CYB 241 Digital Cryptography Techniques

Block Ciphers and DES

Stream Cipher

- Encrypts a digital data stream one bit or one byte at a time
  - Examples:
    - Autokeyed Vigenère cipher
    - Vernam cipher
- In the one-time pad version of the Vernam cipher, the keystream is as long as the plaintext bit stream
  - If the cryptographic keystream is random, then this cipher is unbreakable by any means other than acquiring the keystream
    - Keystream must be provided to both users in advance via some independent and secure channel
    - This introduces logistical problems if the intended data traffic is very large

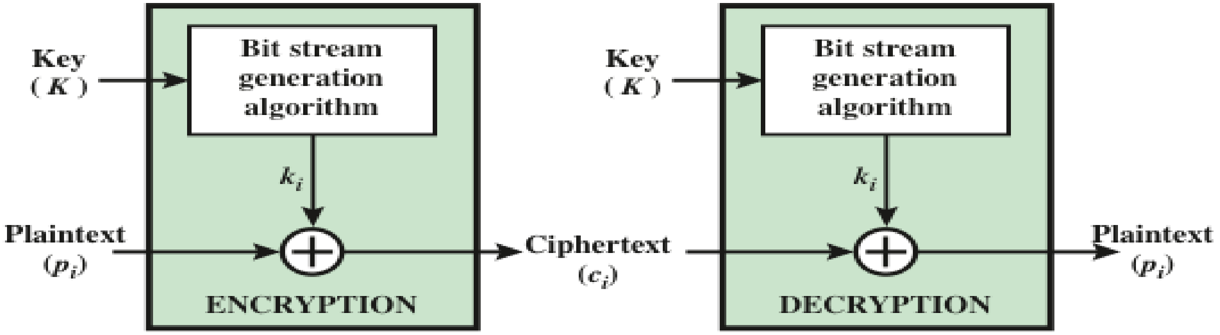
Stream Cipher

- For practical reasons the bit-stream generator must be implemented as an algorithmic procedure so that the cryptographic bit stream can be produced by both users
  - It must be computationally impractical to predict future portions of the bit stream based on previous portions of the bit stream
  - The two users need only share the generating key and each can produce the keystream

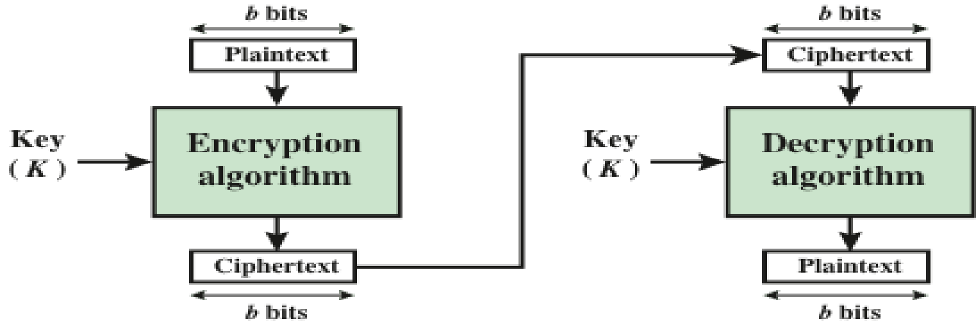
Block Ciphers

- Encrypt data one block at a time
- Used in broader range of applications
- Typical block size 64 – 128 bits
- As with a stream cipher, the two users share a symmetric encryption key
- Most algorithms based on a structure referred to as Feistel block cipher

Figure 4-1 Stream Cipher and Block Cipher



(a) Stream Cipher Using Algorithmic Bit Stream Generator



(b) Block Cipher

Block Cipher Principles

- Input: a plaintext block of n bits
- Output: a ciphertext block of n bits
- 2^n possible plaintext blocks
- Encryption must be reversible (decryption possible)
  - Each plaintext has a unique ciphertext
- $2^n!$ possible mapping between plaintext and ciphertext

Feistel Cipher

- Build strong cipher that alternates substitutions & permutations
- Key length k, block length n
- A product cipher that alternates confusion and diffusion functions
  - **Diffusion**: each plaintext digit affect the value of many ciphertext digits
  - **Confusion**: the way in which the key was used to produce that ciphertext is so complex as to make it difficult to deduce the key

Feistel Cipher Structure

- Input
  - plaintext block of length 2w
  - key K
- Plaintext block divided to LE_0, RE_0
- Pass thru *n* rounds of processing
- Each round i has
  - LE_{i-1}, RE_{i-1} derived from previous round
  - subkey K_i derived from overall K

Feistel Cipher Structure

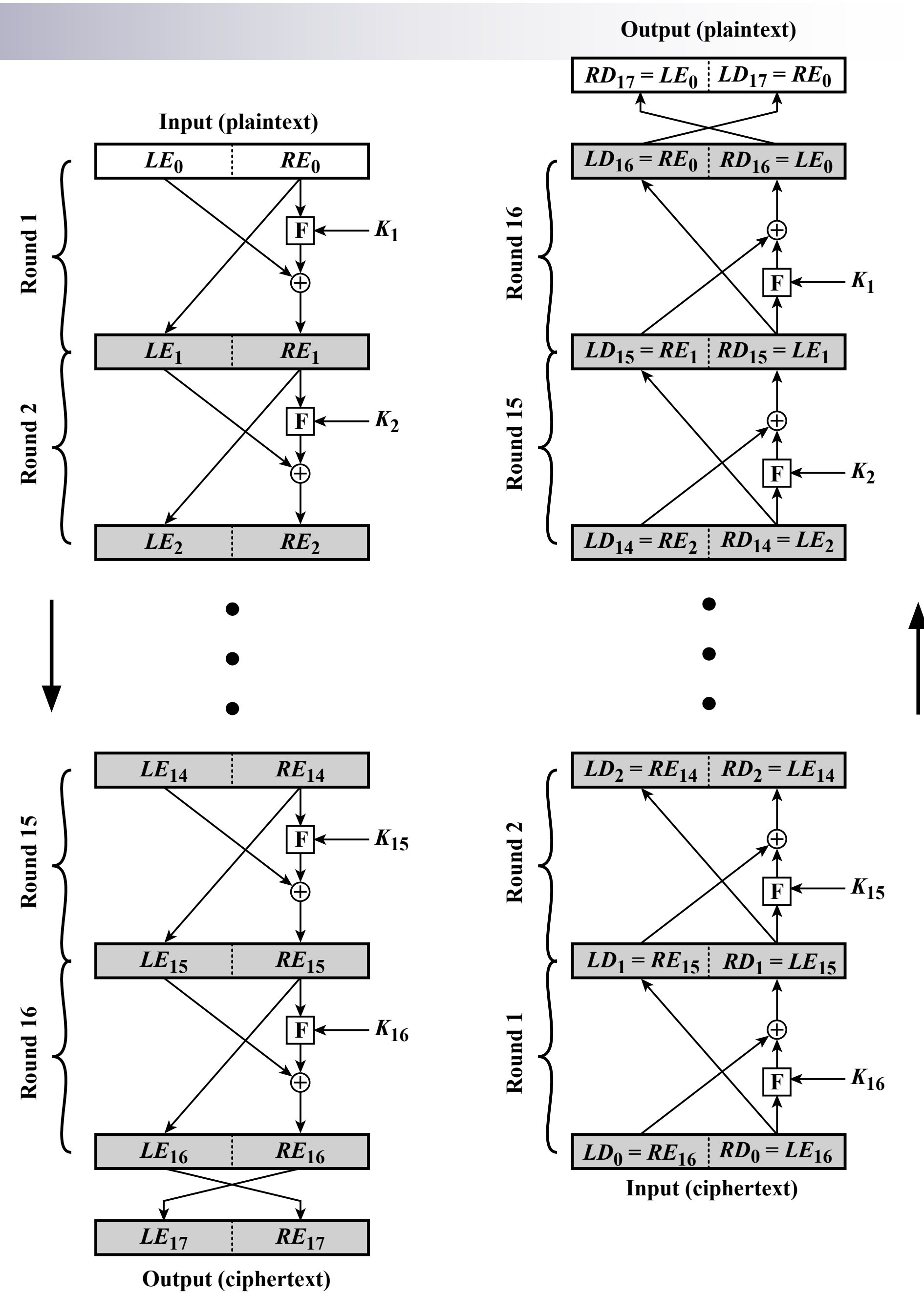


Figure 3.3 Feistel Encryption and Decryption (16 rounds)

Feistel Cipher Structure

- Substitution performed to left half
  - apply round function F to right half
  - take XOR of output with left half
  - F is parameterized by round subkey K_i
- Permutation of left and right halves
  - interchange left and right halves
- Notation
  - LE_i and RE_i: left and right half in encryption
  - LD_i and $RD_{i:}$:left and right half in decryption

Feistel Example

Figure 3.4 Feistel Example

Design Parameters

- Block size
  - larger: greater security (diffusion)
  - smaller: faster encryption, decryption
  - typical: 64 bit, 128 bit AES
- Key size
  - larger: greater security (brute-force resistance)
  - smaller: faster encryption, decryption
  - typical: 128 bit

Design Parameters

- Number of rounds
  - multiple rounds increase security
  - typical: 16
- Subkey generation algorithm
  - complexity makes cryptanalysis difficult
- Round function
  - complexity makes cryptanalysis difficult

Data Encryption Standard (DES)

- Issued in 1977 by the National Bureau of Standards (now NIST)
- Was the most widely used encryption scheme until the introduction of the Advanced Encryption Standard (AES) in 2001
- Algorithm itself is referred to as the Data Encryption Algorithm (DEA)
  - Data are encrypted in 64-bit blocks using a 56-bit key
  - The algorithm transforms 64-bit input in a series of steps into a 64-bit output
  - The same steps, with the same key, are used to reverse the encryption

DES Encryption

- 64-bit plaintext block
- 56-bit key
- Exact structure as Feistel except
  - initial permutation of plaintext
  - final permutation of last round’s output

Avalanche Effect

- Small change in P → large change in C
- 1 bit change in P or K → many bits change in C
- Makes cryptanalysis more difficult
- DES exhibits strong avalanche effect

Avalanche Effect – Example

(a) Change in Plaintext			(b) Change in Key	
Round	Number of bits that differ		Round	Number of bits that differ
0	1		0	0
1	6		1	2
2	21		2	14
3	35		3	28
4	39		4	32
5	34		5	30
6	32		6	32
7	31		7	35
8	29		8	34
9	42		9	40
10	44		10	38
11	32		11	31
12	30		12	33
13	30		13	28
14	26		14	26
15	29		15	34
16	34		16	35

DES Security

- 1977
  - estimated brute-force attack
  - cost: ~ $20 million
  - time: ~ 10 hours
- 1998
  - DES definitely proved insecure
  - EFF designed “DES Cracker”
  - cost: < $250,000
  - time: < 3 days
- Today: 56 bits considered too short to withstand brute force attack

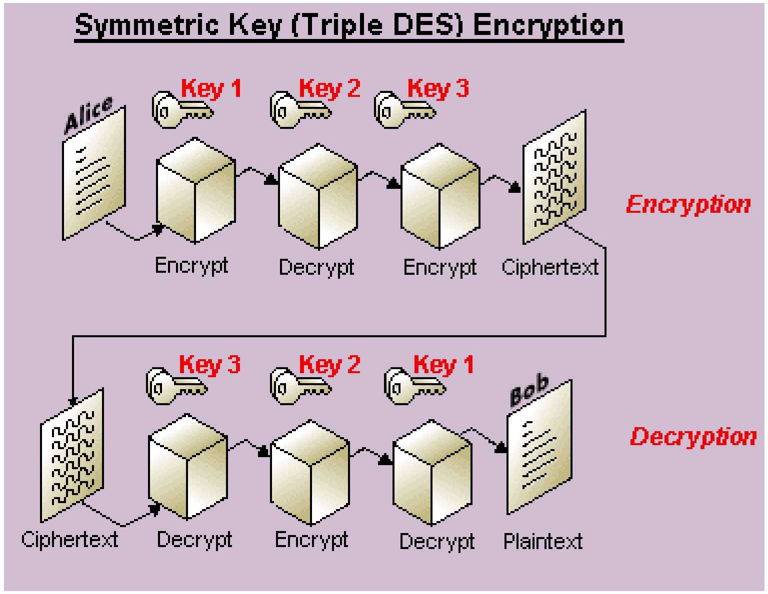
Table 4-5 Average Time Required for Exhaustive Key Search

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} 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 = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years
26 characters (permutation)	Monoalphabetic	$26! = 4 \times 10^{26}$	2×10^{26} ns = 6.3×10^{9} years	6.3×10^{6} years

Pearson

Multiple Encryption with DES

- Alternative block cipher that makes use of DES software/equipment/knowledge: encrypt multiple times with different keys
- Triple DES with 3 keys (168 bits)
  - Why E-D-E?
  - To be compatible with single DES



Reading Assignment

- Textbook
  - chapter 4
    - 4.1, 4.2, 4.3