CS408
Cryptography & Internet Security

Lecture 10:

Randomness,

Pseudo-randomness,

Security of block ciphers

Randomness

- Is essential for cryptography (e.g., for generating keys)
- Random numbers: a sequence of numbers x_1, x_2, … , s.t. for any integer k>0, it is ***impossible*** for an observer to predict x_k even if all of x_1, x_2, …, x_{k-1} are known
- True randomness needs an unpredictable source
  - Example: atmospheric noise, radioactive decay etc.
  - Example: hardware RNG (based on thermal noise, photoelectric effect)
  - Computers cannot generate true randomness

Pseudo-randomness

- Pseudo-random numbers: a sequence of numbers x_1, x_2, … , s.t. for any integer k>0, it is ***hard*** for an observer to predict x_k even if all of x_1, x_2, …, x_{k-1} are known
- Hard means computationally infeasible for all algorithms that run in polynomial time
- Pseudo-random number generator (PRNG) on computers
  - User keystrokes, I/O, least-significant digit voltage measurements
  - Pool of random numbers is constantly replenished

Pseudo-random function (PRF)

- A random function is a function that is chosen at random from the set of all functions defined between a domain set and a range set
- A pseudo-random function (PRF) is a function that is indistinguishable from a random function
  - The adversary is modeled as polynomial-time algorithm which has black-box access to both the random function and the pseudo-random function

Pseudo-random permutation (PRP)

- A pseudo-random permutation (PRP) is a permutation that is indistinguishable from a random permutation
  - The adversary is modeled as polynomial-time algorithm which has black-box access to both the random permutation and the pseudo-random permutation

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 some partial information about the plaintext of some ciphertexts

What Does Security Mean?

- Perfect secrecy
  - Given ciphertexts, cannot learn anything (other than the length) about the plaintext, even with unlimited computational resources (information-theoretic security)
  - One-time pad: Not very useful, since it requires long keys, and keys cannot be reused
- How about "good enough" secrecy?
  - With limited resources, it is extremely unlikely one can learn anything (other than the length) about the plaintext from the ciphertext (computational security)
- How to formalize this?

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 considered an ideal block cipher?
  - Known-plaintext, chosen-plaintext and chosen-ciphertext attacks are ineffective

Security Goal of Block Ciphers

- Indistinguishable from an ideal block cipher (i.e., a random permutation)
- For security purposes, a block cipher is modeled as a pseudo-random permutation (PRP)
  - A PRP is indistinguishable from a random permutation

Definitions of Security

- Semantic Security:

  An adversary should be unable to learn *any partial information* about the plaintext from the ciphertext (besides the length of the plaintext)
- Ciphertext Indistinguishability:

  An adversary should be unable to distinguish pairs of ciphertexts based on the plaintext they encrypt

- These two notions are equivalent, but the latter one is usually used in proofs of security
  - They were proven equivalent under chosen-plaintext (CPA) attacks
- Under chosen-plaintext attacks, these are basic requirements for any modern cryptosystem (IND-CPA)
  - Some cryptosystems achieve stronger security (IND-CCA)

Ciphertext Indistinguishability

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

Ciphertext Indistinguishability (continued)

- A cipher is IND-CPA secure if every probabilistic polynomial-time (PPT) adversary wins the following security game with probability 0.5 + $\varepsilon(k)$, where $\varepsilon(k)$ is a *negligible function* in the security parameter k
  - i.e., the adversary has a negligible “advantage” over random guessing

Ciphertext Indistinguishability (continued)

- A cipher is IND-CPA secure if every probabilistic polynomial-time (PPT) adversary wins the following game with probability $0.5 + \varepsilon(k)$, where $\varepsilon(k)$ is a *negligible function* in the security parameter k
  - i.e., the adversary has a negligible "advantage" over random guessing

IND-CPA security game (between Challenger "Chal" and Adversary "Adv)"

1. Chal chooses a secret key K (K is kept secret and not revealed to Adv)
2. Adv is allowed to perform any number of encryptions or other operations (we say Adv uses Chal as an "encryption oracle" E)
3. Eventually, Adv chooses two distinct plaintexts of equal length m_0 and m_1 and sends them to Chal
4. Chal chooses a bit $b \in \{0,1\}$ uniformly at random, computes c $c = E_k(m_b)$, and sends c back to Adv
5. Adv is allowed to perform any number of encryptions or other operations (i.e., Adv continues to have oracle access to E)
6. Adv outputs a bit b'

The Adversary wins the game if b'=b

Deterministic vs. Probabilistic Encryption

- Probabilistic encryption implies the use of *randomness* in encryption: when encrypting the same plaintext several times, it will result in different ciphertexts
  - Each plaintext will map into a large number of possible ciphertexts
- To achieve semantic security, an encryption algorithm ***must*** be probabilistic
- Why can't deterministic encryption achieve semantic security?
- If a block cipher is a PRP, then using the cipher under the CBC or CTR modes of operation achieves semantic security