



Overview of Cryptographic Techniques

Resources Used

- Lecture slides from Dr Ratan Guha CNT 6519 Wireless Security Forensics
- Cryptography and Network Security, Fourth Edition, by William Stallings
- Lecture slides for the textbook by Lawrie Brown
- Lecture slides by Henric Johnson, Blekinge Institute of Technology, Sweden

Outline

- Some Basic Terminology
- Conventional Encryption Principles
- Characteristics of Cryptographic Techniques
- Symmetric Encryption
- Classical Symmetric Encryption Algorithms
- Modern Symmetric Encryption Techniques

Some Basic Terminology

- **plaintext** - original message
- **ciphertext** - coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - study of principles/methods of deciphering ciphertext *without* knowing key
- **cryptology** - field of both cryptography and cryptanalysis

Conventional 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

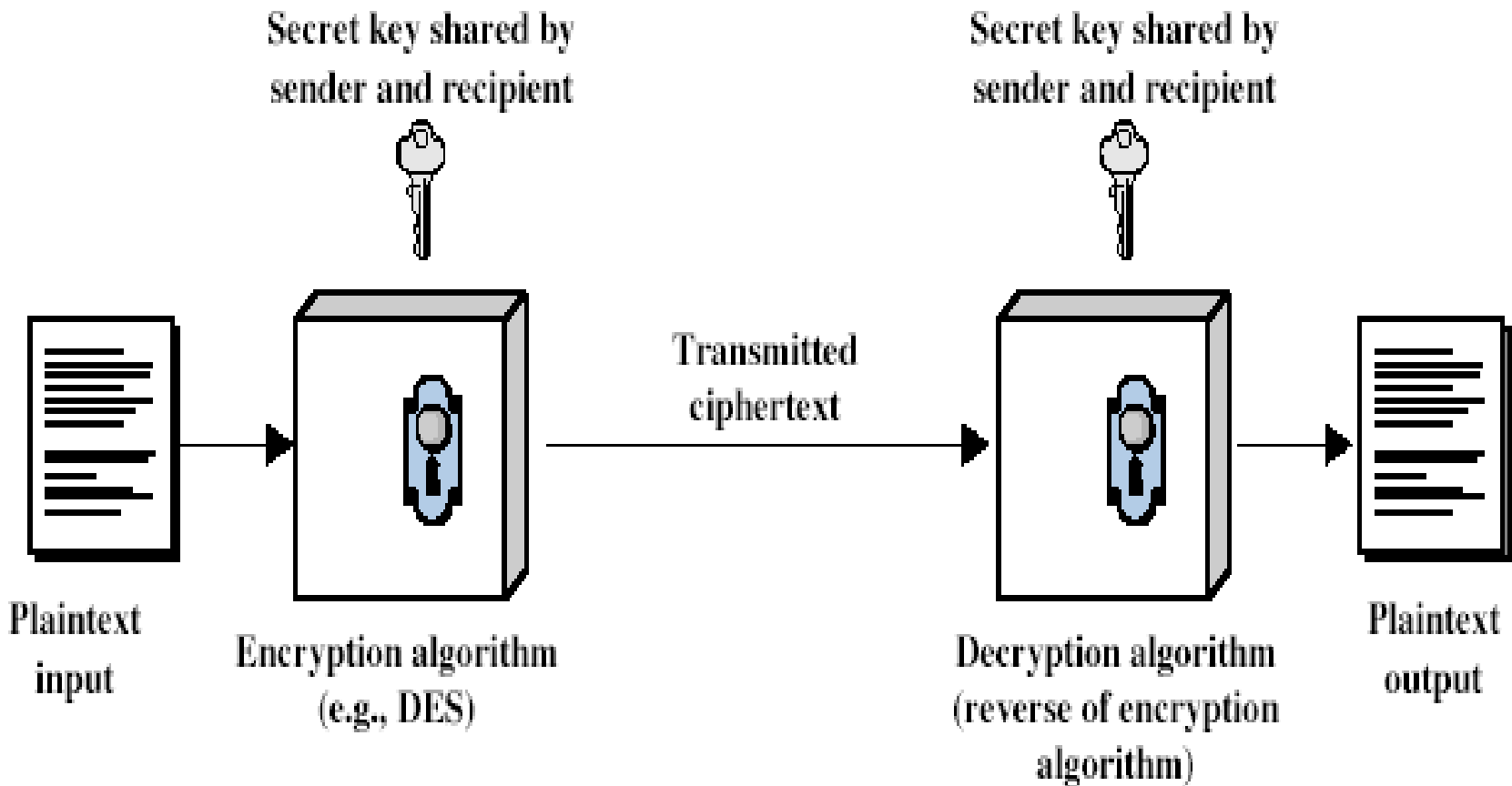
Characteristics of Cryptographic Techniques

- Classified along three independent dimensions:
 - The type of operations used for transforming plaintext to ciphertext
 - The number of keys used
 - symmetric (single key)
 - asymmetric (two-keys, or public-key encryption)
 - The way in which the plaintext is processed

Symmetric Encryption

- or conventional / private-key / single-key
- sender and recipient share a common key
- all classical encryption algorithms are private-key
- was only type prior to invention of public-key in 1970's
- and by far most widely used

Symmetric Cipher Model



Requirements

- two requirements for secure use of symmetric encryption:
 - a strong encryption algorithm
 - a secret key known only to sender / receiver
- mathematically have:
$$Y = E_K(X) \quad [= E(K, X)]$$
$$X = D_K(Y) \quad [= D(K, Y)]$$
- assume encryption algorithm is known
- implies a secure channel to distribute key

Brute Force Search

- always possible to simply try every key
- most basic attack, proportional to key size
- assume either know / recognize plaintext

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