

# Cryptography CS 555

## Lecture 6



Department of Computer Sciences  
Purdue University

# Announcements & Reminders

- HW1 due on now.
- HW2 out
- CERIAS security seminar
- My office hour:
  - Tuesday 3pm to 4pm,
  - Wednesday 11:30am to 12:30pm
- TA office hour:
  - Monday 2:30pm to 3:30pm
  - Friday 3:30pm to 4:30pm

# Review of last lecture

- Modes of operations for block ciphers
  - ECB, CBC, CFB, OFB, CTR
- Attacks on DES
  - exhaustive search, dictionary attack
- 3DES

# Outline

- More on cryptanalysis of DES
  - [Stallings: 3.4,3.5]
- Semantic security of symmetric ciphers
  - [BR: 4.3, 4.4]

# Strengthening DES to avoid Exhaustive Search: DES-X

- Given block cipher  $E_k$
- Define  $E-X_{k_1, k_2, k_3}(M) = E_{k_2}(M \oplus k_3) \oplus k_1$
- DESX: key-length =  $2 * 64 + 56 = 184$  bits
- Fast!
- Security: (Kilian-Rogaway'96)
  - effective key length  $\geq 56 + 64 - 1 - \log p$ , where  $p$  is the number of PT/CT pairs available to the attacker

# Attacks on implementation of ciphers

- Time attacks
- Power consumption

# Differential Cryptanalysis

- Markov Ciphers and Differential Cryptanalysis (1991) J. Lai, J. L. Massey, S. Murphy.
- Main idea:
  - This is a **chosen plaintext attack**, assumes that 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 !!!

# 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
- (\*)  $\Pr [ M_{i_1} \oplus M_{i_2} \oplus \dots \oplus M_{i_u}$   
 $\oplus C_{j_1} \oplus C_{j_2} \oplus \dots \oplus C_{j_v}$   
 $\oplus K_{p_1} \oplus K_{p_2} \oplus \dots \oplus K_{p_w} = 1 ] = 0.5 + \varepsilon$
- 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.
- The key size remains the main attack point.

# DES Strength Against Various Attacks

Attack Method	Known	Chosen	Storage complexity	Processing complexity
Exhaustive precomputation	-	1	$2^{56}$	$2^6$ (table lookup)
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	$2^{47}$ $2^{55}$

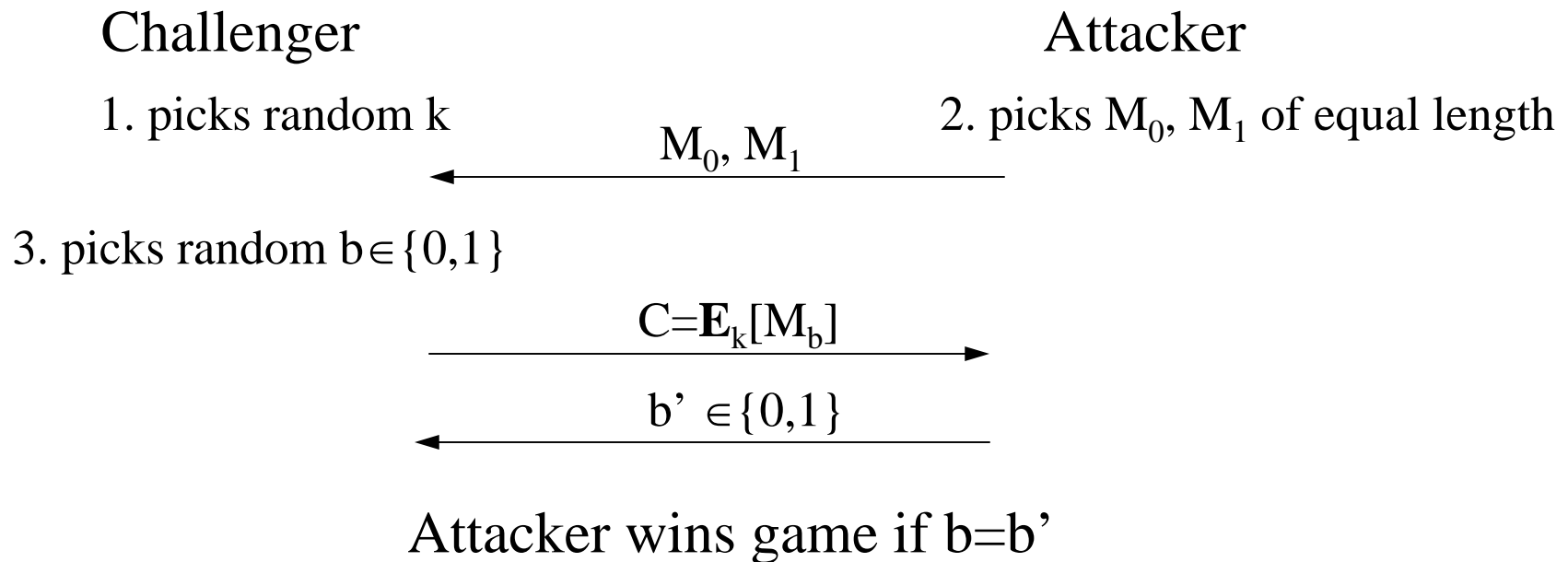
**The weakest point of DES remains the size of the key (56 bits)!**

# What does security mean?

- Perfect secrecy, not very useful.
  - Given  $C$ , cannot learn anything about  $M$
- Approximate perfect secrecy?
  - Given  $C$ , with limited computing resources, it is extremely unlikely one can learn anything about  $M$

# Semantic Security against Eavesdroppers

- A cipher is  $(t, \epsilon)$  semantically secure against eavesdroppers if no  $t$ -time attacker wins the following game with prob.  $\geq 0.5 + \epsilon$



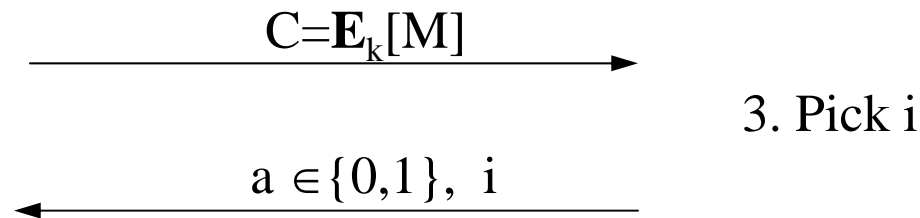
# Why semantic security?

- Introduce another notion of security
- A cipher is  $(t, \epsilon)$  bit secure if no  $t$ -time attacker wins the following game with prob.  $\geq 0.5 + \epsilon$

Challenger

1. picks random  $k$
2. picks random  $M$

Attacker

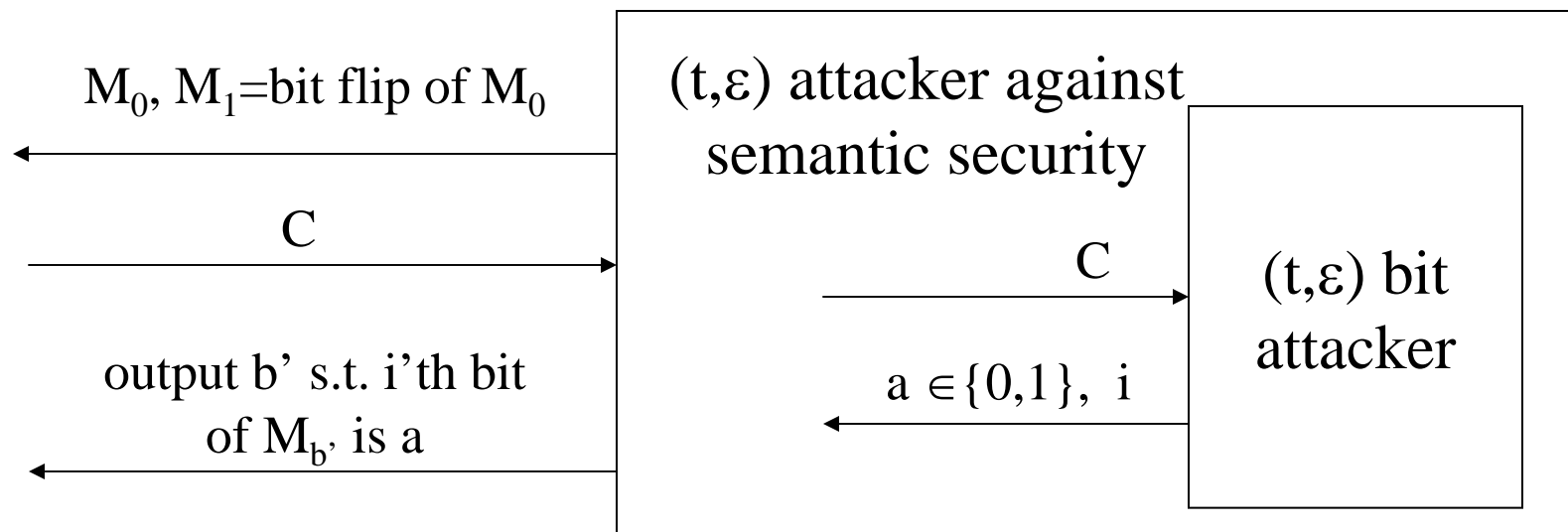


3. Pick  $i$

Attacker wins game if  $a=i$ 'th bit of  $M$

# Justification for semantic security

- Any cipher that is  $(t, \epsilon)$  semantically secure against eavesdroppers is also  $(t, \epsilon)$  bit secure
- Proof. Given a  $(t, \epsilon)$  attacker against bit security, build a  $(t, \epsilon)$  attacker against semantic security.



# ECB is not semantically secure

- Claim: There exists fast attacker that wins semantic security game with prob. close to 1
- Proof: the attacker sends  $M_0$ ="hello hello " and  $M_1$ ="hello world ", then checks whether the two blocks in the ciphertext are the same or not.
- We know that CBC, OFB, & CTR can be shown to be semantically secure, assuming block cipher is pseudo-random permutations.

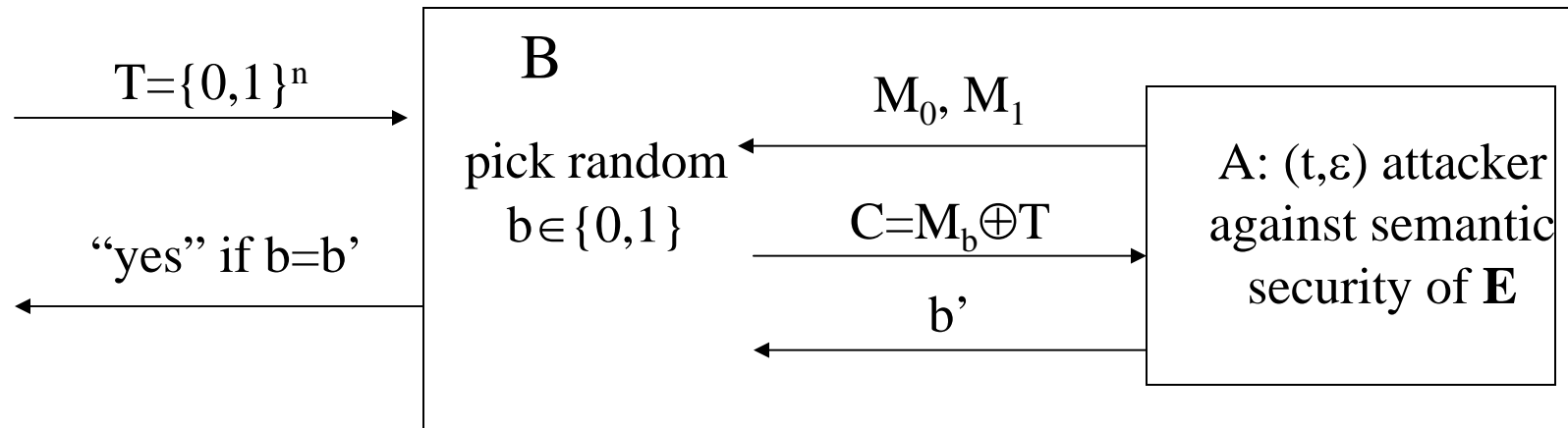
# PRNG

- Definition: a deterministic function  $G: \{0,1\}^s \rightarrow \{0,1\}^n$  ( $n \gg s$ ) is a  $(t, \epsilon)$ -PRNG if
  - there is an “efficient” algorithm to compute  $G$
  - $\forall$   $t$ -time algorithm  $A$ , we have
  - $|\Pr[A(G(S))=\text{“yes”}] - \Pr[A(R)=\text{“yes”}]| \leq \epsilon$ ,  
where  $S \in \{0,1\}^s$  is a random seed  
and  $R \in \{0,1\}^n$  is a length- $n$  random string
- E.g., RC4 with 128-bit key (seed) and  $2^{20}$  bytes of output is believed to be a  $(t, \epsilon)$ -PRNG for  $t=2^{80}$ ,  $\epsilon=1/2^{40}$

# A proof of semantic security

- Theorem: Suppose  $G: \{0,1\}^s \rightarrow \{0,1\}^n$  is a  $(t,\varepsilon)$  PRNG, then  $\mathbf{E}_k[M]=M\oplus G(k)$  is  $(t,\varepsilon)$  semantically secure.
- Proof: Contra-positive.
  - Suppose  $A$   $(t,\varepsilon)$ -breaks the semantic security of  $\mathbf{E}_k$ , build  $B$  that  $(t,\varepsilon)$ -breaks the PRNG security

# A proof of semantic security



- Claim: when  $T = G(S)$ , then  $\Pr[b = b'] > 0.5 + \epsilon$ , when  $T$  is random,  $\Pr[b = b'] = 1/2$ .
- Thus,  $|\Pr[A(G(S)) = \text{"yes"}] - \Pr[A(R) = \text{"yes"}]| > \epsilon$ .

# Next Lecture...

- AES & other block ciphers
- Recommended readings:
  - Stinson Chapter 3
  - Stallings Chapter 5,6