Introduction to Cryptography CS 355

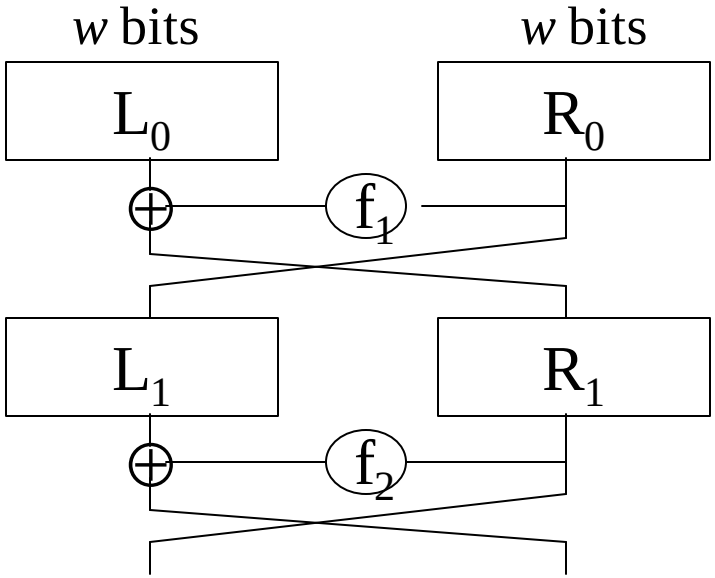
Lecture 16

Encryption Modes & Other Block Ciphers

Announcements

- Homework due
- Mid-term exam Thursday October 13 (7pm to 9pm) in CS G066

Review: Feistel Network



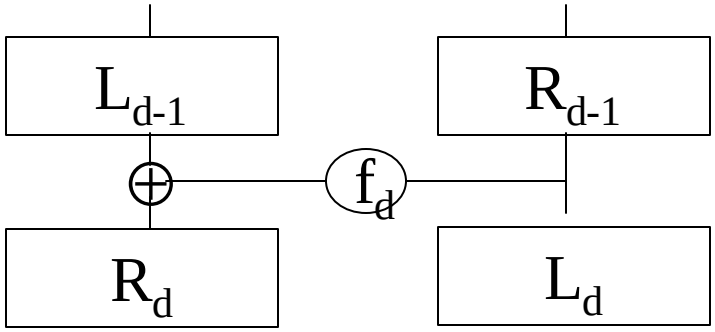
Encryption:

$L_1=R_0 \qquad R_1=L_0 \oplus f_1(R_0)$

$L_2=R_1 \qquad R_2=L_1 \oplus f_2(R_1)$

…

$L_d=R_{d-1} \qquad R_d=L_{d-1} \oplus f_d(R_{d-1})$



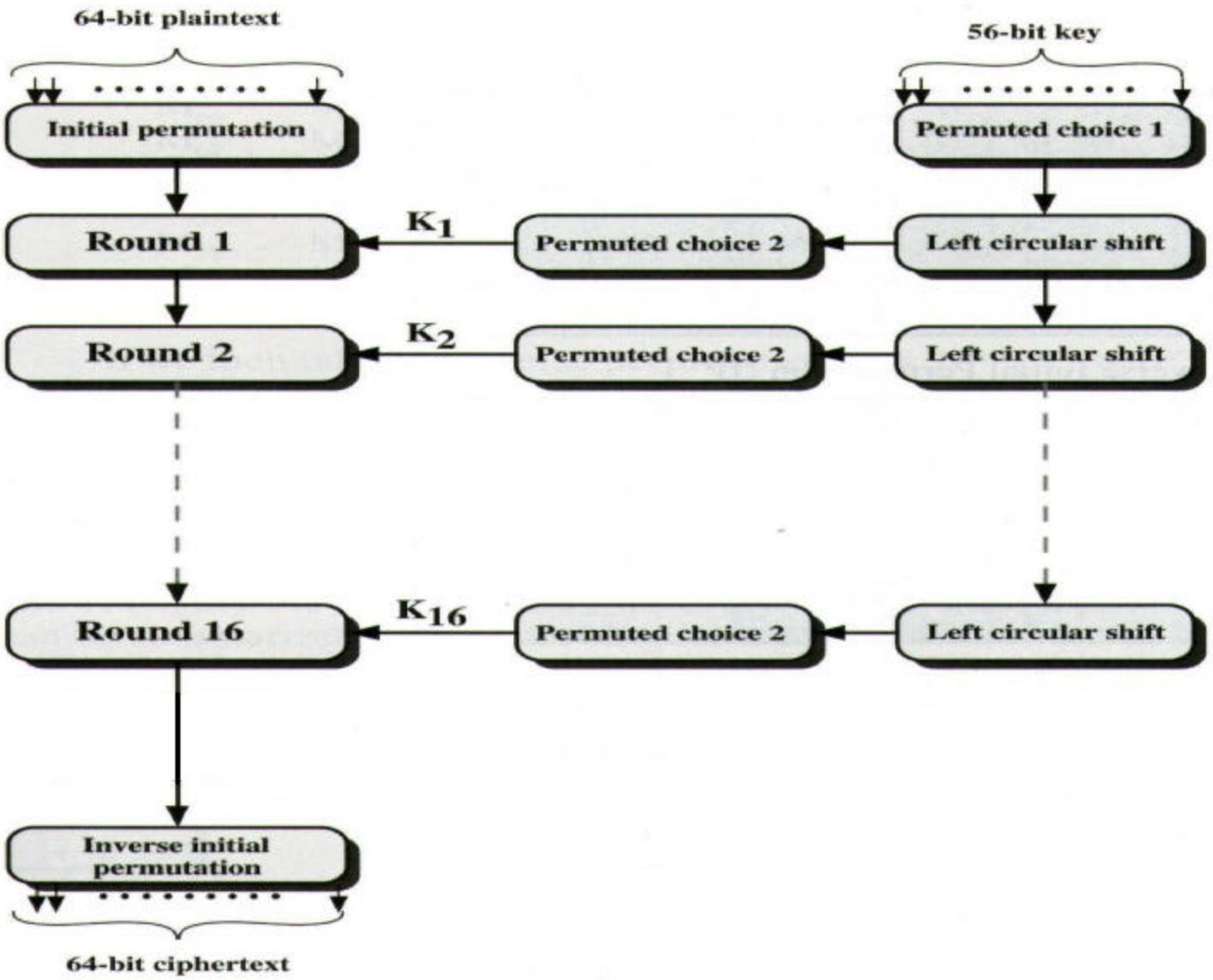
Decryption:

$R_{d-1}=L_d \qquad L_{d-1}=R_d \oplus f_d(L_d)$

…

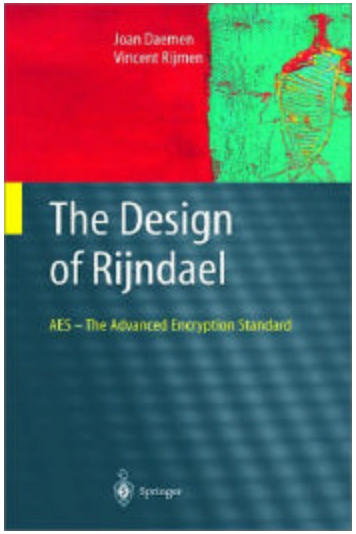
$R_0=L_1; \qquad L_0=R_1 \oplus f_1(L_1)$

Review: DES


64-bit plaintext
56-bit key
Initial permutation
Permuted choice 1
Round 1
K1
Permuted choice 2
Left circular shift
Round 2
K2
Permuted choice 2
Left circular shift
Round 16
K16
Permuted choice 2
Left circular shift
Inverse initial permutation
64-bit ciphertext

Rijndael Features

- Designed to be efficient in both hardware and software across a variety of platforms.
- Not a Feistel Network
- Uses a variable block size, **128,192, 256-bits**, key size **of 128-, 192-, or 256-bits.**
- Variable number of rounds (10, 12, 14):
  - 10 if B = K = 128 bits
  - 12 if either B or K is 192 and the other is ≤ 192
  - 14 if either B or K is 256 bits
- Note: AES uses a 128-bit block size.



Lecture Outline

- Encryption Modes
- Other Block Ciphers

Block Cipher Encryption Modes: ECB

- Message is broken into independent blocks of *block_size* bits;
- Electronic Code Book (ECB): each block encrypted separately.
- **Encryption: $c_i = E_k(x_i)$**
- **Decrytion: $x_i = D_k(c_i)$**

Properties of ECB

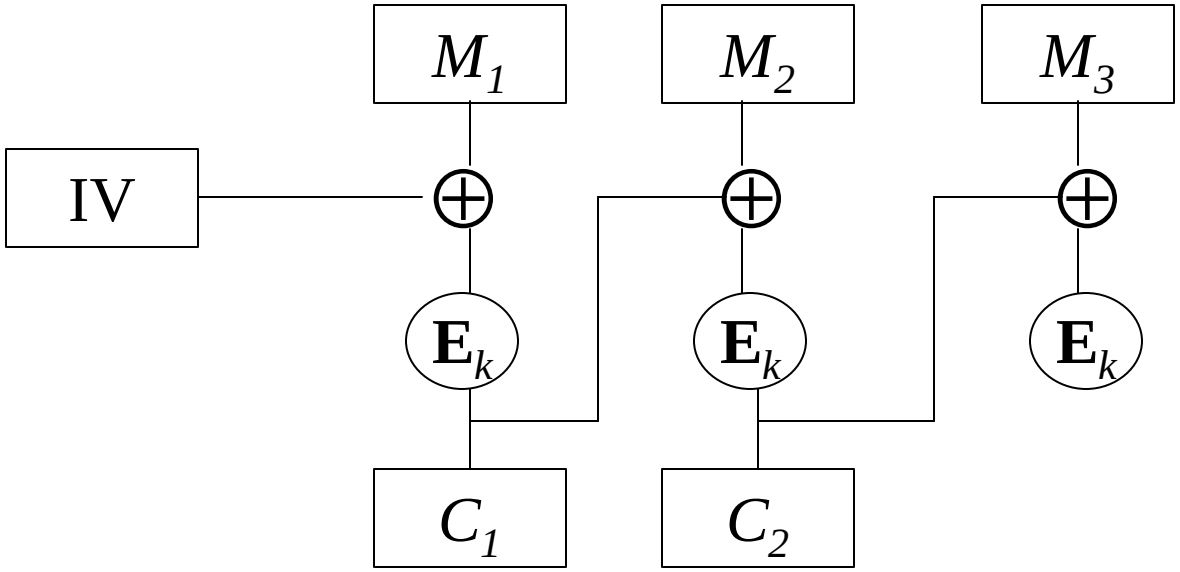
- Deterministic: the same data block gets encrypted the same way, reveals patterns of data when a data block repeats
- Malleable: reordering ciphertext results in reordered plaintext.
- Errors in one ciphertext block do not propagate.
- Usage: not recommended to encrypt more than one block of data

DES Encryption Modes: CBC

- Cipher Block Chaining (CBC): next input depends upon previous output

  Encryption: $C_i = E_k(M_i \oplus C_{i-1})$, **with** $C_0 = IV$

  Decryption: $M_i = C_{i-1} \oplus D_k(C_i)$, **with** $C_0 = IV$



Properties of CBC

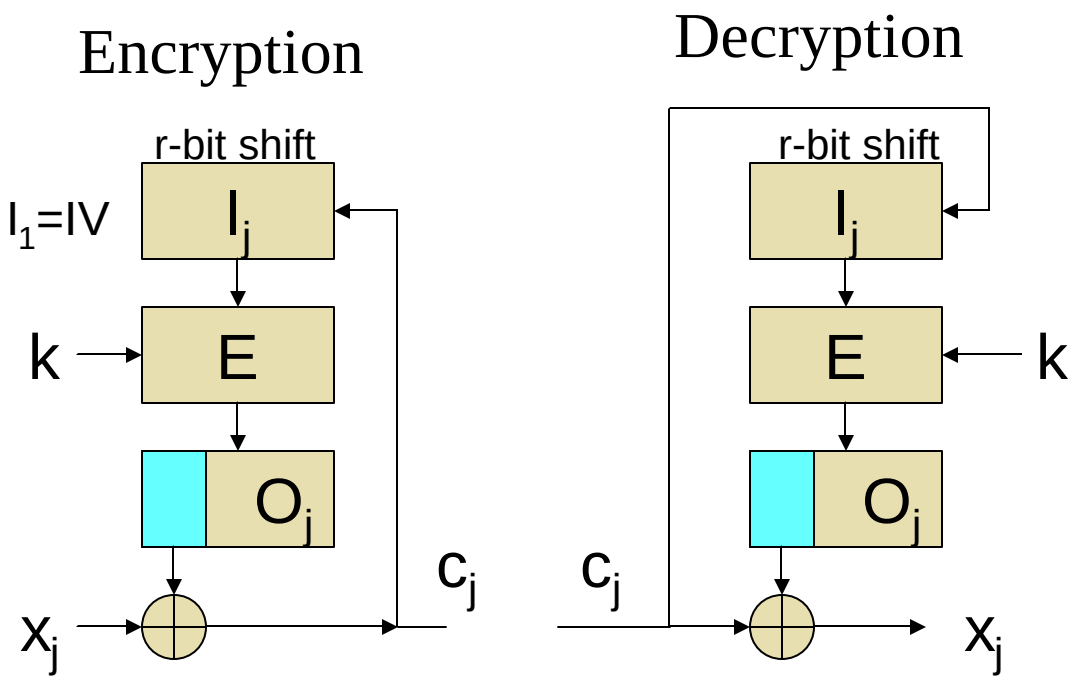
- Randomized encryption: repeated text gets mapped to different encrypted data.
  - can be proven to be “secure” assuming that the block cipher has desirable properties and that random IV’s are used
- A ciphertext block depends on all preceding plaintext blocks; reorder affects decryption
- Errors in one block propagate to two blocks
  - one bit error in C_j affects all bits in M_j and one bit in M_{j+1}
- Sequential encryption, cannot use parallel hardware
- Usage: chooses random IV and protects the integrity of IV
- Observation: if $C_i = C_j$ then $\mathbf{E_k}(M_i \oplus C_{i-1}) = \mathbf{E_k}(M_j \oplus C_{j-1})$; **thus** $M_i \oplus C_{i-1} = M_j \oplus C_{j-1}$; **thus** $M_i \oplus M_j = C_{i-1} \oplus C_{j-1}$

Use DES to construct Stream Ciphers

- Cipher Feedback (CFB)
- Output feedback (OFB)
- Counter Mode (CTR)
- Common properties:
  - uses only the encryption function of the cipher both for encryption and for decryption
  - malleable: possible to make predictable bit changes

Encryption Modes: CFB

- Cipher Feedback (CFB): the message is XORed with the feedback of encrypting the previous block

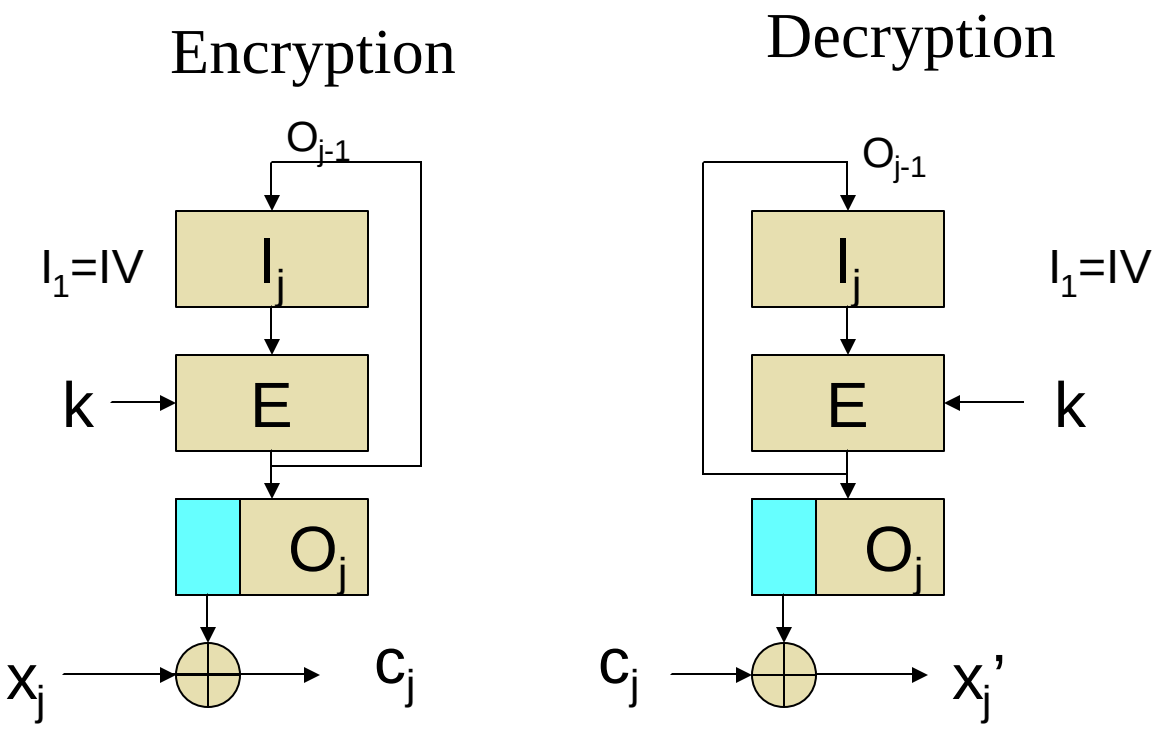


Properties of CFB

- Randomized encryption
- A ciphertext block depends on all preceding plaintext blocks; reorder affects decryption
- Errors propagate for several blocks after the error, but the mode is self-synchronizing (like CBC).
- Decreased throughput.
  - Can vary the number of bits feed back, trading off throughput for ease of use
- Sequential encryption

Encryption Modes: OFB

- Output feedback (OFB):
  - construct a PRNG using DES
  - y_0=IV $y_i = E_k[y_{i-1}]$



Properties of OFB

- Randomized encryption
- Sequential encryption, but pre-processing possible
- Error propagation limited
- Subject to limitation of stream cipher

Encryption Modes:CTR

- Counter Mode (CTR): Another way to construct PRNG using DES
  - $y_i = E_k[\text{counter}+i]$
  - Sender and receiver share: counter (does not need to be secret) and the secret key.

Properties of CTR

- Software and hardware efficiency: different blocks can be encrypted in parallel.
- Preprocessing: the encryption part can be done offline and when the message is known, just do the XOR.
- Random Access: decryption of a block can be done in random order, very useful for hard-disk encryption.
- Messages of Arbitrary Length: ciphertext is the same length with the plaintext (i.e., no IV).

International Data Encryption Algorithm (IDEA)

- Originally designed by Massey and Lai at ETH (Zurich), 1990.
- Based on mixing operations from different algebraic groups (XOR, addition mod 2^{16} , multiplication mod 2^{16} +1).
- All operations are on 16-bit sub-blocks, with no permutations used.
- Speed: faster than DES in software.

IDEA

- Features:
  - 128-bit key
  - 64 bit blocks
  - 8 rounds,
  - operates on 16-bit numbers

RC5

- Proprietary cipher owned by RSA Data Security (designed by Ron Rivest).
- Very fast, operates on words.
- Variable key size, block size and number of rounds.
- Clean and simple design.

RC5 Features

- RC5 is a family of ciphers rc5-w/r/b
  - W = word size in bits (16/32/64) nb data=2w
  - R = number of rounds (0..255)
  - B = number of bytes in the key (0..255)

- Widely used version is RC5-32/12/16
  - 32-bit words so encrypts 64-bit data blocks
  - Using 12 rounds
  - 16 bytes (128-bit) secret key

Coming Attractions …

- Cryptanalysis of DES
- Security of Block Ciphers