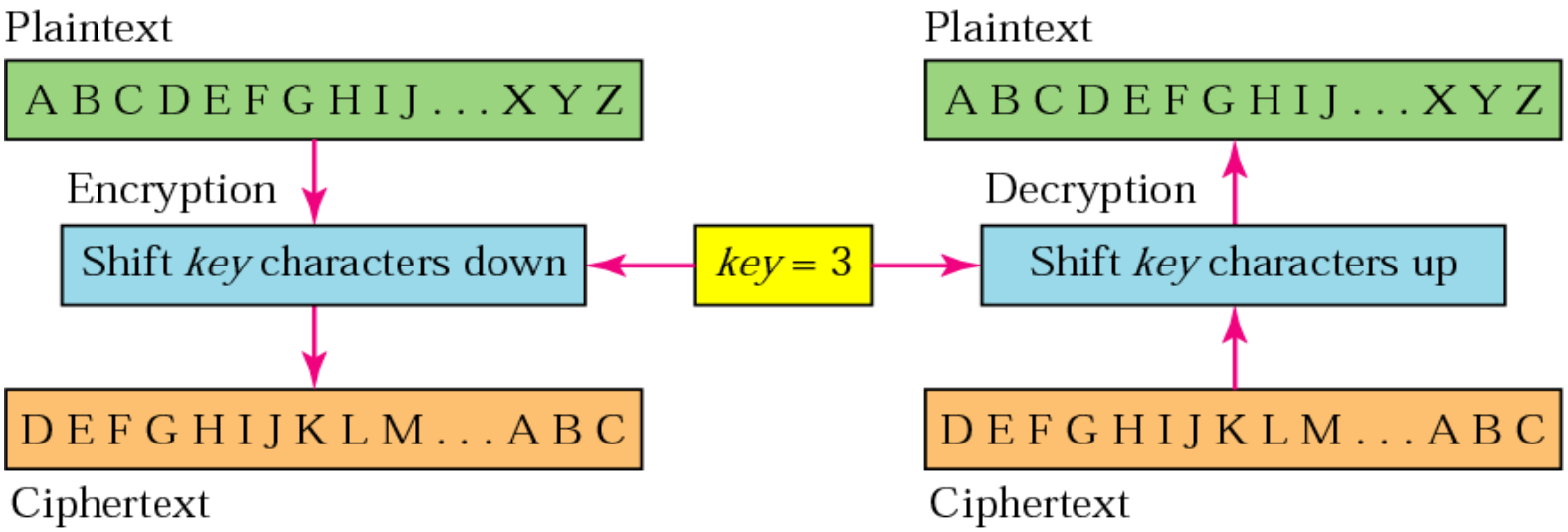
Cryptography : Encryption and Decryption



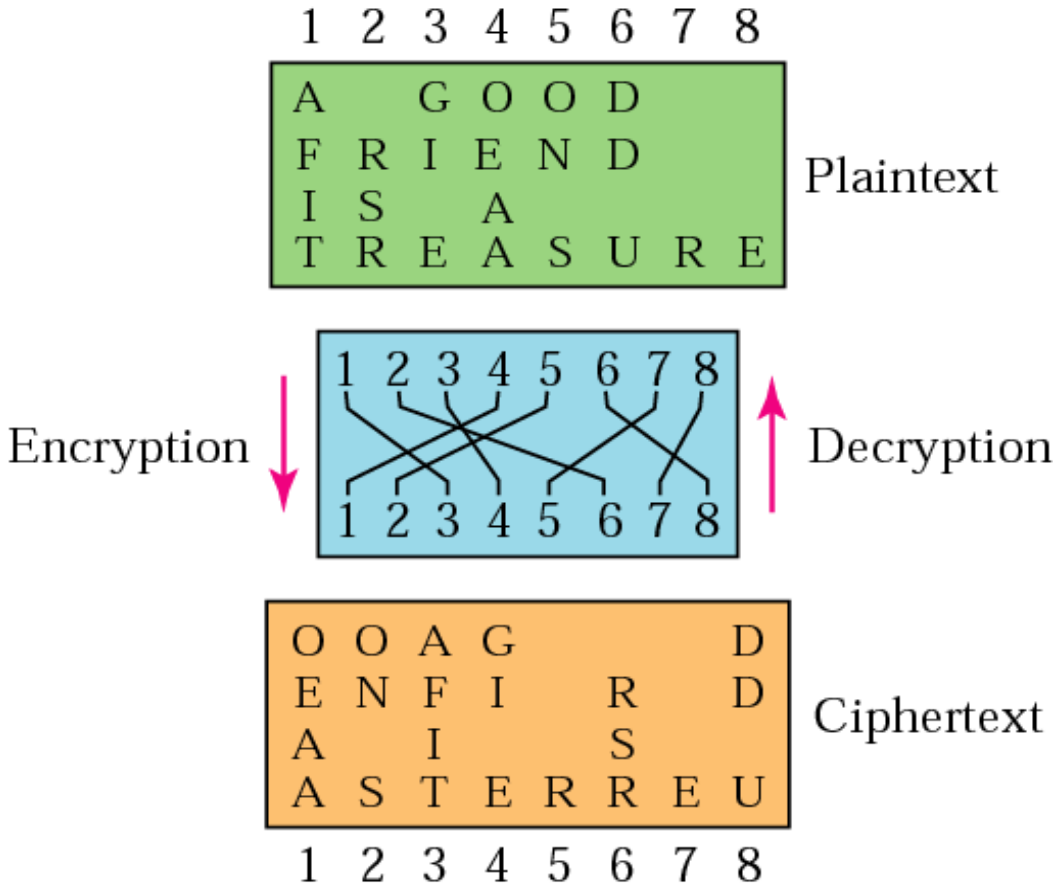
Cryptography : Symmetric- Key Cryptography



Symmetric-Key Cryptography : Caesar Cipher



Symmetric Encryption: Transposition Cipher



Symmetric Encryption : Vigenere Cipher

- Proposed by *Blaise de Vigenere* from the court of France in the sixteenth century.
- It is based on Polyalphabetic substitution.
- A Polyalphabetic substitution cipher involves the use of two or more cipher alphabets.

EXAMPLE

- KEYWORD : RELATIONS
- PLAINTEXT : TO BE OR NOT TO BE THAT IS THE QUESTION
- CIPHERTEXT : KS ME HZ BBL KS ME MPOG AJ XSE JCSFLZSY

VERIFY WITH VIGENERE TABLE

Symmetric Encryption: Vigenere 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
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

Vigenere Cipher: Encryption and Decryption

ENCRYPTION

(CIPHERTEXT = INTERSECTION OF KEYWORDS AND PLAINTEXT)

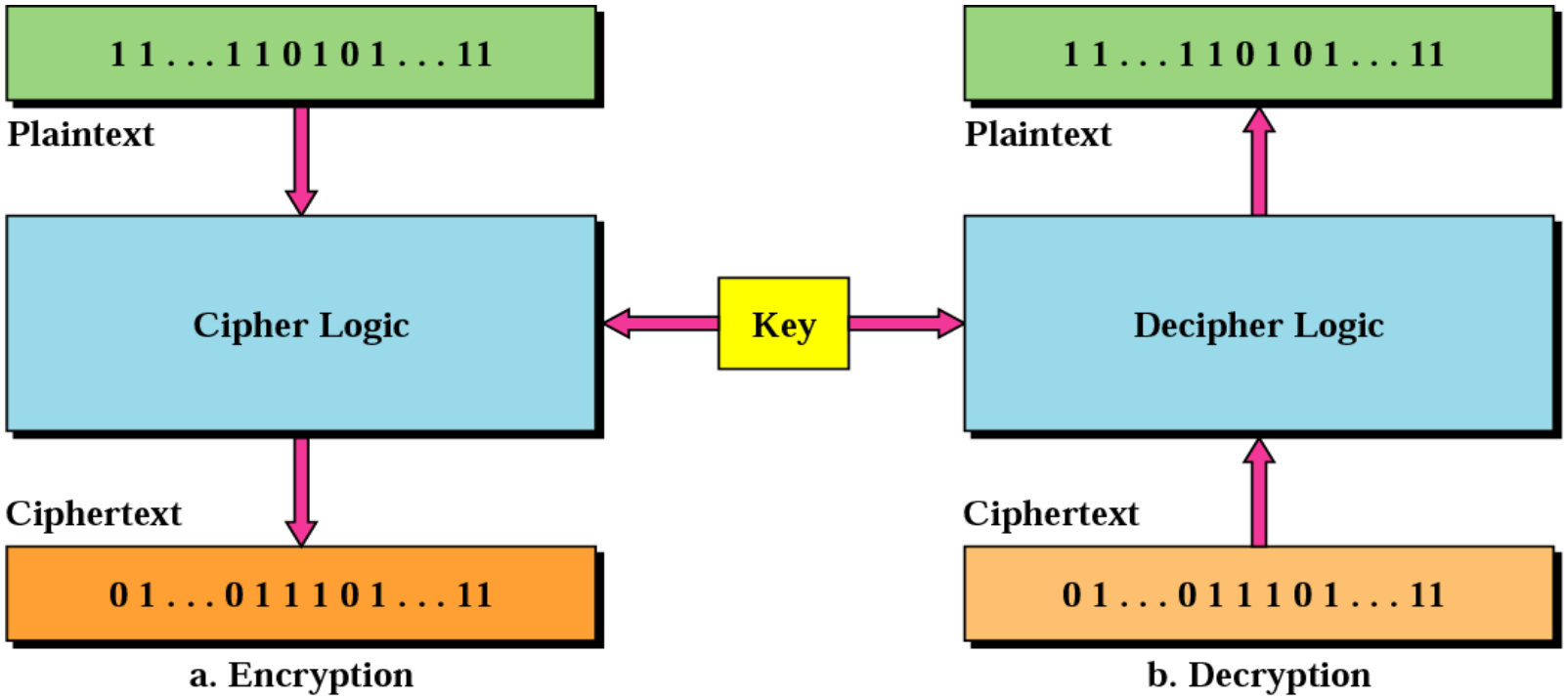
- KEYWORD : RELATIONS
- PLAINTEXT : TO BE OR NOT TO BE THAT IS THE QUESTION
- CIPHERTEXT : KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY

DECRYPTION

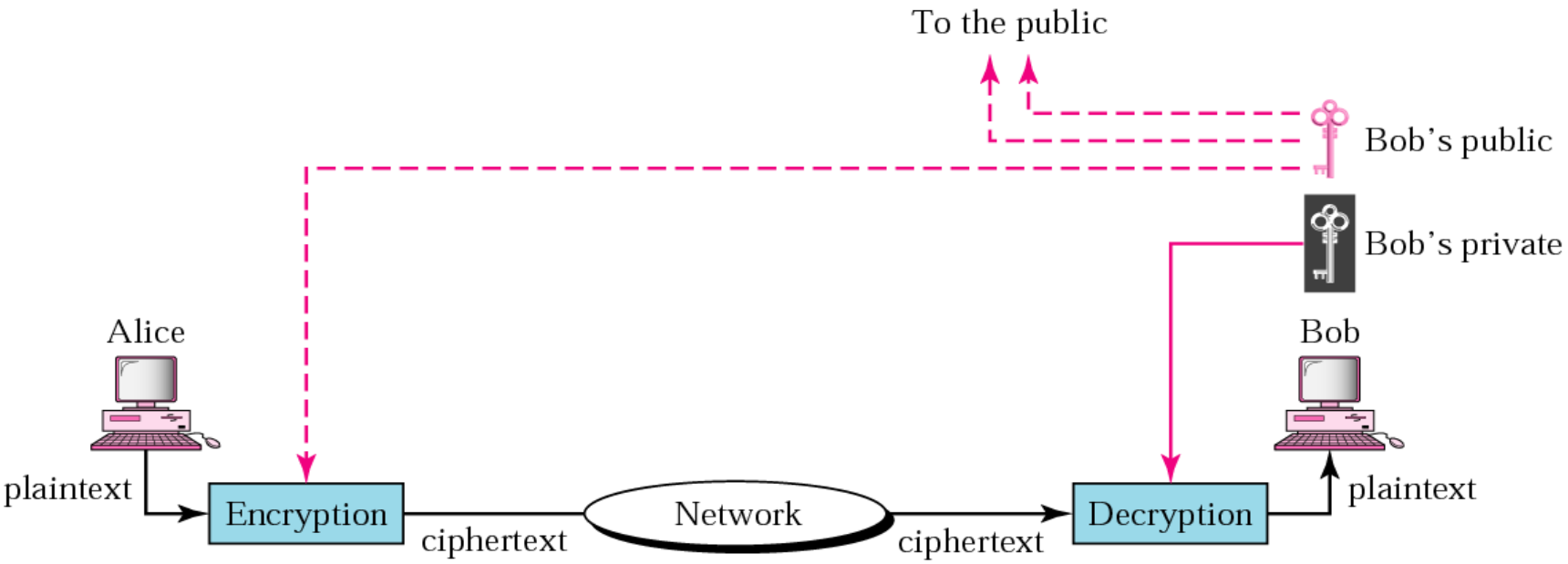
(PLAINTEXT = INDEX OF THE ROW CONTAINING CIPHER TEXT)

- KEYWORD : RELATIONS
- CIPHERTEXT : KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY
- PLAINTEXT : TO BE OR NOT TO BE THAT IS THE QUESTION

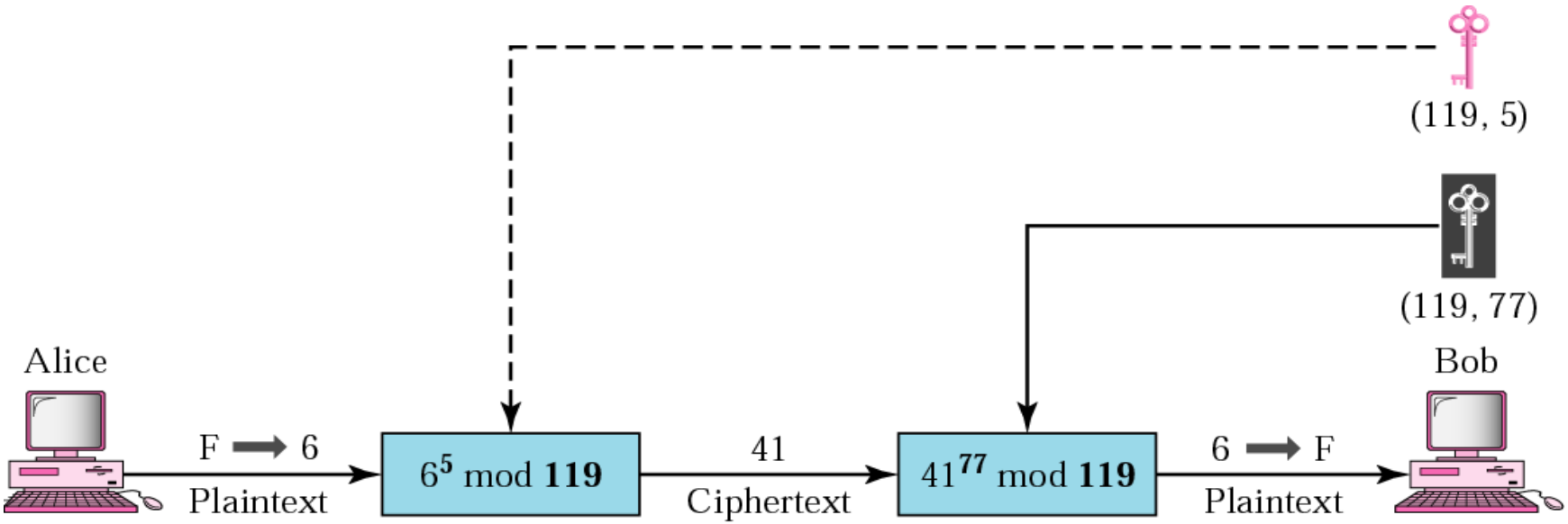
Symmetric Encryption: Block Cipher



Cryptography : Public- Key Cryptography



Public-Key Cryptography : RSA (Rivest, Shamir, Adleman)



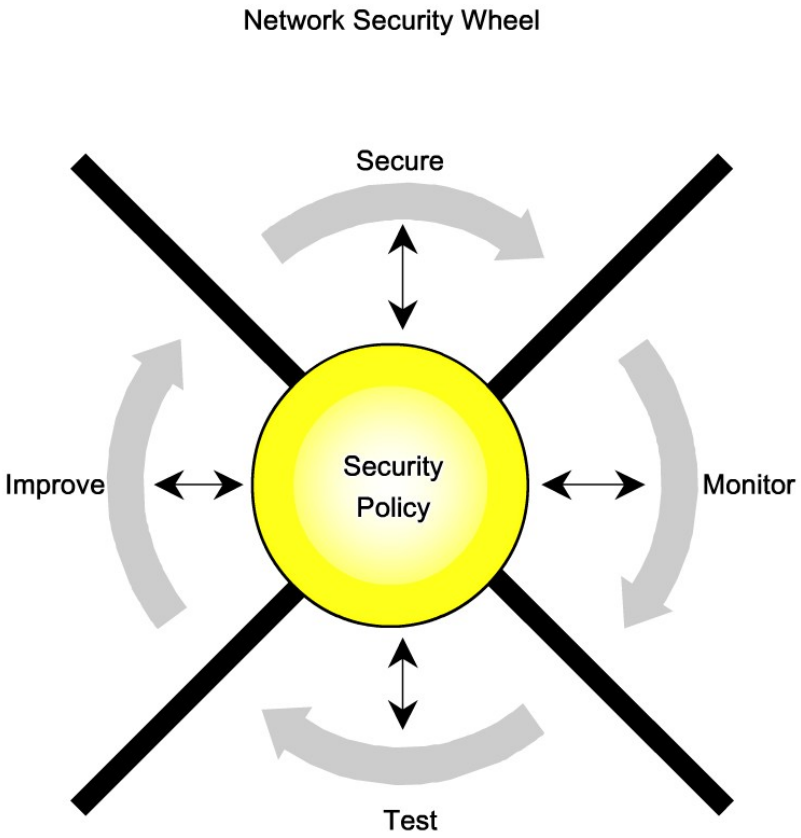
Cryptanalysis : Computationally Secu

- An Encryption scheme is computationally secure if the Ciphertext generated by the scheme meets one or both of the following criteria.

- ✓ The cost of breaking the cipher exceeds the value of the encrypted information.

- ✓ The time required to break the cipher exceeds the useful lifetime of the information.

Network Security Wheels



Firewall : What it is ??

- A Firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.

- The use of single choke point simplifies security management because security capabilities are consolidate on a single system.

- A Firewall provides a location for monitoring security-related events.

- Audits and Alarms can be implemented on the Firewall system.

Firewall : Design goals ??

- All Traffic from inside to outside and vice versa must pass through the Firewall.
- It is achieved by physically blocking all access to the local network except via the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- The Firewall itself is immune to penetration. => Trusted System with secure Operating Systems.

Firewall : Control Access Methods?

1. Service Control
   - Filter traffic on the basis of IP address or TCP Port Address.
   - Example : Block Port 80, Allow Port 23

2. Direction Control
   - Determine the direction => Inbound/outbound.

3. User Control
   - Internal or External Users.

4. Behavior Control
   - Filter e-mail to eliminate Spam.

Firewall : Types of Firewall

1. Packet Filtering Router

- It applies a set of rules to each incoming IP Packet.
- The router is configured to filter packets going in both directions.
- Filtering rules are based on IP and Transport header.

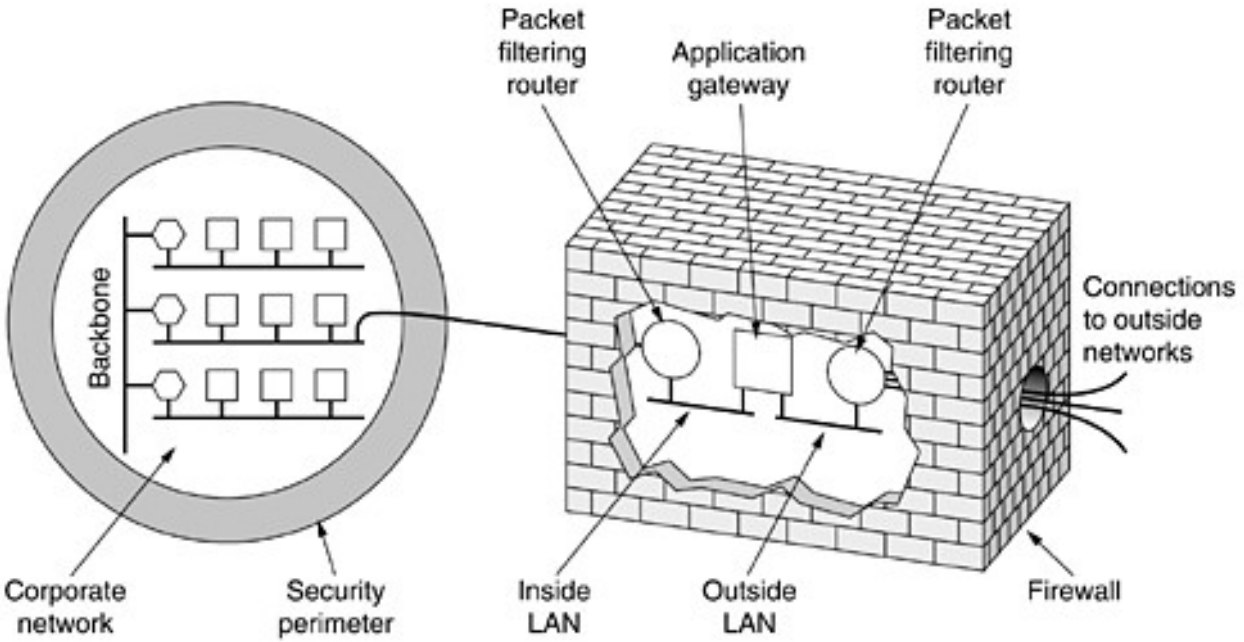
2. Application Level Gateway

- They are called Proxy Servers and acts as a relay of application level traffic.

3. Circuit Level Gateway

- It does not permit an end to end TCP Connection directly.
- The gateway setups two TCP Connections (IN and OUT).
- Once two connections are established => Gateway Relays

Firewall : Types of Firewall



Thank You