Introduction to Cryptography CS 355

Lecture 18

Security of Symmetric Encryption Schemes

Lecture Outline

- Ideal Block Cipher
- Pseudorandom Permutation (PRP)
- Semantic security (a.k.a. Indistinguishability Security)

Ideal block cipher

- An ideal block cipher is a substitution cipher from $\{0,1\}^n$ to $\{0,1\}^n$
  - Also known as a random permutation
  - Each key determines one permutation on the plaintext space
  - A random key is chosen
- Why is this an ideal block cipher?
  - Known-plaintext, chosen plaintext, and chosen ciphertext attacks are totally ineffective

Ideal block cipher

- What is the key space for the ideal block cipher of block size n?
  - total number of keys: $2^n!$
  - insecure when n is small
  - impractical when n is large: key length

$$s = \log(2^n!) > \log 2^n + \log(2^n - 1) + \ldots + \log 2^{n-1}$$

$$> \log 2^{n-1} + \log(2^{n-1}) + \ldots + \log 2^{n-1} > (n-1)2^{n-1}$$

  - For n=64, key length is log $(2^{64}!) > 64 \cdot 2^{63}$

Security Goal of Block Cipher

- Indistinguishable from an ideal block cipher (i.e., a random permutation)
- The best block cipher should be a pseudo-random permutation (PRP)
- For all existing block ciphers, if there is no known attacks, they are assumed to be PRP for some suitable parameters.

Symmetric Encryption Schemes

- A block cipher operates on one block
- An encryption scheme encrypts much longer messages
- Randomized vs. deterministic schemes
  - CBC is randomized

What Does Security Mean?

- What does insecurity mean?
  - from a few ciphertexts, can recover the encryption key
  - from a few ciphertexts, can recover the plaintext of some ciphertexts
  - from a few ciphertexts, can recover partial information of some ciphertexts

What Does Security Mean?

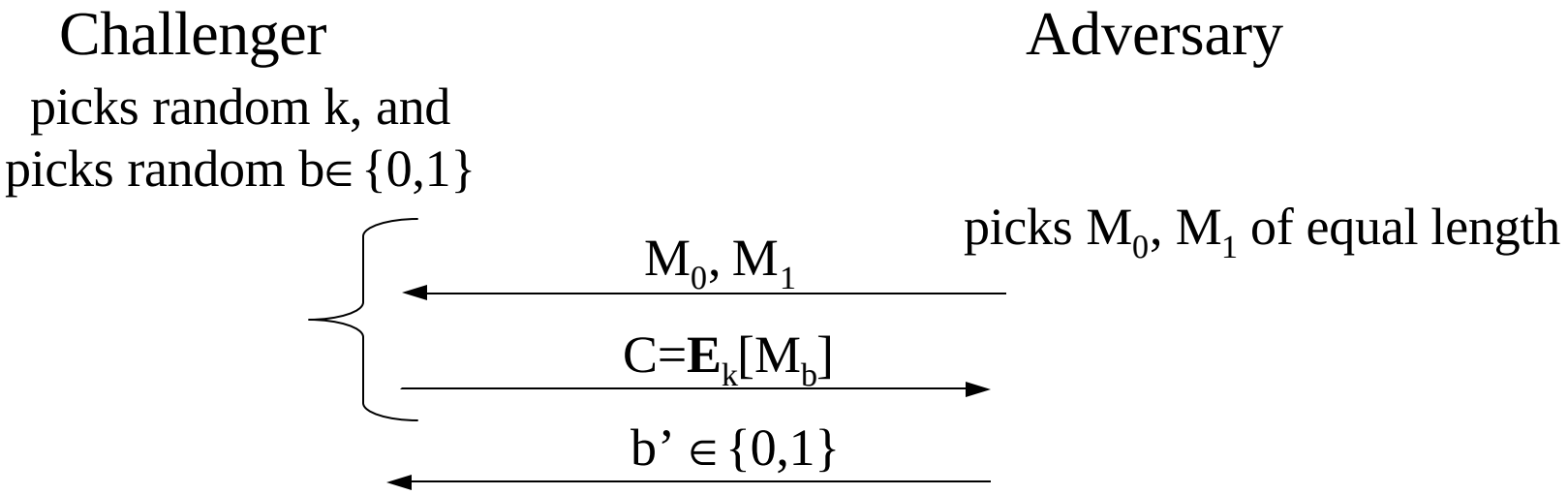
- Perfect secrecy
  - Given ciphertexts, cannot learn anything (other than the length of the message) about the plaintext
  - not very useful as requires long keys
- Approximate perfect secrecy?
  - with limited computing resources, it is extremely unlikely one can learn anything (other than the length) about the plaintexts from the ciphertexts
- How to formalize this?

Towards Semantic Security

- Suppose that the adversary knows that a ciphertext results from one of two possible plaintexts, the adversary should not be able to tell that which one plaintext is more likely to be the actual one.

IND-CPA

- a.k.a Semantic Security
- A cipher is (t,ε) IND-CPA secure if no t-time adversary wins the following game with prob. ≥ 0.5 + ε



Attacker wins game if b=b'

Block Cipher Modes Revisited

- If a block cipher is a PRP, then using this cipher under the CBC, CTR modes has semantic security.

Coming Attractions …

- RSA