CS 601.442/642 – Modern Cryptography Instructor: Abhishek Jain

Homework 1

Deadline: September 14; 2022, 1:30 PM

Instructions

- The solutions must be submitted via Gradescope (entry code: **RZ733P**)
- You can either type your solutions using LaTeX or submit a scanned copy of of handwritten solutions. In the case of the latter, please make sure your handwriting is legible. Please don't use text editors such as MS Word, Pages, Notepad, etc.
- This homework is based on the topics covered in class on August 31st and September 7th. Some terms might seem unfamiliar at first, but they will make sense after the class on Sept 7.
- The final question is **extra credit**. Completing it is not required.

Problems

1. (15 Points) There is nothing exclusively special about strings and XOR in one-time pad. We can get the same properties using integers $\mathsf{mod}\ n$ and addition $\mathsf{mod}\ n$. This problem considers a variant of one-time pad, in which the keys, plaintexts, and ciphertexts are all elements of $\mathbb{Z}_n$ instead of $\{0,1\}^n$.

   (a) What is the decryption algorithm that corresponds to the following encryption algorithm?

   $$\mathsf{Enc}(k, m) : c = (k + m)\ \mathsf{mod}\ n$$

   Show that the resulting scheme satisfies **correctness**

   (b) Show that the above scheme satisfies **one-time uniform ciphertext security**

   (c) It's not just the distribution of keys that is important. The way that the key is combined with the plaintext is also important. Show that a scheme with the following encryption algorithm does **not** satisfy **one-time uniform ciphertext security**

   $$\mathsf{Enc}(k, m) : c = (k \cdot m)\ \mathsf{mod}\ n$$

2. (10 Points) Alice is using one-time pad and notices that when her key is the all-zeroes string $k = 0^n$, then $\mathsf{Enc}(k, m) = m$ and her message is sent in the clear! To avoid this problem, she decides to modify KeyGen to exclude the all-zeroes key. She modifies KeyGen to choose a key uniformly from $\{0,1\}^n \backslash \{0^n\}$, the set of all n-bit strings except 0^n . In this way, she guarantees that her plaintext is never sent in the clear.

   (a) Describe an attack demonstrating that the modified scheme does **not** satisfy **one-time uniform ciphertext security**

(b) Describe an attack demonstrating that the modified scheme does **not** satisfy **one-time perfect security**

3. (10 Points) The following scheme encrypts a plaintext by simply reordering its bits, according to the secret permutation k:

$\mathcal{K} = \{$ permutations of $\{1, ..., n\}\}$
$\mathcal{M} = \{0,1\}^n$
$\mathcal{C} = \{0,1\}^n$

$\underline{\mathsf{KeyGen}(1^n)}$:
  $k \leftarrow \mathcal{K}$
  return k

$\underline{\mathsf{Enc}(k, m)}$:
  for $i := 1$ to n :
    $c_{k(i)} := m_i$
  return $c_1 ... c_n$

$\underline{\mathsf{Dec}(k, c)}$:
  for $i := 1$ to n :
    $m_i := c_{k(i)}$
  return $m_1 ... m_n$

Describe an attack demonstrating that the scheme does **not** satisfy **one-time perfect security**.

4. (10 Points) Consider the following variant of one-time perfect security, where Eve can obtain two ciphertexts (on chosen plaintexts) encrypted under the same key, called **two-time perfect security**

We say that an encryption scheme is two-time perfectly secure if $\forall m_{11}, m_{12}, m_{21}, m_{22} \in \mathcal{M}$ chosen by Eve, the following distributions are identical:

- $\mathcal{D}_1 := \{c_1 := \mathsf{Enc}(k, m_{11}), c_2 := \mathsf{Enc}(k, m_{12}); k \leftarrow \mathsf{KeyGen}(1^n)\}$
- $\mathcal{D}_2 := \{c_1 := \mathsf{Enc}(k, m_{21}), c_2 := \mathsf{Enc}(k, m_{22}); k \leftarrow \mathsf{KeyGen}(1^n)\}$

Describe an attack demonstrating that one-time pad does **not** satisfy this security definition.

5. (15 Points) Let $\mathcal{E}_1 = (\mathsf{KeyGen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ and $\mathcal{E}_2 = (\mathsf{KeyGen}_2, \mathsf{Enc}_2, \mathsf{Dec}_2)$ be two encryption schemes such that only one of them satisfies one-time perfect security, **but you don't know which one**. Using both $\mathcal{E}_1$ and $\mathcal{E}_2$ (but no other encryption scheme), construct an encryption scheme with one-time perfect security and prove its security.

6. (extra credit, 15 Points) Prove that if an encryption scheme has $|\mathcal{K}| < |\mathcal{M}$ (i.e. there are fewer possible *keys* than there are possible *messages*), then it **cannot** satisfy **one-time perfect security**. Try to structure your proof as an explicit attack on the scheme, i.e. a distinguisher between the distributions $\mathcal{D}_1$ and $\mathcal{D}_2$.

   Hint: There is no restriction on the running time of the attacker. Exhaustive brute-force attacks are therefore valid.