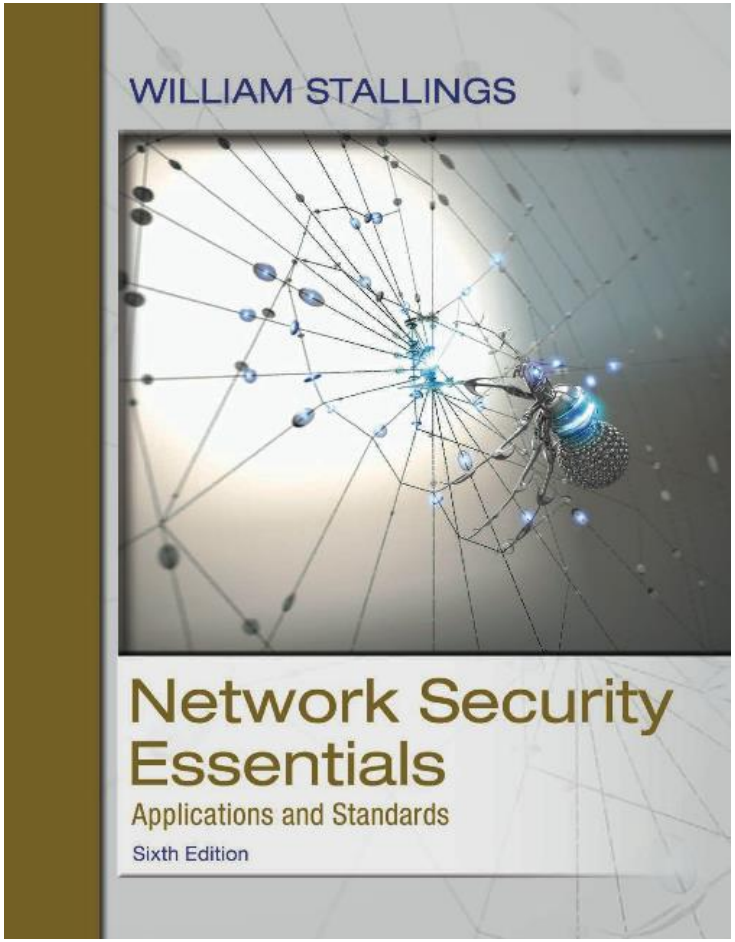
Network Security Essentials: Applications and Standards

Sixth Edition



Chapter 2

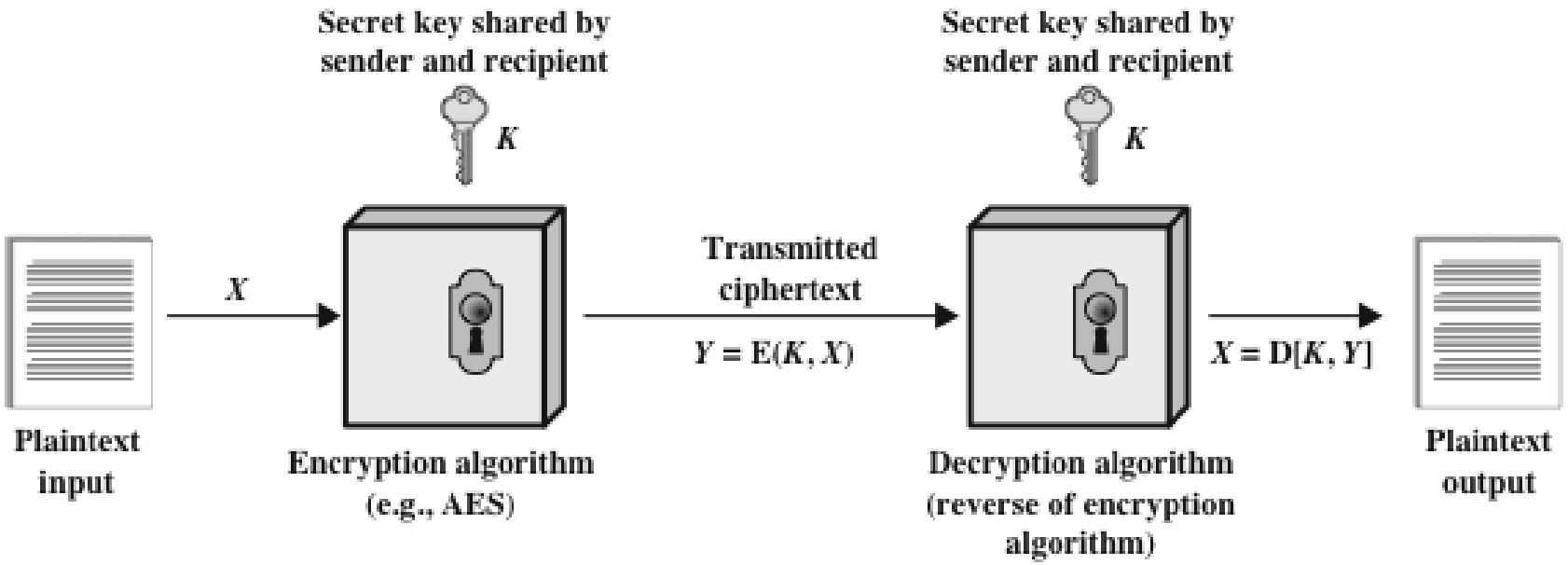
Symmetric Encryption and Message Confidentiality

Pearson

Symmetric encryption

- Also known as conventional encryption, single-key encryption, and secret-key encryption.
- Most widely used encryption scheme.

Figure 2-1: Simplified Model of Symmetric Encryption



Requirements (1 of 2)

- There are two requirements for secure use of symmetric encryption:
  - 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
- The security of symmetric encryption depends on the secrecy of the key, not the secrecy of the algorithm
  - This makes it feasible for widespread use

Requirements (2 of 2)

- Manufacturers can and have developed low-cost chip implementations of data encryption algorithms
- These chips are widely available and incorporated into a number of products

Cryptography (1 of 3)

Cryptographic systems are generically classified along three independent dimensions:

- **The type of operations used for transforming plaintext to ciphertext**
  - Substitution
    - Each element in the plaintext is mapped into another element
  - Transposition
    - Elements in the plaintext are rearranged
    - Fundamental requirement is that no information be lost

Cryptography (2 of 3)

  - Product systems
    - Involve multiple stages of substitutions and transpositions

- **The number of keys used**
  - Referred to as symmetric, single-key, secret-key, or conventional encryption if both sender and receiver use the same key
  - Referred to as asymmetric, two-key, or public-key encryption if the sender and receiver each use a different key

Cryptography (3 of 3)

- **The way in which the plaintext is processed**
  - Block cipher processes the input one block of elements at a time, producing an output block for each input block
  - Stream cipher processes the input elements continuously, producing output one element at a time, as it goes along

Table 2-1: Types of Attacks on Encrypted Messages (1 of 2)

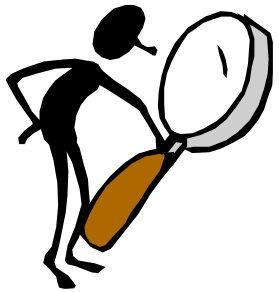
Type of Attack	Known to Cryptanalyst
Ciphertext only	•Encryption algorithm •Ciphertext to be decoded
Known plaintext	•Encryption algorithm •Ciphertext to be decoded •One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst. together with its corresponding ciphertext generated with the secret key

Table 2-1: Types of Attacks on Encrypted Messages (2 of 2)

Chosen ciphertext	•Encryption algorithm •Ciphertext to be decoded •Purported ciphertext chosen by cryptanalyst. together with its corresponding decrypted plaintext generated with the secret key
Chosen text	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst. together with its corresponding ciphertext generated with the secret key •Purported ciphertext chosen by cryptanalyst. together with its corresponding decrypted plaintext generated with the secret key

Cryptanalysis

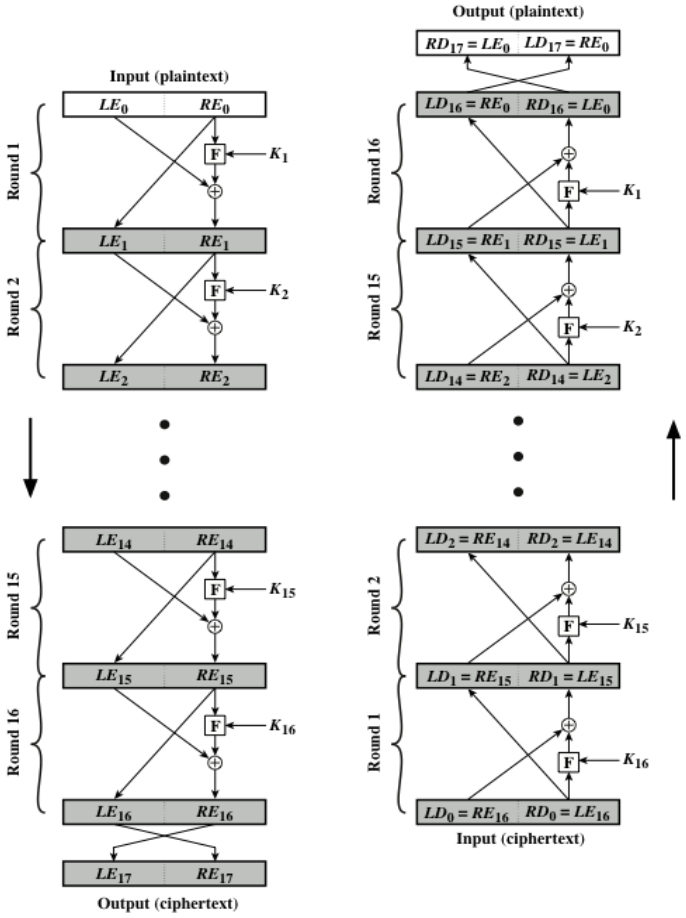
- An encryption scheme is computationally secure if the ciphertext generated by the scheme meets one or both of the following criteria:
  - The cost of breaking the cipher exceeds the value of the encrypted information
  - The time required to break the cipher exceeds the useful lifetime of the information



Brute Force Attack

- Involves trying every possible key until an intelligible translation of the cipher text into plaintext is obtained
- On average, half of all possible keys must be tried to achieve success
- Unless known plaintext is provided, the analyst must be able to recognize plaintext as plaintext
- To supplement the brute-force approach
  - Some degree of knowledge about the expected plaintext is needed
  - Some means of automatically distinguishing plaintext from garble is also needed

Figure 2-2: Feistel Encryption and Decryption (16 Rounds)



Feistel Cipher Design Elements (1 of 3)

Block size

- Larger block sizes mean greater security but reduced encryption/decryption speed

Key size

- Larger key size means greater security but may decrease encryption/decryption speed

Number of rounds

- The essence of a symmetric block cipher is that a single round offers inadequate security but that multiple rounds offer increasing security

Feistel Cipher Design Elements (2 of 3)

Sub key generation algorithm

- Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis

Round function

- Greater complexity generally means greater resistance to cryptanalysis

Feistel Cipher Design Elements (3 of 3)

Fast software encryption/decryption

- In many cases, encryption is embedded in applications or utility functions in such a way as to preclude a hardware implementation; accordingly, the seed of execution of the algorithm becomes a concern

Ease of analysis

- If the algorithm can be concisely and clearly explained, it is easier to analyze that algorithm for cryptanalytic vulnerabilities and therefore develop a higher level of assurance as to its strength

Symmetric Block Encryption Algorithms

- Block cipher
  - The most commonly used symmetric encryption algorithms
  - Processes the plaintext input in fixed-sized blocks and produces a block of ciphertext of equal size for each plaintext block
- The three most important symmetric block ciphers
  - Data Encryption Standard (DES)
  - Triple DES (3DES)
  - Advanced Encryption Standard (AES)

Data Encryption Standard (DES)

- Most widely used encryption scheme
- Issued in 1977 as Federal Information Processing Standard 46 (FIPS 46) by the National Institute of Standards and Technology (NIST)
- The algorithm itself is referred to as the Data Encryption Algorithm (DEA)

DES Algorithm (1 of 2)

- Description of the algorithm:
  - Plaintext is 64 bits in length
  - Key is 56 bits in length
  - Structure is a minor variation of the Feistel network
  - There are 16 rounds of processing
  - Process of decryption is essentially the same as the encryption process

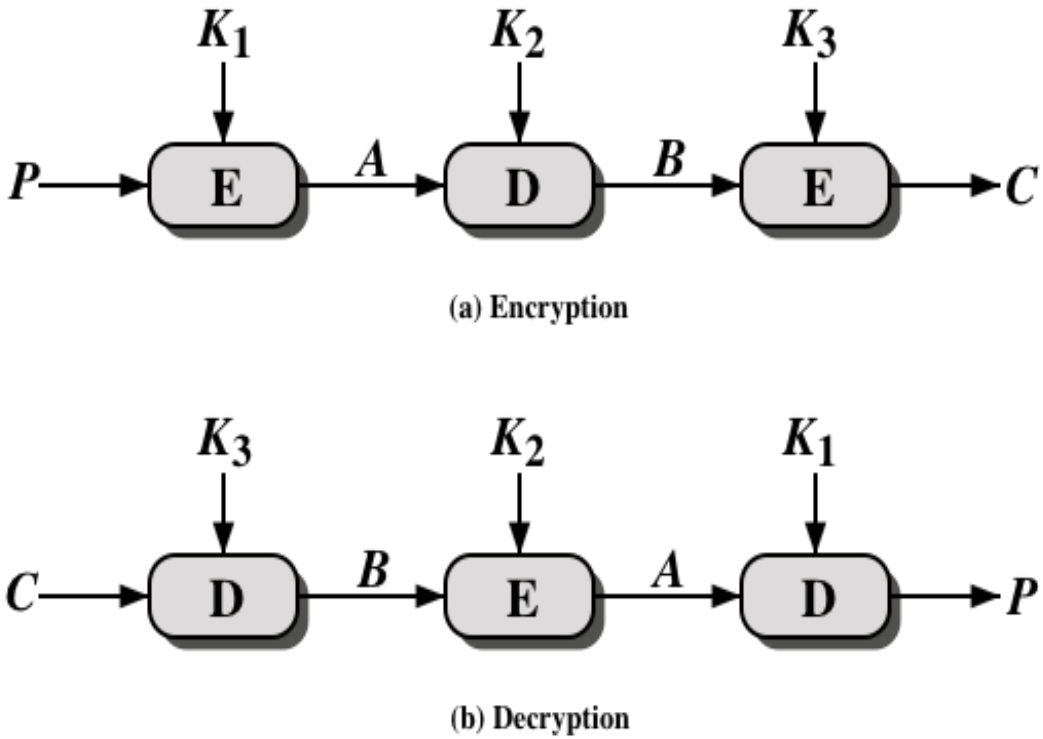
DES Algorithm (2 of 2)

- The strength of DES:
  - Concerns fall into two categories
    - The algorithm itself
      - Refers to the possibility that cryptanalysis is possible by exploiting the characteristics of the algorithm
    - The use of a 56-bit key
      - Speed of commercial, off-the-shelf processors threatens the security

Table 2-2: Average Time Required for Exhaustive Key Search

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at decryptions/s	Time Required at decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns $= 1.125$ years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns $= 5.3 \times 10^{21}$ *years*	5.3×10^{17} *years*
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns $= 5.8 \times 10^{33}$ years	5.8×10^{29} *years*
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns $= 9.8 \times 10^{40}$ years	9.8×10^{36} *years*
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns $= 1.8 \times 10^{60}$ years	1.8×10^{56} *years*

Figure 2-3: Triple DES



3DES Guidelines

- FIPS 46-3 includes the following guidelines for 3DES:
  - 3DES is the FIPS-approved symmetric encryption algorithm of choice
  - The original DES, which uses a single 56-bit key, is permitted under the standard for legacy systems only; new procurements should support 3DES
  - Government organizations with legacy DES systems are encouraged to transition to 3DES
  - It is anticipated that 3DES and the Advanced Encryption Standard (AES) will coexist as FIPS-approved algorithms, allowing for a gradual transition to AES

Advanced Encryption Standard (AES) (1 of 2)

- In 1997 NIST issued a call for proposals for a new AES:
  - Should have a security strength equal to or better than 3DES and significantly improved efficiency
  - Must be a symmetric block cipher with a block length of 128 bits and support for key lengths of 128, 192, and 256 bits
  - Evaluation criteria included security, computational efficiency, memory requirements, hardware and software suitability, and flexibility

Advanced Encryption Standard (AES) (2 of 2)

- NIST selected Rijndael as the proposed AES algorithm
  - FIPS PUB 197
  - Developers were two cryptographers from Belgium: Dr. Joan Daemen and Dr. Vincent Rijmen

Figure 2-4: AES Encryption and Decryption

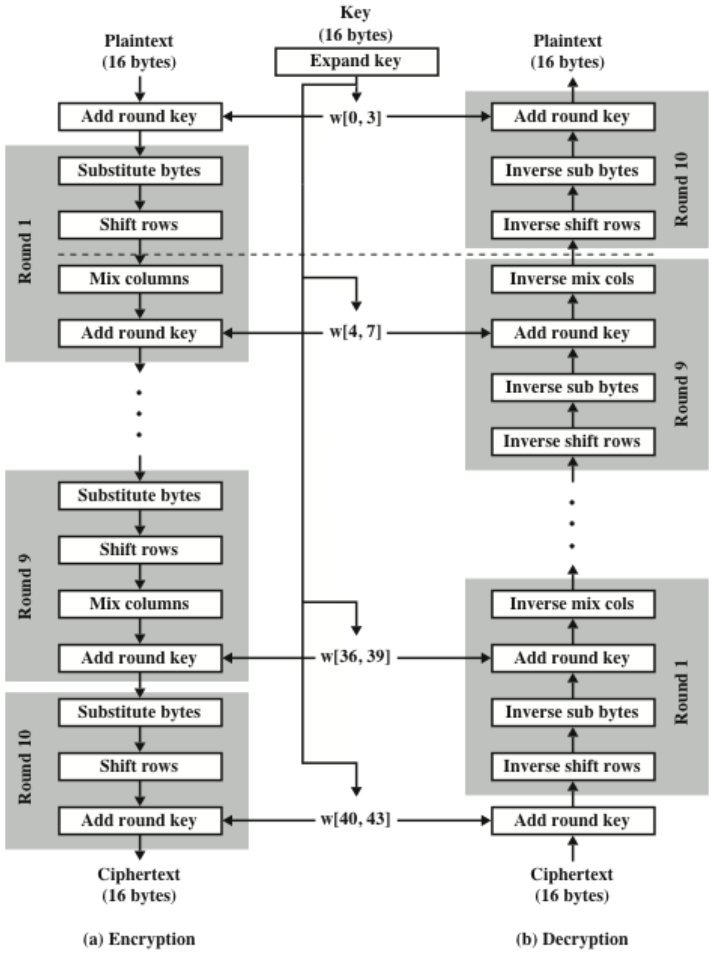
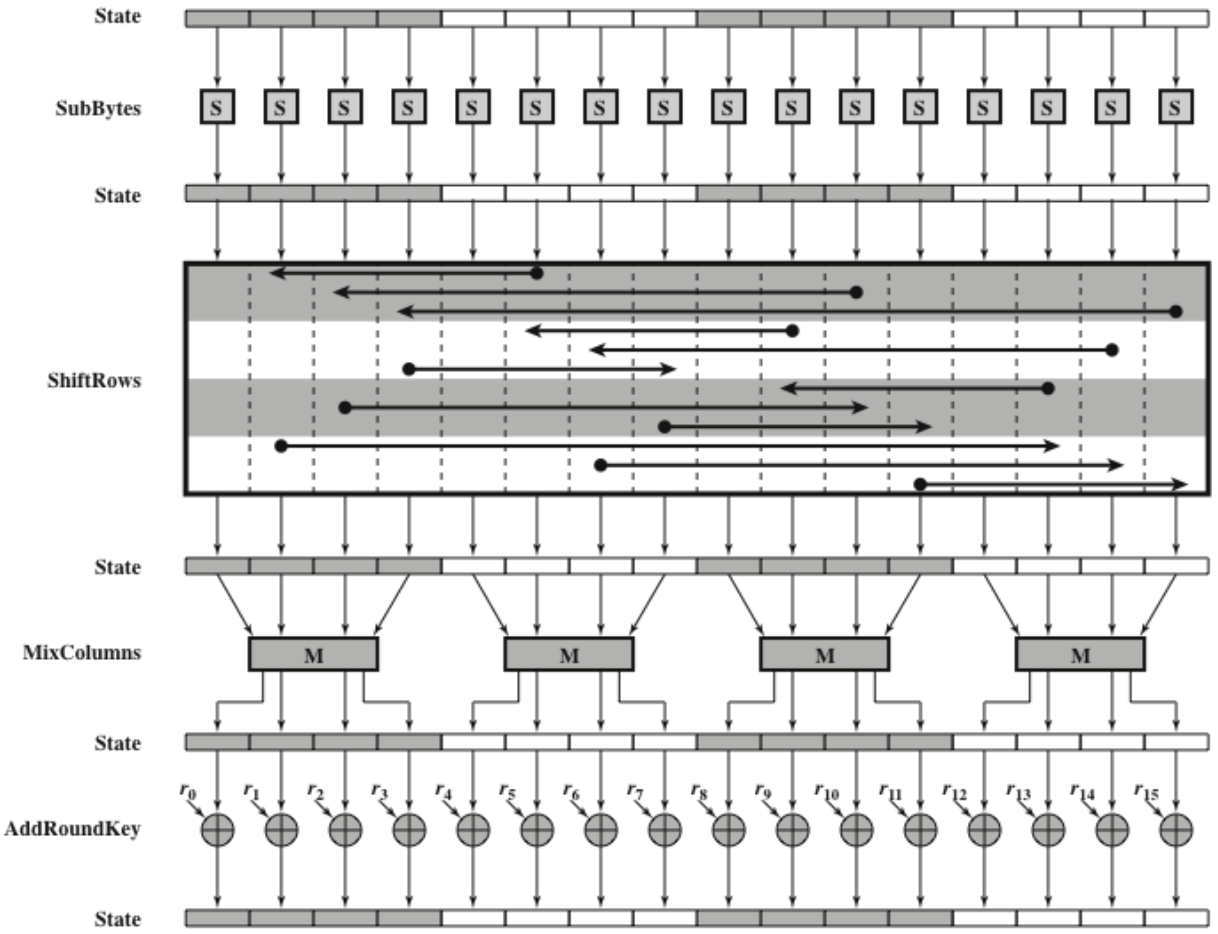


Figure 2-5: AES Encryption Round



AES modes of operations

- AES has several modes of operations
  - ECB (Electronic Codebook): Encrypts each block of plaintext separately
  - CBC (Cipher Block Chaining): XORs each plaintext block with the previous ciphertext block
  - CFB (Cipher feedback): Encrypts the initialization vector (IV) and XOR the resulting output with the plaintext.
  - …….

Initialization Vector (IV) in AES

- IV is required for some modes in AES such as the CFB mode.
  - CFB (Cipher feedback): Encrypts the initialization vector (IV) and XOR the resulting output with the plaintext.
- Purpose: to enhance security, different encryption should use unique IV (but not secret IV).
  - Consider encrypting a pdf file, which has the same header field.
  - Without using IV, all encrypted pdf file will have the same first few blocks – some information is leaked.
  - Using IV solves this problem

Symmetric Encryption in Python

- There are several cryptography libraries in Python
- On linprog, pycryptodomex has been installed.
- See lect15/encryption.py for an example AES encryption/decryption class.

Copyright