RV College of Engineering®

Go, change the world

NETWORK SECURITY

Unit – 1

20MCA242

Need for Security in the Networked World

- For a long time, security was largely ignored in the community
  - The computer industry was in “survival mode”, struggling to overcome technological and economic hurdles
  - As a result, a lot of corners were cut and many compromises made
  - There was lots of theory, and even examples of systems built with very good security, but were largely ignored or unsuccessful

Contents

- Need for Security
- Computer Security Concepts
- OSI Security Architecture
- Security Attacks
- Security Services
- Security Mechanisms
- A Model for Network Security
- Standards

Contents Contd…

- Number Theory
- Divisibility
- Greatest Common Divisor
- Euclid Algorithm
- Modular Arithmetic
- Remainder Arithmetic
- General Principles
- Euler’s theorem

The Definition of Security

- *Security* is a state of well-being of information and infrastructures in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable
- Security rests on Confidentiality, Authenticity, Integrity, and Availability

Two Related Terms

- **Information security:** Preservation of confidentiality, integrity, and availability of information. In addition, other properties—such as authenticity, accountability, non-repudiation, and reliability—can also be involved.
- **Network security:** Protection of networks and their services from unauthorized modification, destruction, or disclosure and provision of assurance that the network performs its critical functions correctly and that there are no harmful side effects.

Essential Network Security Components

Confidentiality:

- Data Confidentiality Concealment of information or resources.

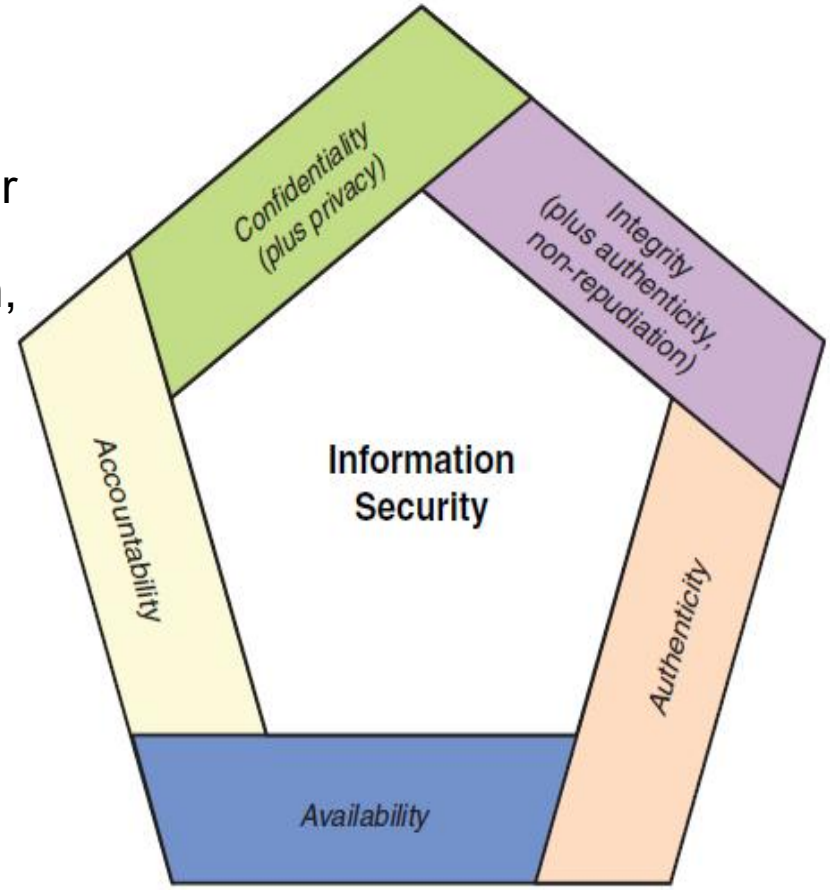
ie Only sender, intended receiver should "understand" message contents

- Privacy: Individual control for collection, storage, disclosure

Authenticity: Identification and assurance of the origin of information.

Integrity: Trustworthiness of data or resources in terms of preventing improper and unauthorized changes.

Availability: Ability to use the information or resource desired.



OSI Security Architecture

- ITU-T X.800 Security Architecture for OSI

Focuses on

- **Security Attacks:** Any Action that compromises the security of information owned by the organization

- **Security Mechanism:** A process/device that is designed to detect, prevent or recover from security attack

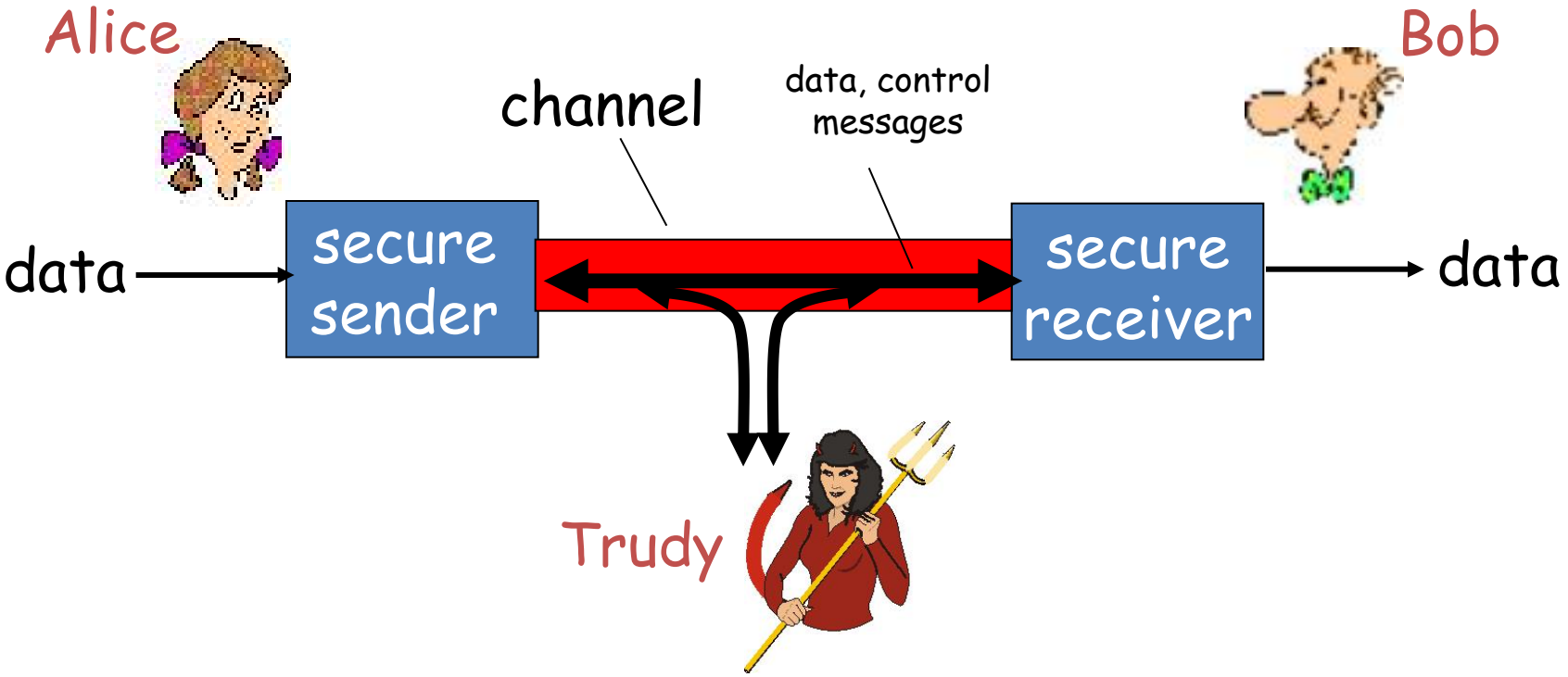
- **Security Services:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization

Security Threats and Attacks

- A threat/vulnerability is a *potential* violation of security.
  - Flaws in design, implementation, and operation.
- An attack is any *action* that violates security.
  - Active *adversary*
- An attack has an implicit concept of "intent"
  - Router mis-configuration or server crash can also cause loss of availability, but they are not attacks

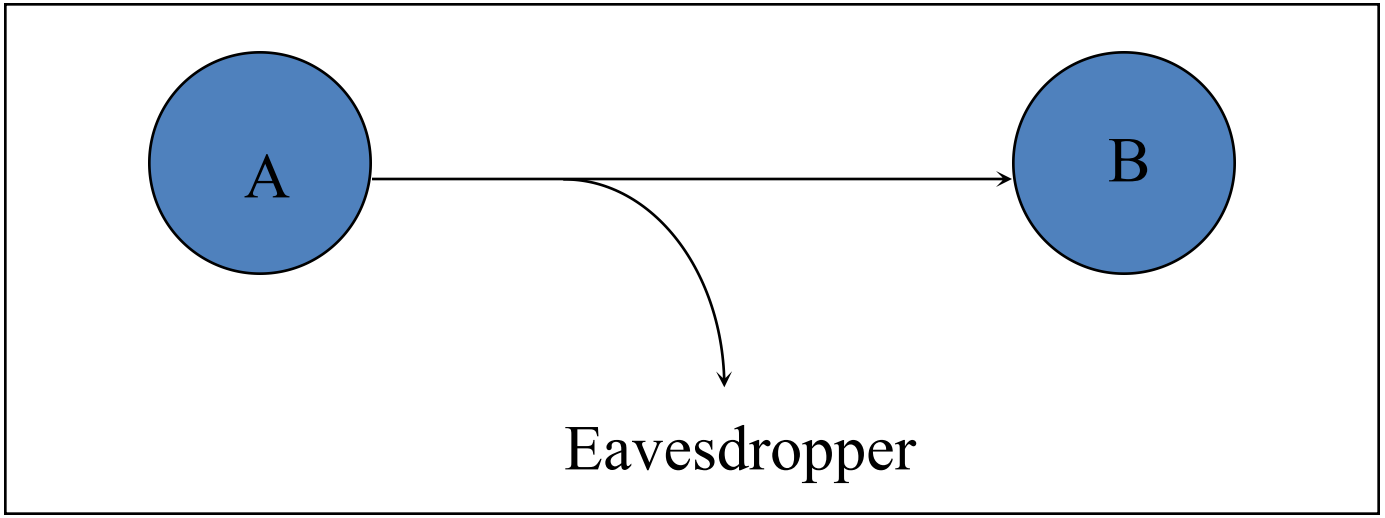
Friends and enemies: Alice, Bob, Trudy

- well-known in network security world
- Bob, Alice (lovers!) want to communicate "securely"
- Trudy (intruder) may intercept, delete, add messages



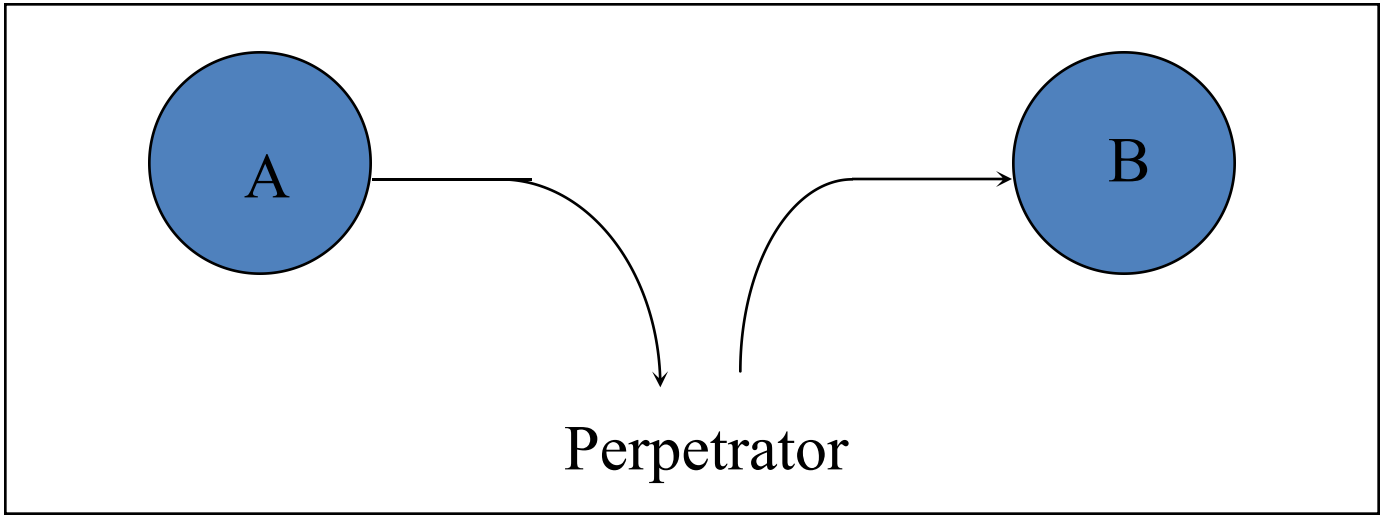
Eavesdropping - Message Interception (Attack on Confidentiality)

- Unauthorized access to information
- Packet sniffers and wiretappers
- Illicit copying of files and programs



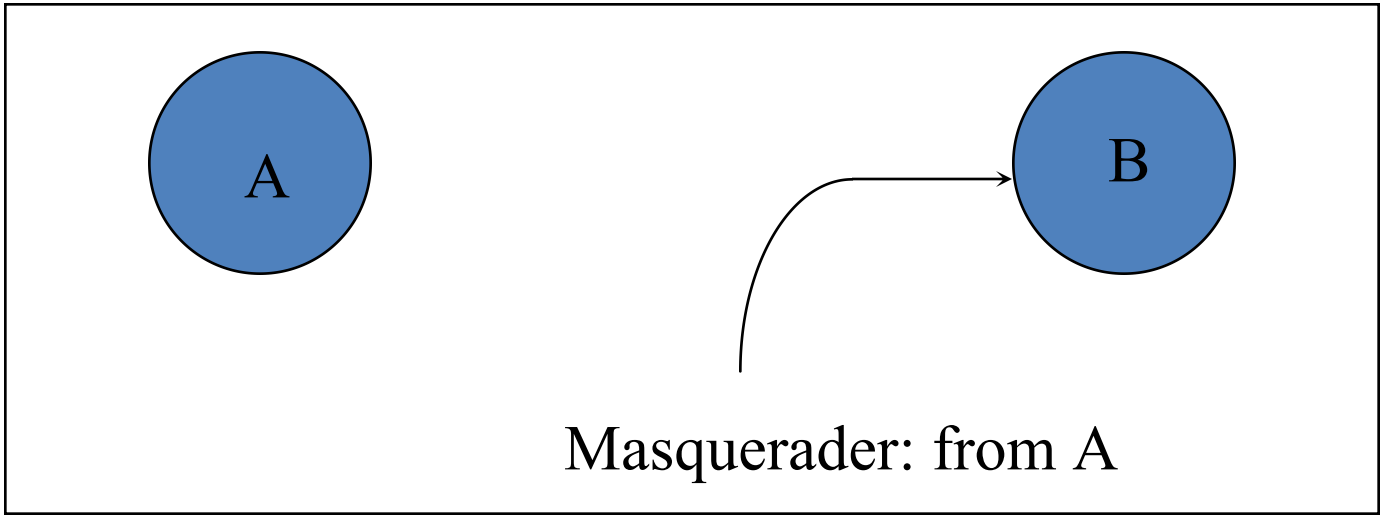
Integrity Attack - Tampering With Messages

- Stop the flow of the message
- Delay and optionally modify the message
- Release the message again



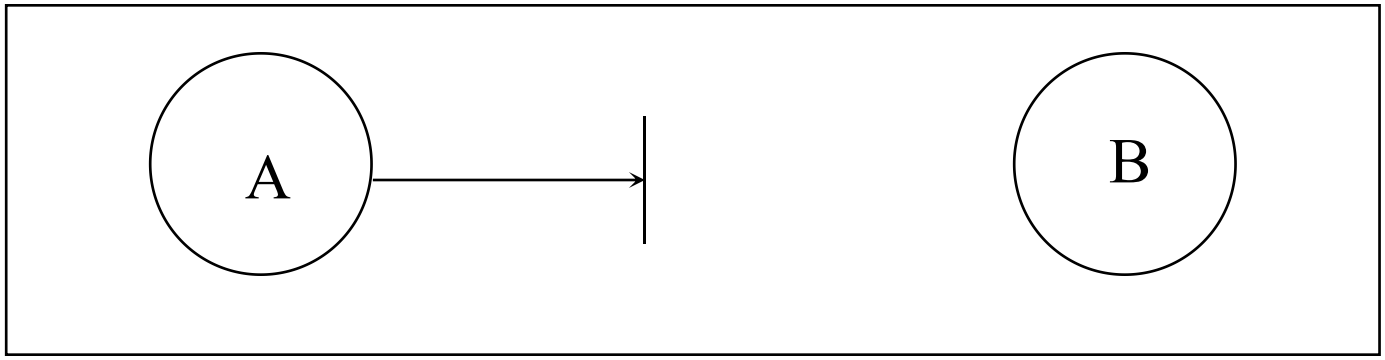
Authenticity Attack - Fabrication

- Unauthorized assumption of other's identity
- Generate and distribute objects under this identity



Attack on Availability

- Destroy hardware (cutting fiber) or software
- Modify software in a subtle way (alias commands)
- Corrupt packets in transit



- Blatant *denial of service* (DoS):
  - Crashing the server
  - Overwhelm the server (use up its resource)

Classification of Security Attacks

- **Passive attacks** - eavesdropping on, or monitoring of, transmissions to:
  - obtain message contents, or
  - monitor traffic flows
- **Active attacks** – modification of data stream to:
  - masquerade of one entity as some other
  - replay previous messages
  - modify messages in transit
  - denial of service

Security Policy and Mechanism

- Policy: a statement of what is and is not allowed.
- Mechanism: a procedure, tool, or method of enforcing a policy.
- Security mechanisms implement functions that help *prevent, detect, and respond to recovery from* security attacks.
- Security functions are typically made available to users as a set of security services through APIs or integrated interfaces.
- Cryptography underlies many security mechanisms.

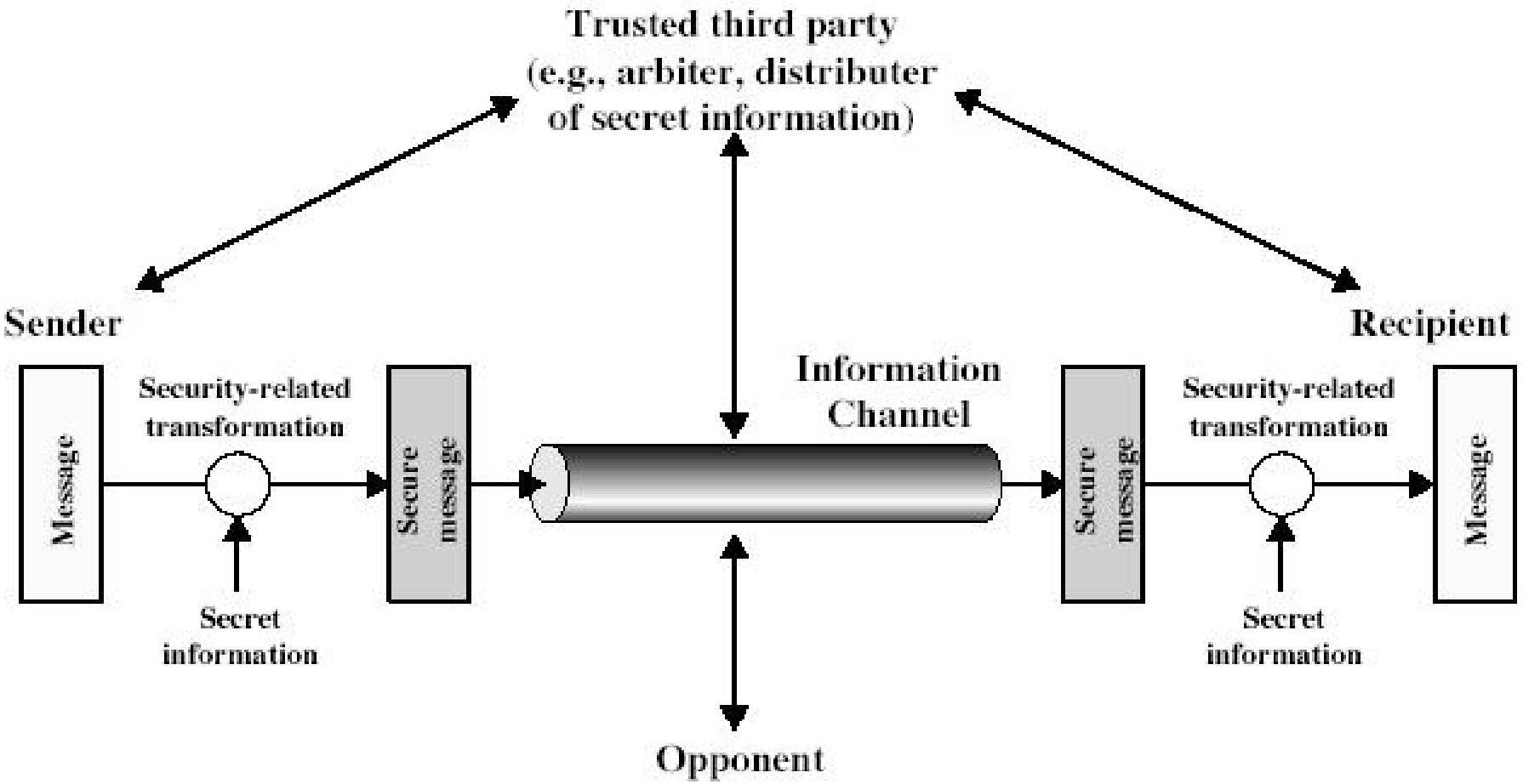
Security Services (X.800)

- **Authentication** - assurance that the communicating entity is the one claimed
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication

Security Mechanisms (X.800)

- Specific security mechanisms:
  - Encipherment
  - Digital signatures
  - Access controls
  - Data integrity
  - Authentication exchange
  - Traffic padding
  - Routing control
  - Notarization
- Pervasive security mechanisms:
  - Trusted functionality
  - Security labels
  - Event detection
  - Security audit trails
  - Security recovery

Model for Network Security



Mechanisms

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

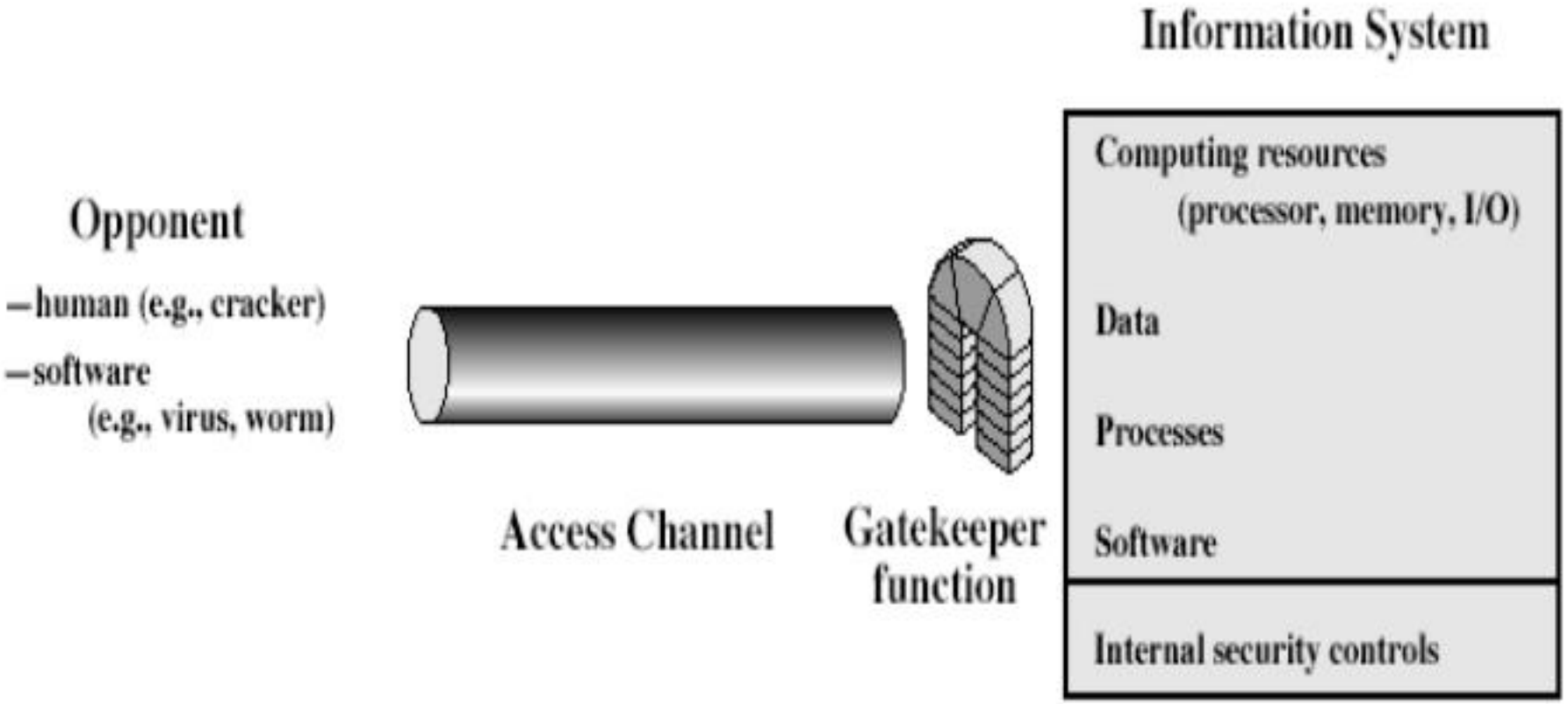
Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

Model for Network Security

- Using this model requires us to:
  - Design a suitable algorithm for the security transformation
  - Generate the secret information (keys) used by the algorithm
  - Develop methods to distribute and share the secret information
  - Specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



Model for Network Access Security

- Using this model requires us to:
  - Select appropriate gatekeeper functions to identify users
  - Implement security controls to ensure only authorised users access designated information or resources
- Trusted computer systems can be used to implement this model

How to Make a System Trustworthy

- Specification What to do?
  - A statement of desired functions
- Design How to do?
  - A translation of specifications to a set of components
- Implementation Do it
  - Realization of a system that satisfies the design
- Assurance Test and Validate
  - The process to ensure that the above steps are carried out correctly
  - Inspections, proofs, testing, etc.

The Security Life Cycle

- The *iterations* of
  - Threats
  - Policy
  - Specification
  - Design
  - Implementation
  - Operation and maintenance

1.2 The Value of Standards and Best Practices Documents

TABLE 1.1 Important Best Practices and Standards Documents

Source	Title	Date
ISF	Standard of Good Practice for Information Security	2016
ISO	ISO 27002: Code of Practice for Information Security Controls	2013
NIST	Framework for Improving Critical Infrastructure Cybersecurity	2017
Center for Internet Security (CIS)	CIS Critical Security Controls for Effective Cyber Defense Version 7	2018
ISACA	COBIT 5 for Information Security	2012
PCI Security Standards Council	Data Security Standard v3.2: Requirements and Security Assessment Procedures	2016

Symmetric Encryption and Message Confidentiality

Topic Outline

1. Symmetric Encryption Principles
2. Symmetric Block Encryption Algorithms
3. Stream Ciphers and RC4

Symmetric Encryption Principles

- An encryption scheme has five ingredients:
  - Plaintext
  - Encryption algorithm
  - Secret key
  - Ciphertext
  - Decryption algorithm
- Security depends on the secrecy of the key, not the secrecy of the algorithm

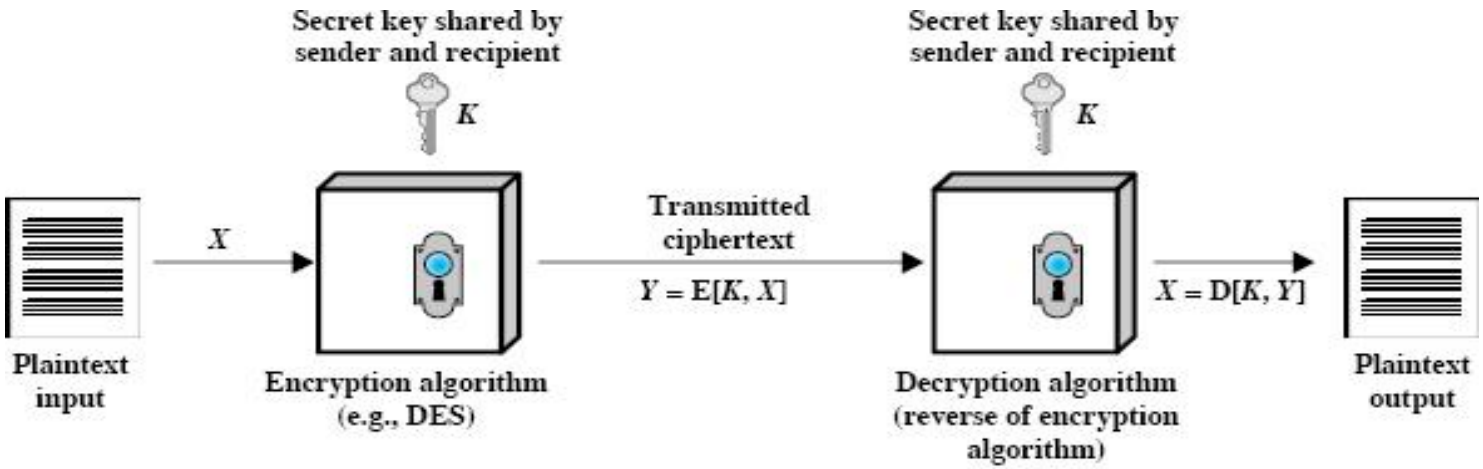


Figure 2.1 Simplified Model of Symmetric Encryption

Cryptography

- Classified along three independent dimensions
  - The type of operations used for transforming plaintext to ciphertext
    - Substitution
    - Transposition
  - The number of keys used
    - Symmetric (single key)
    - Asymmetric (two-keys, or public-key encryption)
  - The way in which the plaintext is processed
    - Block cipher
    - Stream cipher

Table 2.1 Types of Attacks on Encrypted Messages

Type of Attack	Known to Cryptanalyst
Ciphertext only	•Encryption algorithm •Ciphertext to be decoded
Known plaintext	•Encryption algorithm •Ciphertext to be decoded •One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	•Encryption algorithm •Ciphertext to be decoded •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Table 2.2 Average Time Required for Exhaustive Key Search

Key Size (bits)	Number of Alternative Keys	Time required at 1 encryption/μs	Time required at 10^6 encryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years

Feistel Cipher Structure

- Virtually all conventional block encryption algorithms, including DES, have a structure first described by Horst Feistel of IBM in 1973
- The realization of a Feistel Network depends on the choice of the following parameters and design features (see next slide):

Feistel Cipher Structure

- **Block size**: larger block sizes mean greater security
- **Key Size**: larger key size means greater security
- **Number of rounds**: multiple rounds offer increasing security
- **Subkey generation algorithm**: greater complexity will lead to greater difficulty of cryptanalysis
- **Round function**: greater complexity means greater resistance of cryptanalysis
- **Fast software encryption/decryption**: the speed of execution of the algorithm becomes a concern
- **Ease of analysis**

Symmetric Encryption Algorithms

- Processes the plaintext input in fixed-size blocks and produces a block of ciphertext of equal size for each plaintext block.
- Focuses on three symmetric block ciphers:
  1. Data Encryption Standard (DES)
  2. Triple DES (3DES)
  3. Advanced Encryption Standard (AES)

1. Data Encryption Standard (DES)

- The most widely used encryption scheme.
- NIST (National Institute of Standards & Technology), as FIPS PUB 46 (Federal Information Processing Standards).
- The algorithm is referred to the Data Encryption Algorithm (DEA).
- DES is a block cipher.
- Minor variation of Feistel.
- It has 16 rounds of processing.
- The plaintext is processed in 64-bit blocks.
- The key is 56 bits in length, which is divided into 16 subkeys, each one is used for each round.
- Decryption:
  - Use ciphertext as input to DES.
- Use subkeys K_i in reverse order till K is reached. i.e K_{16} to K_2, K_1.

- With key length of 56bits, there are $2^{56} = 7.2 \times 10^{16}$ possible keys.
- Here, brute-force attack appears impractical. How?
- Trying each key per microsecond would take more than 10 thousand years to break cipher.
- So? DES is secure?
- Yes or No?
- DES finally and definitively proved insecure in July 1998, when the Electronic Frontier Foundation (EFF98) announced that it had broken a DES encryption using a special-purpose "DES Cracker" machine that was built for less than $250,000.
- The attack took less than 3 days to break cipher.
- Problem?
- Solution?
- So a 128-bit key is guaranteed to result in an algorithm that is unbreakable by brute force or EFF98.
- 128-bit key would take over 10^{18}years to break the code using the EFF cracker.
- This is shown in next figure.

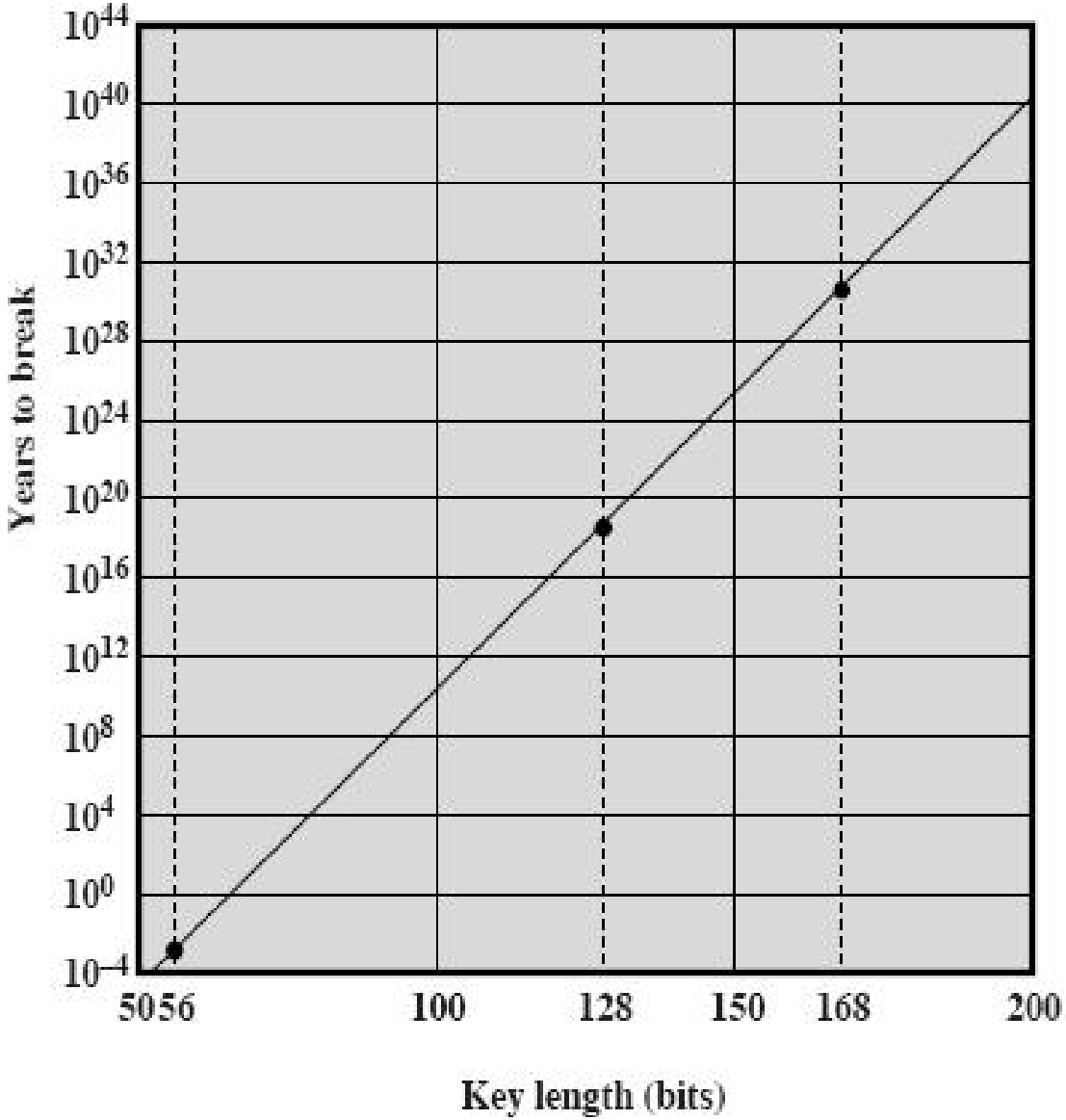
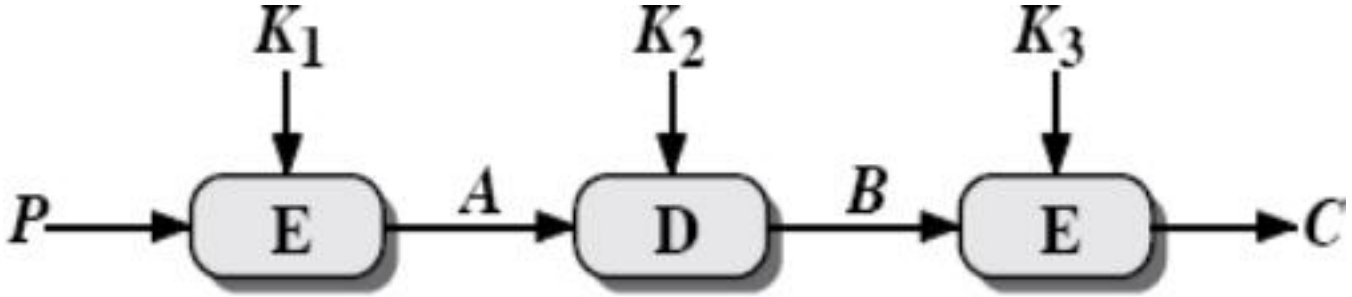


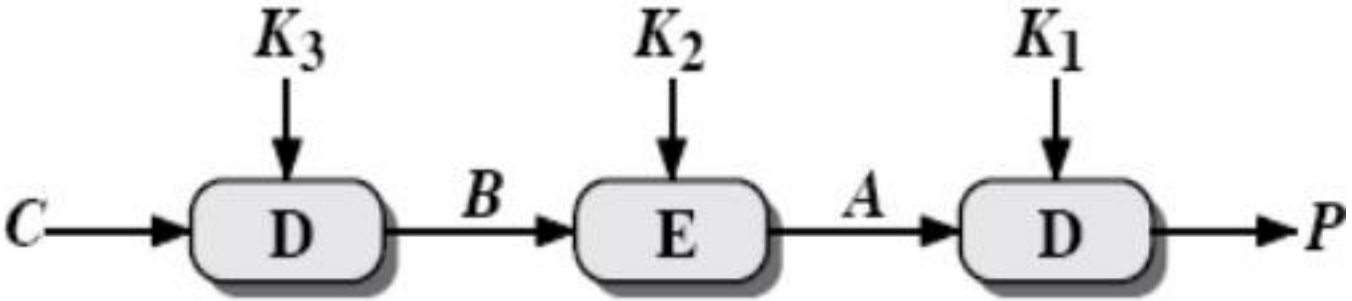
Figure 2.3 Time to Break a Code (assuming 10^6 decryptions/μs)

2. Triple DES

- Triple DES(3DES) was first standardized for use in financial applications in ANSI standard X9.17 in 1985.
- 3DES was incorporated as part of the Data Encryption Standard in 1999, with the publication of FIPS PUB 46-3.
- Guidelines for 3DES:
  - 3DES is the FIPS approved symmetric encryption algorithm.
  - The original DES, which uses a single 56-bit key should support 3DES.
  - Government organizations with legacy DES systems are encouraged to transition to 3DES.
  - 3DES and the Advanced Encryption Standard (AES) will coexist as FIPS-approved algorithms, allowing for a gradual transition to AES.



(a) Encryption



(b) Decryption

Figure 2.4 Triple DES

$$C = E[K_3, D[K_2, E[K_1, P]]]$$

$$P = D[K_1, E[K_2, D[K_3, C]]]$$

- Encryption:
- Decryption:

$$C = E[K_3, D[K_2, E[K_1, P]]] = E[K,P)$$

  - C = ciphertext
  - P = plaintext
  - E[K, X] = encryption of X using key K
  - D[K, Y] = decryption of Y using key K
- Use three keys and three executions of the DES algorithm.
- Encrypt-Decrypt-Encrypt.
- Effective key length of 168 bits.
- FIPS 46-3 also allows for the use of two keys, with K1 = K3; this provides for a key length of 112 bits.
- Advantage: with 168bit key length brute force attacks are effectively impossible.

- Advantage/ Attraction of People:
  - 168 bit key length which overcomes the vulnerability of brute force attack.
  - Same algorithm procedure as DES.
  - Very resistant to cryptanalysis.
- Disadvantage:
  - Algorithm is relatively sluggish in software, does not produce efficient software codes.
  - Slower due to 3 times more rounds then DES.
  - Both DES and 3DES use 64 bit block size, larger block size is desirable for efficiency and security.
- Solution?
- AES.

3. Advanced Encryption Standard (AES)

- NIST in 1997issues a call for proposals for a new Advanced Encryption Standard.
- Requirements:
  - Security better or equal to 3DES,
  - Improved efficiency.
  - Mustbe a symetric block cipher with a block length of 128 bits and support for key lengths of 128, 192, and 256 bits.
- Evaluation criteria:
  - include security,
  - computational efficiency,
  - memory requirements,
  - hardware and software suitability, and
  - flexibility.

- In first round, 15 proposals were accepted, out of which in 2nd round 5 algorithms were shortlisted and out of them Rijndeal was proposed as AES developed by cryptographers from Belgium, i.e Dr. Joan Daemen and Dr.Vincent Rijmen.
- AES uses block length of 128bits and a key length that can be 128, 192 or 256 bits.
- It is not like Feistel Structure.
- Next figure shows overall structure of AES.

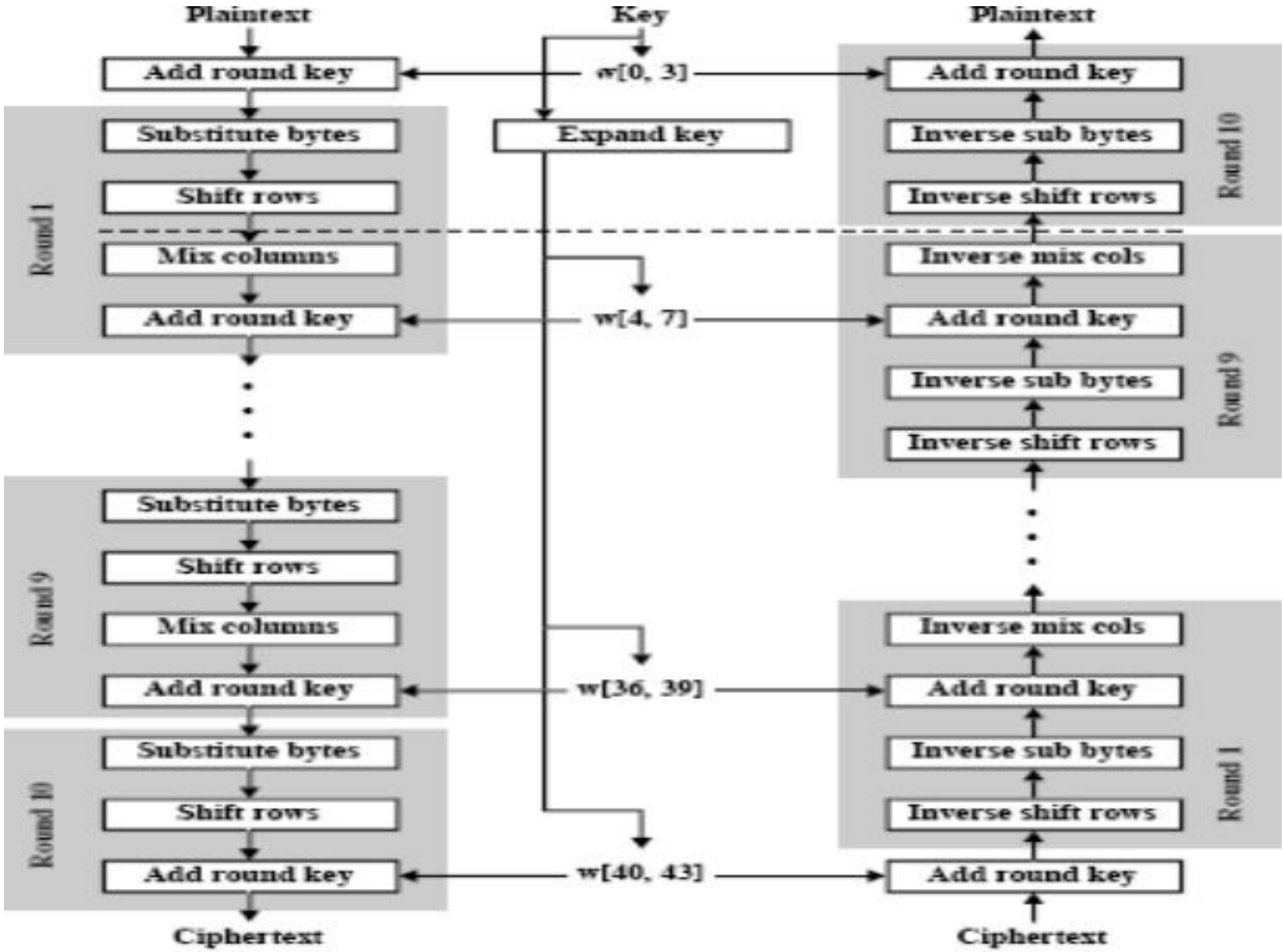


Figure 2.5 AES Encryption and Decryption

AES Procedural Operations:

- Single 128-bit block appearing as square matrix of bytes is copied into 'State' array which is modified at each stage of E and D.
- After the final stage, 'State' is copied to an output matrix (that's y only 3 stages).
- Key Expansion: 128-bit key is depicted as a square matrix of bytes. This key is then expanded into an array of key schedule words: each word is four bytes and the total key schedule is 44 words upto (4*44=176) 176-bits for the 128-bit key. Ordering of bytes is in column order.
- Lets study each step in each round…

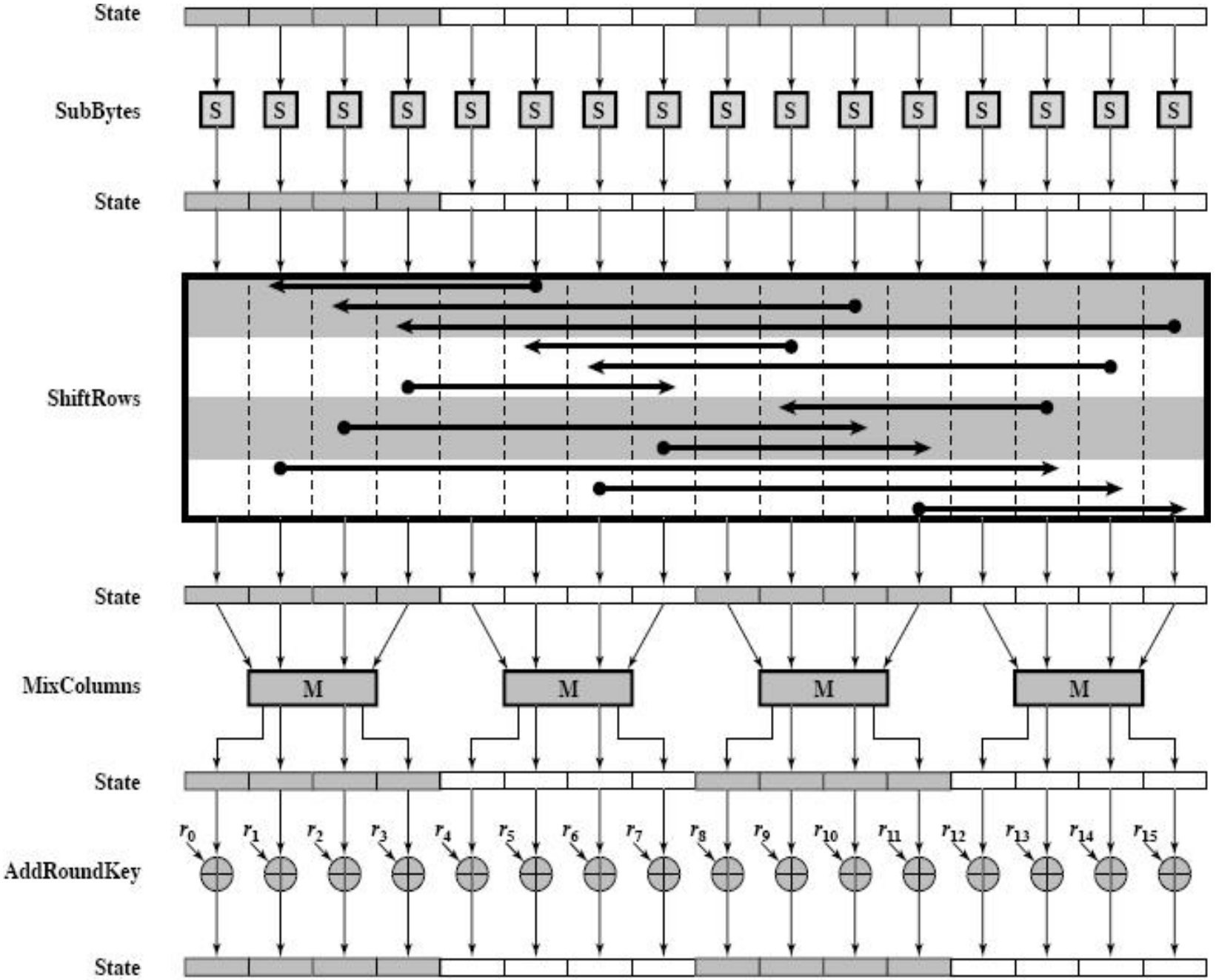


Figure 2.6 AES Encryption Round

1. Substitute Bytes: Uses S-box to perform byte by byte substitution of block.
2. Shift Rows: Simple permutation row by row.
3. Mix columns: Substitution that alters each byte in column as a function of all of bytes in column.
4. Add Round Keys: Simple bitwise XOR of current block with a portion of expanded key.

- For both encryption and decryption, the cipher begins with an
  - Add Round Key stage, followed by
  - Nine rounds that each includes all four stages,
  - Followed by a tenth round of three stages.
- Only the Add Round Key stage makes use of the key. For this reason, the cipher begins and ends with an Add Round Key stage.
- Advantage: Each stage is easily reversible.

Block Cipher v/s Stream Cipher

- A block cipher processes the input one block of elements at a time, producing an output block for each input block.
- Popular Block Ciphers: DES, 3DES, AES.
- Application: File Transfer, Email, Database.

- A stream cipher processes the input elements continuously, producing output one element at a time.
- Popular Stream Ciphers: RC4.
- Application: Data communication channels, web/browser link.

Stream Ciphers and RC4

- Topics:
  1. Stream Cipher Structure
  2. RC4 (Rivest Cipher 4)

1. Stream Cipher Structure
   - Encrypts plaintext one byte at a time.
   - Similar to one time pad.
   - Then what is the difference?
     - One time pad uses genuine random number stream.
     - Stream cipher uses a pseudorandom number stream.

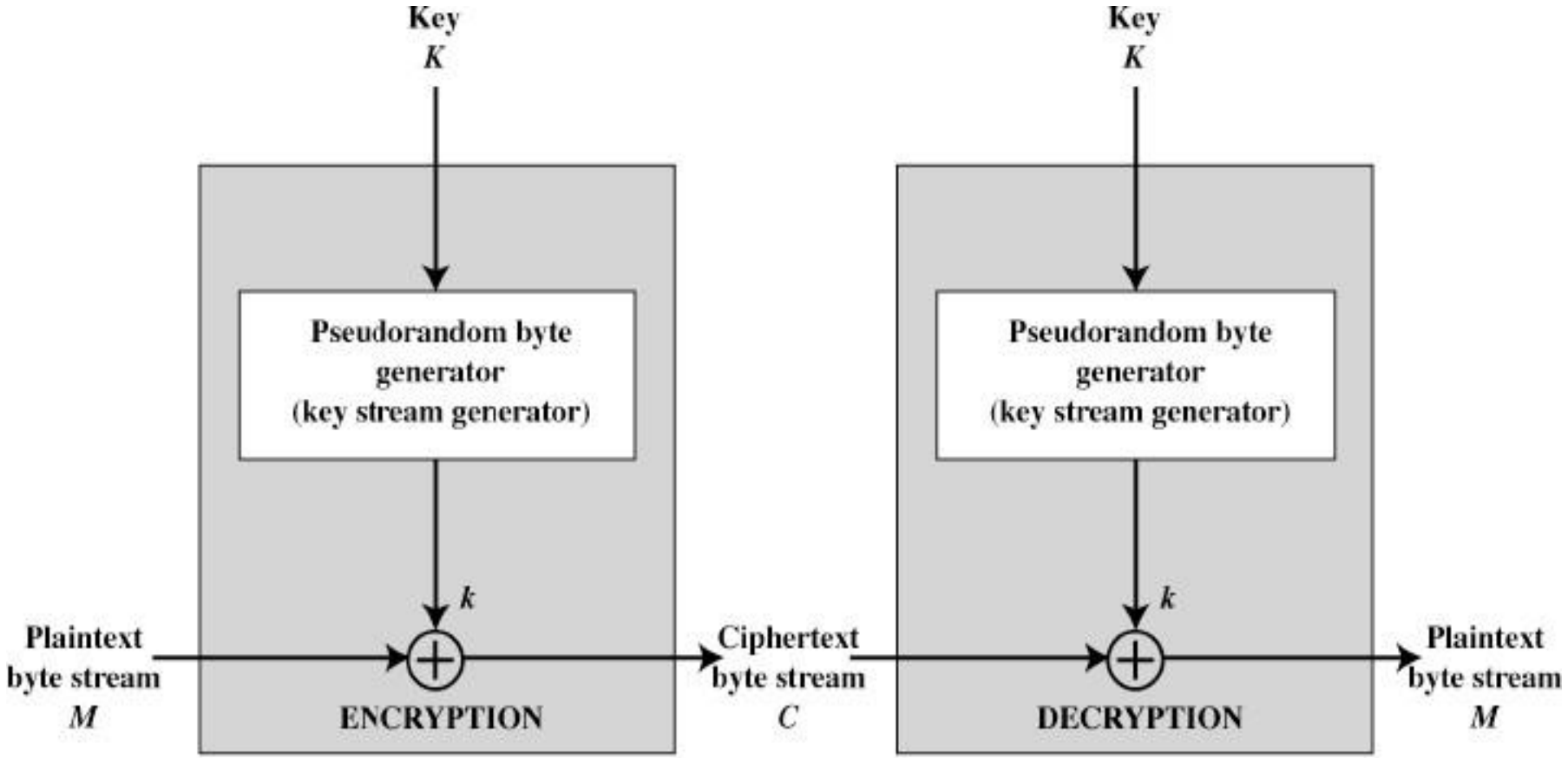


Figure 2.7 Stream Cipher Diagram

- Encryption:

  11001100 plaintext XORed with

  01101100 key stream resulting to

  10100000 cipher text

- Decryption:

  10100000 ciphertext XORed with

  01101100 key stream resulting to

  11001100 plaintext

- A key is input to a **pseudorandom bit generator** that produces a stream of 8-bit numbers that are apparently random.
- The output of the generator, called a **key-stream**, is combined one byte at a time with the plaintext stream using the bitwise exclusive-OR (XOR).
- A **pseudorandom stream** is one that is unpredictable without knowledge of the input key and which has an apparently random character.
- Advantage over block ciphers:
  - With pseudorandom number generator, a stream cipher can be as secure as block cipher of comparable key length.
  - Stream ciphers are always faster than block cipher.
    - Use far less code than block cipher.
- Disadvantage under block ciphers:
  - Block ciphers can re-use keys but not stream ciphers.
- Application:
  - Data communication channels, web/browser link.

- Some design considerations for stream cipher ==>
  a) The encryption sequence should have a large period. A pseudorandom number generator uses a function that produces a deterministic stream of bits that eventually repeats. The longer the period of repeat, the more difficult it will be do cryptanalysis.
  b) For example, there should be an approximately equal number of 1s and 0s. more random-appearing the keystream is, the more randomized the ciphertext is, making cryptanalysis more difficult.
  c) To guard against brute-force attacks, the key needs to be sufficiently long.

2. RC4

- RC4 is a stream cipher designed in 1987 by Ron Rivest for RSA Security.
- It is a variable key-size stream cipher with byte-oriented operations.
- Uses: a random permutation.
- Used with:
  - Secure Sockets Layer/Transport Layer Security (SSL/TLS) standards that have been defined for communication between Web browsers and servers.
  - Used in the Wired Equivalent Privacy (WEP) protocol and the newer WiFi Protected Access (WPA) protocol that are part of the IEEE802.11 wireless LAN standard.
- RC4 was kept as a trade secret by RSA Security.
- But in September 1994, the RC4 algorithm was posted on the Internet on the Cypherpunk's remailers list.
- Algorithm is simple and quite easy to explain

1. Initialize S: Variable length key of from 1 to 256 bytes (8 to 2048 bits) is used to initialize a 256-byte state vector S, with elements S[0], S[1], . . ., S[255].
2. *k is generated* from S by selecting one of the 255 entries in a systematic fashion.
3. Then the entries in S are once again permuted.
4. A temporary vector T, is also created.
5. Set vector T: If the length of the key K is 256 bytes, then K is transferred to T. Otherwise, for a key of length *keylen bytes, the first keylen elements* of T are copied from K, and then K is repeated as many times as necessary to fill out T. These preliminary operations can be summarized as:

```
/* Initialization */
for i=0 to 255 do
S[i] = i;
T[i] = K[i mod keylen];
```

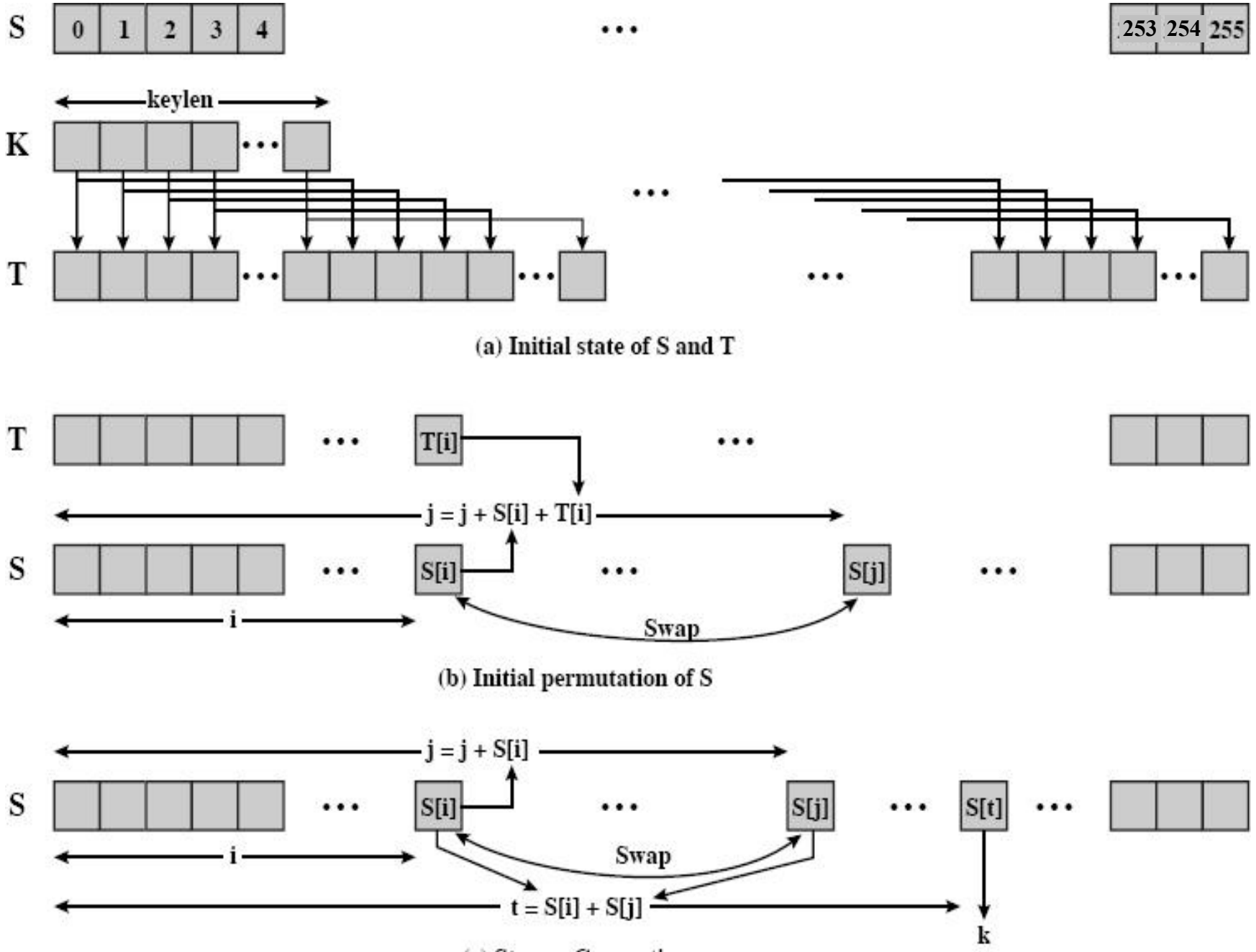


Figure 2.8 RC4

Given table shows the execution speed of RC4 in comparison with other methods.
See last line, it performs well in Pentium II Processor.

Table 2.3 Speed Comparisons of Symmetric Ciphers on a Pentium II

Cipher	Key Length	Speed (Mbps)
DES	56	9
3DES	168	3
RC2	variable	0.9
RC4	variable	45

- Advantage:
  - Vulnerable to attacks after many tries.
- Dis-advantage:
  - WEP Protocol needs confidentiality that it is secure from attacks, but RC4 could not give it. Reason? The way in which the key is generated is not secure and errorfree.
- Conclusion:
  - Difficulty in designing a secure system that involves both cryptographic functions and protocols specific.

Location of Encryption Devices

- We need to decide what to encrypt and where the encryption gear should be located. Alternatives:
- Link Encryption
  - A lot of encryption devices
  - High level of security
  - Disadvantage: Decrypt each packet at every switch
- End-to-End Encryption
  - The source encrypts and the receiver decrypts
  - Message is transmitted unaltered across the n/w.
  - Secure Data against attacks on network links and switches.
  - Disadvantage: Router cannot read Destination address, so can't route the packet on optimum path.
- High Security
  - Both link and end-to-end encryption are needed (see Figure 2.11)

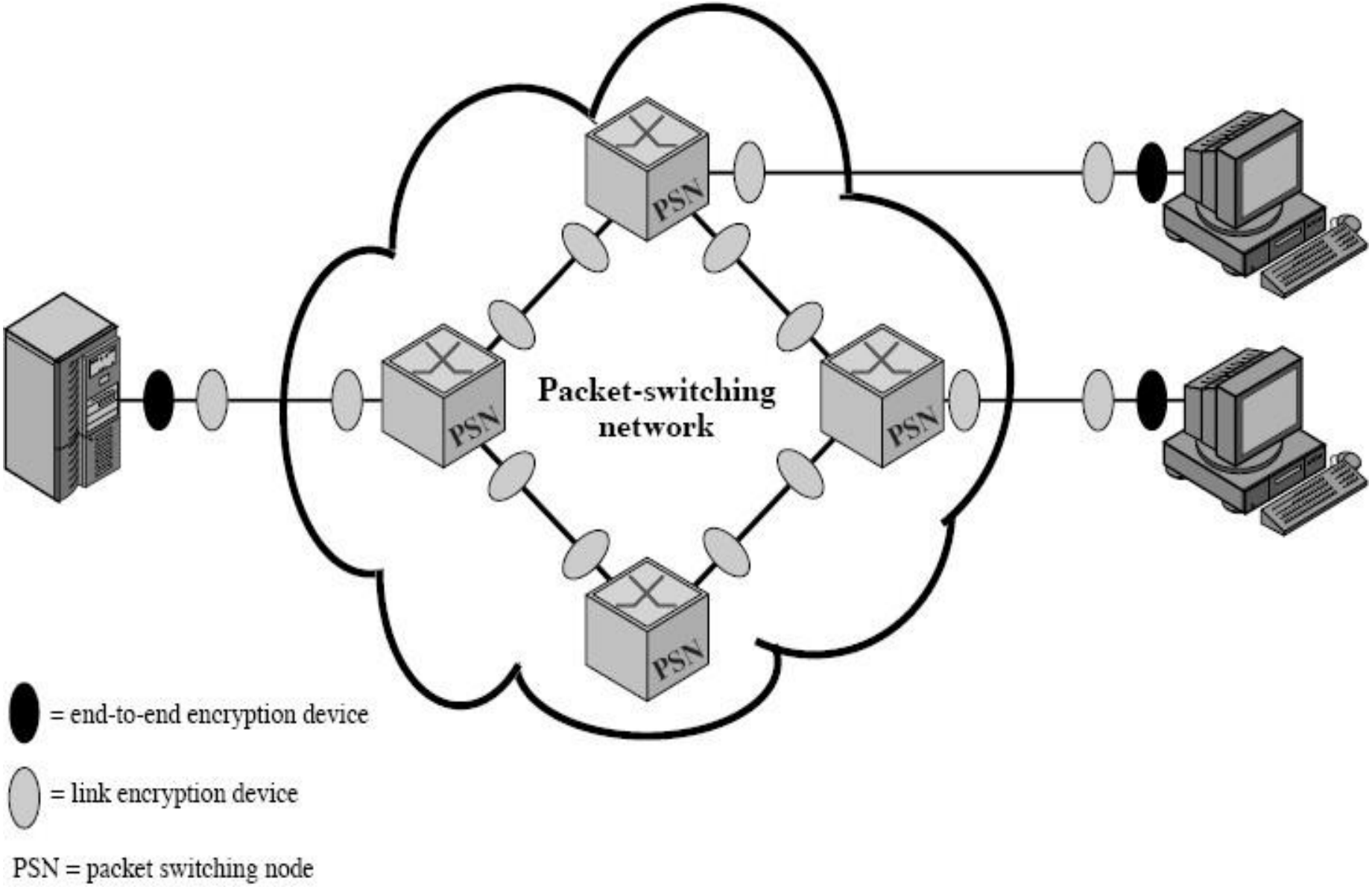


Figure 2.11 Encryption Across a Packet-Switching Network

Key Distribution

Key distribution can be achieved in following ways:

1. A key could be selected by A and physically delivered to B.
2. A third party could select the key and physically deliver it to A and B.
3. If A and B have previously used a key, one party could transmit the new key to the other, encrypted using the old key.
4. If A and B each have an encrypted connection to a third party C, C could deliver a key on the encrypted links to A and B.

- Two kind of keys are identified by schema:

1. Session key
   - Data encrypted with a one-time session key; At the conclusion of the session the key is destroyed.
2. Permanent key
   - Used between entities for the purpose of distributing session keys.

- Elements of Key distribution:

1. Key Distribution Center (KDC):
   - Determine which systems are allowed to communicate.
   - Once permission granted provides one time session key to concerned parties communicating.
2. Security Service Module (SSM):
   - Consist of functionality of protocol layer.
   - Performs End to End Encryption.
   - Obtain session keys on behalf of users.

- See Figure.

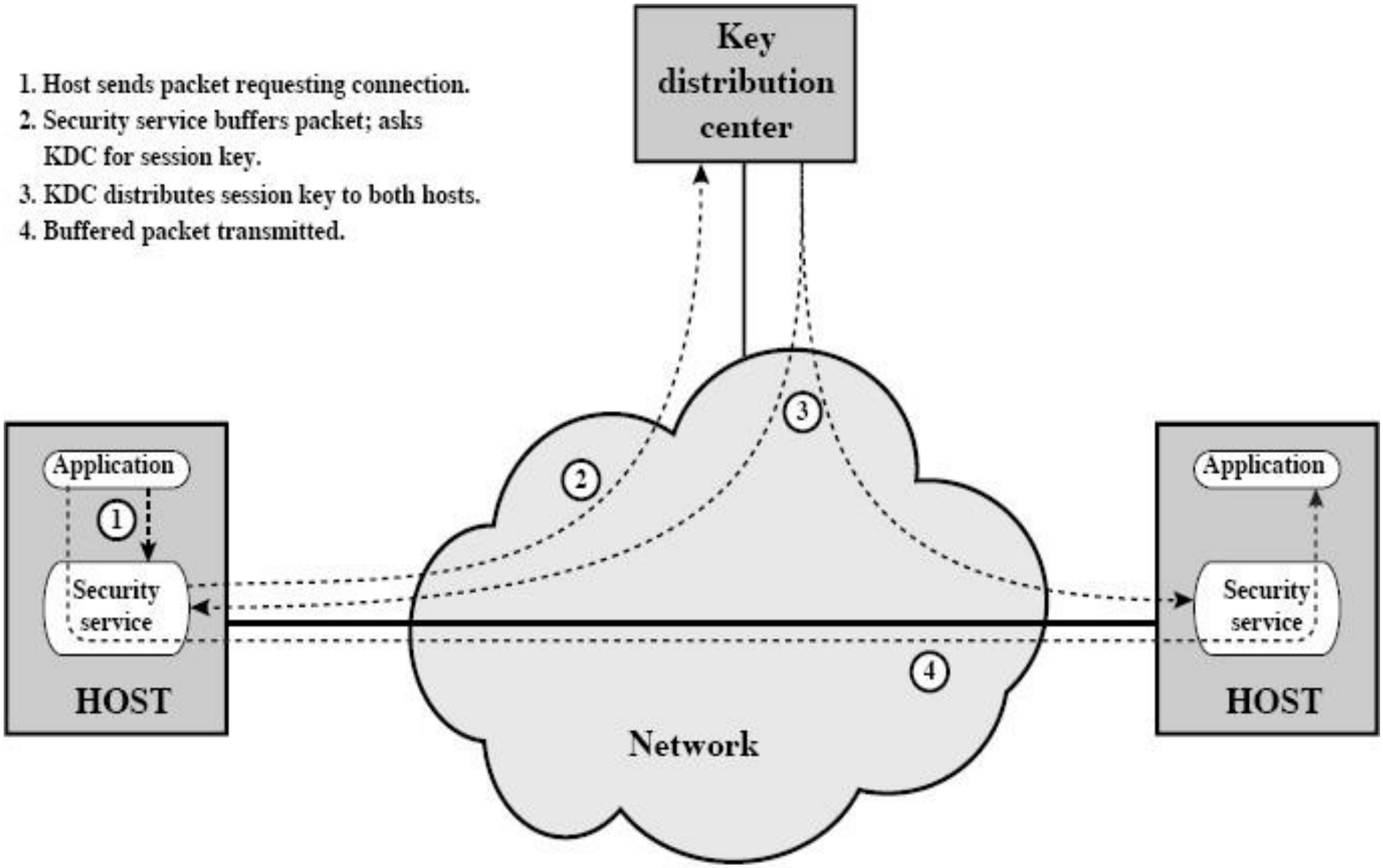


Figure 2.12 Automatic Key Distribution for Connection-Oriented Protocol