

CS355: Cryptography

Lecture 15: Semantic security.

-
- What can we say about security of block ciphers and encryption modes?

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

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 (key size, block size, number of rounds).

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 Insecurity Mean?

- Attacker can recover the encryption key
- Attacker can recover the plaintext of some ciphertexts
- Attacker can recover partial information of some ciphertexts

What Does Security Mean?

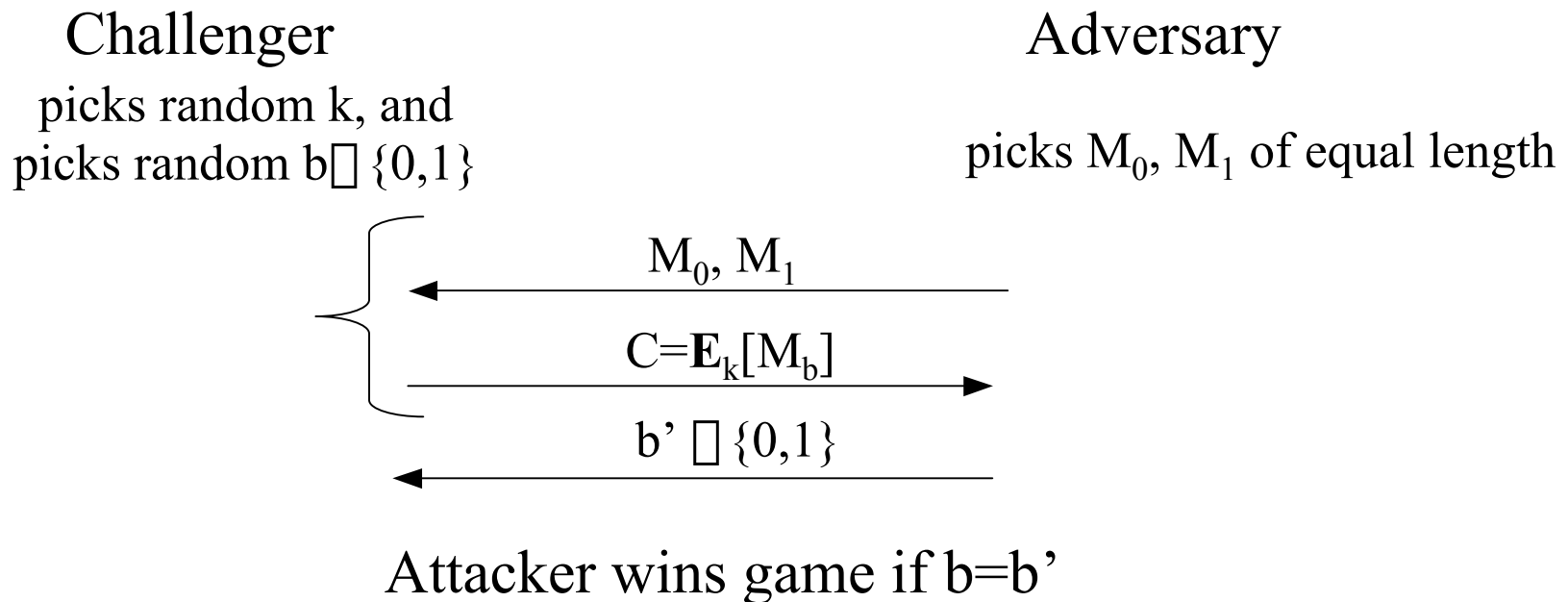
- Perfect secrecy
 - Given ciphertexts, cannot learn anything (other than the length of the message) about the plaintext
 - not very useful as requires long keys
- Approximate perfect secrecy?
 - with limited computing resources, it is extremely unlikely one can learn anything (other than the length) 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. $\geq 0.5 + \epsilon$



Block Cipher Modes Revisited

- If a block cipher is a PRP, then using this cipher under the CBC, CTR modes have semantic security.
- How about CBC with a fixed IV?

Modulo Operation

Definition:

$$a \bmod n = r \quad \exists q, \text{ s.t. } a = q \cdot n + r$$

where $0 \leq r < n$

Example:

$$7 \bmod 3 = 1$$

$$-7 \bmod 3 = 2$$

Definition (Congruence):

$$a \equiv b \pmod{n} \iff a \bmod n = b \bmod n$$

Congruence Relation Properties

- 1) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then:
 $a \pm c \equiv b \pm d \pmod{n}$ and
 $ac \equiv bd \pmod{n}$
- 2) If $a \equiv b \pmod{n}$ and $d \mid n$ then:
 $a \equiv b \pmod{d}$
- 3) $a \equiv b \pmod{n}$, $a \equiv b \pmod{m}$ and $\gcd(m, n)=1$, then
 $a \equiv b \pmod{mn}$

Congruence Relation

Theorem

Congruence mod n is an equivalence relation:

Reflexive: $a \equiv a \pmod{n}$

Symmetric: $a \equiv b \pmod{n}$ iff $b \equiv a \pmod{n}$.

Transitive: $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ \square
 $a \equiv c \pmod{n}$

Linear Equation Modulo n

If $\gcd(a, n) = 1$, the equation

$$ax \equiv 1 \pmod{n}$$

has a unique solution, $0 < x < n$. This solution is often represented as $a^{-1} \pmod{n}$

Proof: if $ax_1 \equiv 1 \pmod{n}$ and $ax_2 \equiv 1 \pmod{n}$,
then $a(x_1 - x_2) \equiv 0 \pmod{n}$, then $n \mid a(x_1 - x_2)$,
then $n \mid (x_1 - x_2)$, then $x_1 - x_2 = 0$

How to compute x ?

Linear Equation Modulo (cont.)

If $\gcd(a, n) = d$, the equation

$$ax \equiv b \pmod{n}$$

has a solution **iff $d \mid b$** .

Eq has a solution

$d \mid b$

Proof Sketch:

“ \Rightarrow ” $ax = qn + b$; $b = ax - qn$

d divides a and n , so divides any linear combination, so $d \mid b$

“ \Leftarrow ” $d \mid b$ then $b = dt$, by theorem we have $d = au + bn$, so $dt = a(ut) + b(nt) = b$, so $x = ut$ is a solution of $ax \equiv b \pmod{n}$

Solving Linear Equation Modulo

To solve the equation

$$ax \equiv b \pmod{n}$$

When $\gcd(a,n)=1$, compute $x = a^{-1} b \pmod{n}$.

When $\gcd(a,n) = d > 1$, do the following

- If d does not divide b , there is no solution.
- Assume $d|b$. Solve the new congruence, get x_0

$$(a/d)x \equiv b/d \pmod{n/d}$$

- The solutions of the original congruence are $x_0, x_0+(n/d), x_0+2(n/d), \dots, x_0+(d-1)(n/d) \pmod{n}$.

Chinese Remainder Theorem

Theorem

Let m , and n be integers s.t. $\gcd(m, n) = 1$.

$$x \equiv a \pmod{m}$$

$$x \equiv b \pmod{n}$$

There exists a unique solution modulo mn

Chinese Remainder Theorem

$\gcd(m, n) = 1$, then exist integers s and t such that $ms+nt=1$;
Note that $ms \equiv 1 \pmod n$ and $nt \equiv 1 \pmod m$

Idea is to show that $x = bms + ant$ is a solution congruent to both eq.

$$(bms + ant) \pmod m \equiv ant \pmod m \equiv a \pmod m$$
$$(bms + ant) \pmod n \equiv bms \pmod n \equiv b \pmod n$$

Assume that there are two solutions x and y then we obtain

$x \equiv y \pmod m$ and $x \equiv y \pmod n$, so $x-y$ is a multiple of both m and n ,
so a multiple of mn

So $x \equiv y \pmod{mn}$

Example of CRT

Solve $x = 3 \pmod{7}$ and $x = 5 \pmod{15}$

Since $80 = 3 \pmod{7}$ and $80 = 5 \pmod{15}$, then 80 is a solution, solution is uniquely determined modulo $7 * 15 = 105$

How to do it: list all numbers modulo that are 5 modulo 15 then check which ones are 3 modulo 7.

Chinese Remainder Theorem (CRT)

Theorem

Let n_1, n_2, \dots, n_k be integers s.t. $\gcd(n_i, n_j) = 1$ for any $i \neq j$.

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

...

$$x \equiv a_k \pmod{n_k}$$

There exists a unique solution modulo
 $n = n_1 n_2 \dots n_k$