

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 $O\left(\binom{q}{2} \frac{1}{2^{n/2}}\right)$.

True

False

Solution: True

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

True

False

Solution: True

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

True

False

Solution: False

4. A pseudorandom function implies a pseudorandom generator.

True

False

Solution: True

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

True

False

Solution: False

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

True

Name:

False

Solution: True

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

True

False

Solution: 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

Solution: True

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

True

False

Solution: False

10. An unforgeable encryption implies a MAC scheme.

True

False

Solution: True

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

$$g(x, i) = \boxed{\text{Solution: } h(x_{-i}), x_i, i}$$

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

Solution: If g is not one-way, we will break the one-wayness of h . Specifically, given $y = h(z)$ for a randomly chosen $z \in \{0, 1\}^n$, we will choose a random $i \in \{1, \dots, n\}$ and a bit $x_i \in \{0, 1\}$ and run the adversary \mathcal{A} against the one-way ness of g on input (y, x_i, i) . \mathcal{A} gives an output x' and we output x'_{-i} .

3. Define the function $p_k : \{0, 1\}^n \rightarrow \{0, 1\}$ as $p_k(x) = x_k$ (where x_k denotes the k -th bit of the input). For every $k \in \{1, \dots, n\}$, 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 $(y, b, j) \in \{0, 1\}^{n-1} \times \{0, 1\} \times \{1, 2, 3, \dots, n\}$, \mathcal{A} does the following.

Name:

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

4. $\Pr_{(x,i) \leftarrow \{0,1\}^n \times \{1,2,\dots,n\}} [A(g(x,i)) = p_k(x)] = \boxed{\text{Solution: } 1/2 + 1/2n}$

(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 $F : \{0, 1\}^{2n} \rightarrow \{0, 1\}^{2n}$ 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 .

- Enc(k, m) : Sample the randomness r of length n uniformly and output $c =$ **Solution:** $F_k(m||r)$

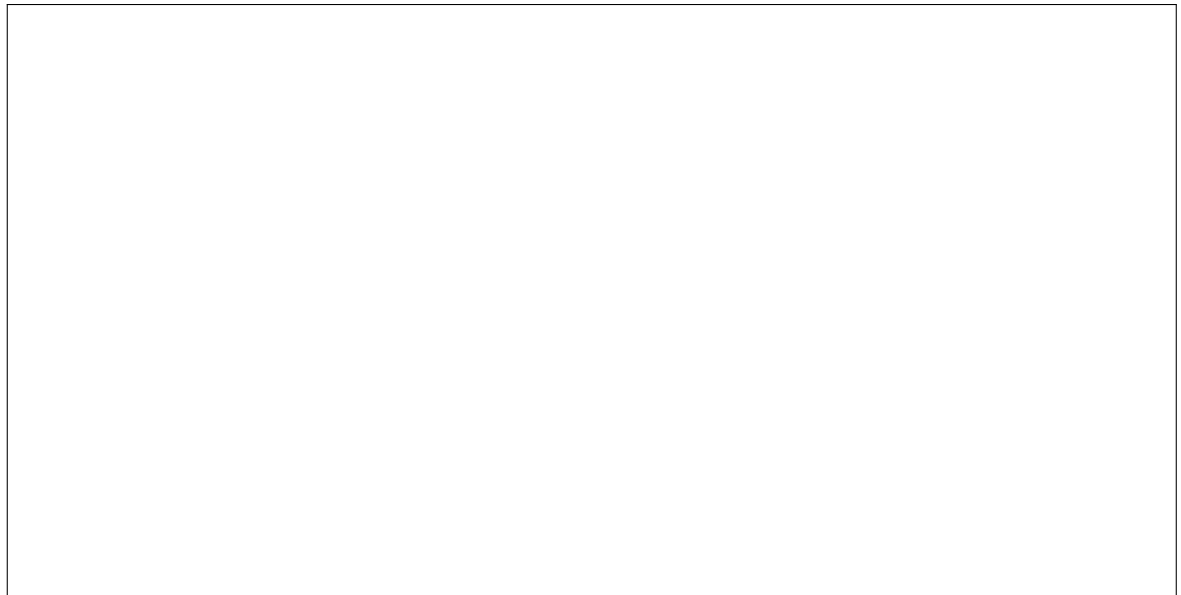
- Dec(k, c) : Output $m =$ **Solution:** The first n bits of $F_k^{-1}(c)$

2. Show that (Gen, Enc, Dec) is a CCA-secure encryption.

Name:

Solution: This is proved through a hybrid argument. In the first hybrid, we are given oracle access to F_k, F_k^{-1} for a randomly chosen k . Using these two oracles, it is easy to simulate the encryption and the decryption queries. Specifically, for every encryption query on a message m , we choose a uniform random string r of length n and query F_k on $m||r$. For every decryption query on a ciphertext c , we will query F_k^{-1} on c and output the first n bits. The second hybrid is defined as giving oracle access to a randomly chosen permutation π and π^{-1} . It follows from the security of strong PRP that these two hybrids are computationally indistinguishable. Now, in the last hybrid, the message inside the challenge ciphertext is perfectly hidden since the permutation π is completely random and the probability that in any query the adversary will be able to guess r used in the challenge ciphertext is 2^{-n} .

3. Show that (Gen, Enc, Dec) is not unforgeable.



Solution: Every string of length $2n$ is a valid ciphertext and hence, this encryption scheme is trivially forgeable.

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 \hat{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, \dots, 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 \hat{f} -sometimes called the DES mangler function - is constructed using the substitution-permutation paradigm. In more detail, computation of $\hat{f}(k_i, R)$ 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 $DES_{k_1, \dots, k_{16}}(x) = \overline{DES_{\bar{k}_1, \dots, \bar{k}_{16}}(\bar{x})}$ for every set of keys k_1, \dots, k_{16} and input x . Here, \bar{y} denotes the bitwise complement of the string y .

Name:

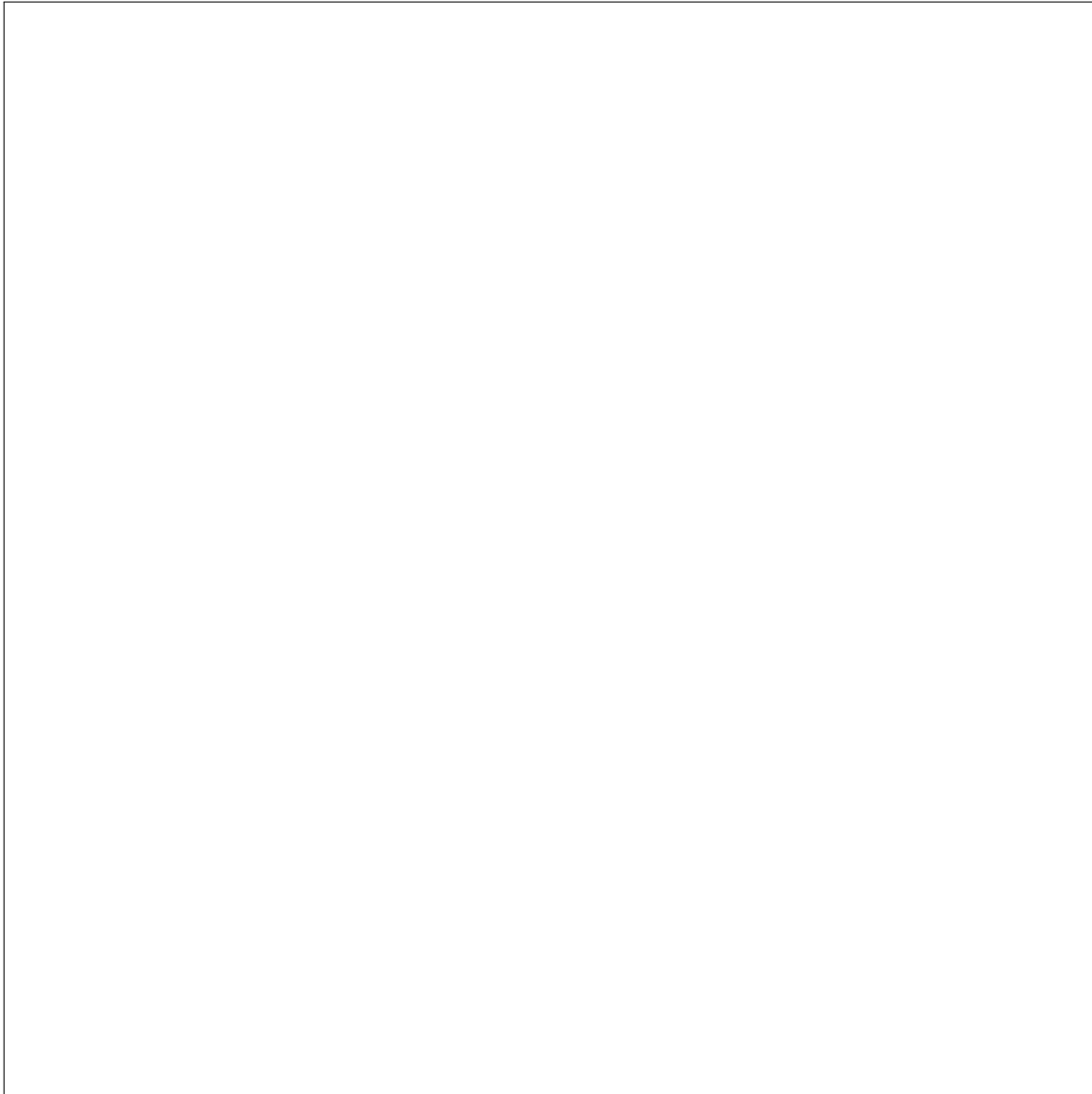
Solution: Let \widehat{f} be the DES mangler function. We first claim that for every key k and every input x , it holds that $\widehat{f}(k, x) = \widehat{f}(\overline{k}, \overline{x})$. To see this, notice that for input x and key k , the input to the S-boxes equals $E(x) \oplus k$ where E is the expansion function. Since E simply duplicates half of the bits of its input, we have that $E(\overline{x}) = \overline{E(x)}$. Therefore $E(\overline{x}) \oplus \overline{k} = \overline{E(x)} \oplus \overline{k} = E(x) \oplus k$. Since the input to the S-boxes is the same, the output from the S-boxes is also the same. Applying the mixing permutation does not change the fact that the outputs are equal. We conclude that $\widehat{f}(k, x) = \widehat{f}(\overline{k}, \overline{x})$.

Next look at the entire Feistel structure. For input L_0, R_0 and key k , the values after the first round are $L_1 = R_0$ and $R_1 = L_0 \oplus \widehat{f}(k, R_0)$. By the above, for input $\overline{L_0}, \overline{R_0}$ and key \overline{k} the values after the first round are $L'_1 = \overline{R_0} = \overline{L_1}$ and

$$R'_1 = \overline{L_0} \oplus \widehat{f}(\overline{k}, \overline{x}) = \overline{L_0} \oplus \widehat{f}(k, x) = \overline{R_1}.$$

5 Collision-Resistant Hash function (25 points)

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



Solution: (this is homework)

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 $\text{Gen}_1(1^n) : s \xleftarrow{\$} \text{Gen}(1^n)$. 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.

Name: _____

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

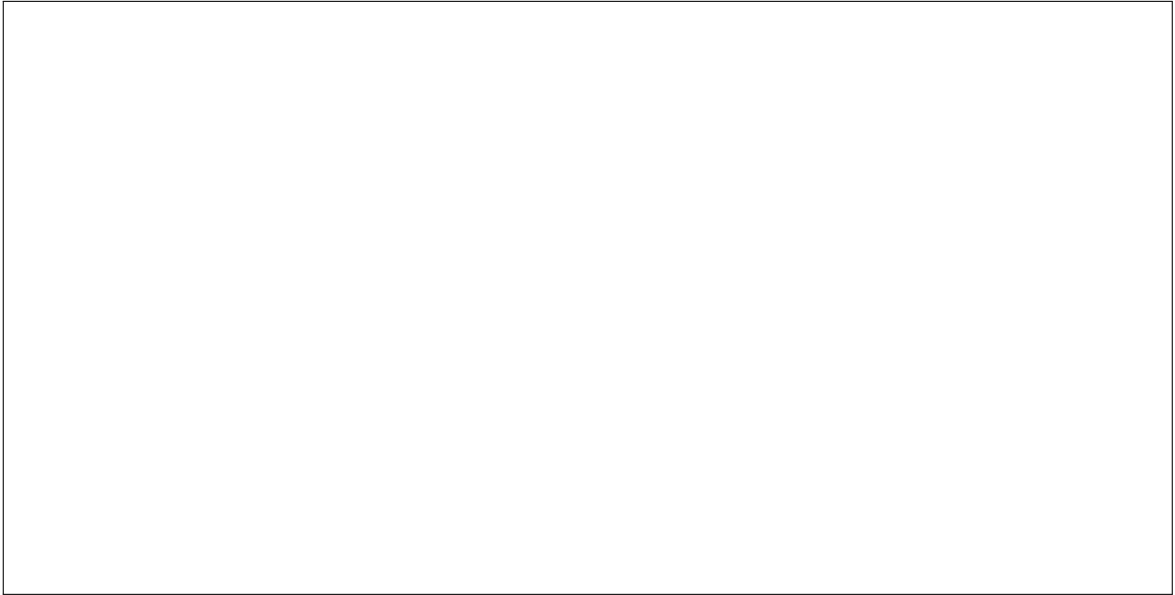
(b) Show that (Gen_1, H_1) is collision-resistant assuming (Gen, H) is collision-resistant.

Solution: Assume that there exists an \mathcal{A} that on input s outputs distinct x, x' such that $H_1^s(x) = H_1^s(x')$ with noticeable probability. We will run this adversary on the key s and obtain x, x' . Now we show that x, x' can be used to output a collision in H .

First, if $H_1^s(x), H_1^s(x') \neq h$ then $x, x' \neq x_1$. It follows that either $H^s(x) = H^s(x')$, in which case (x, x') is a collision in H , or (w.l.o.g.) x is such that $H^s(x) = H^s(x_1)$, in which case (x, x_1) is a collision in H .

Next, consider the case that $H_1^s(x), H_1^s(x') = h$. If $H^s(x_1) \neq h$ then the only value such that $H_1^s(x) = h$ is x_1 and hence there cannot be any valid collisions in H_1 with the image being h . So let us assume that $H^s(x_1) = h$. Then, we again observe that x, x' will be a valid collision in H as $H^s(x) = H^s(x') = h$.

-
- (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.



Solution: x_0, x_1 will be a collision for H_2 .