CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

Previous class

- User Authentication
- Access Control

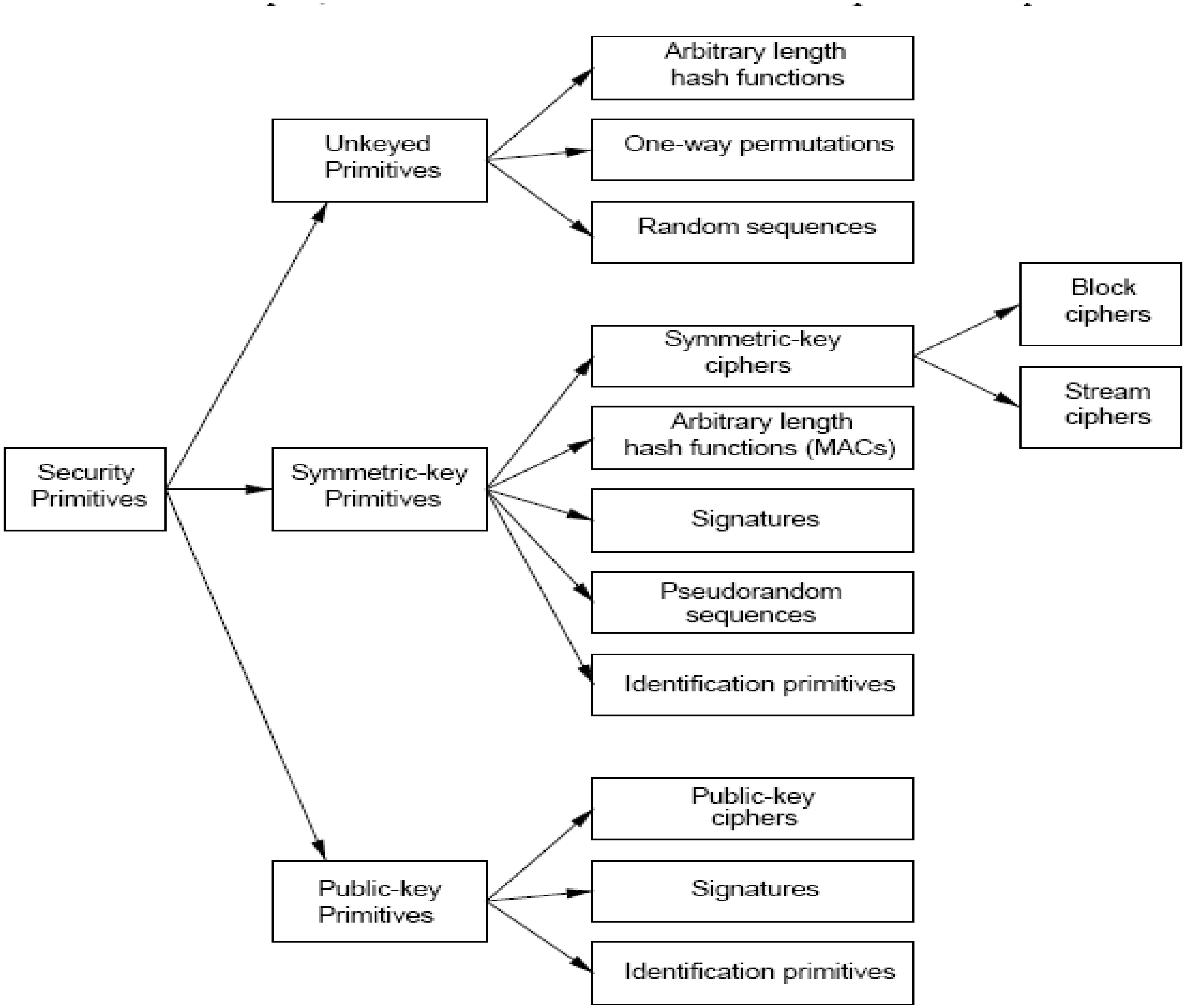
Present class

- Crypto Basics

- Cryptographic algorithms
  - important element in security services

- review various types of elements
  - symmetric encryption
  - public-key (asymmetric) encryption
  - Cryptographic hash functions
  - digital signatures

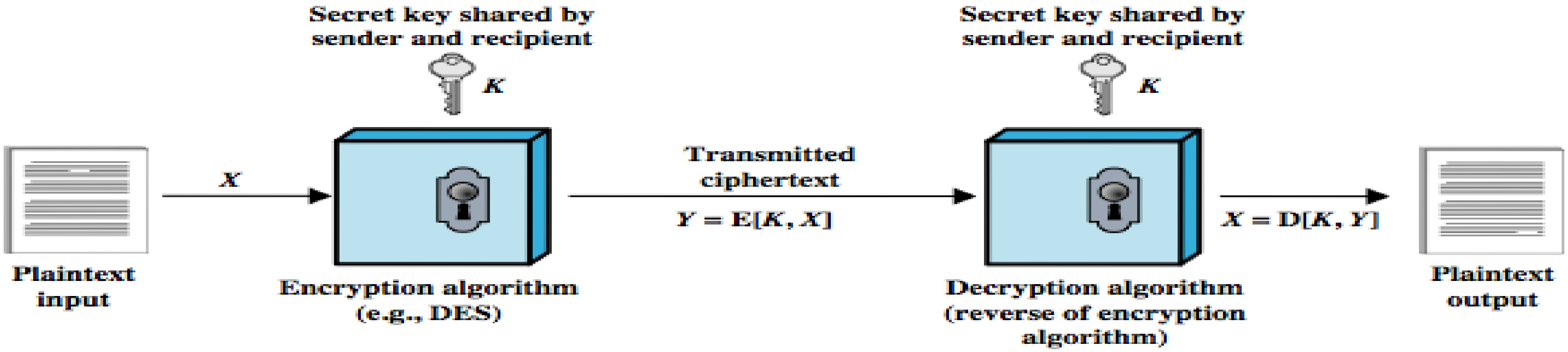
A Taxonomy of Cryptographic Primitives



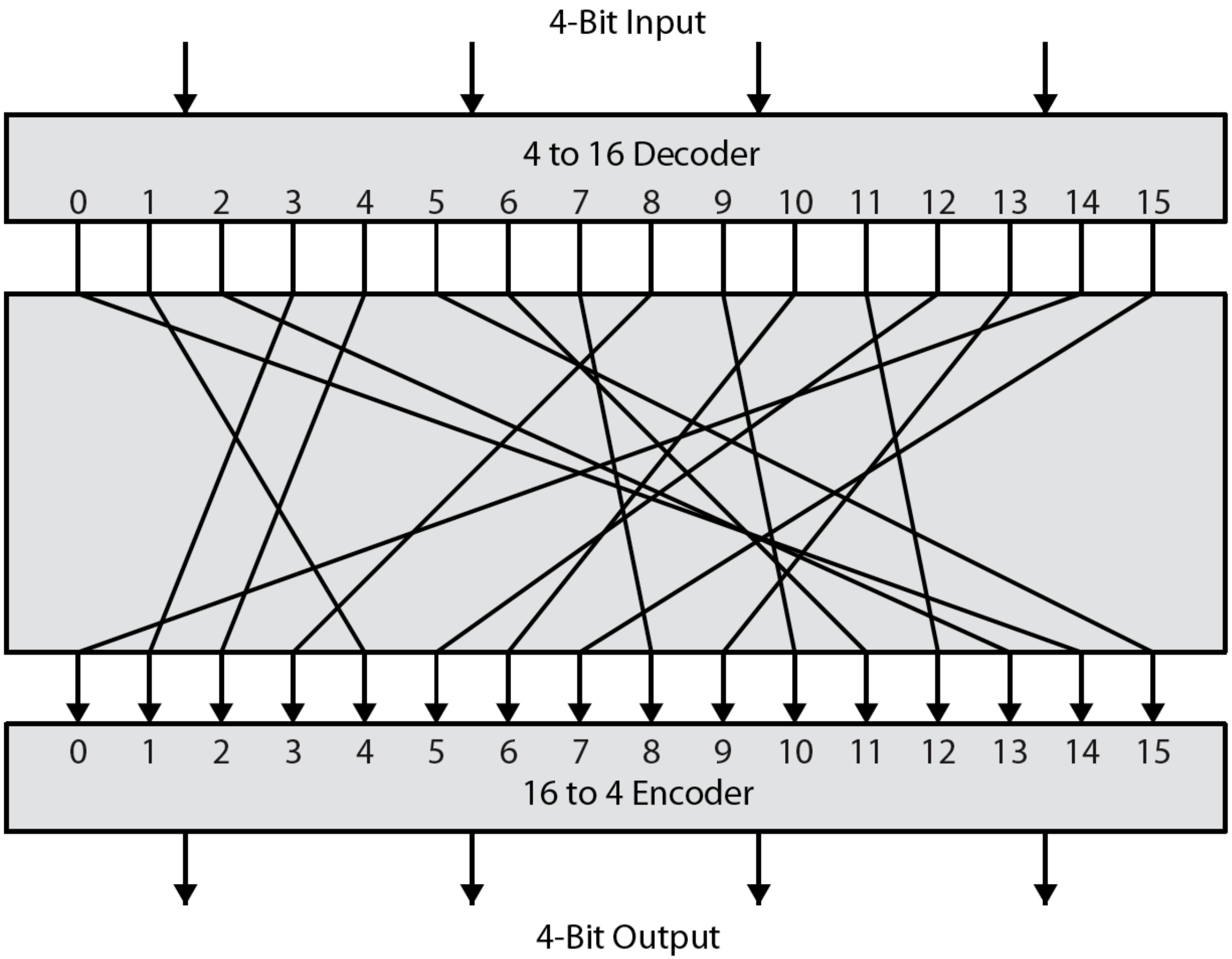
Symmetric Encryption

- universal technique for providing confidentiality
- also referred to as single-key encryption

- two requirements for secure use:
  - need a strong encryption algorithm
  - sender and receiver must have obtained copies of the secret key in a secure fashion
    - and must keep the key secure


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E[K, X]
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Ideal Block Cipher



Block cipher Design Principle

- Confusion:
  - The relation between the statistics of cipher text and plain texts must be complex
- Diffusion:
  - Every bit of the cipher text should depend on the every bit of key and plain text

Ex.: Suppose encrypting plaintext 1111111111111111 produces ciphertext 0110110000101001

Then encrypt 1111111011111111, can't predict anything about ciphertext

- These two important properties can be achieved by repeatedly using of keyed substitutions and permutations.
  - Block cipher in this principle is called Iterated Block cipher

Common Building Blocks

Substitution-Permutation Network (SPN)

- General term for sequence of operations that performs substitutions and permutations on bits

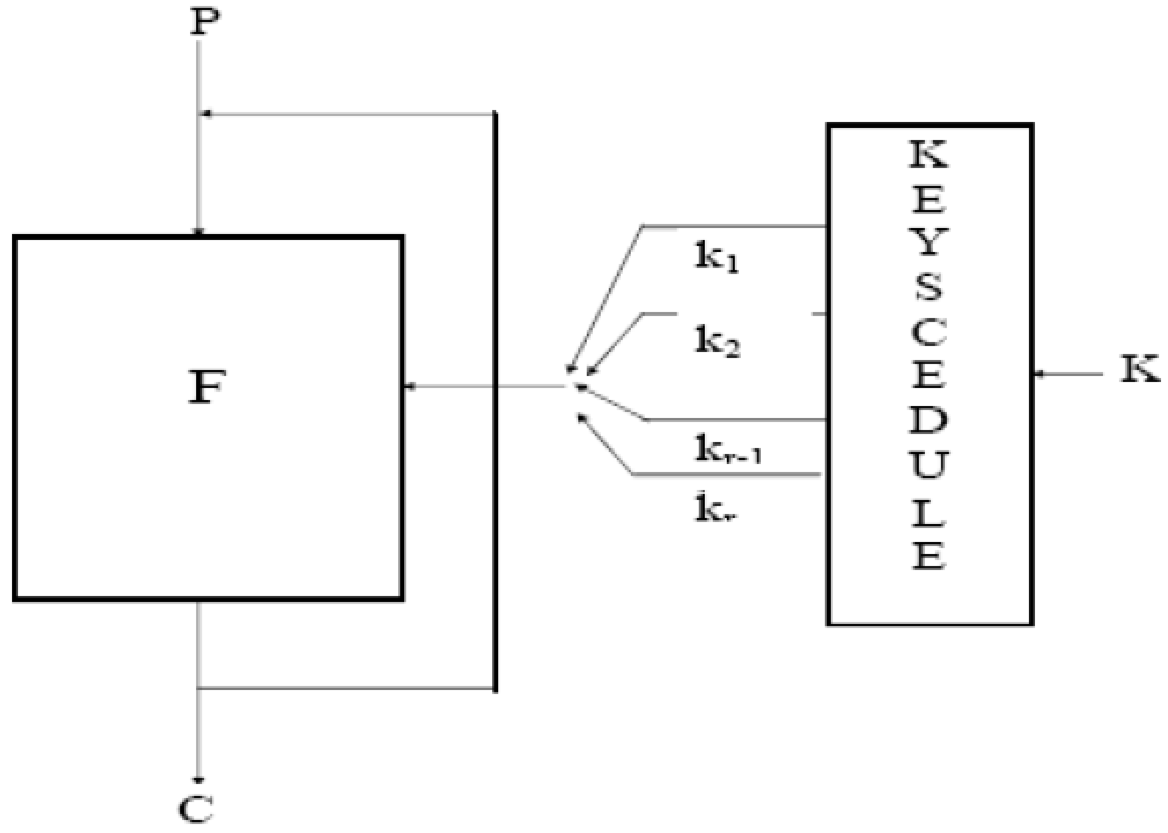
Feistel Network

- For input $L_0 \mid\mid R_0$ and any function F
- $L_i = R_{i-1}$
- $R_i = L_{i-1} \oplus F(R_{i-1},K_i)$
- K_i = other input to F, (ex. key material)

Whitening

- XOR data with key material ($X \oplus K$)
- Helps break relationship between output of one round and input to next round

Iterative Block cipher



Ex.: DES, AES

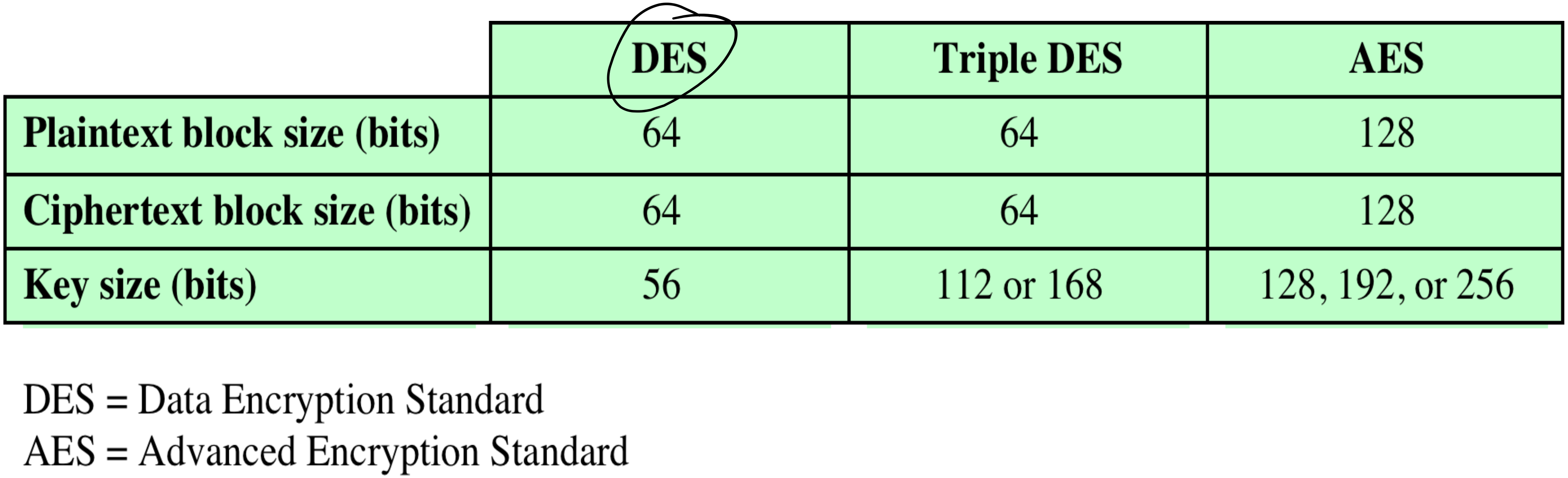
Attacking Symmetric Encryption

- Cryptanalytic Attacks
  - rely on:
  - nature of the algorithm
  - plus some knowledge of the general characteristics of the plaintext
  - even some sample plaintext-ciphertext pairs
  - exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used
  - if successful all future and past messages encrypted with that key are compromised

Brute-Force Attack

- try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained
  - on average half of all possible keys must be tried to achieve success

Symmetric Encryption Algorithms



	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard
AES = Advanced Encryption Standard