AMERICAN UNIVERSITY OF BEIRUT

Applied Cryptography

CMPS 297AD/396AI, Fall 2025

Instructor: Nadim Kobeissi **Website:** https://appliedcryptography.page

Problem Set 1: Provable Security Foundations

Instructions: This problem set covers the foundations of provable security from parts 1.1[a], 1.2[b] and 1.3[c] of the course. Submit your solutions as a neatly formatted PDF. You are encouraged to collaborate with classmates in studying the material, but your submitted solutions must be your own work. For proofs, clearly state your assumptions, steps, and conclusions.

[a] https://appliedcryptography.page/slides/1-1.pdf
[b] https://appliedcryptography.page/slides/1-2.pdf
[c] https://appliedcryptography.page/slides/1-3.pdf

1 Cryptographic Foundations (20 points)

1.1 Basic Concepts (10 points)

1. (3 points) Define the three primary security goals of cryptography in your own words and provide a real-world example for each that wasn't explicitly mentioned in the lectures.
2. (3 points) Explain Kerckhoff's principle and why it remains fundamental to modern cryptography. Provide an example of a security system that violates this principle and describe the potential consequences.
3. (4 points) Compare and contrast symmetric and asymmetric cryptography:
   (a) Explain the fundamental difference in their key management approach.
   (b) For each type, identify which mathematical or computational assumptions their security typically relies on.
   (c) Describe a scenario where one would be clearly preferable to the other.

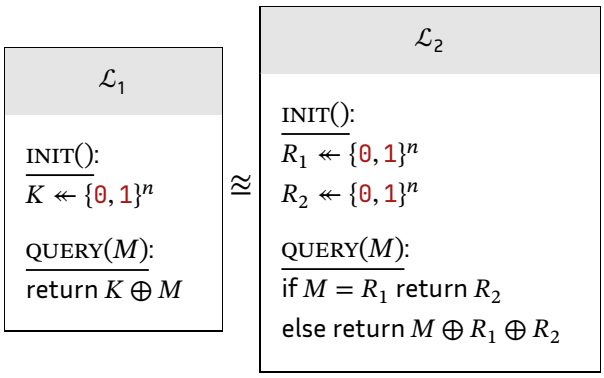
1.2 Perfect Secrecy (10 points)

1. (3 points) Consider a modified one-time pad where we use the bitwise AND ($\wedge$) operation instead of XOR ($\oplus$):
   $\text{Enc}(K, M) = K \wedge M$ and $\text{Dec}(K, C) = ?$
   (a) Is this scheme correct? If yes, specify the decryption function. If not, explain why.
   (b) Does this scheme provide perfect secrecy? Justify your answer.
2. (4 points) Consider the following variant of a one-time pad operating on decimal digits (0-9):
   $\text{Enc}(K, M) = (K + M) \bmod 10$ and $\text{Dec}(K, C) = (C - K) \bmod 10$
   where $K, M, C \in \{0, 1, 2, \ldots, 9\}$.
   (a) Prove that this scheme is correct.
   (b) Prove that this scheme provides perfect secrecy, assuming K is chosen uniformly at random.
3. (3 points) Consider a one-time pad where the key length is half the message length:
   $\text{Enc}(K, M) = (K \oplus M_1, K \oplus M_2)$ where $M = (M_1, M_2)$ and $|M_1| = |M_2| = |K|$.
   Provide a specific attack that breaks the confidentiality of this scheme, showing clearly the information an attacker can extract from the ciphertext.

2 Provable Security (20 points)

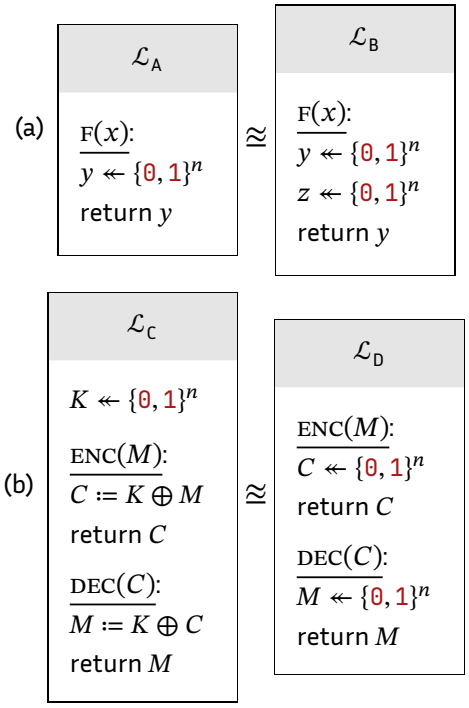
2.1 Libraries and Interchangeability (10 points)

1. (5 points) Consider the following libraries:



   Are these libraries interchangeable? Either prove they are interchangeable or provide a distinguisher program that can tell them apart with non-negligible probability.

2. (5 points) For each of the following pairs of libraries, state whether they are interchangeable and briefly justify your answer:



2.2 Security Proofs (10 points)

1. (5 points) Let $\Sigma = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be a secure encryption scheme for messages in $\{0,1\}^n$. Consider the following modified scheme $\Sigma' = (\mathsf{KeyGen}', \mathsf{Enc}', \mathsf{Dec}')$:

$$\mathsf{KeyGen}'() = K \twoheadleftarrow \mathsf{KeyGen}()$$
$$\mathsf{Enc}'(K, M) = (C_1, C_2) \text{ where } C_1 \twoheadleftarrow \mathsf{Enc}(K, M) \text{ and } C_2 \twoheadleftarrow \mathsf{Enc}(K, M \oplus 1^n)$$
$$\mathsf{Dec}'(K, (C_1, C_2)) = \mathsf{Dec}(K, C_1)$$

   Determine whether Σ' is a secure encryption scheme. If it is secure, provide a formal proof. If it is not secure, describe a concrete attack that breaks its confidentiality and explain why the attack works.

2. (5 points) Consider the following game between a challenger and an adversary $\mathcal{A}$:
   (a) The adversary selects two messages M_0 and M_1 of the same length.
   (b) The challenger selects a uniform random bit $b \leftarrow \{0,1\}$ and a uniform random key $K \leftarrow \{0,1\}^n$.
   (c) The challenger computes $C = K \oplus M_b$ and gives C to the adversary.
   (d) The adversary outputs a bit b' as its guess for b.

   Prove that for any adversary $\mathcal{A}$, the probability that $b' = b$ is exactly $1/2$. Explain what this result tells us about the security of the one-time pad.

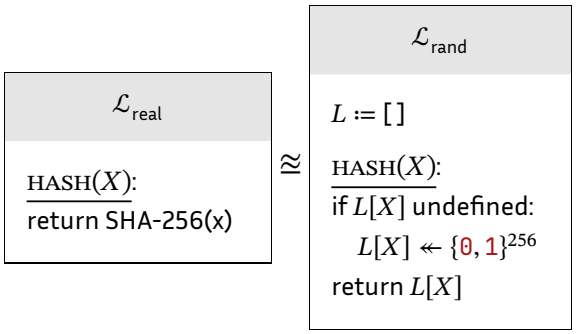
3 Computational Cryptography (30 points)

3.1 Computational Security Concepts (15 points)

1. (5 points) Explain why computational security is important in practice despite the existence of information-theoretic security. Discuss the limitations of both approaches.
2. (4 points) Consider a brute-force attack on AES-128:
   (a) Using the monetary cost table provided in the lecture, estimate how much it would cost to try all possible keys.
   (b) Discuss whether the computational approach to security makes sense in light of this cost.
3. (3 points) Define a negligible function formally. Then determine which of the following functions are negligible (where λ is the security parameter):
   (a) $f_1(\lambda) = 2^{-\lambda}$
   (b) $f_2(\lambda) = \lambda^{-\log \lambda}$
   (c) $f_3(\lambda) = 2^{-\sqrt{\lambda}}$
   (d) $f_4(\lambda) = \frac{1}{\lambda \cdot 2^{\lambda/2}}$
4. (3 points) The "birthday paradox" is crucial for understanding many cryptographic attacks. If a hash function produces outputs of length n bits:
   (a) Approximately how many random inputs would you need to hash before finding a collision with 50% probability?
   (b) How many bits of output would a hash function need to be reasonably secure against birthday attacks for the next decade?

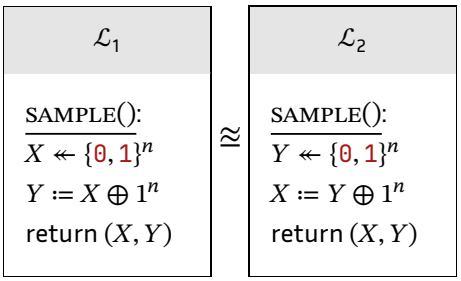
3.2 Distinguishability and Bad Events (15 points)

1. (6 points) Consider the following two libraries that implement a 256-bit hash function:



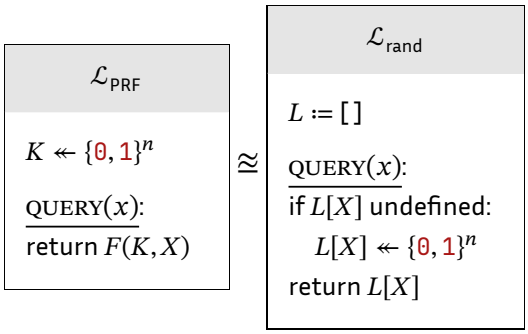
   (a) Describe the "bad event" that would allow these libraries to be distinguished.
   (b) If an adversary is limited to q queries, what is the probability of triggering this bad event?
   (c) Using the "bad event" proof technique, show that these libraries are computationally indistinguishable when q is polynomial in the security parameter.

2. (4 points) Consider the following two libraries:



Use the hybrid proof technique to show these libraries are interchangeable. Clearly describe each intermediate hybrid library.

3. (5 points) Consider a PRF $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ and the following two libraries:



Suppose we have a program $\mathcal{A}$ that can distinguish between these libraries with advantage ε. Construct a program $\mathcal{B}$ that uses $\mathcal{A}$ as a subroutine to distinguish a PRF from a truly random function with the same advantage ε.

4 Application of Cryptographic Principles (30 points)

1. (10 points) **Block Cipher Mode Analysis**

   The lecture demonstrated how ECB mode reveals patterns in the plaintext. For each of the following block cipher modes, explain:

   (a) How the encryption and decryption work.
   (b) What would happen if the same key and IV (when applicable) were reused for multiple messages.
   (c) A specific real-world situation where this mode would be most appropriate.

   Modes to analyze:

   (a) Cipher Block Chaining (CBC)
   (b) Counter Mode (CTR)

2. (10 points) **One-Time Pad in the Real World**

   A startup claims to have developed a "quantum-resistant ultra-secure messaging system" based on the one-time pad. They provide the following details:

   - The system uses a hardware random number generator to produce one-time pads.
   - Each user receives a 1TB USB drive containing pre-generated pad data during account registration.
   - When sending a message, the app encrypts it with a portion of the pad, marks that portion as used, and sends the ciphertext.
   - When the user has used 80% of their pad, the app automatically requests a new USB drive.

   Provide a detailed critique of this system:

(a) Identify at least three practical problems with this implementation.
(b) Explain how each problem compromises security or usability.
(c) Suggest improvements to address each issue while maintaining the theoretical security of OTP.

3. (10 points) **Symmetric Encryption Protocol Analysis**

A software company is implementing a secure communication protocol for their instant messaging application. They propose the following scheme:

- Each user generates a random 128-bit key K during account creation.
- To send a message M, the sender computes $C = K \oplus M$ and transmits C.
- When two users want to communicate, they first exchange their keys through a "top secret channel" established by the company's server.
- The company claims their protocol is "as secure as one-time pad" because they use the XOR operation.

Address the following aspects of this system:

(a) Using the provable security framework discussed in class, analyze whether this scheme provides the confidentiality properties claimed by the company.
(b) Identify at least three major security vulnerabilities in the described approach.
(c) The company is considering having users generate new keys daily instead of just once. Explain whether this modification would address the vulnerabilities you identified.
(d) Propose a modified protocol that would significantly improve security while still using only symmetric cryptography concepts covered in class so far. Justify your choices using the security principles we've discussed.

Bonus Challenge (20 extra points): The discrete logarithm problem is fundamental to many cryptographic systems. Consider a cyclic group G of prime order p with generator g. The discrete logarithm problem is: given $h \in G$, find x such that $g^x = h$.
Imagine a scenario where the discrete logarithm problem could be solved efficiently. Select one modern cryptographic protocol that relies on the hardness of this problem, and analyze:

1. The specific impact on the protocol's security.
2. How the protocol would need to be modified to remain secure.
3. Whether any alternative mathematical problems could serve as suitable replacements.

Your answer should demonstrate deep understanding of both the protocol and the underlying mathematical principles.