Introduction to Cryptography CS 355

Lecture 17

Cryptanalysis of Block Ciphers

Lecture Outline

- Cryptanalysis of DES
  - Weak keys
  - Brute force attack
  - 2DES and 3DES
  - Differential cryptanalysis
  - Linear cryptanalysis

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)

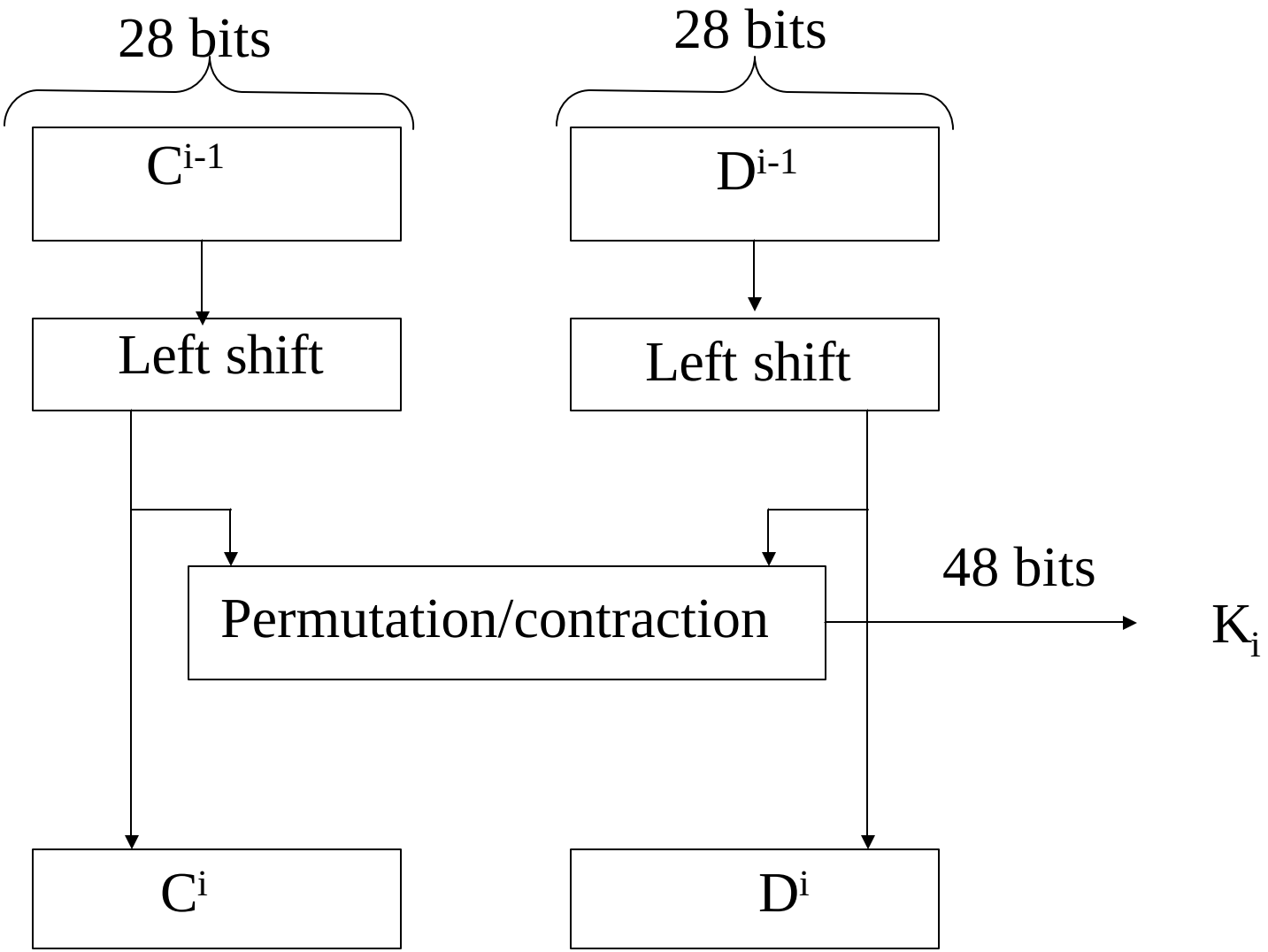
  0000000 0000000

  0000000 FFFFFFF

  FFFFFFF 0000000

  FFFFFFF FFFFFFF
- Weak keys should be avoided at key generation.

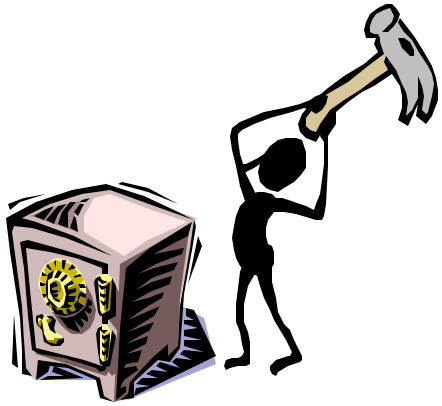
DES Key Scheduling



DES semi-weak keys

- 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)
  - msg="the unknown message is :xxxxxxxx"
  - CT=" C1 | C2 | C3 | C4"
  - 1997 Internet search: 3 months
  - 1998 EFF machine (costs $250K): 3 days
  - 1999 Combined: 22 hours

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

Strengthening DES to avoid Exhaustive Search: 3DES

- Triple-DES
- Let $\mathbf{E}_k[M]$ be a symmetric block cipher
- Define: $3\mathbf{E}_{k1,k2,k3}[M] = \mathbf{E}_{k1}[\mathbf{D}_{k2}[\mathbf{E}_{k3}[M]]]$
- Observe: when k1=k2=k3, $3\mathbf{E}_{k1,k2,k3}[M]=\mathbf{E}_k[M]$
- For triple DES, key=168 bits
- Why not 2DES?
  - $E_{k1,k2}[M] = E_{k1}[E_{k2}[M]]$

Attack on 2DES

- Given (M,C), where C=$\mathbf{E}_{k1,k2}[M]$
- Then $\mathbf{D}_{k1}[C] = \mathbf{E}_{k2}[M]$
- Build table of all encryptions of M
- Then for each possible k, test if $\mathbf{D}_{k}(C)$ is in the table
- Takes about 2^{56} time
- Requires $\approx 2^{56}$ space $\approx 10^{16}$
- Possible to trade time off space
- Effective key length is 56 << 2*56=112
- How effective is this attack on 3DES?

Differential Cryptanalysis

- Main idea:
  - This is a chosen plaintext attack, assumes than an attacker knows (plaintext, ciphertext) pairs
  - Difference $?_P = P_1 \oplus P_2$, $?_C = C_1 \oplus C_2$
  - Distribution of $?_C$'s given $?_P$ 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.

Basic idea of linear cryptanalysis

- Suppose that
- **(*) Pr [** $M_{i1} \oplus M_{i2} \oplus \ldots \oplus M_{iu}$
  $\oplus C_{j1} \oplus C_{j2} \oplus \ldots \oplus C_{jv}$
  $\oplus K_{p1} \oplus k_{p2} \oplus \ldots \oplus k_{pw} = 1$ **]** $= 0.5 + \varepsilon$
- Then one can recover some key bits given large number of PT/CT pairs
- For DES, exists (*) with $\varepsilon = 2^{-21}$
- Using this method, one can find 14 key bits using $(2^{21})^2$ PT/CT pairs

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.

Attacks on implementation of ciphers

- Timing attacks
- Power consumption attacks

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} 2^{38}	- -	For texts	2^{43} 2^{50}
Differential cryptanalysis	- 2^{55}	2^{47} -	For texts	2^{47} 2^{55}

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

Coming Attractions …

- Ideal Block Cipher and Their Security