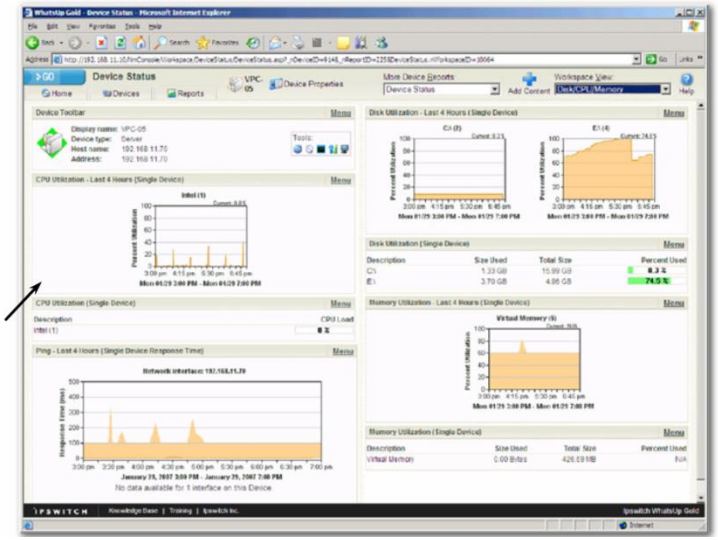
Computer Networks: Network Management & Security

By,

Mr. Kumar Pudashine, (MEng, AIT, Bangkok)
CISA, CISM, CRISC, CNDA, CDCP, COBIT 5, CCNP (Enterprise), JNCIA, CEH v9, ITIL, ISO 27001:2013, AcitivIdentity Certified
Senior Section Chief, Network and Security
Agricultural Development Bank,
Kathmandu

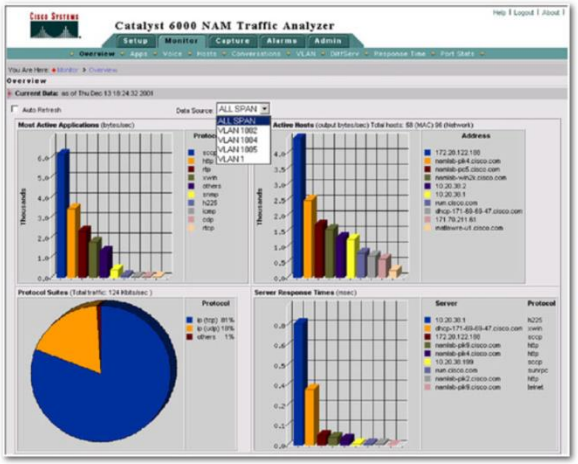
Troubleshooting Tools : Hardware & Software

Software Troubleshooting Tools

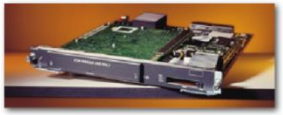


WhatsUp Gold NMS Device Status display

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)

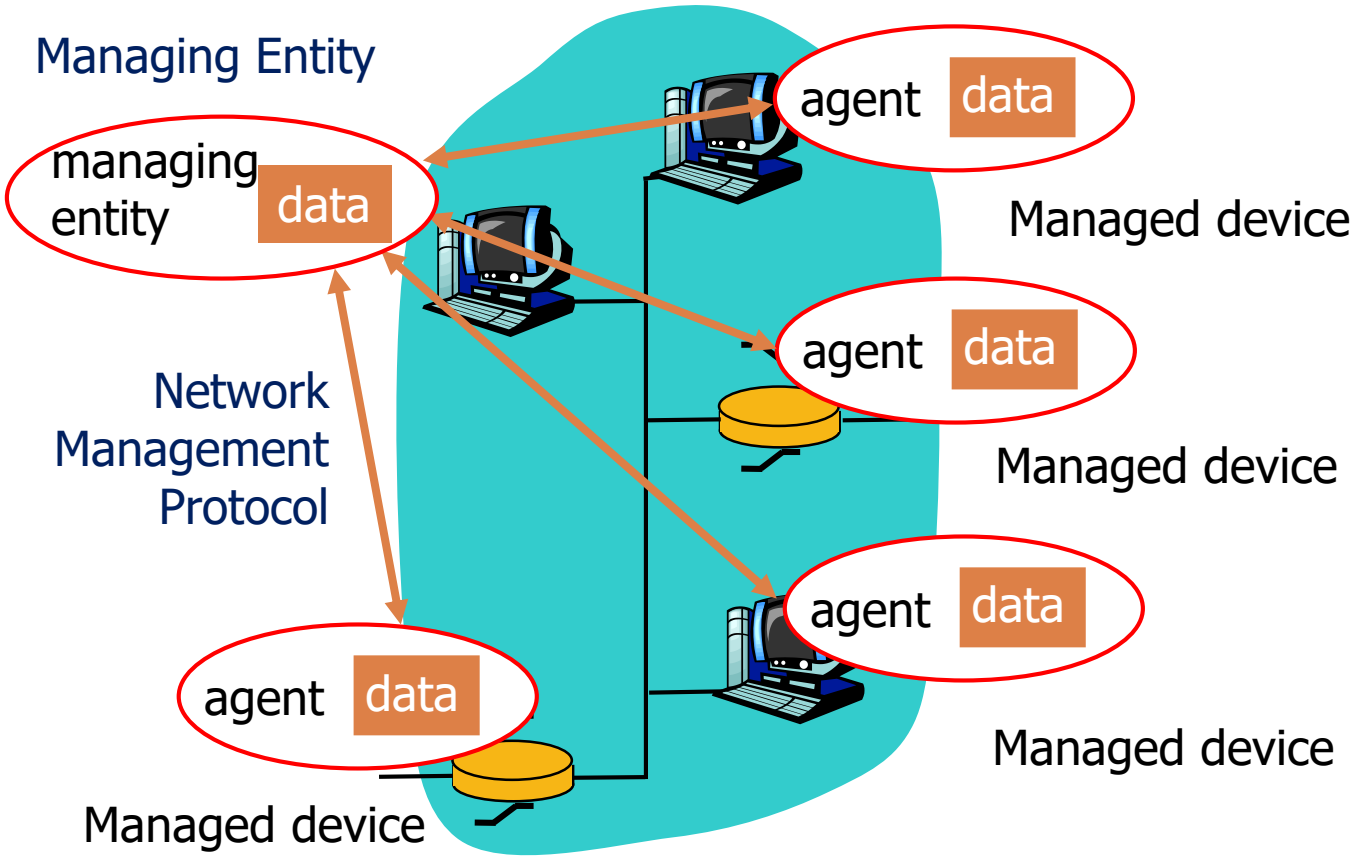
2. Fault Management
   - To log, detect and respond to fault conditions in the network.

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)

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.

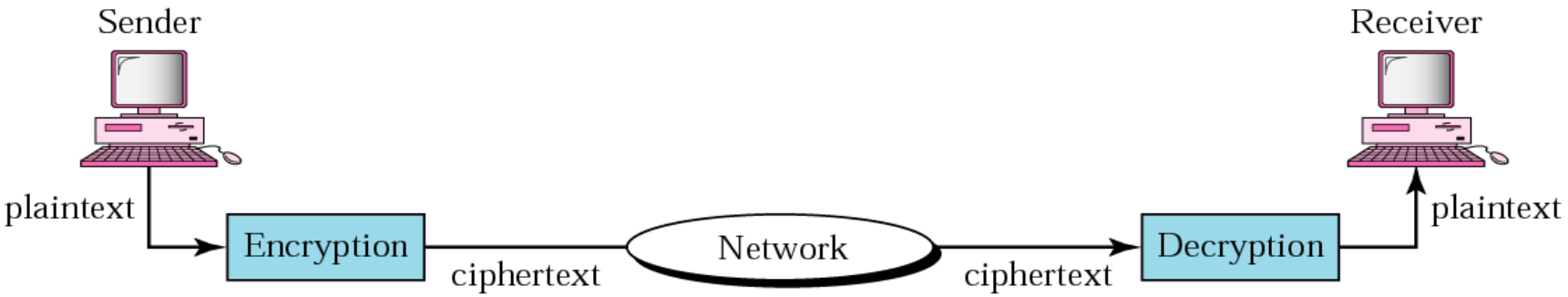
- SNMPv2 managing entity sends a requests to SNMPv2 agent of Managed Device.
- The SNMPv2 receives the request, perform actions and sends a reply.
- Typically request => To query of modify MIB object values.

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

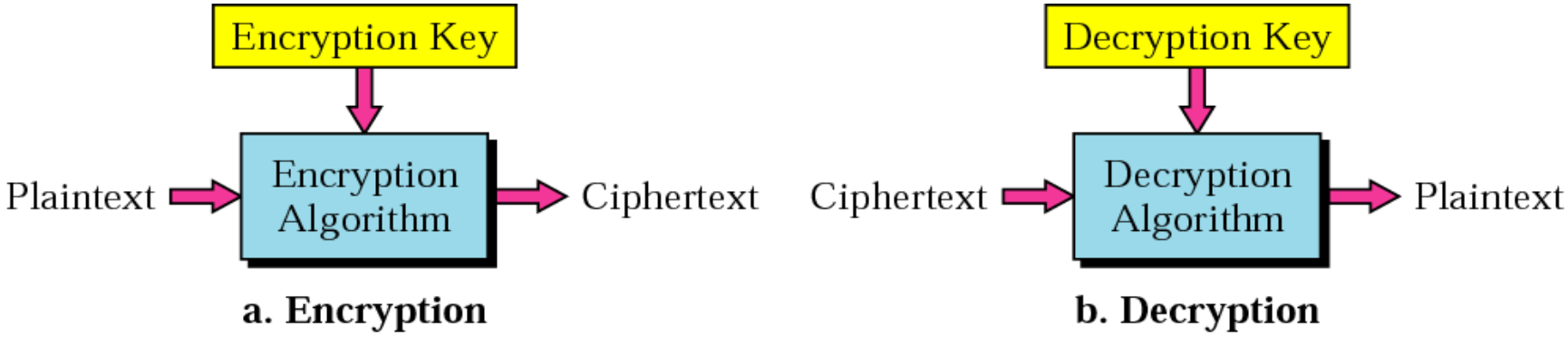
Cryptography : What it is ??

- 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.

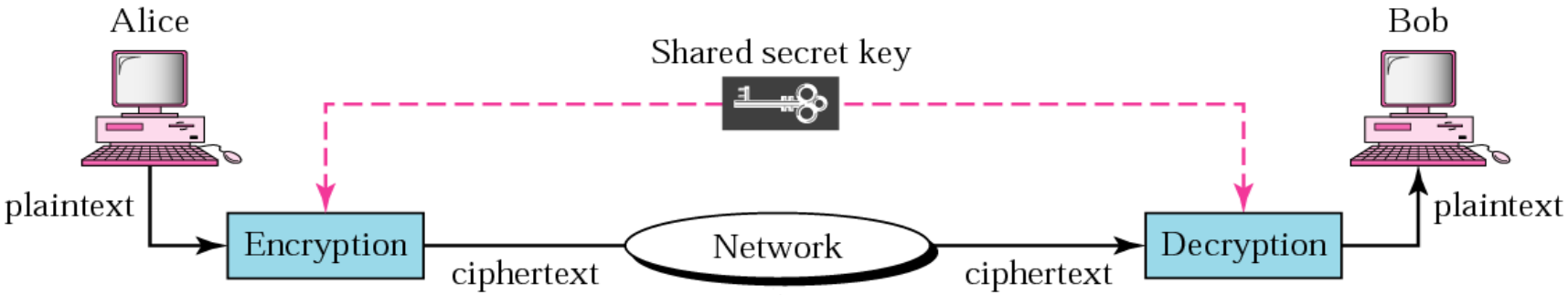
Cryptography : Components



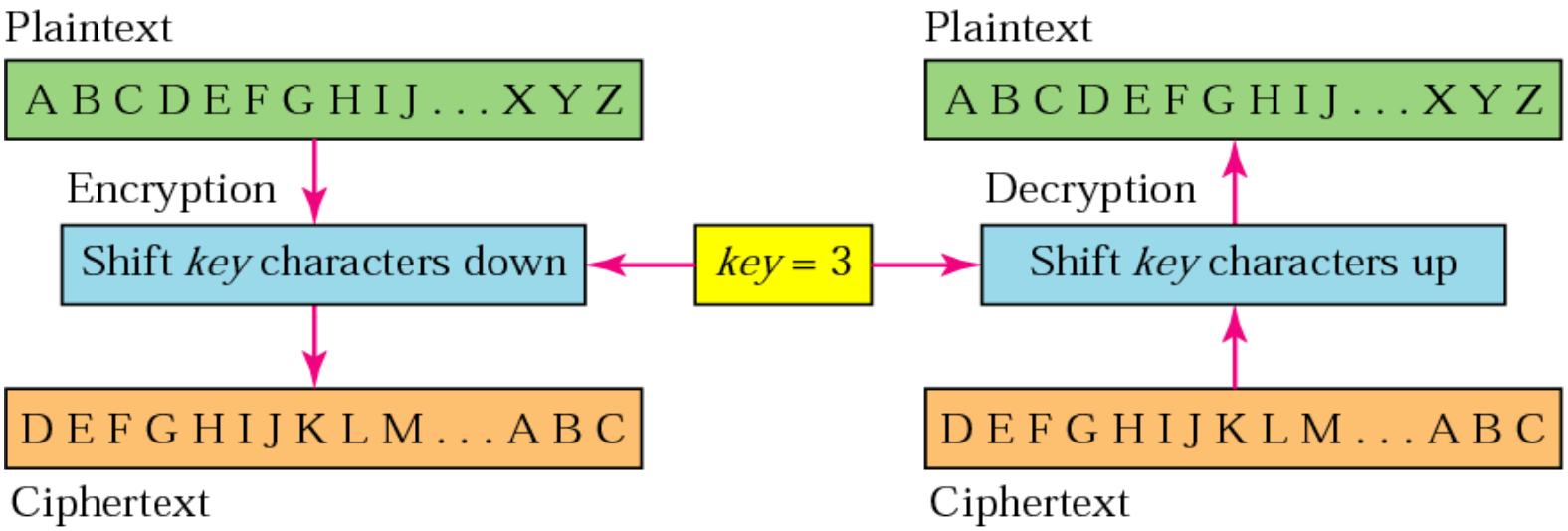
Cryptography : Encryption and Decryption



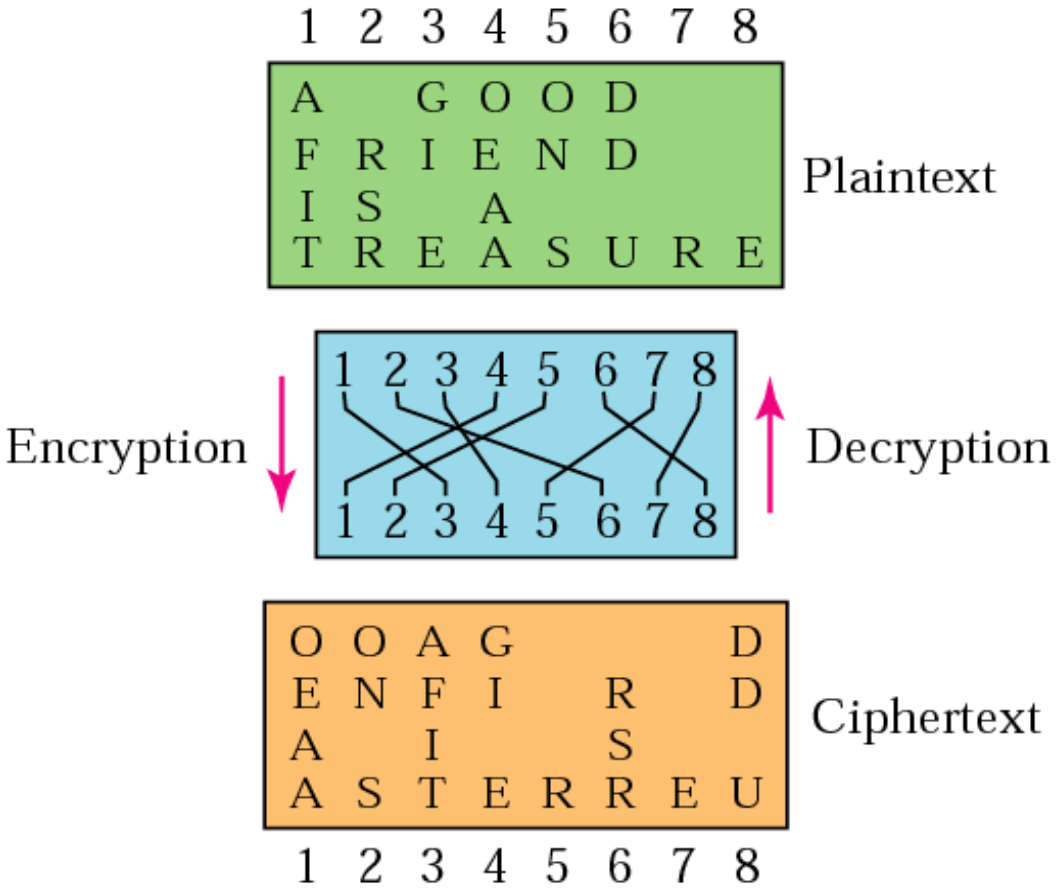
Cryptography : Symmetric- Key Cryptography



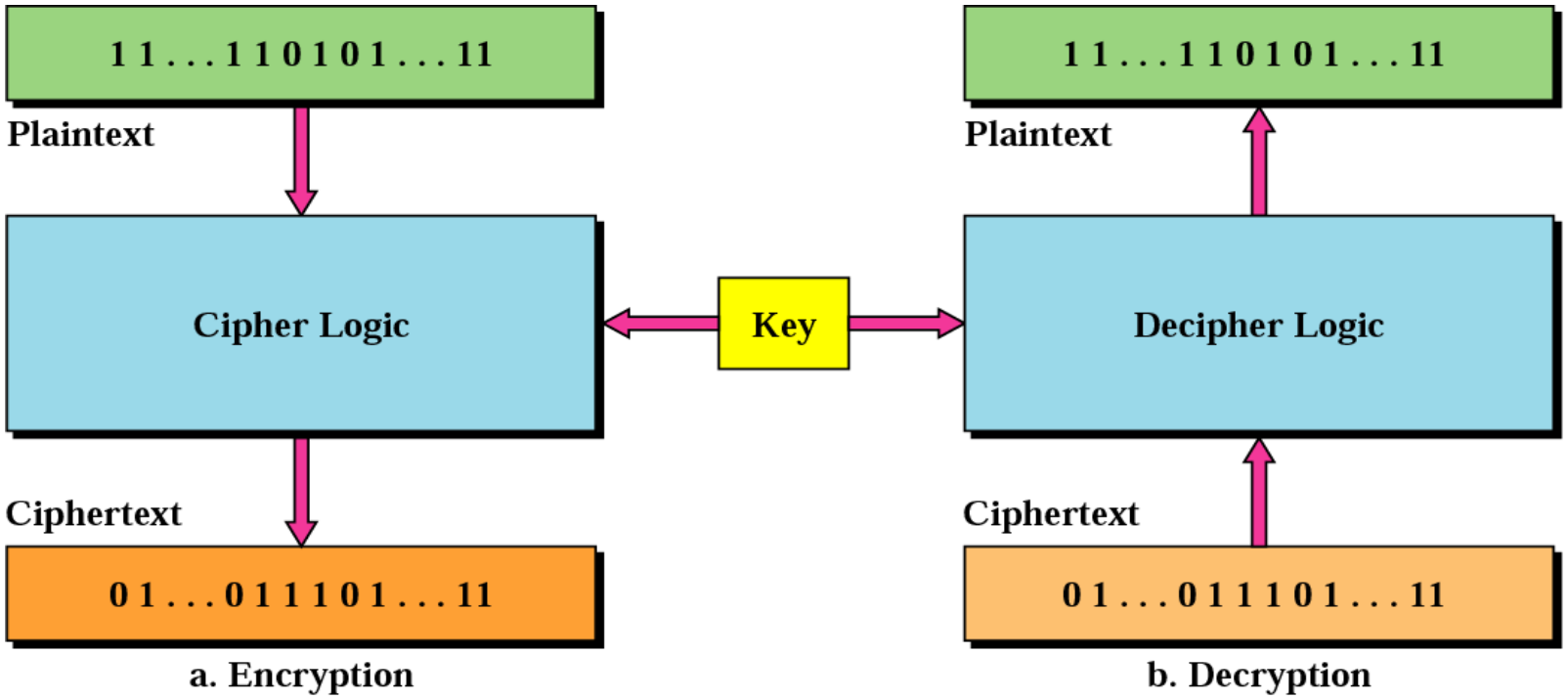
Symmetric-Key Cryptography : Caesar Cipher



Symmetric Encryption: Transposition Cipher



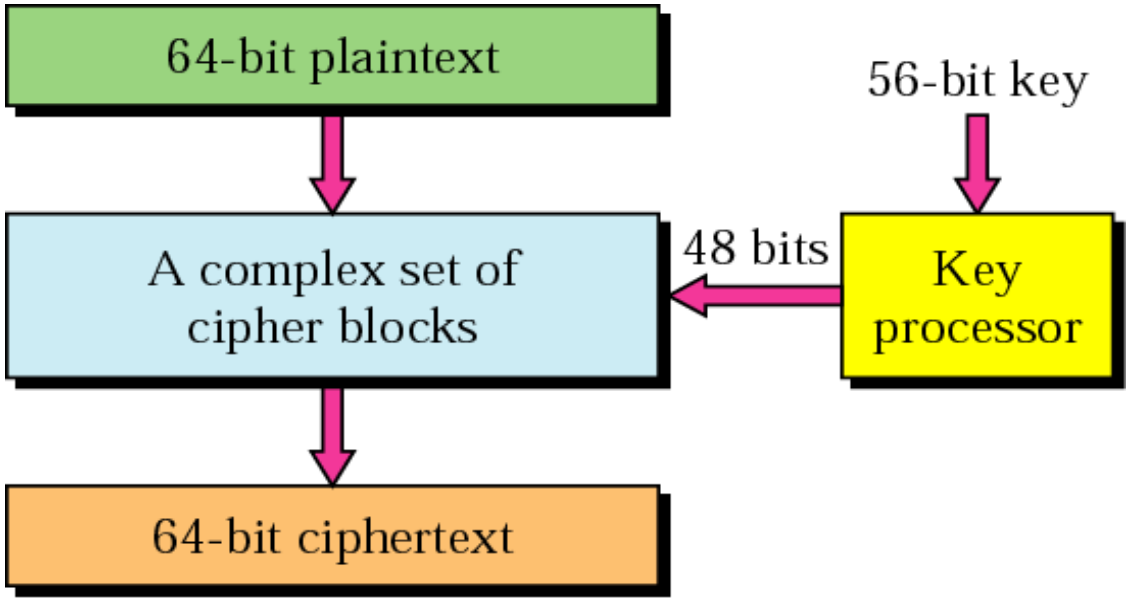
Symmetric Encryption: Block Cipher



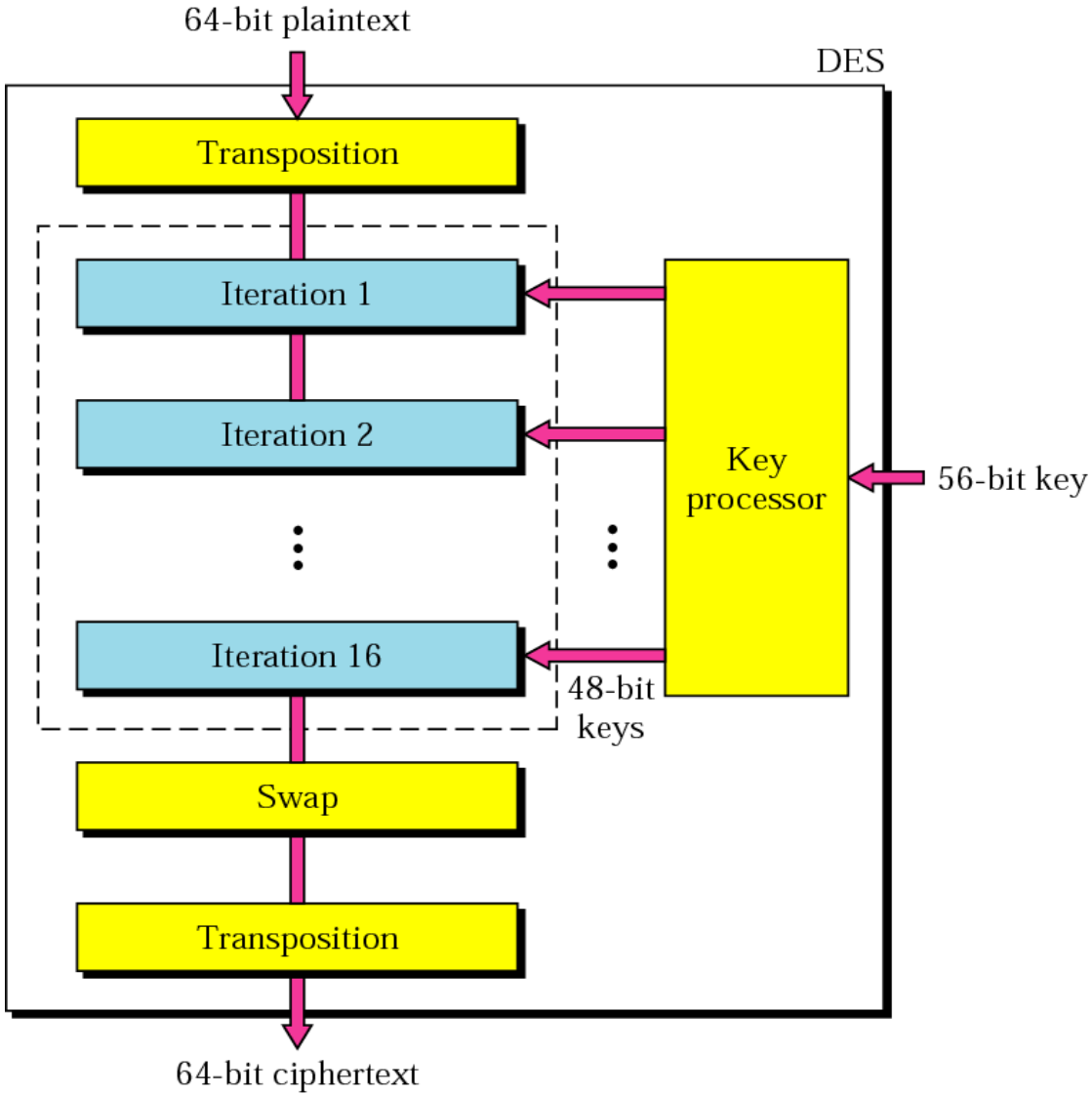
Symmetric Encryption : DES

- Data Encryption Standard
- It was developed in the 1970s by the National Bureau of Standards with the help of the National Security Agency.
- It is officially described in **FIPS PUB 46**
- Federal Information Processing Standards Publications
- The cryptographic algorithm specified in this standard transforms a 64-bit binary value into a unique 64-bit binary value based on a 56-bit variable.
- There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used

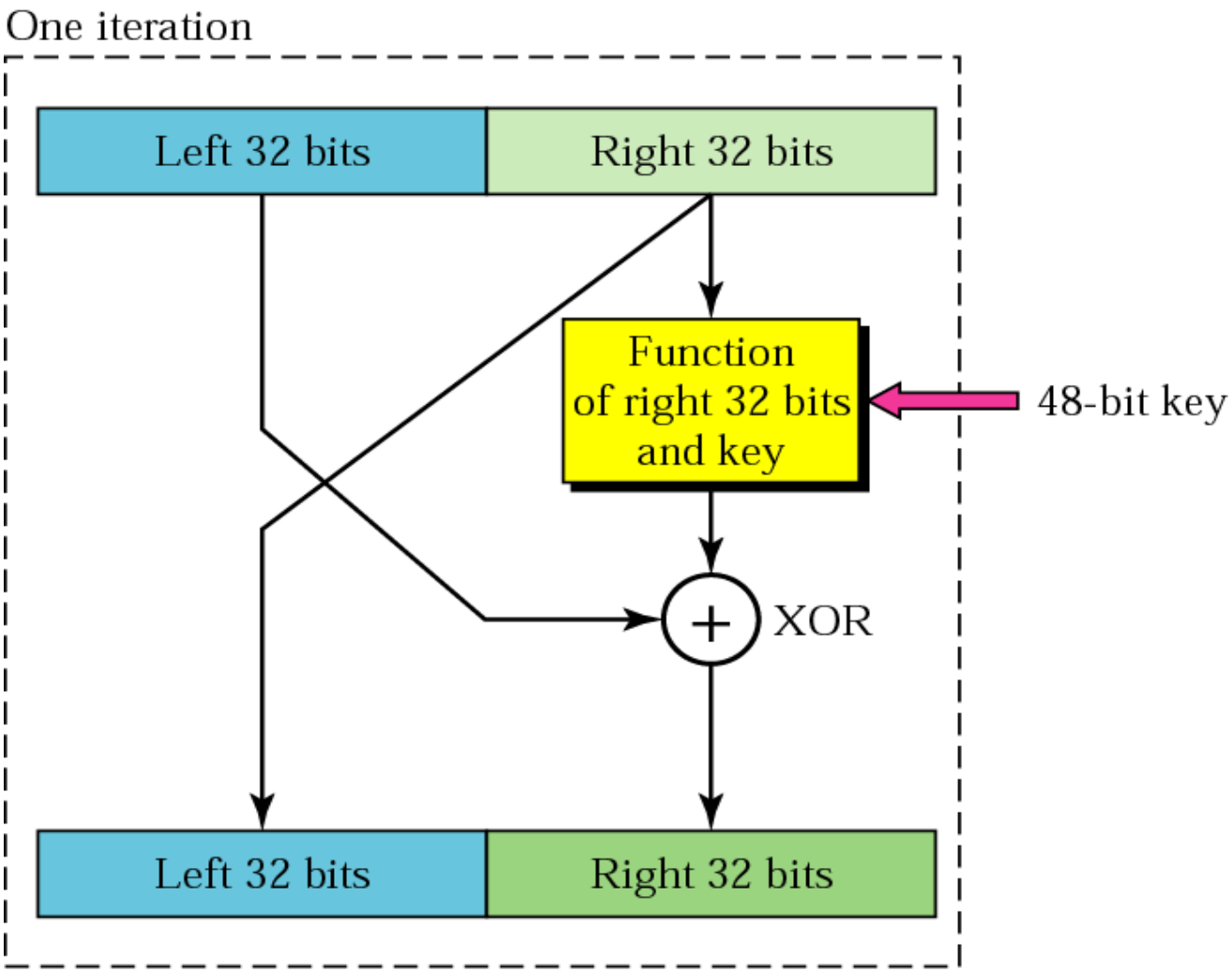
DES: Data Encryption Standard



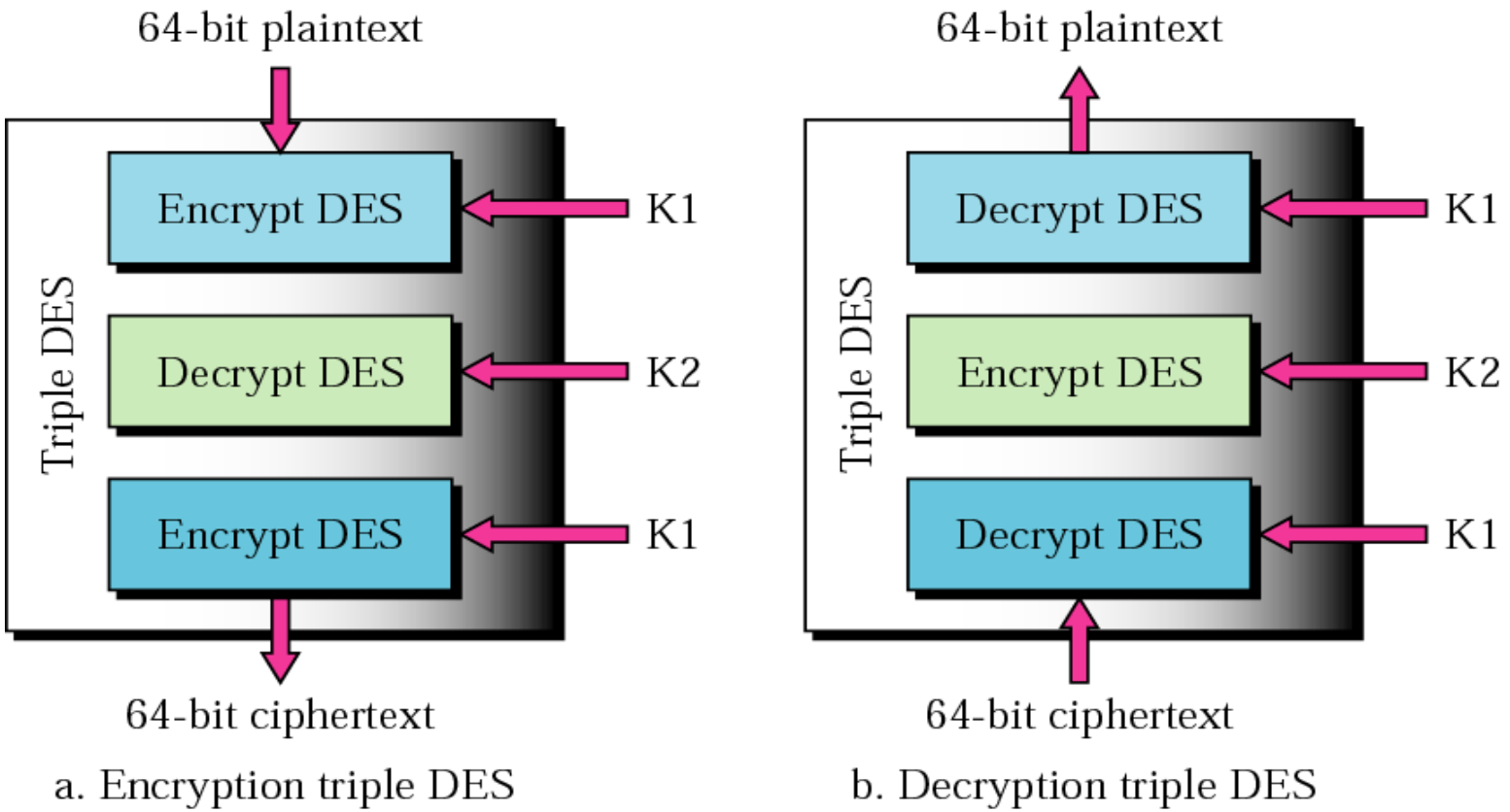
Data Encryption Standard: General Scheme



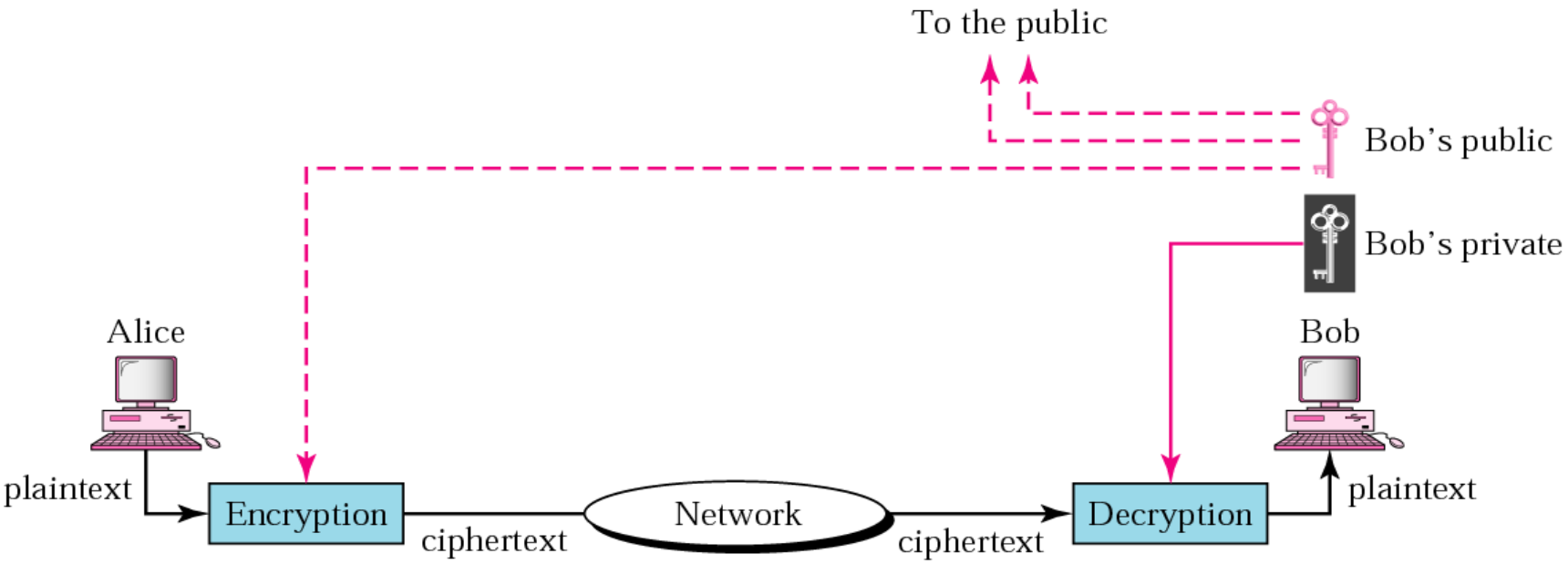
DES: Iteration Block



Triple DES



Cryptography：Public- Key Cryptography



RSA Algorithm : Key Generation

1. Generate Two Large Prime Numbers, *p* and *q*
2. Let *n* = *pq*
3. Let *m* = *(p-1)(q-1)*

4. Choose a small number *e* (1 < e < m), coprime to *m* such that *GCD(e, m)* = 1.

5. Find *d*, such that *de % m = 1.* Where *d = (1 + m * i)/e*

6. Publish *e* and *n* as the Public Key
7. Keep *d* and *n* as the Private Key

Key Generation : Steps

1. Generate Two Large Prime Numbers, *p* and *q*
   Let p =7 and q = 19

2. Let *n* = *pq*
   *n = 7 * 19*
   n = 133

3. Let m = (p-1)(q-1)
   m = (7-1) (19-1)
   m = 6 * 18
   m = 108

Key Generation : Steps

4. Choose a small number *e* (1 < e < m), coprime to *m* such that *GCD(e, m)* = 1

   e = 2 => GCD(e, 108) = 2 (no)
   e = 3 => GCD(e, 108) = 3 (no)
   e = 4 => GCD(e, 108) = 4 (no)
   e = 5 => GCD(e, 108) = 1 (yes!) => GCD(e, m) = 1

5. Find *d*, such that *de % m = 1.* Where *d = (1 + m * i)/e*
   [Go through Values of *i* until Integer Solution is Found]

   i = 0 => d = 1 / 5 (No Integer)
   i = 1 => d = 109 / 5 (No Integer)
   i = 2 => d = 217 / 5 (No Integer)
   i = 3 => d = 325 / 5 = 65 (Yes !! Satisfies the Condition)

6. (n, e) = (133,5) AND (n,d) = (133,65)

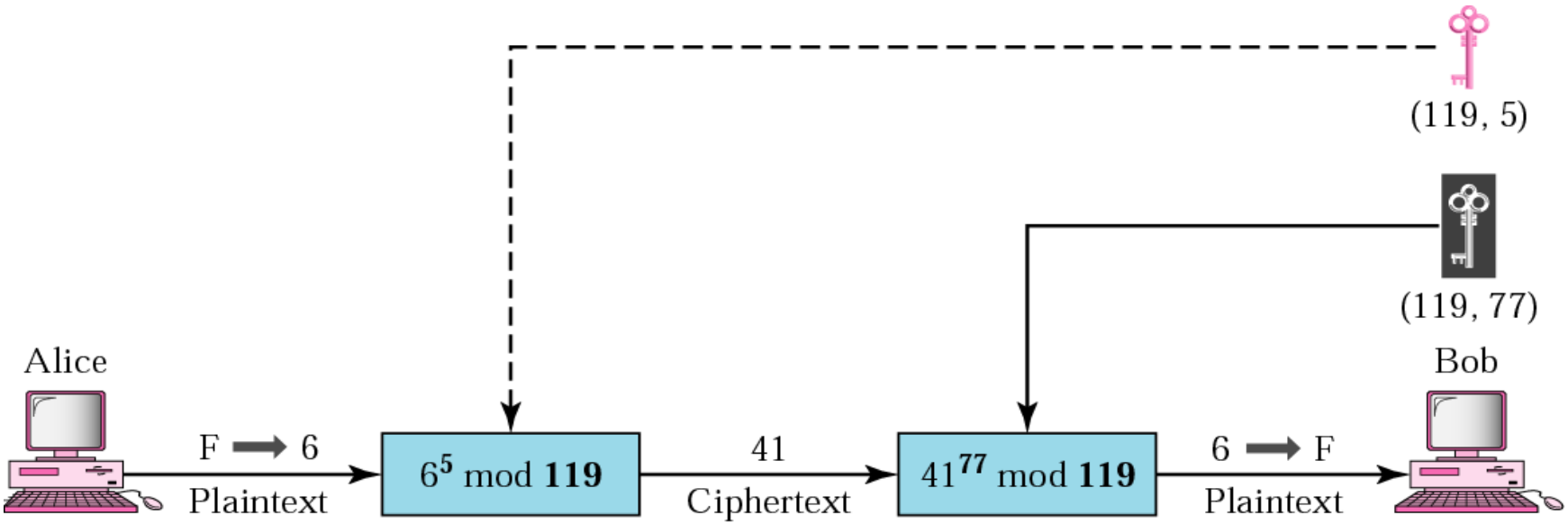
RSA Algorithm: Encryption/Decryption

- Public Key Pair => (n, e) => (119,5)
- Private Key Pair => (n, d) => (119,77)
- Encryption Algorithm

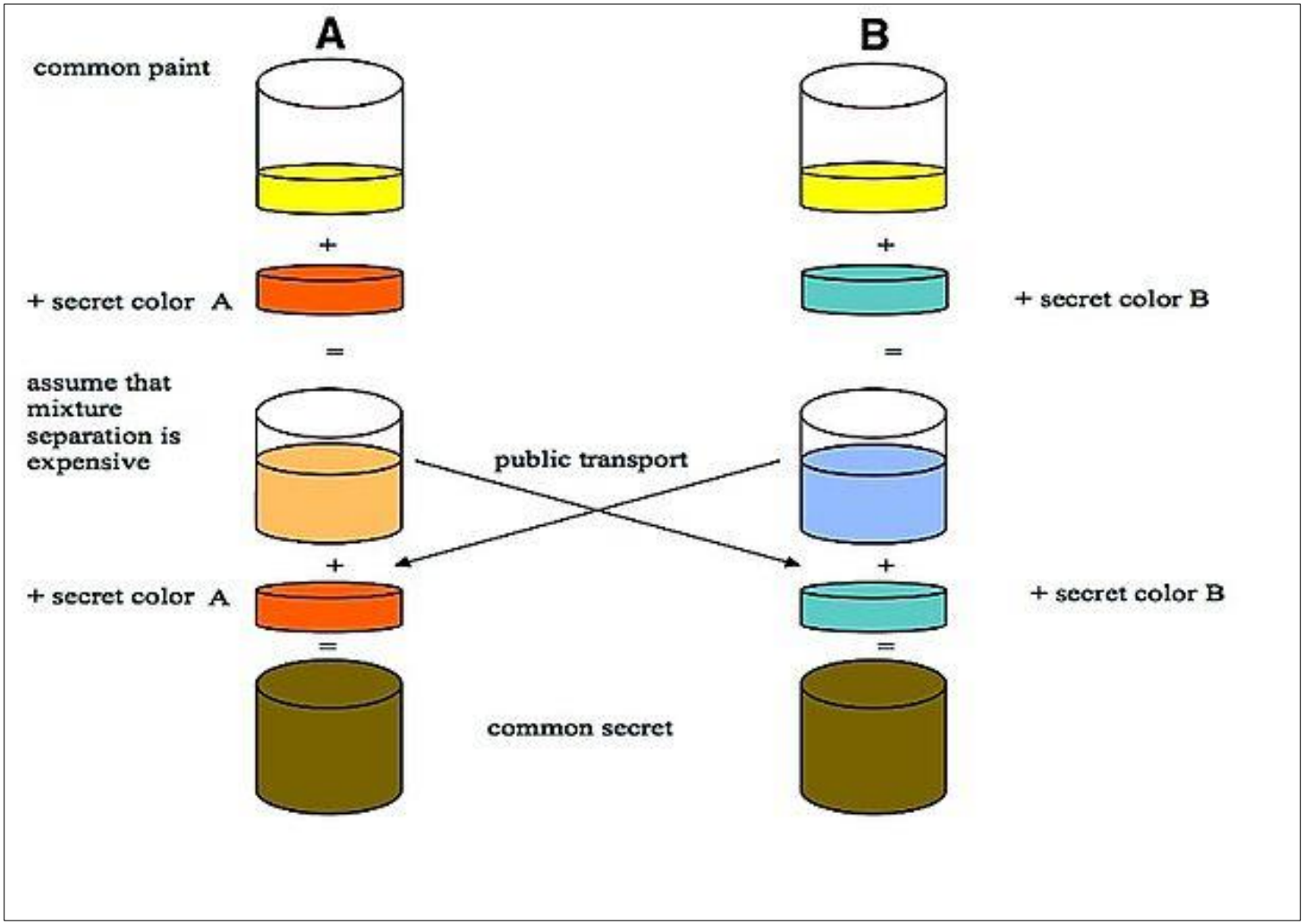
  $C = P^e \% n$
- Decryption Algorithm

  $P = C^d \% n$

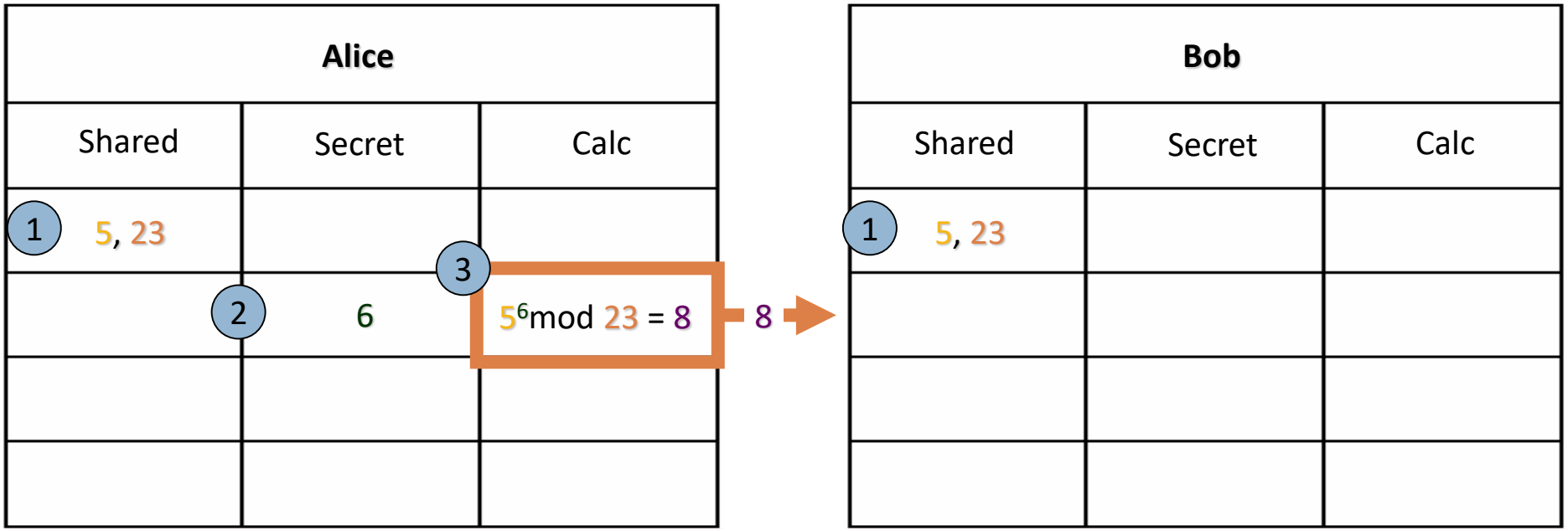
Public-Key Cryptography : RSA (Rivest, Shamir, Adleman)



Diffie-Hellman : Key Exchange Protocol Analogy

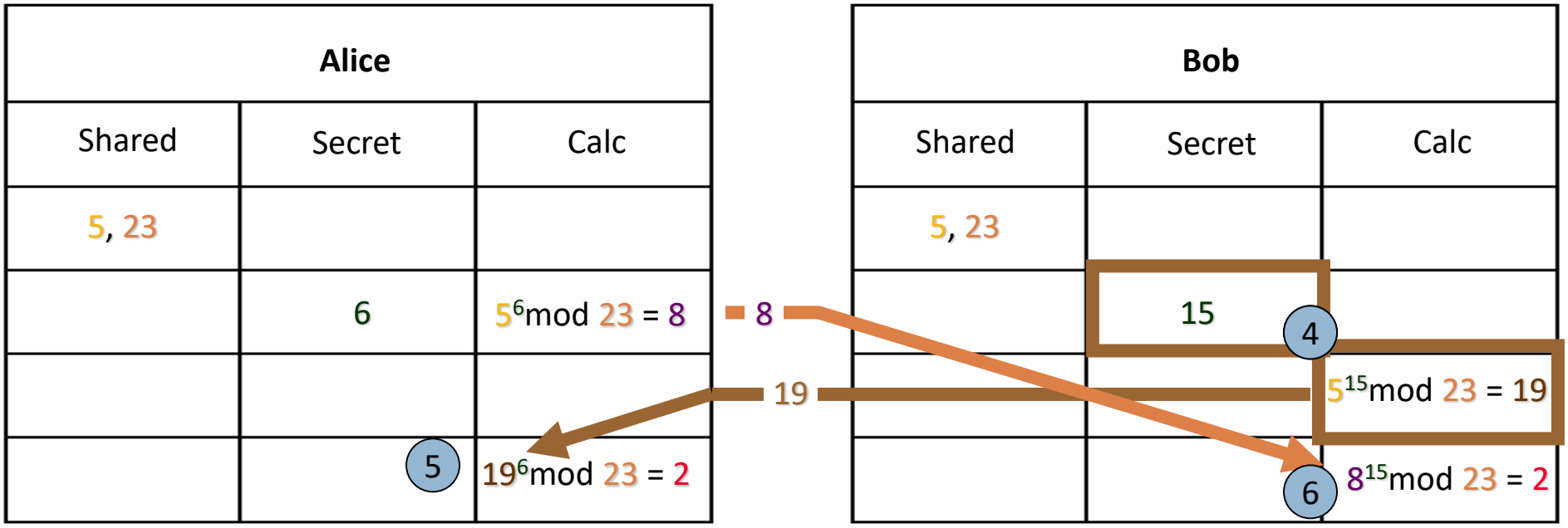


Diffie-Hellman : Step by Step Illustration



1. Alice and Bob agree to use the same two numbers. For example, the Base Number g=5 and Prime Number P =23
2. Alice now chooses a Secret Number x=6.
3. Alice performs the DH algorithm: g^x MOD P = (5^6 modulo 23) = 8 (Y) and sends the New number 8 (Y) to Bob

Diffie-Hellman : Step by Step Illustration



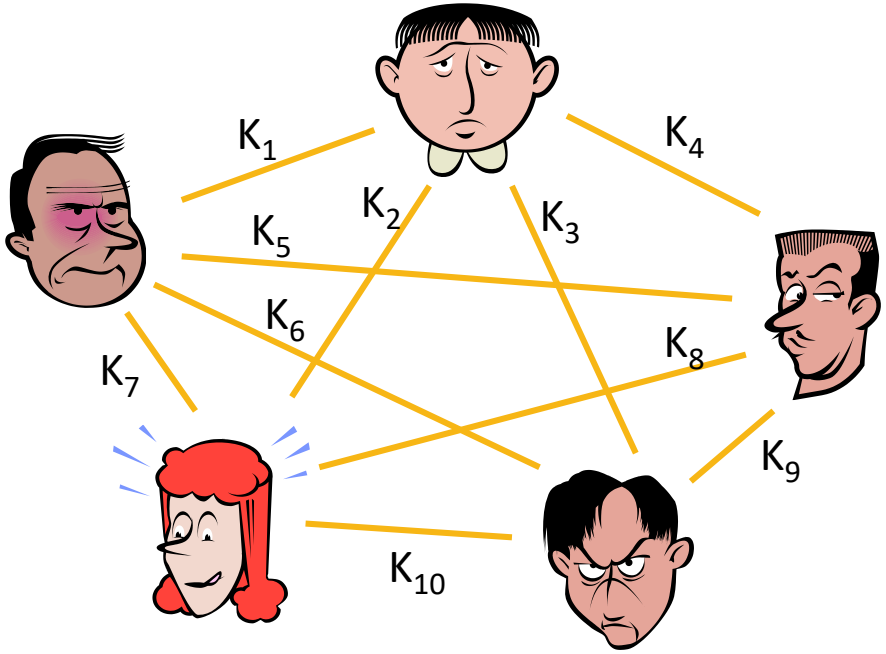
4. Meanwhile Bob has also chosen a Secret Number x=15, performed the DH algorithm: g^x modulo P = (5^{15} MOD 23) = 19 (Y) and sent the new number 19 (Y) to Alice.

5. Alice now computes Y^x modulo P = (19^6 MOD 23) = 2.

6. Bob now computes Y^x modulo P = (8^{15} MOD 23) = 2.

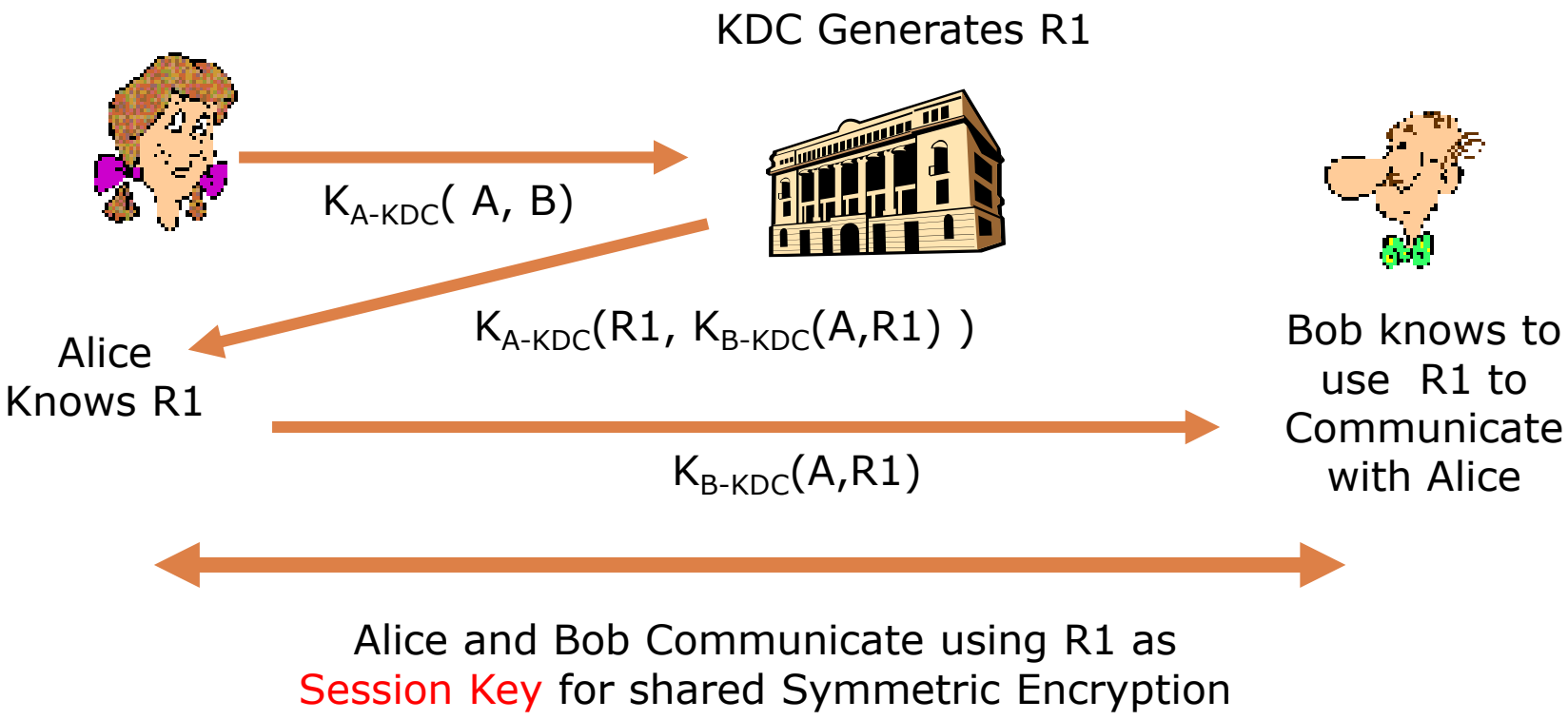
The Result (2) is the same for both Alice and Bob. This number can now be used as a shared secret key by the encryption algorithm.

Symmetric Key Management



- How to reduce the Number of Shared Keys in the System ?
  - ✓ Centralize Key Management via KDC
  - ✓ Public Key Management via CA

KDC : Operations



KDC: Operations

- Alice sends a message $K_{A\text{-}KDC}(A,B)$ to the KDC saying She (*A*) wants to communicate with Bob (*B*).
- The KDC, knowing $K_{A\text{-}KDC}$, decrypts $K_{A\text{-}KDC}(A,B)$.
- The KDC then authenticates Alice and generates a Random Number ***R1***
- The Message from the KDC to Alice is thus $K_{A\text{-}KDC}(R1, K_{B\text{-}KDC}(R1))$.
- $K_{B\text{-}KDC}(A,R1)$ => A Pair Values ***A, R1*** Encrypted by the KDC using Bob's key.
- Alice receives the message from the KDC, verifies the **nonce**, extracts *R1* from the message and saves it.
- Alice now knows the one-time session key, ***R1***
- Alice also extracts $K_{B\text{-}KDC}(A,R1)$ and forwards this to Bob.
- Bob decrypts the received message, $K_{B\text{-}KDC}(A,R1)$, using $K_{B\text{-}KDC}$ and extracts A and *R1*

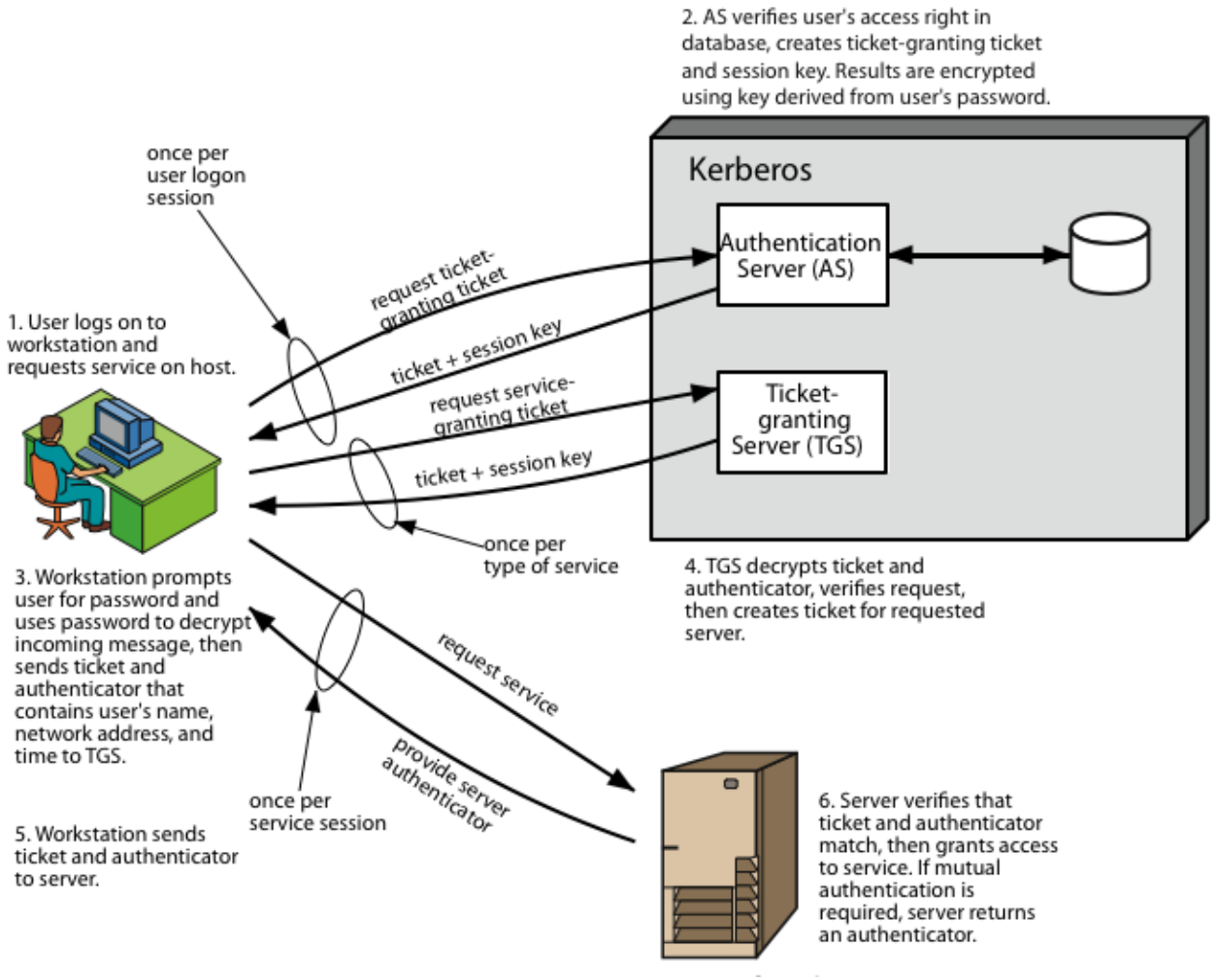
Kerberos: Meaning ??

- In Greek Mythology, *Kerberos* (or *Cerberus*) is the Horrible three-headed guard dog of Hades.
- Hades was the Ancient Greek god of the Underworld.
- The Underworld is a region which is thought to be under the surface of the Earth.

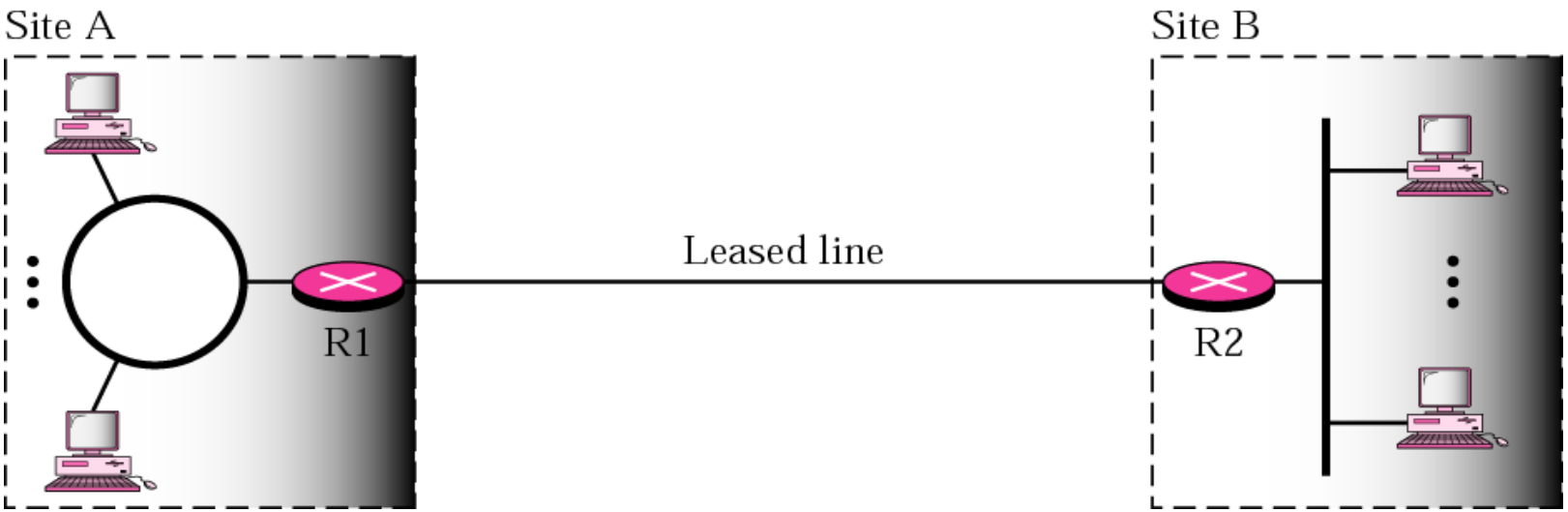
Kerberos: What it is ??

- Kerberos is an authentication service developed as part of Project Athena @ MIT.
- It is one of the best known and most widely implemented **Trusted Third Party** key Distribution Systems.
- Designed to Provide Strong Authentication for Client/Server Applications by using Secret-Key Cryptography.
- It uses **Strong Cryptography** so that a Client can Prove its Identity to a Server (and vice versa) across an Insecure Network Connection.
- Two Versions of Kerberos are in Common Use: v4 & v5.

Kerberos 4: Overview



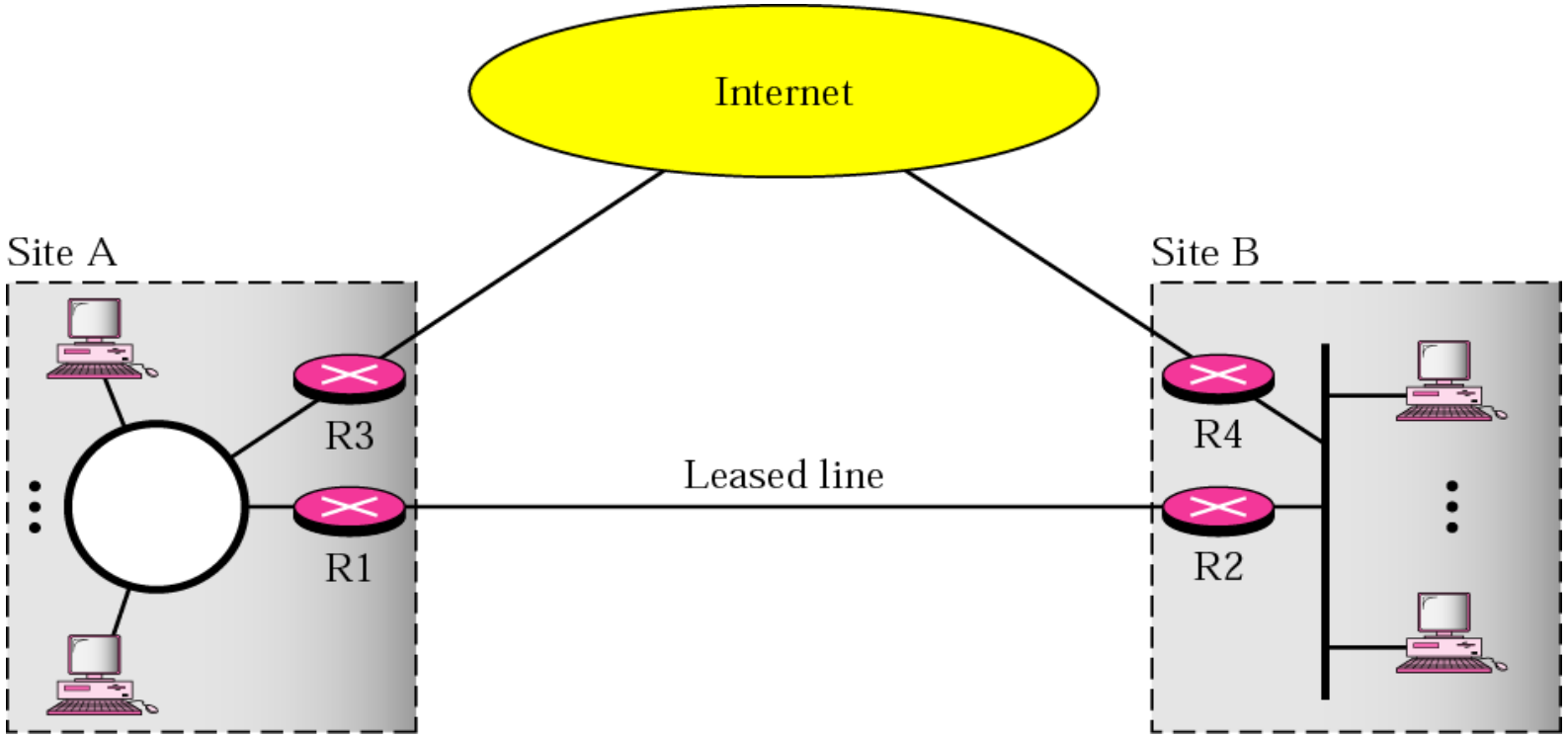
Private Networks



Hybrid Networks : What it is ??

- Two Links => Private and Public
- Private Link => Leased Line or Optical Fiber
- Private Link for Intranet
- Public Link for Internet.
- All Intraorganization data are routed through the Private Link.
- All Interorganization data are routed through the Public Link.

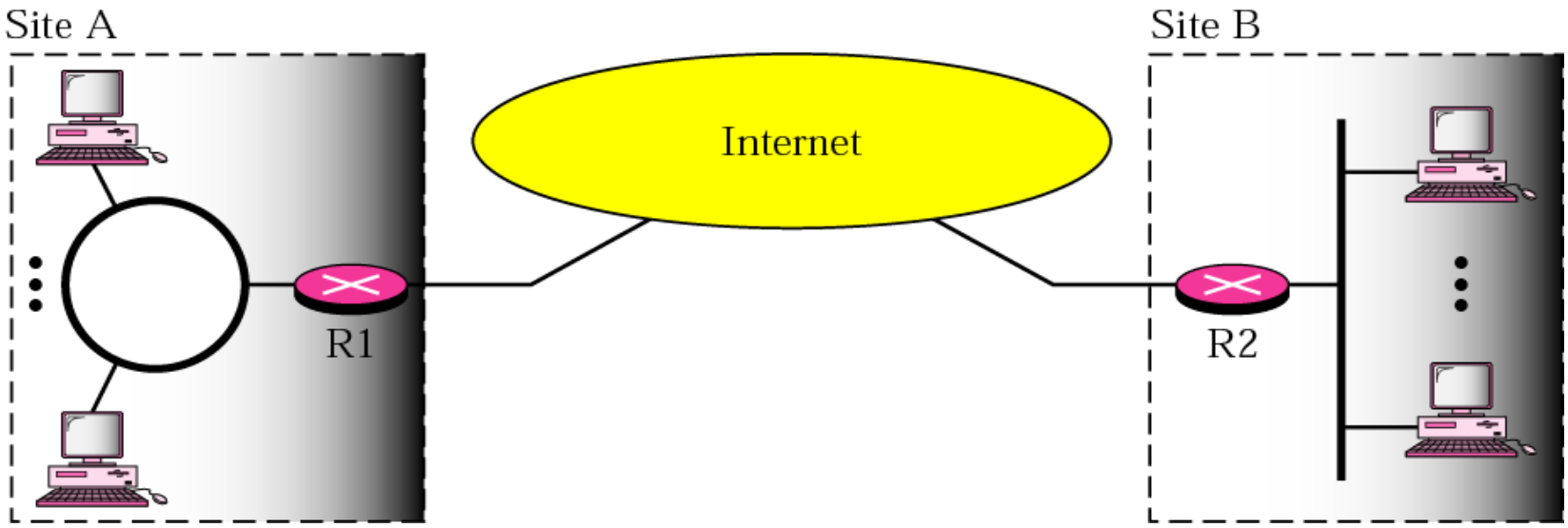
Hybrid Networks



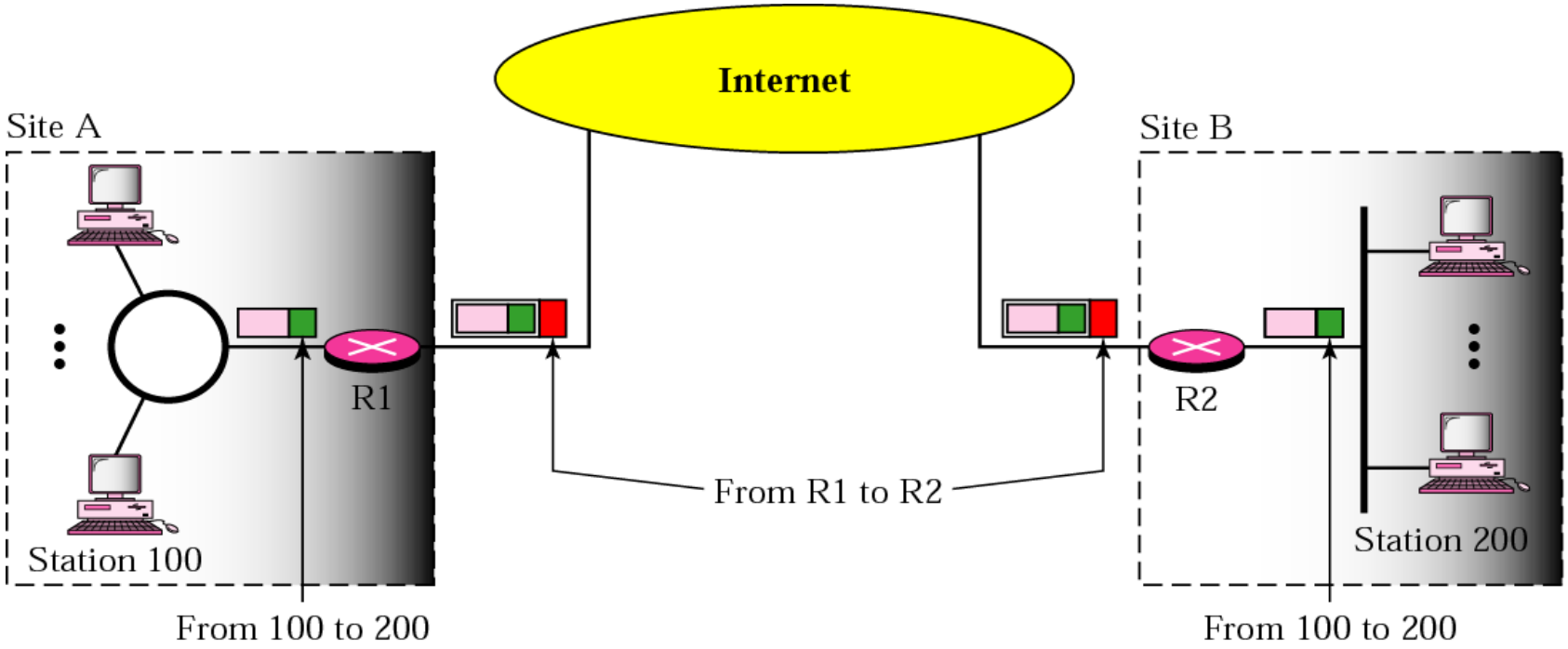
VPN : Virtual Private Networks

- Both Private and Hybrid Networks are Expensive.
- Solution to use global Internet for both Private and Public Communication => VPN
- VPN Creates a Network that is Private but Virtual.
- It is Private because it guarantees Privacy inside the Organization.
- It is Virtual because it does not use Real Private WANs.
- The Network is Physically Public but Virtually Private.
- VPN Use IPSec in the Tunnel Mode to Provide Authentication, Integrity and Privacy.

VPN : Virtual Private Networks



Addressing in VPN



To use IPSec in Tunneling mode VPN need to use Two sets of Addressing

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.

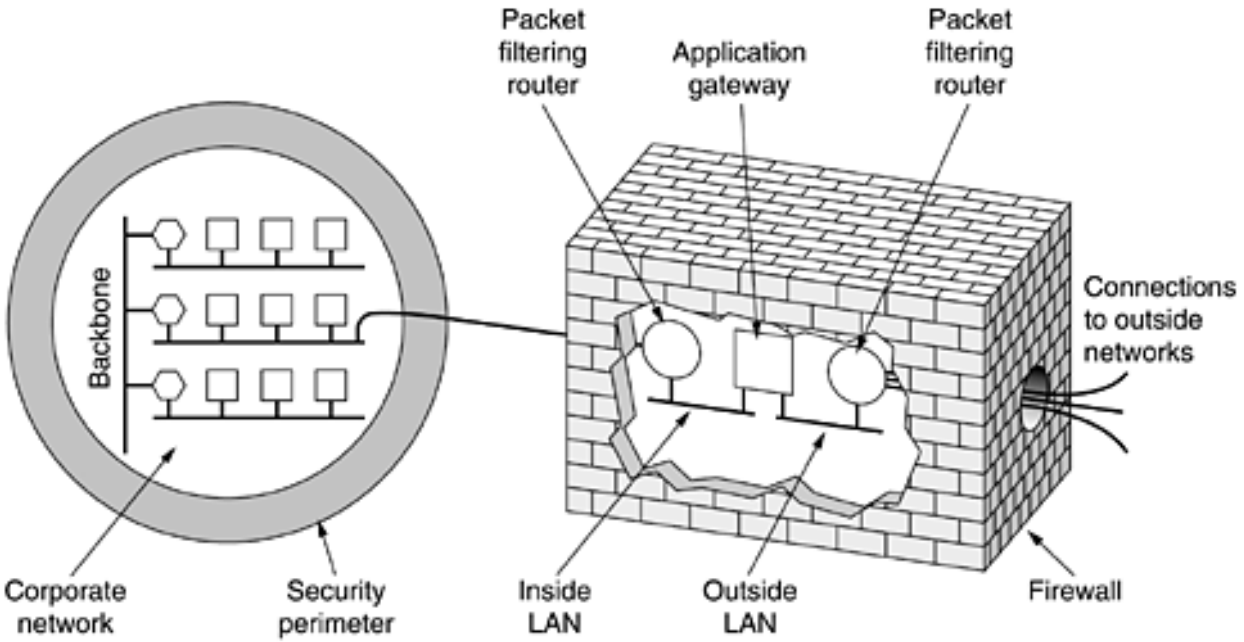
2. Application Level Gateway

- 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