Conventional Encryption Message Confidentiality

Data and Network Security

Cryptography

- Why do we need cryptography?
  - Requirement
    - Be sure our confidential information can't be understood by anyone other than the intended

- Protect against interception

Cryptography

- Classified along three independent dimensions:
  1. The type of operations used for transforming plain-text to cipher text
     - *Substitution: each element is mapped to another element*
     - *Transposition: elements are rearranged*
  2. The number of keys used
     - *symmetric (single key)*
     - *asymmetric (two-keys, or public-key encryption)*
  3. The way in which the plain-text is processed
     - *block cipher*
     - *stream cipher*

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
- Most important algorithms:
  1. Data Encryption Standard – DES
  2. Triple DEA – TDEA
  3. International Data Encryption Algorithm - IDEA

Conventional Encryption Principles

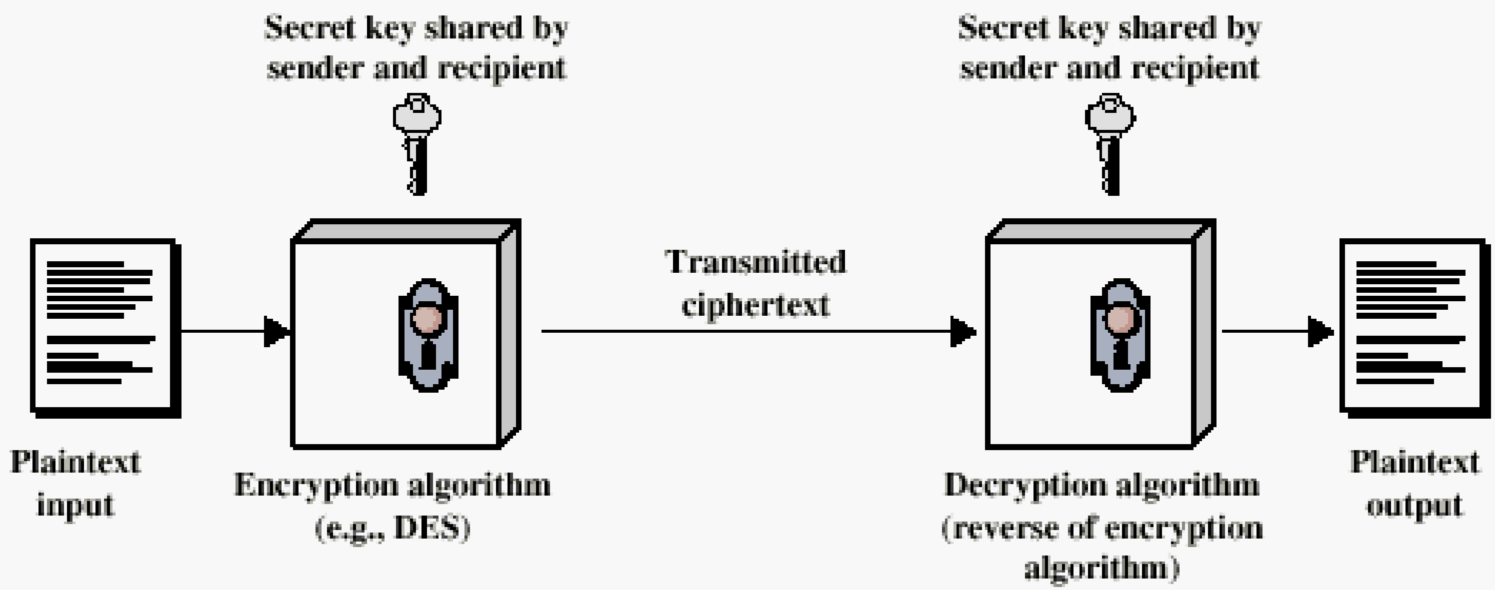

Figure 2.1 Simplified Model of Conventional Encryption

Cryptography

- There are two requirements for secure use of symmetric encryption
  - We 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

Cryptanalysis

- The process of attempting to discover the plaintext or key is known as cryptanalysis.
- Cryptanalysis attack
  - Ciphertext only
  - Known plaintext
  - Chosen plaintext

Average time required for exhaustive key search

Key Size (bits)	Number of Alternative Keys	Time required at 10^6 Decryption/µs
32	$2^{32} = 4.3 \times 10^9$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	10 hours
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} years

Claude Shannon and Substitution-Permutation Ciphers

- 1949 Claude Shannon introduced idea of substitution-permutation (S-P) networks
  - modern substitution-transposition product cipher
- These form the basis of modern block ciphers
- S-P networks are based on the two primitive cryptographic operations we have seen before:
  - substitution (S-box)
  - permutation (P-box)
- provide confusion and diffusion of message

Claude Shannon and Substitution-Permutation Ciphers

- Cipher needs to completely obscure statistical properties of original message
- A one-time pad does this
- More practically Shannon suggested combining elements to obtain:
- **Diffusion** – dissipates statistical structure of plain-text over bulk of cipher-text
- **Confusion** – makes relationship between cipher-text and key as complex as possible

Feistel Cipher Structure

- Virtually all conventional block encryption algorithms, including DES have a structure first described by **Horst Feistel** of IBM in 1973
- The realisation of a Fesitel Network depends on the choice of the following parameters and design features:
  - **Block size**: larger block sizes mean greater security
  - **Key Size**: larger key size means greater security
  - **Number of rounds**: multiple rounds offer increasing security
  - **Sub-key generation algorithm**: greater complexity will lead to greater difficulty of cryptanalysis.
  - **Fast software encryption/decryption**: the speed of execution of the algorithm becomes a concern
- Implements Shannon's substitution-permutation network concept

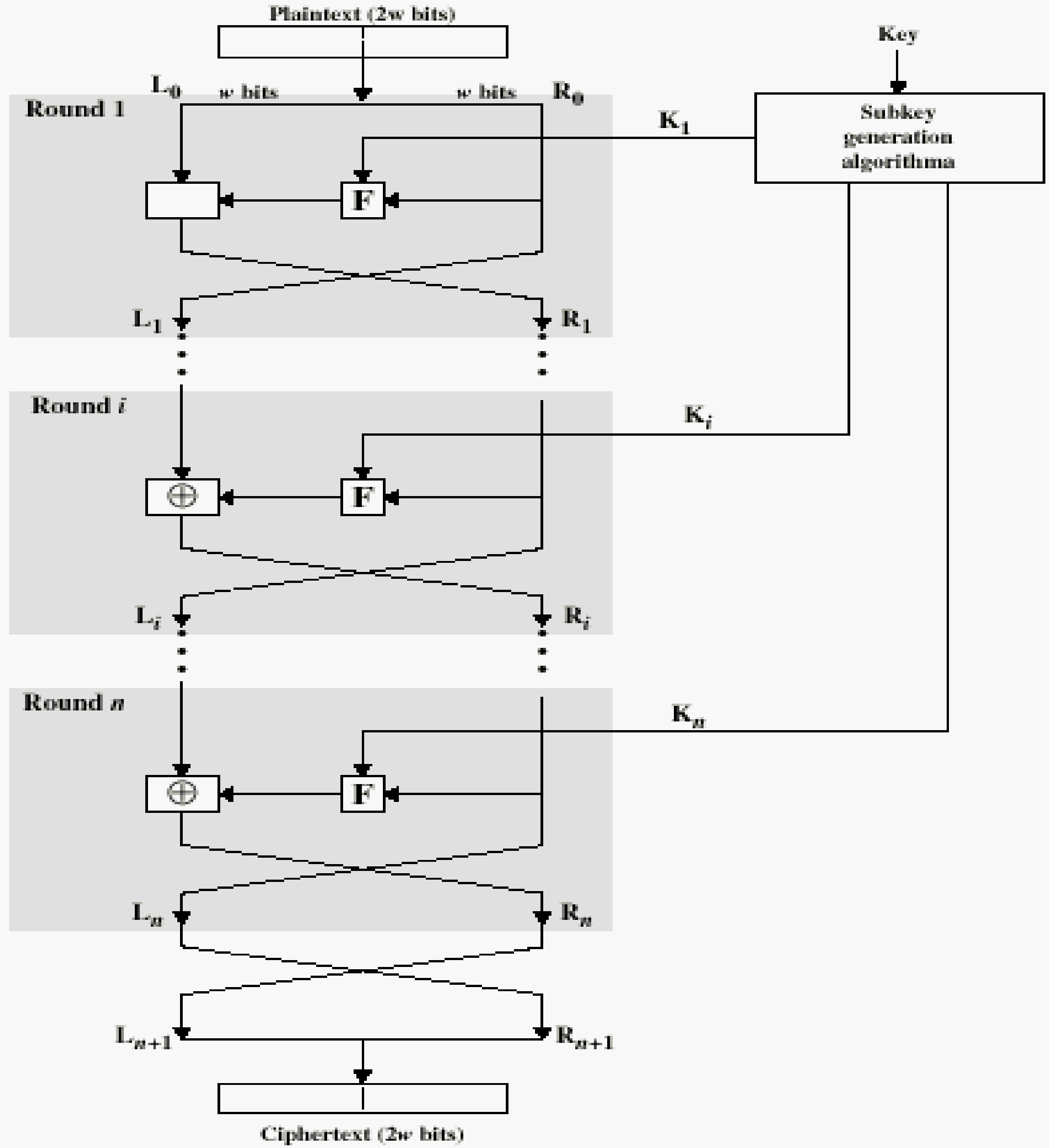

Figure 2.2 Classical Feistel Network

DES

- Data Encryption Standard (DES)
  - The most widely used encryption scheme
  - The algorithm is referred to the Data Encryption Algorithm (DEA)
  - DES is a block cipher
  - The plain-text is processed in 64-bit blocks
  - The key is 56-bits in length
  - 16 rounds of processing
  - 16 subkeys are generated
  - Decryption process is the same as the encryption
    - ciphertext as input
    - Keys in reverse order

Strength of DES

- Concerns about the strength of DES fall into two categories:
  - Algorithm its self
    - DES the most-studied encryption algorithm in existence
    - no one has so far succeeded in discovering a fatal weakness in DES
  - Key size
    - A more serious concern is key length
    - 56 bits, there are 2^{56} possible keys, which is approximately 7.2×10^{16} keys
    - Single decryption per micro sec. take ten years
    - In 1998, Electronic Frontier Foundation (EFF), announced that it had broken DES.
    - In less than 3 days.

Strength of DES

- It is important to note that there is more to a key-search attack than simply running through all possible keys.
  - Unless known plaintext is provided, the analyst must be able to recognize plaintext as plaintext
  - If the message is just plain text in English, then the result pops out easily
  - Task of recognizing English would have to be automated
  - If text message has been compressed before encryption, then recognition is more difficult
  - And if the message is some more general type of data, such as a numerical file, and this has been compressed, the problem becomes even more difficult to automate

Strength of DES

- Thus, to supplement the brute-force approach, some degree of knowledge about the expected plaintext is needed, and some means of automatically distinguishing plaintext from garble is also needed
- The EFF approach addresses this issue as well and introduces some automated techniques that would be effective in many contexts.
- **A final point:** If the only form of attack that could be made on an encryption algorithm is brute force, then the way to counter such attacks is obvious: use longer keys.

Strength of DES

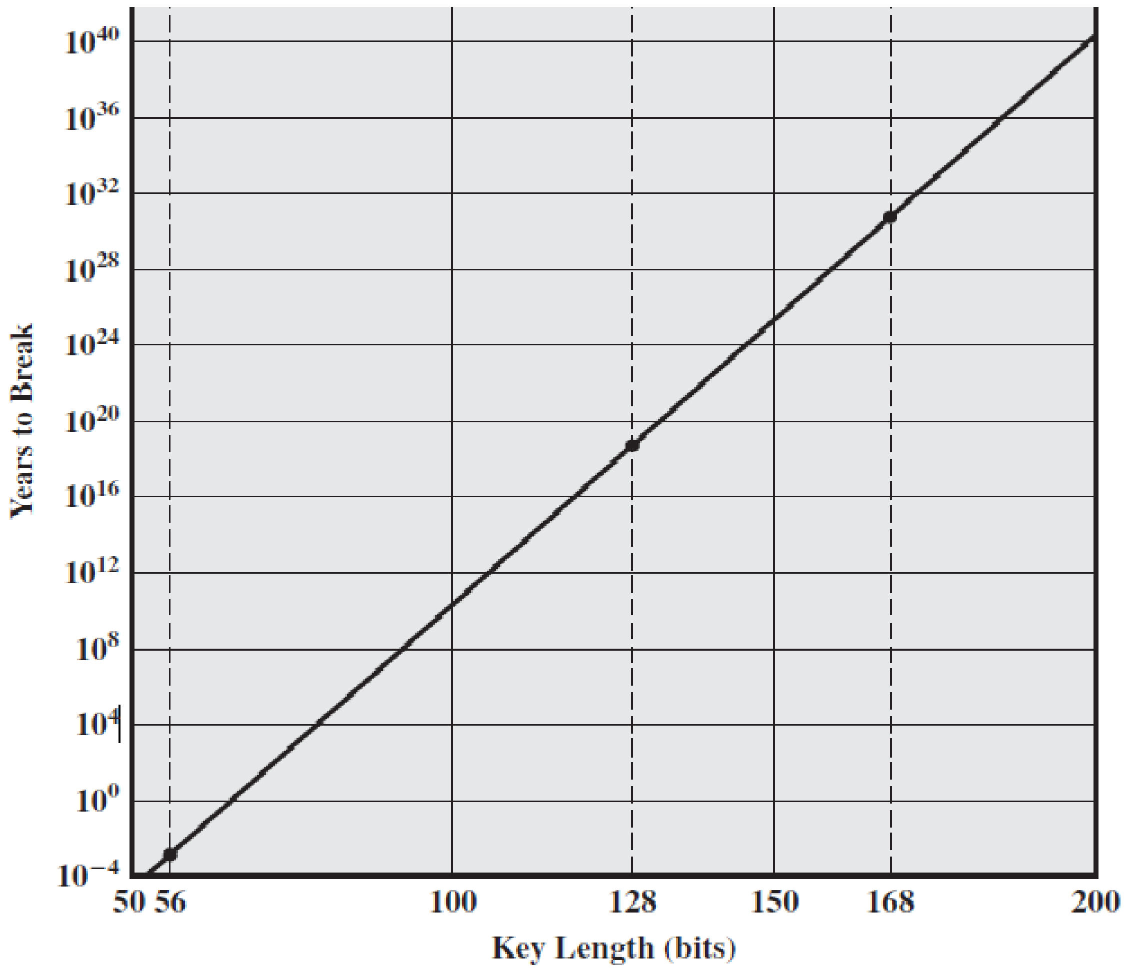

Figure 2.3 Time to Break a Code (assuming 10^6 decryptions/μs)

Triple DEA

- Use three keys and three executions of the DES algorithm (encryptdecrypt-encrypt)
  - C = Cipher-text
  - P = Plain-text
  - EK[X] = encryption of X using key K
  - DK[Y] = decryption of Y using key K

- Effective key length of 168 bits

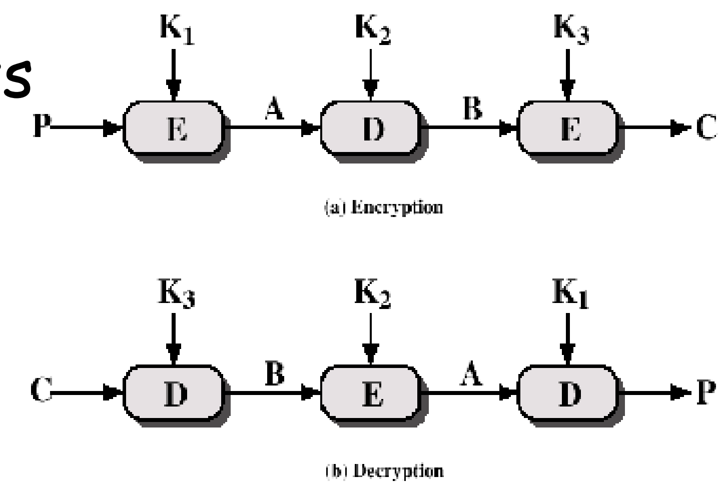

Figure 2.6 Triple DEA

Other Symmetric Block Ciphers

- International Data Encryption Algorithm (IDEA)
  - 128-bit key
  - Used in PGP
- • Blowfish
  - Easy to implement
  - High execution speed
  - Run in less than 5K of memory
- • RC5
  - Suitable for hardware and software
  - Fast, simple
  - Adaptable to processors of different word lengths
  - Variable number of rounds
  - Variable-length key
  - Low memory requirement
  - High security
  - Data-dependent rotations

Location of Encryption Device

- Link encryption
  - A lot of encryption devices
  - High level of security
  - Decrypt each packet at every switch
- End-to-end encryption
  - The source encrypt and the receiver decrypts
  - Payload encrypted
  - Header in the clear
- For High Security both link and end-to-end encryption are needed

Key Distribution

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.

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

THE END