Introduction to Cryptography CS 355

Lecture 22

Mid Term Review

Grade Distribution for mid-term

- 90 to 94 4
- 80 to 89 6
- 70 to 79 7
- 60 to 69 8
- under 60 3

Projected Grade Distribution

- Formula used for projection
  - [(HW1+HW2+HW3)*0.06 + (Q1+Q2+Q3)/9 + MT *0.3] * 2
- Over 90 2
- 80 to 89 7
- 70 to 79 9
- 58 to 69 9
- Under 57 1

Problem 1

- 1.a $0.9^2 + 0.1^2 = 0.81 + 0.01 = 0.82$
- 1.b Most likely key length is 3
- 1.c Kasiski attack
- 1.d
  - In known-plaintext attacks, one is given some random pairs of plaintexts and ciphertexts. In chosen-plaintext attacks, one can choose some plaintexts and get corresponding ciphertexts.
- 1.e frequency analysis

Problem 2

- 2-a Require keys as long as messages
- 2-b
  - No. Any cipher that has perfect secrecy must have keys as long as messages
- 2-c $63 = 2^6-1$, so answer is 6 stages
- 2-d
  - No. LFSR output is predictable given a short output sequence.
- 2-e $x_{n+3} = x_{n+2} + x_n$ 001110100111

Problem 3

- 3-a 128, 192, 256
- 3-b 56, 57, 112
- 3-c block size: 64, key size: 56+128=184
- 3-d use meet-in-the-middle attack
  - $C = DES_{k1}[IDEA_{k2}[M]]$
  - So $DES_{k1}^{-1}[C] = IDEA_{k2}[M]$
  - Build a table that contains DES decryption of C under all 2^{56} keys
  - Then do exhaustive key search on k2
  - Each time finding a match, use (M',C') and (M'',C'') to verify whether this is indeed the key

Problem 4

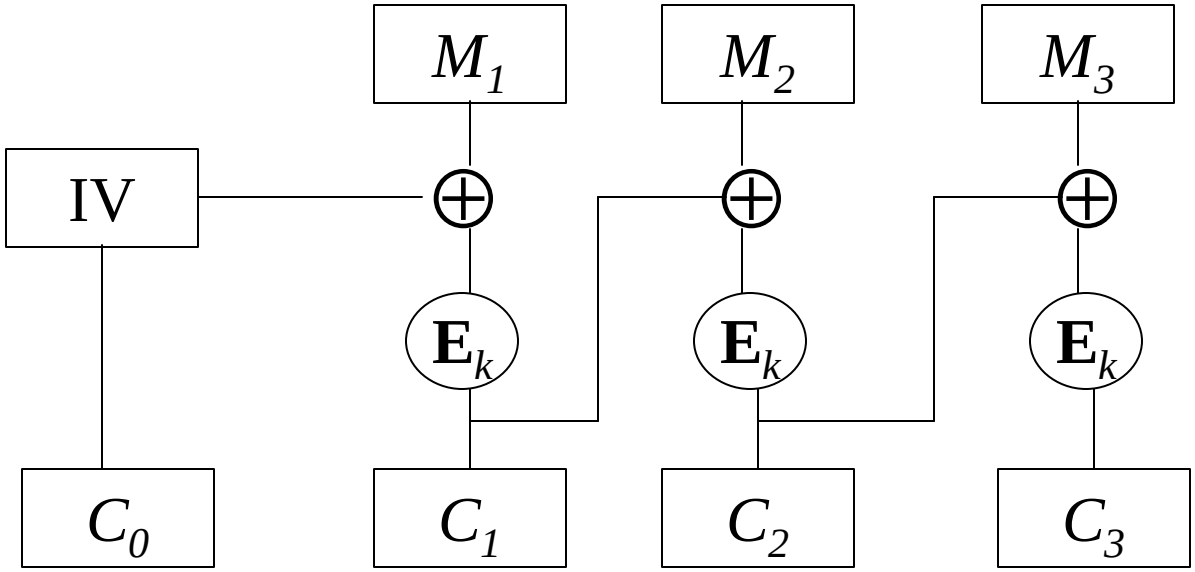
- 4-a ECB, CTR
  - all other modes use previous ciphertext as input
- 4-b CTR
- 4-c $C_1=E_k[M_1 \oplus C_0]$, $C_2=E_k[M_2 \oplus C_1]$
- 4-d
  - The adversary can picks M_0 to be two repeating blocks and M_1 to be two different blocks.
  - If the ciphertext is two repeating blocks, then M_0 is encrypted; otherwise, M_1 is.

DES Encryption Modes: CBC

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

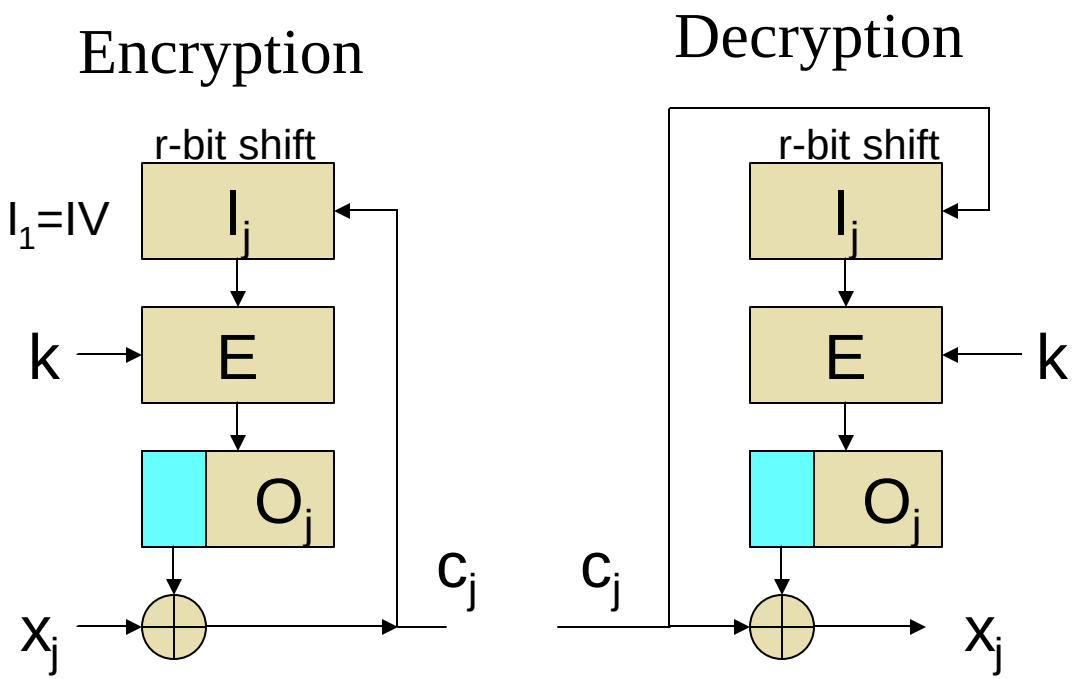
  Encryption: $C_i = E_k(M_i \oplus C_{i-1})$, **with** $C_0 = IV$

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



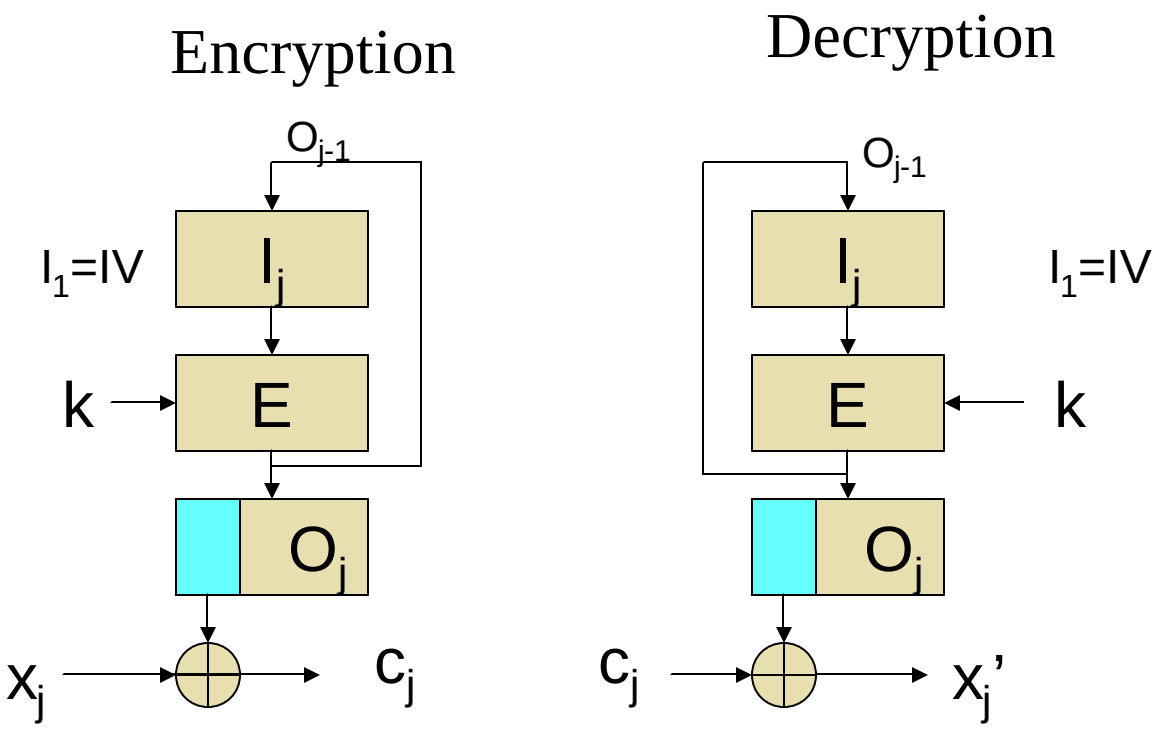
Encryption Modes: CFB

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



Encryption Modes: OFB

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



Problem 5

- 5-a
  - $L_2 = R_1 = L_0 \oplus DES_{k1}[R_0]$
  - $R_2 = L_1 \oplus DES_{k2}[R_1] = R_0 \oplus DES_{k2}[L_0 \oplus DES_{k1}[R_0]]$
- 5-b
  - $R_1 = L_2$, $L_1 = R_2 \oplus DES_{k2}[R_1]$ $R_0 = L_1 = R_2 \oplus DES_{k2}[L_2]$
  - $L_0 = R_1 \oplus DES_{k1}[R_0] = L_2 \oplus DES_{k1}[R_0]$
- 5-c
  - $L_2 \oplus L_0 = DES_{k1}[R_0]$ exhaustive key search finds k1
  - $R_0 \oplus R_2 = DES_{k2}[L_2]$ exhaustive key search finds k2
- 5-d no

Problem 6

- 6-a
  - $6x \equiv 9 \pmod{50}$ no solution
  - $7x \equiv 10 \pmod{50}$ 1 solution
  - $8x \equiv 12 \pmod{50}$ 2 solutions
- 6-b $\phi(99) = \phi(9) \cdot \phi(11) = 6 \cdot 10 = 60$
- 6-c
  - $493^{64} \equiv 3^{64} \equiv (3^4)^{16} \equiv 1^{16} \equiv 1 \pmod{10}$
    - $3^2 \equiv 9 \pmod{10}$ $3^4 \equiv 9^2 \equiv 1 \pmod{10}$
    - $\phi(10) = \phi(2) \cdot \phi(5) = 4$
- 6-d See HW2 solution

Problem 7-b

- Need to show that $(M^e)^d \pmod n = M$, $n = pq$
  - $ed \equiv 1 \pmod{\phi(n)}$, so $ed = k\,\phi(n) + 1$, for some integer k.
- When gcd(M, n) = 1, then

$$M^{ed} \equiv M^{1+k\phi(n)} \equiv M \cdot (M^{\phi(n)})^k \equiv M \pmod n$$

- When gcd(M, n) $\neq$1. Wlog, assume gcd(M,n)=p
  - $M^{ed} \bmod p = (M \bmod p)^{ed} \bmod p = 0$
    so $M^{ed} \equiv M \bmod p$
  - $M^{ed} \bmod q = (M^{k*\Phi(n)} \bmod q)\,(M \bmod q) = M \bmod q$
    so $M^{ed} \equiv M \bmod q$
  - As p and q are distinct primes, it follows from the CRT that $M^{ed} \equiv M \bmod pq$

Coming Attractions …

- Attacks on RSA