


Cryptography and Network Security



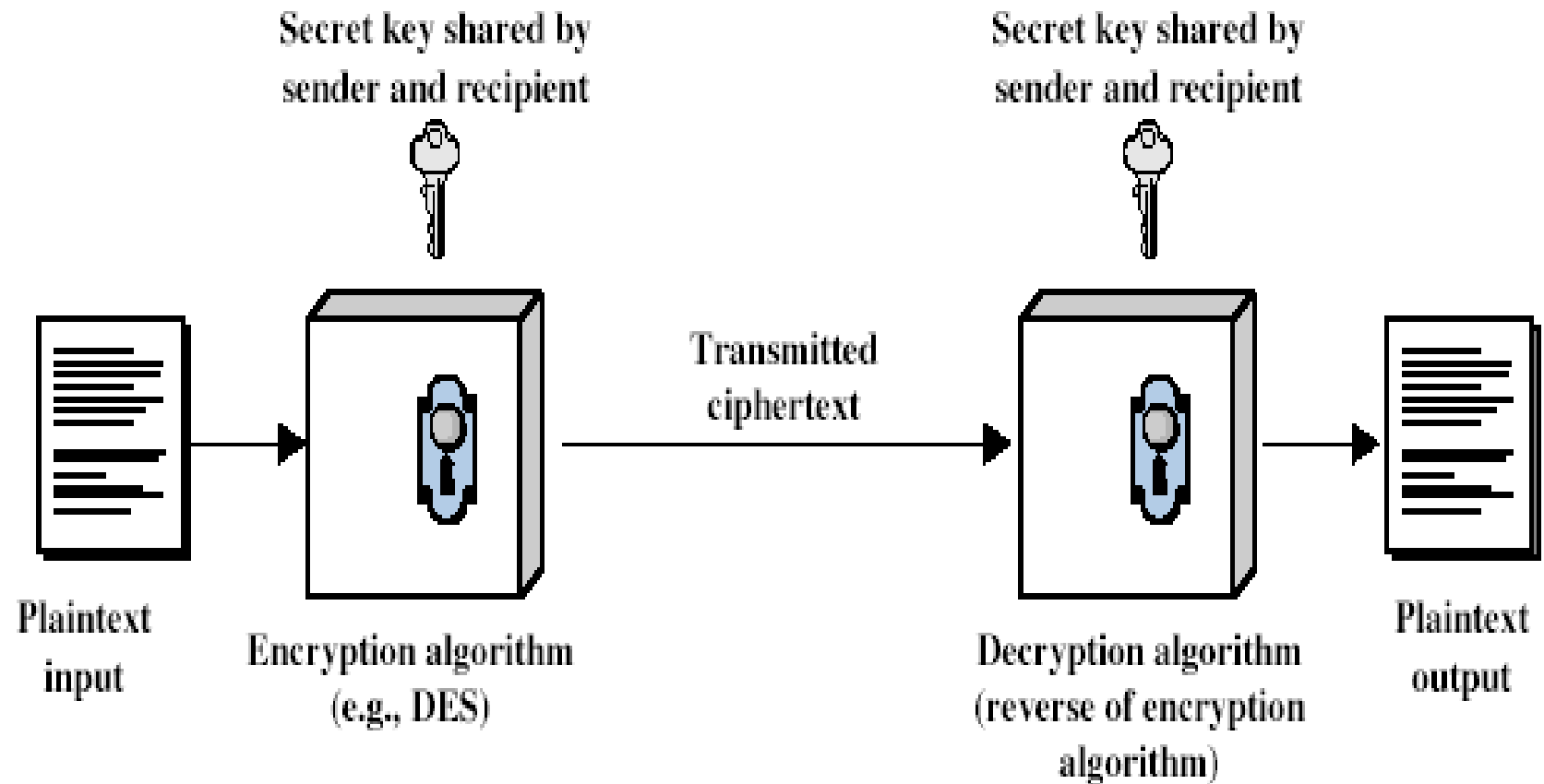
Symmetric Encryption

- 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
- 
- The bottom right corner of the slide features several decorative concentric circles in a lighter shade of purple, resembling ripples in water. There are three main sets of these circles, with the largest one being the most prominent.

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

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:
$$Y = E_K(X)$$
$$X = D_K(Y)$$
- assume encryption algorithm is known
- implies a secure channel to distribute key

Cryptography

- characterize cryptographic system by:
 - type of encryption operations used
 - substitution / transposition / product
 - number of keys used
 - single-key or private / two-key or public
 - way in which plaintext is processed
 - block / stream

