Basic Cryptographic Concepts

Part I

Lecture 32: Basic cryptographic concepts – Part I

On completion, the student will be able to:

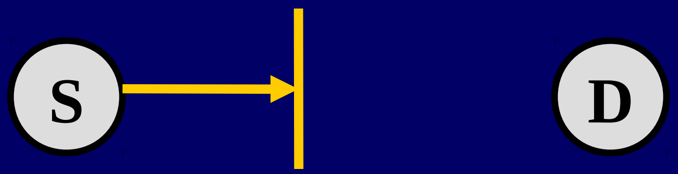
- Define the basic cryptographic terms commonly used.
- Identify the different security threats in the Internet scenario.
- Distinguish between symmetric and public-key cryptography techniques.
- Explain a practical symmetric key encryption / decryption scheme.

Basic Concepts

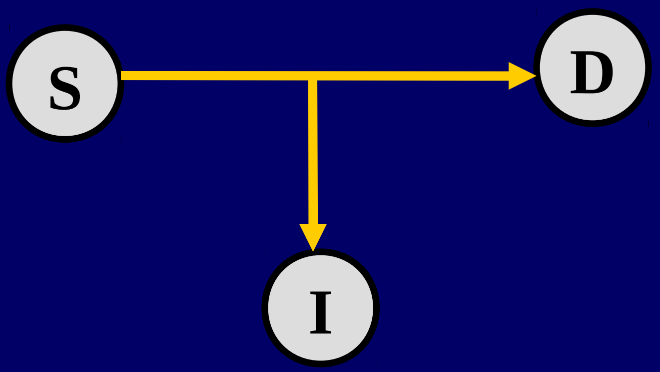
Security Attacks

- Any action that compromises the security of information.
- Four types of attack:
  - Interruption
  - Interception
  - Modification
  - Fabrication
- Basic model:

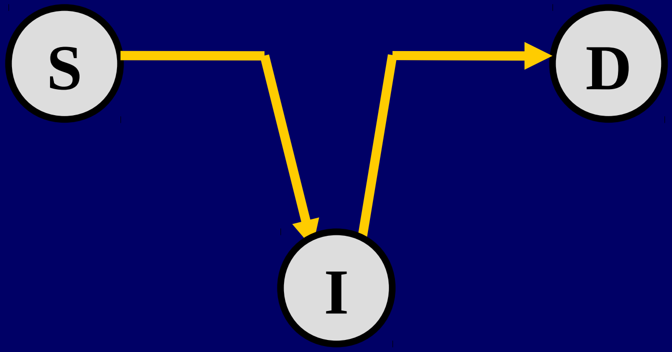
- **Interruption:**
  - **Attack on availability**



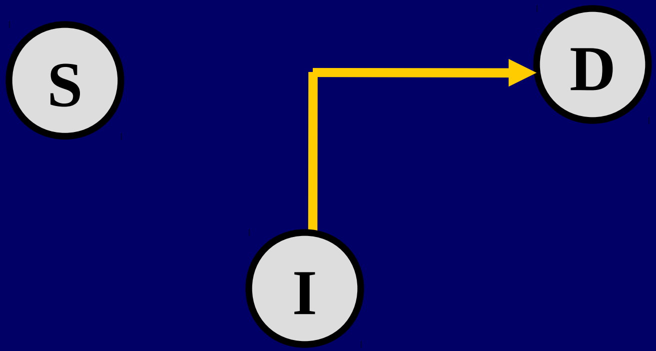
- **Interception:**
  - **Attack on confidentiality**



- **Modification:**
  - **Attack on integrity**



- **Fabrication:**
  - **Attack on authenticity**



Passive and Active Attacks

- **Passive attacks**
  - **Obtain information that is being transmitted (eavesdropping).**
  - **Two types:**
    - **Release of message contents.**
    - **Traffic analysis.**
  - **Very difficult to detect.**

- **Active attacks**
  - **Involve some modification of the data stream or the creation of a false stream.**
  - **Four categories:**
    - **Masquerade:- One entity pretends to be a different entity.**
    - **Replay:- Passive capture of a transaction and subsequent replay.**

- **Modification:- Some portion of a message is altered on its way.**
- **Denial of service:- Prevents access to resources.**

Security Services

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (parties cannot later deny)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files

Network Access Security Model

Opponent:

- Human
- Virus
- Worm

ACCESS CHANNEL

GATEWAY

Internal Network

Computers

Software resources

Databases

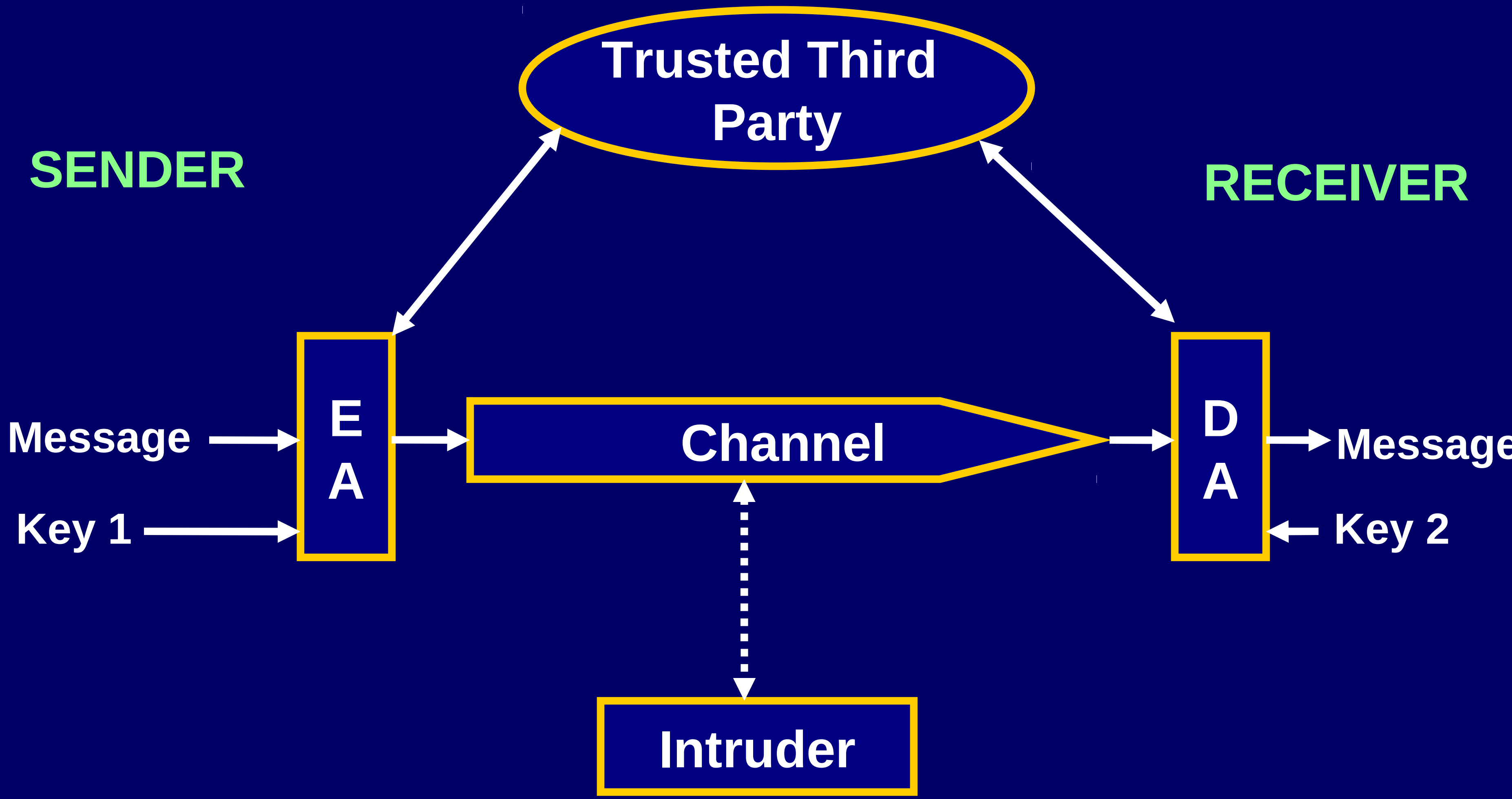
Security Control

Cryptography Terminologies

Introduction

- Most important concept behind network security is *encryption*.
- Two forms of encryption:
  - Private (or Symmetric)
    - Single key shared by sender and receiver.
  - Public-key (or Asymmetric)
    - Separate keys for sender and receiver.

Typical Flow

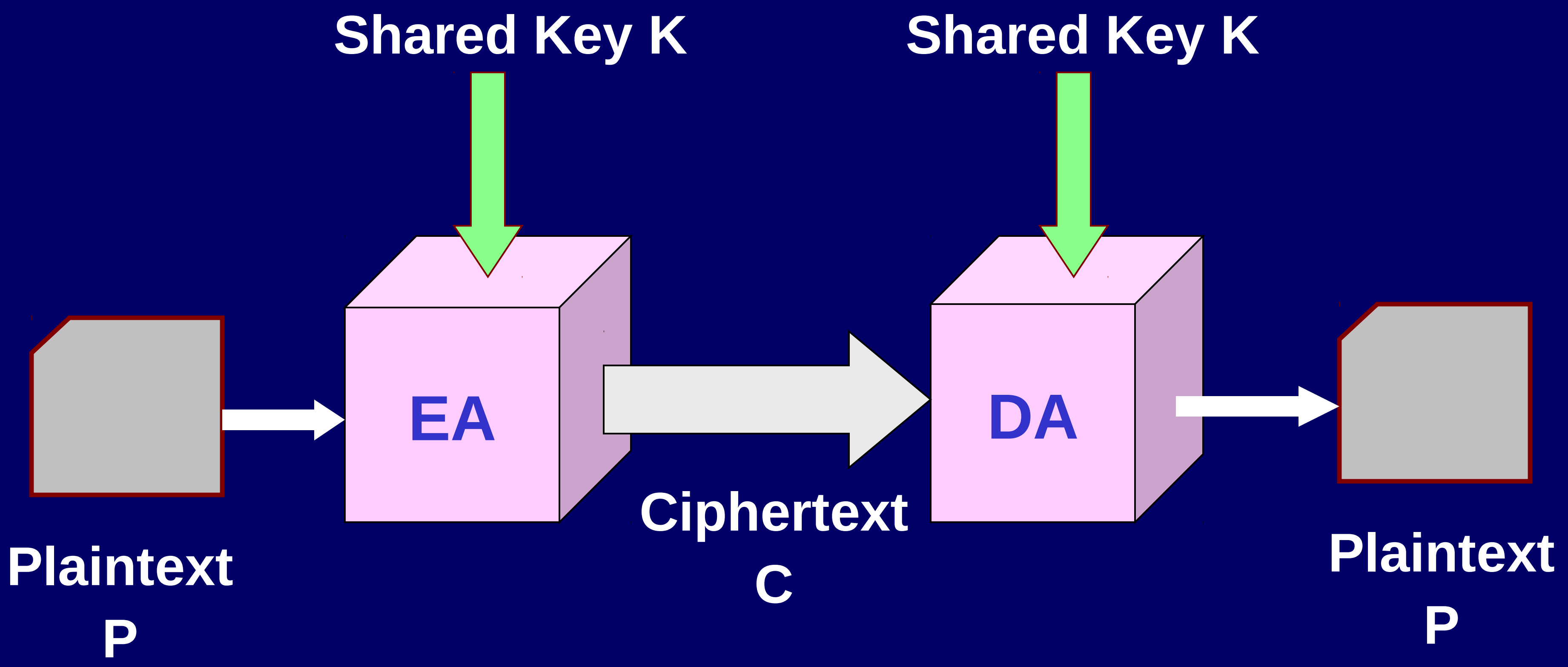


Symmetric Key Cryptography

- **Basic ingredients of the scheme:**
  - **Plaintext (P)**
    - **Message to be encrypted**
  - **Secret Key (K)**
    - **Shared among the two parties**
  - **Ciphertext (C)**
    - **Message after encryption**
  - **Encryption algorithm (EA)**
    - **Uses P and K**
  - **Decryption algorithm (DA)**
    - **Uses C and K**

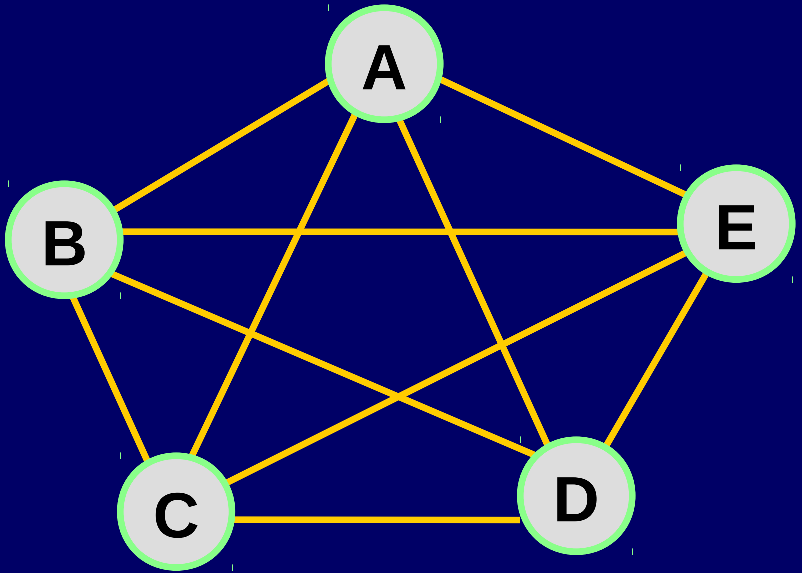
- Security of the scheme
    - Depends on the secrecy of the key.
    - Does not depend on the secrecy of the algorithm.
- Assumptions that we make:
    - Algorithms for encryption/decryption are known to the public.
    - Keys used are kept secret.

Illustration



Some Points to Observe

- ***Key distribution*** **problem of secret key systems:**
  - **Establish key before communication.**
  - **Need *n(n-1)/2* keys with *n* different parties.**



Classical Techniques

- Broadly falls under two categories:
  - Substitution ciphers
    - Each letter or group of letters of the plaintext are replaced by some other letter or group of letters, to obtain the ciphertext.
  - Transposition ciphers
    - Letters of the plaintext are permuted in some form.

A Simple Example

Caesar Cipher (a substitution cipher):

- **Earliest known substitution cipher.**
- **Replace each letter of the alphabet with the letter *three places* after that alphabet.**
- **Alphabets are assumed to be wrapped around (Z is followed by A, etc.).**

P: H A P P Y N E W Y E A R

C: K D S S B Q H Z B H D U

- We can generalize the idea by replacing each letter by the k^{th} following letter.
- If we assign a number to each letter (A=1, B=2, etc), then

$$C = E(P) = (P + k - 1) \ \% \ 26 + 1$$

$$P = D(C) = (C - k + 25) \ \% \ 26 + 1$$

- **Drawback**:
  - Brute force attack is easy
  - Try out all the 25 possible keys

<u>Mono-alphabetic Cipher</u>:

- Allow any arbitrary substitution.
- There can be 26! or 4x1026 possible keys.
- A typical key may be:

  (ZAQWSXCDERFVBGTYHNMJUIKLOP)

- <u>Drawbacks</u>:
  - We can make guesses by observing the relative frequency of letters, digrams, and trigrams in the text.
  - Easy to break in general.

Transposition Ciphers

- Many techniques were proposed under this category.
- A simple scheme:
  - Write out the plaintext in a rectangle, row by row, and read the message column by column, by permuting the order of the columns.
  - Order of the column becomes the key.

P: we are attending one conference at IIT Kharagpur

Key:	4	3	1	2	5	6	7
	w	e	a	r	e	a	t
	t	e	n	d	i	n	g
	o	n	e	c	o	n	f
	e	r	e	n	c	e	a
	t	I	I	T	K	h	a
	r	a	g	p	u	r	-

C: aneelg rdcnTp eenrla wtoetr eiocKu annehr tgfaa-

- **Drawbacks**:
  - The ciphertext has the same letter frequency as the original plaintext.
  - Guessing the number of columns and some probable words in the plaintext holds the key.

Stream Ciphers vs. Block Ciphers

- A stream cipher encrypts the plaintext bit by bit (in streams).
- A block cipher encrypts n-bit blocks at a time.
  - For example, a 256-bit cipher encrypts 256-bit blocks at a time.
  - Short blocks have to be padded.

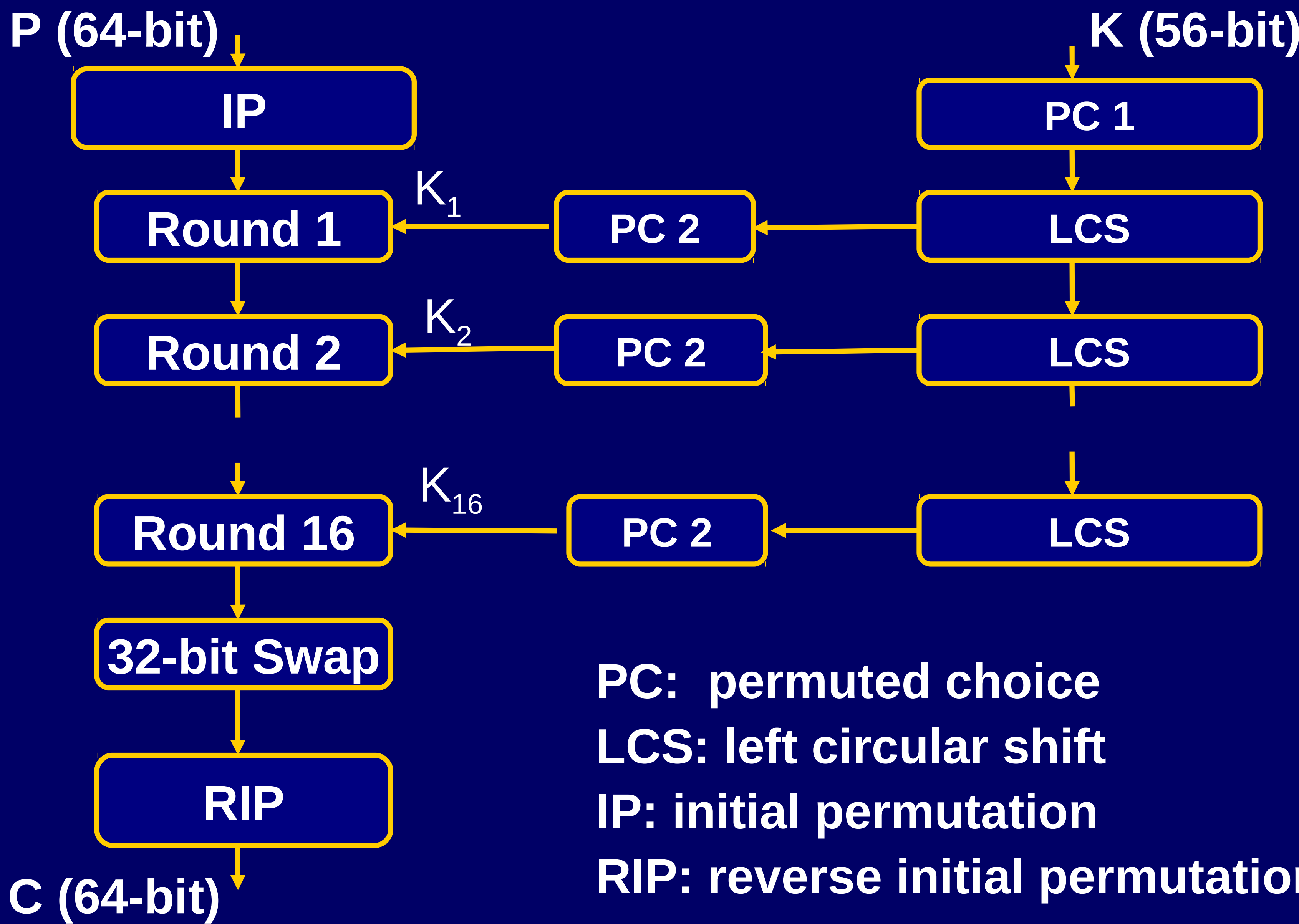
Practical Algorithms

- Data Encryption Standard (DES)
  - Block size is 64 bits.
  - Key is 56 bits.
- IDEA
  - Block size is 64 bits.
  - Key size is 128 bits.
- Advanced Encryption Standard (AES)
  - Also known as Rijndael cryptosystem.
  - Block size can be 128, 192, or 256 bits.
  - Key size can be 128, 192, or 256 bits.

Data Encryption Standard (DES)

- The most widely used encryption scheme.
  - Also known as the Data Encryption Algorithm (DEA).
  - It is a block cipher.
    - The plaintext is 64-bits in length.
    - The key is 56-bits in length.
    - Longer plaintexts are processed in 64-bit blocks.

General Schematic of DES



PC: permuted choice

LCS: left circular shift

IP: initial permutation

RIP: reverse initial permutation

DES

- The overall processing at each iteration:
  - $L_i = R_{i-1}$
  - $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

  Fiestel Structure
- Concerns about:
  - The algorithm and the key length (56-bits)
  - Longer key lengths essential for critical applications

Triple DES

- Use three keys and three executions of the DES algorithm (encrypt-decrypt -encrypt).

$$C = E_{K3} [D_{K2} [E_{K1} [P]]]$$

C = ciphertext

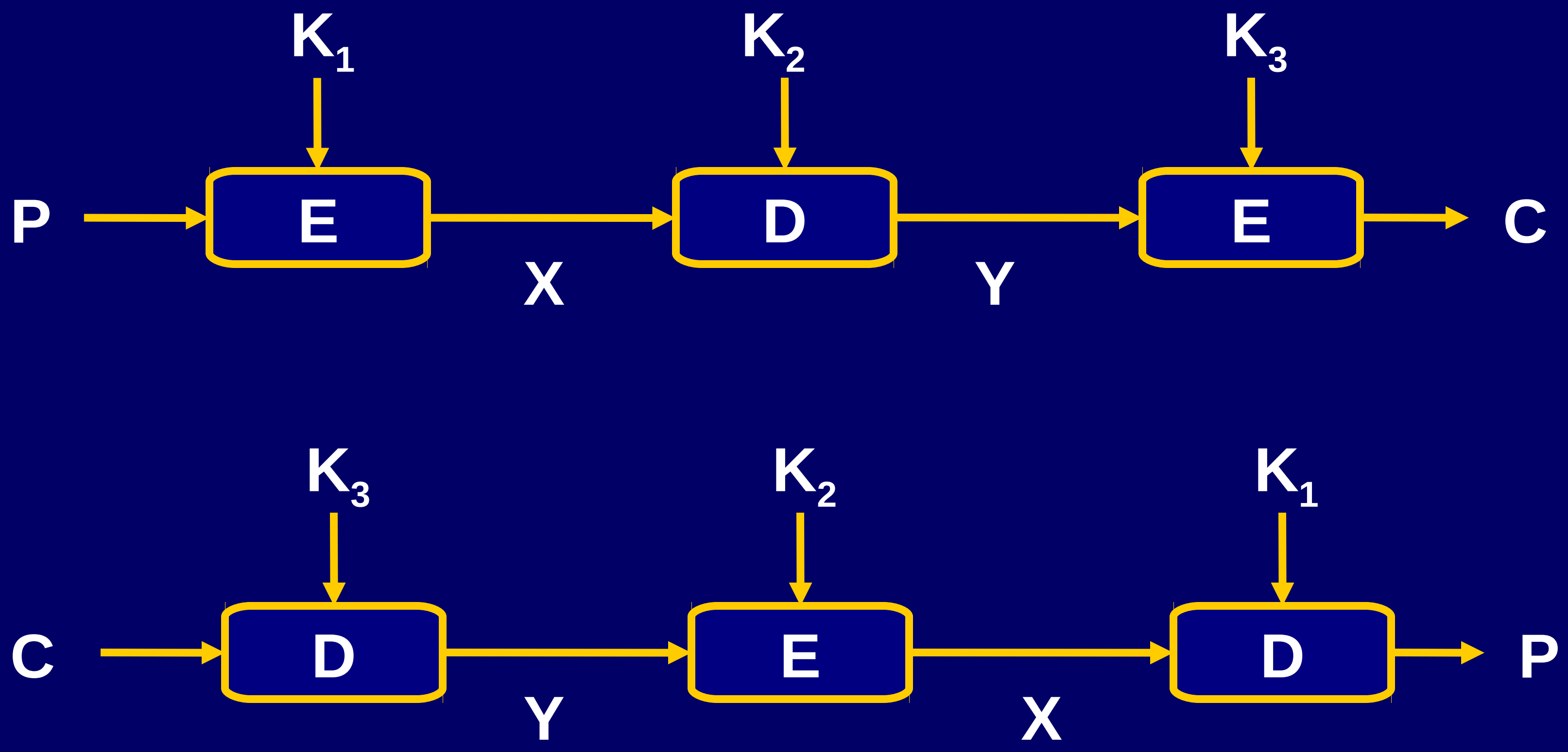
P = Plaintext

$E_K[X]$ = encryption of X using key K

$D_K[Y]$ = decryption of Y using key K

- Effective key length of 168 bits.

Triple DES: Illustration



Need for a new standard

- DES had been in use for a long time.
- A replacement for DES was needed.
  - Theoretical attacks that can break it.
  - Demonstration of exhaustive key search attacks.
- Can use Triple-DES – but slow with small blocks.
- US NIST issued call for ciphers in 1997.
  - 15 candidates accepted in June 1998.
  - 5 were short-listed in August 1999.
- Rijndael was selected as the Advanced Encryption Standard in October 2000.

The AES Cryptosystem

- In the Rijndael proposal, the block length and the key length can be independently specified to be 128, 192, or 256 bits.
- The AES standard limits the block length to 128 bits.
  - Key length can be 128, 192, or 256 bits.
- Easy to implement, both in hardware and software.
- Resistant against all known attacks.

End of Lecture 32