Cristina Nita-Rotaru

# CS355: Cryptography

## Lecture 8: Cryptanalysis of DES. Encryption modes.

# DES weak keys

- Definition: A DES weak key is a key K such that $E_K(E_K(x))=x$ for all x, i.e., encryption and the decryption is the same
  - these keys make the same sub-key to be generated in all rounds.
- DES has 4 weak keys (only the 56-bit part of it)

  0000000 0000000

  0000000 FFFFFFF

  FFFFFFF 0000000

  FFFFFFF FFFFFFF

- Weak keys should be avoided at key generation.

# DES semi-weak keys

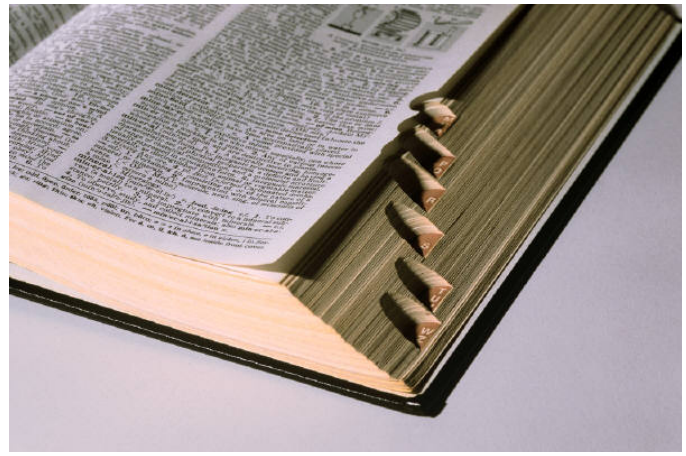
- Definition: A pair of DES semi-weak keys is a pair (K1,K2) with $E_{K1}(E_{K2}(x))=x$
- There are six pairs of DES semi-weak keys

# Cryptanalysis of DES: Brute force

- Known-Plaintext Attack
- Try all $2^{56}$ possible keys
- Requires constant memory
- Time-consuming
- DES challenges: (RSA)
  - 1997 Internet search: 3 months
  - 1998 EFF machine (costs $250K): 3 days
  - 1999 Combined: 22 hours
  - 2006 COPACOBANA machine,Universities of Bochum and Kiel, costs $10K

# Cryptanalysis of DES

**Dictionary attack:**



- Each plaintext may result in $2^{64}$ different ciphertexts, but there are only $2^{56}$ possible different values.
- Encrypt the known plaintext with all possible keys.
- Keep a look up table of size $2^{56}$.
- Given a PT/CT pair ($M$,$C$), look up $C$ in the table

# Double DES

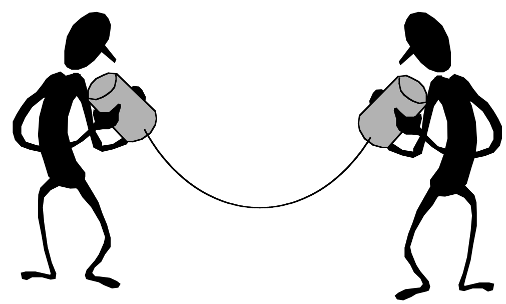
- DES uses a 56-bit key, this raised concerns about brute force attacks.
- One proposed solution: double DES.
- Apply DES twice using two keys, K1 and K2.

$$C = E_{K_2}[\, E_{K_1}[\, P \,]\,]$$
$$P = D_{K_2}[\, D_{K_1}[\, C \,]\,]$$

- This leads to a 2x56=112 bit key, so it is more secure than DES. **Is it?**

# Meet-in-the-middle attack

- Goal: given the pair (P, C) find keys $K_1$ and $K_2$.
- Based on the observation:



$$C = E_{K_2}[\, E_{K_1}[\, P \,]\,]$$

$$D_{K_2}[\, C \,] = E_{K_1}[\, P \,]$$

- The attack has higher chance of succeeding if another pair (P', C') is available to the cryptanalysis.

# Meet-in-the-middle attack (cont.)

$$C = E_{K_2}[\,E_{K_1}[\,P\,]\,]$$
$$E_{K_1}[\,P\,] = D_{K_2}[\,C\,]$$

Attack, assumes the attacker knows two pairs (P,C) and (P' C' ):

- Encrypt P with all $2^{56}$ possible keys $K_1$
- Store all pairs ( $K_1$, $E_{K_1}[P]$ ), sorted by $E_{K_1}[P]$.
- Decrypt C using all $2^{56}$ possible keys $K_2$
- For each decrypted result, check to see if there is a match $D_{K_2}(C) = E_{K_1}(P)$.
- If yes, try another pair (P' , C' )
- If a match is found on the new pair, accept the keys $K_1$ and $K_2$.

# Why two pairs (P, C)?

- DES encrypts 64-bit blocks, so for a given plaintext P, there are $2^{64}$ potential ciphertexts C.
- Key space: two 56-bit key, so there are $2^{112}$ potential double keys that can map P to C.
- Given a pair (P, C), the number of double keys $(K_1, K_2)$ that produce $C = E_{K_2} [E_{K_1} [P] ]$ is at most $2^{112}/2^{64} = 2^{48}$
- Therefore, for a pair (P, C), $2^{48}$ false alarms are expected.

# Why two pairs (P, C)? (cont.)

- With one more pair (P', C'), extra 64-bit of known text, the alarm rate is $2^{48}/2^{64} = 1/2^{16}$
- If meet-in-the-middle is performed on two pairs (P, C) and (P', C'), the correct keys $K_1$ and $K_2$ can be determined with probability $1 - 1/2^{16}$.
- Known plaintext attack against double DES succeeds in $2^{56}$ as opposed to $2^{55}$ for DES (average).
- **The 112-bit key provides a security level similar to the 56-bit key.**


Cristina Nita-Rotaru

# Triple DES

- Use three different keys

  Encrypt: $C = E_{K_3}[ D_{K_2}[ E_{K_1}[P] ] ]$
  Decrypt: $P = D_{K_3}[ E_{K_2}[ D_{K_1}[C] ] ]$

- Key space is 56 x 3 = 168 bits
- No known practical attack against it.
- Many protocols/applications use 3DES (example PGP)

# Differential cryptanalysis

- Main idea:
  - This is a chosen plaintext attack, assumes than an attacker knows (plaintext, ciphertext) pairs
  - Difference $\Delta_P = P_1 \oplus P_2$, $\Delta_C = C_1 \oplus C_2$
  - Distribution of $\Delta_C$' s given $\Delta_P$ may reveal information about the key (certain key bits)
  - After finding several bits, use brute-force for the rest of the bits to find the key.

# Differential cryptanalysis of DES

- Surprisingly … DES was resistant to differential cryptanalysis.
- At the time DES was designed, the authors knew about differential cryptanalysis. S-boxes were designed to resist differential cryptanalysis.
- Against 8-round DES, attack requires $2^{38}$ known plaintext-ciphertext pairs.
- Against 16-round DES, attack requires $2^{47}$ chosen plaintexts.
- Differential cryptanalysis not effective against DES in practice.

# Linear cryptanalysis of DES

- Another attack described in 1993 M. Matsui
- Instead of looking for isolated points at which a block cipher behaves like something simpler, it involves trying to create a simpler approximation to the block cipher as a whole.
- It is an attack that can be applied to an iterated cipher.

# Linear cryptanalysis of DES

- M. Matsui showed (1993/1994) that DES can be broke:
  - 8 rounds: $2^{21}$ known plaintext
  - 16 rounds: $2^{43}$ known plaintext, 40 days to generate the pairs (plaintext, ciphertext) and 10 days to find the key
- The attack has no practical implication, requires too many pairs.
- Exhaustive search remains the most effective attack.

# DES strength against various attacks

| Attack Method | Known | Chosen | Storage complexity | Processing complexity |
|---|---|---|---|---|
| Exhaustive precomputation | - | 1 | $2^{56}$ | 1 |
| Exhaustive search | 1 | - | negligible | $2^{55}$ |
| Linear cryptanalysis | $2^{43}$<br>$2^{38}$ | -<br>- | For texts | $2^{43}$<br>$2^{50}$ |
| Differential cryptanalysis | -<br>$2^{55}$ | $2^{47}$<br>- | For texts | $2^{47}$<br>$2^{55}$ |

**The weakest point of DES remains the size of the key (56 bits)!**

# Encryption modes: ECB

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

# 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.

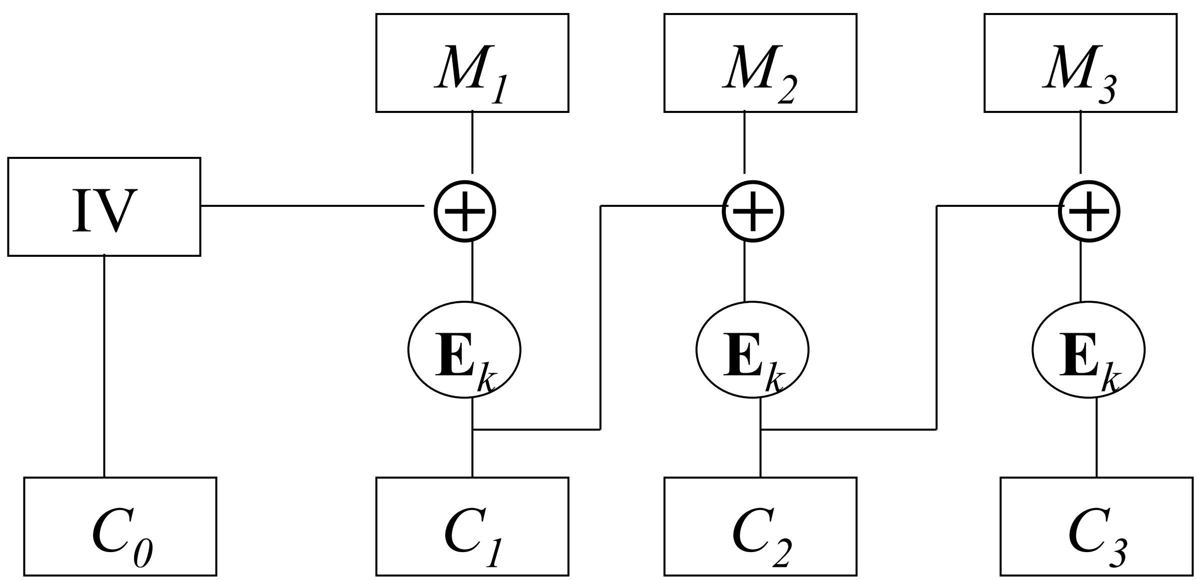
- Usage: not recommended to encrypt more than one block of data.

# Encryption modes: CBC

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

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

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



# 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 $M_{j+1}$

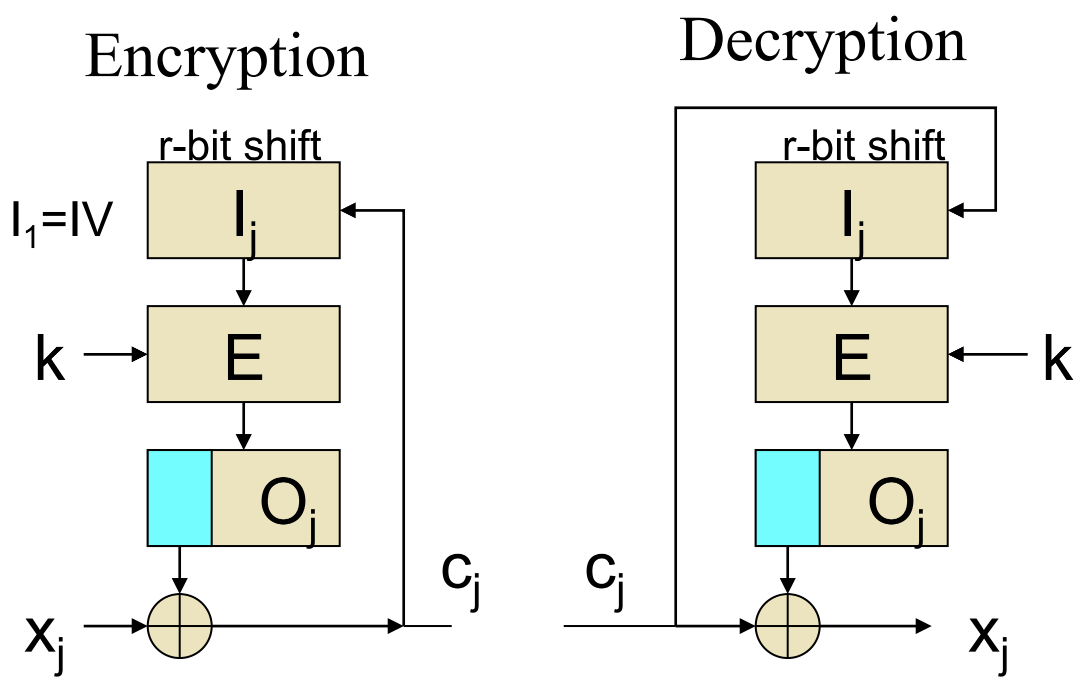
- Sequential encryption, cannot use parallel hardware
- Usage: chooses random IV and protects the integrity of IV
- Observation: if $C_i = C_j$ then $\mathbf{E_k}\ (M_i \oplus C_{i-1}) = \mathbf{E_k}\ (M_j \oplus C_{j-1})$**; thus** $M_i \oplus C_{i-1} = M_j \oplus C_{j-1}$**; thus** $M_i \oplus M_j = C_{i-1} \oplus C_{j-1}$

# 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




 Cristina Nita-Rotaru

# Properties of CFB

- Randomized encryption

- A ciphertext block depends on all preceding plaintext blocks; reorder affects decryption

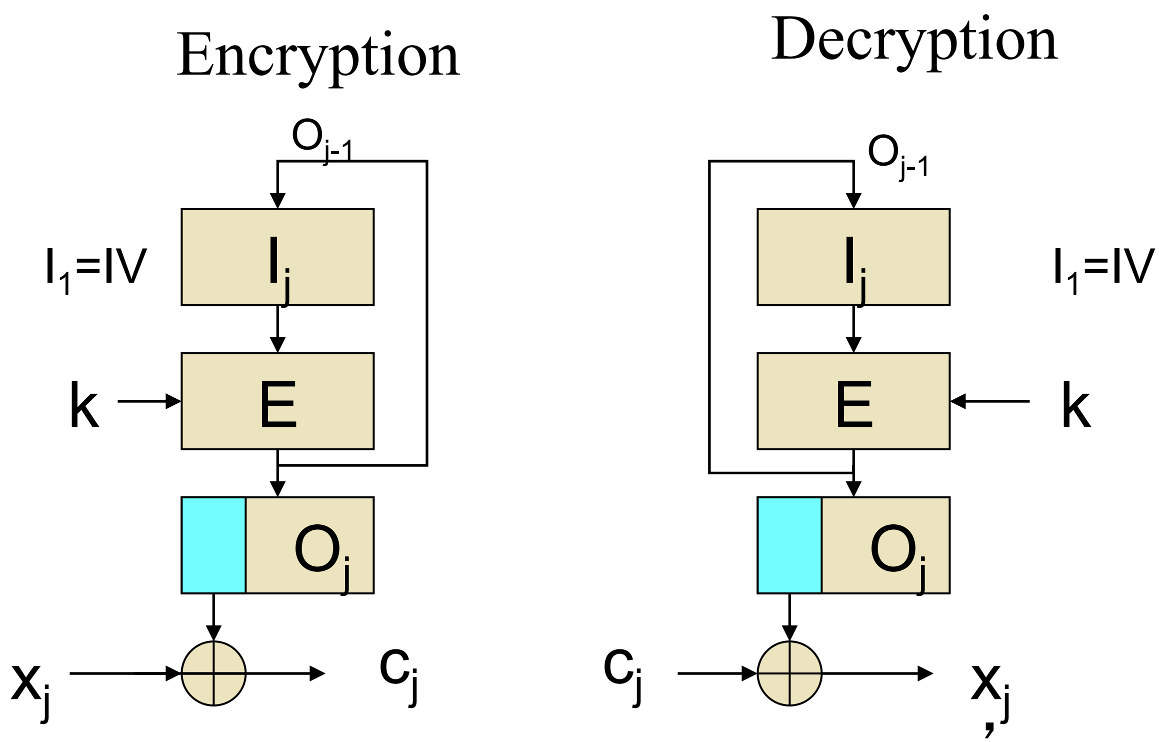
- Errors propagate for several blocks after the error, but the mode is self-synchronizing (like CBC).

- 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).

# Summary

- DES is not secure,  main problem is that the key is too short, brute force attacks are practical
- Block ciphers must be used with encryption modes when encrypting larger messages: CBC or CTR modes