Modern Cryptography
University of Amsterdam, 2019

Team Name: Your team name
Student Names: Your names

Homework set 2

Contents

Group Project [8 pt]

Read up on what a Fermi estimate is.

1. Give a Fermi estimate for all passwords used in the world.
2. Assume all passwords used in the world are distinct. How long do most of them have to be?

Post your results to this discussion forum. Remember that when doing Fermi estimates, it is important to state clearly what assumptions you make when giving your answer.

Question 1 [1 pt]: 2 messages with the same key

Two ASCII messages containing English letters and spaces only are encrypted using the one-time pad and the same key. The 8th byte of the first ciphertext is observed to be `0xAA` and the 8th byte of the second ciphertext is observed to be `0xE8`. Let m_1 (resp., m_2) denote the 8th ASCII character in the first (resp., second) message. What is the most you can conclude about m_1 and m_2?

1. Nothing can be determined about m_1 or m_2 since the one-time pad is perfectly secret.
2. m_1 is the character `A` and m_2 is the character `D`.
3. One of m_1 or $_2$ is the space character, and the other is the character `b`.
4. m_1 is the character `b` and m_2 is the space character.
5. m_1 is the space character and m_2 is the character `b`.

Solution: Your solution here. Answers have to be fully justified in order to get the full amount of points.
□

Question 2 [2 pt]: 3 messages with the same key

Three ASCII messages containing English letters and spaces only are encrypted using the one-time pad and the same key. The 10th byte of the first ciphertext is observed to be `0x66`, the 10th byte of the second ciphertext is observed to be `0x32`, and the 10th byte of the third ciphertext is observed to be `0x23`. Let m_1 (resp., m_2, m_3) denote the 10th ASCII character in the first (resp., second, third) message. Explain how to determine m_1, m_2 and m_3. (1/3 points for the values they obtain, 1 for the correct derivation).

Solution: Your solution here □

Question 3 [1 pt]

Which of the following is a negligible function?

1. $f(n) = \frac{1}{2^n}$
2. $f(n) = \frac{n}{2^n}$
3. $f(n) = \frac{1}{n}$
4. $f(n) = \frac{1}{2}$

Solution: justify your answers □

Question 4 [3 pt]: Non-equal-length messages, Exercise 3.3 from [KL]

Say $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is such that for $k \in \{0,1\}^n$, algorithm Enc_k is only defined for messages of length at most $\ell(n)$ (for some polynomial ℓ). Assuming Enc_k is EAV-secure, construct a scheme Π' satisfying Definition 3.8 even when the adversary is *not* restricted to outputting equal-length messages in $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$.

Solution: □

Question 5 [2 pt]: Success probability in a reduction

Assume that algorithm A efficiently solves problem P_1 and there is an efficient reduction from problem P_2 to problem P_1. Prove that there exists an algorithm B for which

$$\Pr[A \text{ succeeds in solving } P_1] \leq \Pr[B \text{ succeeds in solving } P_2] .$$

Solution: □

Question 6 [1 pt]: Pseudo One-Time Pad using a PRG

Let G be a function mapping n-bit inputs to $2n$-bit outputs. Which of the following is true of the pseudo one-time pad encryption scheme based on G? (Check all that apply.)

1. The scheme can be used to securely encrypt multiple messages using the same key.
2. The scheme is perfectly secret.
3. The key space of the scheme is at least as large as the message space.
4. The scheme is computationally secret if G is a pseudorandom generator.

Solution: □

Question 7 [3 pt]

Let n be even and let G be a pseudorandom generator with expansion factor $\ell(n) = 4n$. In this exercise, we want to show that $G'(s) := G(s_1, \ldots, s_{\lceil n/2 \rceil})$, where $s = s_1 \cdots s_n$, is a PRG.

Let D be an efficient distinguisher for G' with distinguishing advantage

$$\varepsilon'(n) := |\Pr_{s \leftarrow \{0,1\}^n}[D(G'(s)) = 1] - \Pr_{r \leftarrow \{0,1\}^{2n}}[D(r) = 1]|$$

Let us define the distinguishing advantage of D for G as

$$\varepsilon(n) := |\Pr_{s \leftarrow \{0,1\}^n}[D(G(s)) = 1] - \Pr_{r \leftarrow \{0,1\}^{4n}}[D(r) = 1]| .$$

Now, argue (1pt) that $\varepsilon'(n) = \varepsilon(n/2)$. Then use this derivation to conclude that G' is a PRG (2pts).

Solution: □

Question 8 [2 pt]

Let n be even and let G be a pseudorandom generator with expansion factor $\ell(n) = 4n$. Define $G'(s) := G(0^{|s|} \| s)$. Prove that G' is not a PRG.
Hint: use the Question 7 above.

Solution: $\square$

Question 9 [2 pt]

Let n be even and let G be a pseudorandom generator with expansion factor $\ell(n) = 4n$. Define $G'(s) := G(s) \| G(s \oplus 0^{n-1}1)$. Show that G' is not a PRG.
Hint: use the Question 7 above.

Solution: □

Question 10 [4 pt]

Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG. Describe a computationally unbounded adversary $\mathcal{A}$ that distinguishes the output of G from a uniform $2n$-bit string with probability exponentially close to 1. How does it work? Compute its exact distinguishing advantage.
Hint: Use practice problem 4.

What is $\Pr[PRG_{\mathcal{A},G}(n) = 1]$ for this adversary (where $PRG_{\mathcal{A},G}$ is the experiment defined in Figure 2 of problem set 2)?

Solution: □

Programming Question 11 [8 pt]

Solve programming assignment 2. Describe the solution and how you proceeded. You may use any programming language you like to solve the problem. In this github repo, you can find some possibly helpful python code. Use your program to solve this same type of problem as well.

Solution: □