UC Berkeley — CS194-34 : Undergraduate Cryptography Midterm II
Prof. Sanjam Garg October 30, 2019

Midterm II

Name:

SID:

Do not turn this page until your instructor tells you to do so.

- After the exam starts, write your name on every odd-numbered page. We reserve the right to deduct points if you do not, and you will not be allowed to do so after time is called.
- For short question, your answers must be written clearly inside the box region. Any answer outside the box will not be graded. For longer questions, if you run out of space, you must clearly mention in the space provided for the question if part of your answers is elsewhere.
- Try to answer all questions. Not all parts of a problem are weighted equally. Before you answer any question, read the problem carefully. Be precise and concise in your answers.
- You may consult at most *20 sheets of notes.* Apart from that, you may not look at books, notes, etc. Calculators, phones, computers, and other electronic devices are NOT permitted.
- There are **11** pages on the exam (counting this one). Notify a proctor immediately if a page is missing.
- **You have 80 minutes: there are 5 questions on this exam worth a total of 100 points.**

1 True/False (20 points)

Bubble in the right answer. No explanation needed. +2 points for correct answer and ***-1 points for wrong answers!*** *If you leave a question unanswered, then there is no penalty. This part will be graded automatically. Please mark your answer clearly.*

1. Let H be a random function mapping $\{0,1\}^n \rightarrow \{0,1\}^{n/2}$. Then the probability that there exists a collision in q distinct queries to H is $O(\binom{q}{2}\frac{1}{2^{n/2}})$.

   ○ True

   ○ False

2. A pseudorandom generator implies a CCA-secure encryption.

   ○ True

   ○ False

3. A CCA-secure encryption is also an authenticated encryption.

   ○ True

   ○ False

4. A pseudorandom function implies a pseudorandom generator.

   ○ True

   ○ False

5. The Authenticate-then-encrypt approach yields an authenticated encryption scheme.

   ○ True

   ○ False

6. A CPA-secure encryption scheme implies a pseudorandom function.

   ○ True

   ○ False

7. Two or more rounds are sufficient for the security of Fiestel network.

   ○ True

   ○ False

8. A 3-round SPN network with 64 bit sub-keys and output key mixing can be broken in time 2^{192}.

   ○ True

   ○ False

9. One-way functions do not exist if discrete logarithm is solvable in polynomial time.

   ○ True

   ○ False

10. An unforgeable encryption implies a MAC scheme.

    ○ True

    ○ False

2 Hardcore Predicate (20 points)

In this question, we will show the existence of a one-way function where every bit of the input is not a hardcore predicate.

1. Assume that $h : \{0,1\}^{n-1} \to \{0,1\}^{n-1}$ is a one-way function. We now define a function $g : \{0,1\}^n \times \{1,2,3,\ldots,n\} \to \{0,1\}^{n-1} \times \{0,1\} \times \{1,2,3,\ldots,n\}$ as follows.

$$g(x,i) = \boxed{}$$

2. Show that g is a one-way function assuming h is a one-way function.

3. Define the function $p_k : \{0,1\}^n \to \{0,1\}$ as $p_k(x) = x_k$ (where x_k denotes the k-th bit of the input). For every $k \in \{1,\ldots,n\}$, we will construct an adversary $\mathcal{A}$ who given $g(x,i)$ can predict the output $p_k(x)$ with non-negligible probability. On input $(y,b,j) \in \{0,1\}^{n-1} \times \{0,1\} \times \{1,2,3,\ldots,n\}$, $\mathcal{A}$ does the following.

$$\mathcal{A}((y,b,j)) = \begin{cases} \boxed{} & \text{if } k = j \\ \boxed{} & \text{otherwise} \end{cases}$$

4. $\Pr_{(x,i) \xleftarrow{\$} \{0,1\}^n \times \{1,2,\ldots,n\}}[A(g(x,i)) = p_k(x)] = \boxed{\qquad\qquad}$

(We want the exact answer. A generic answer like non-negligible will get you 0 points.)

3 Unforgeable Encryption (20 points)

In this problem, we will show the existence of an encryption system that is CCA-secure but not unforgeable.

1. Assume $F : \{0,1\}^{2n} \to \{0,1\}^{2n}$ is a strong pseudorandom permutation. We will consider the following encryption scheme for messages of length n bits.
    - Gen : Sample a random key k for F.
    - $\mathsf{Enc}(k, m)$: Sample the randomness r of length n uniformly and output $c = \boxed{}$
    - $\mathsf{Dec}(k, c)$: Output $m = \boxed{}$
2. Show that $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a CCA-secure encryption.

3. Show that $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is not unforgeable.

4 Data Encryption Standard (15 points)

Here is the information about DES taken verbatim from the textbook.

The DES block cipher is a 16-round Feistel network with a block size of 64 bits and a key length of 56 bits. The same round function $\widehat{f}$ is used in each of the 16 rounds. The round function takes a 48-bit subkey and, as expected for a (balanced) Feistel network, a 32-bit input (namely, half a block). The key schedule of DES is used to derive a sequence of 48-bit sub-keys $k_1, \ldots, k_{16}$ from the 56-bit master key. (It is not important for this problem on how exactly is the key schedule defined).

The DES round function $\widehat{f}$-sometimes called the DES mangler function - is constructed using the substitution-permutation paradigm. In more detail, computation of $\widehat{f}(k_i, R)$ with $k_i \in \{0,1\}^{48}$ and $R \in \{0,1\}^{32}$ proceeds as follows: first, R is expanded to a 48-bit value R'. This is carried out by simply duplicating half of the bits of R; we denote this by $R' := E(R)$ where E is called the expansion function. Following this, the computation proceeds exactly as a SPN: The expanded value R' is XORed with k_i, which is also 48 bits long, and the resulting value is divided into 8 blocks, each of which is 6 bits long. Each block is passed through a (different) S-box that takes a 6-bit input and yields a 4-bit output; concatenating the output from 8 S-boxes gives a 32-bit result. A mixing permutation is then applied to the bits of this result to obtain the final output.

Show that DES has the property that $DES_{k_1,\ldots,k_{16}}(x) = \overline{DES_{\overline{k}_1,\ldots,\overline{k}_{16}}(\overline{x})}$ for every set of keys $k_1, \ldots, k_{16}$ and input x. Here, $\overline{y}$ denotes the bitwise complement of the string y.

5 Collision-Resistant Hash function (25 points)

1. Show that collision-resistant hash functions imply one-way functions.

2. Let (Gen, H) be a collision-resistant hash function with output length ℓ. In this problem, we will construct another collision-resistant hash function (Gen_1, H_1) such that if the output of H_1 is truncated by one bit, then it is no longer collision resistant.

   (a) We define $\mathsf{Gen}_1(1^n) : s \overset{\$}{\leftarrow} \mathsf{Gen}(1^n)$. Let x_0, x_1 be two different input strings from the message space, and set h as $H(x_0)$ with the last bit flipped.

$$H_1^s(x) = \begin{cases} \boxed{\qquad\qquad} & \text{if } x = x_1 \\ \boxed{\qquad\qquad} & \text{if } H^s(x) = h \\ \boxed{\qquad\qquad} & \text{otherwise} \end{cases}$$

(b) Show that (Gen_1, H_1) is collision-resistant assuming (Gen, H) is collision-resistant.

(c) Show that (Gen_1, H_2) is not collision resistant where H_2 is defined as follows: compute H_1 and output all the bits except the last bit.