CS 198 Codebreaking at Cal
Spring 2023 Homework

HW 2

1 Question 1

Briefly explain why even the best CSPRNG is the world is only as secure as its initial seeding.

Question 2

Recall that we can define the *Shannon entropy* of a probability distribution to be

$$H(x) = \sum_i -x_i \cdot \log_2(x_i)$$

Prove that the uniform distribution ($x_i = \frac{1}{n}$ for n elements) provides the maximum entropy.

HINT: Jensen's equality states that, for convex $f(x)$ over $[a,b]$ and numbers $y_1, \ldots, y_n \in [a,b]$,

$$n \cdot f(\frac{y_1 + \ldots + y_n}{n}) \geq f(y_1) + \ldots + f(y_n)$$

HINT: The function $f(x) = -x \cdot \log_2(x)$ is convex over $[0,1]$.

Question 3

Prove that the Vigenere system is perfectly secure **if the key is as long as the plaintext**. You may use either a direct proof or a semantic security game.

HINT: Read Note 2's proof on OTP perfect secrecy for an outline of a direct proof, or revisit the lecture slides for a semantic security game example.

Question 4

Consider the following symmetric cryptosystem:

$$\begin{aligned} IV &:= \text{n-bit uniformly random bitstring} \\ Enc(k,m) &= IV \oplus k \oplus m \\ C &= (IV, Enc(k,m)) \end{aligned}$$

C in this case is 2-tuple, so decryptors can access the IV at C[0] and the ciphertext at C[1] like an array. **Note that the IV is randomly generated for every encryption, even if the key remains constant.**

1. Write down the decryption function for this system (takes in k, C and outputs m).
2. Is this scheme IND-CPA secure? Explain why or why not.

Question 5

Prove or disprove each of the following statements.

1. Semantic security implies IND-CPA security.
2. IND-CPA security implies semantic security.

Contributors:

- Ryan Cottone