CS 601.442/642 – Modern Cryptography Instructor: Abhishek Jain

Homework 1

Deadline: September 13; 2020, 11:59 PM EST

Instructions

- The solutions must be submitted via Gradescope (Entry Code: M5EVWN).
- You can either type your solutions on LaTeX or submit a scanned copy of handwritten solutions. In 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 Sept 2 and 9. Some terms might seem unfamiliar at first, but they will make sense after the class on Sept 9.

Problems

1. (25 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 $\{0,1\}^n$. The keys are sampled uniformly at random from $\mathbb{Z}_n$.

   (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) 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.

3. (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.