Applied Cryptography Mid-term Examination

Spring Semester 2023

(263-4660-00L)

K. G. Paterson

Student name: ________________________________

Legi number: ________________________________

Examination Rules:

(a) **DO NOT TURN OVER THIS PAGE UNTIL INSTRUCTED TO DO SO BY AN EXAMINER.**

(b) Closed-book, written exam, 75 minutes total.

(c) If you feel disturbed or have questions about the exam, raise your hand to call an assistant.

(d) You are permitted to leave the exam early, but not within the last 10 minutes of the exam. If you wish to leave, please raise your hand and wait for an assistant.

(e) There are two problems in the exam, worth 25 marks each. You should attempt as many parts as you can, but you do not need to complete every part of every problem to obtain the best possible grade.

(f) Read all the problems before beginning.

(g) Write your name, legi and seat number at the top of each sheet of paper that you use.

(h) Start each problem on a new sheet of paper.

(i) Write as clearly as you can and show all your work. For some questions, you may get partial credit even if the end result is wrong due to a calculation error.

(j) Write with a black or blue pen (no pencil, no green or red ink).

(k) Turn off your mobile phone. No electronic devices are allowed on desks, except for watches. Smartwatches are not permitted.

Problem	1	2	$\sum$
Max. Points	25	25	50
Points			
Signature			

Problem 1 (Block ciphers and CBC mode).

(a) Explain what it means for a block cipher E to be (q, t, ϵ)-secure as a PRP. You may use a diagram or pseudo-code to illustrate your answer. [3 marks]

(b) In the PRP-PRF distinguishing game an adversary $\mathcal{A}$ tries to distinguish between an oracle returning values from a random permutation $\pi : \{0,1\}^n \to \{0,1\}^n$ (when $b = 0$) and an oracle returning values from a random function $f : \{0,1\}^n \to \{0,1\}^n$ (when $b = 1$). Let b' denote $\mathcal{A}$'s output and define:

$$\mathbf{Adv}^{\text{PRP-PRF}}(\mathcal{A}) := |2\Pr[b' = b] - 1|.$$

Prove that for any such adversary $\mathcal{A}$ making at most q queries:

$$\mathbf{Adv}^{\text{PRP-PRF}}(\mathcal{A}) \leq q^2/2^{n+1}.$$

Hint: Recall that to simulate either π or f, one can use lazy sampling of oracle responses (without or with replacement, respectively). You may make use of the difference lemma and the advantage rewriting lemma. [5 marks]

(c) Define (q, t, ϵ)-IND-CPA security for a symmetric encryption scheme SE = (KGen, Enc, Dec). You may use a diagram or pseudo-code to illustrate your answer. [3 marks]

(d) Consider the following simplified version of CBC-mode encryption for *single-block* messages m, using block cipher E:

1) CBC[E].KGen: selects $K \leftarrow_\$ \{0,1\}^k$ and returns K;
2) CBC[E].Enc on input $K \in \{0,1\}^k$ and $m \in \{0,1\}^n$: sets $c_0 \leftarrow_\$ \{0,1\}^n$, $c_1 = \mathsf{E}(K, c_0 \oplus m)$ and returns $c_0 \,\|\, c_1$.
3) CBC[E].Dec on input $K \in \{0,1\}^k$ and $c \in \{0,1\}^{2n}$: parses $c \leftarrow c_0 \,\|\, c_1$ where $c_0, c_1 \in \{0,1\}^n$, and returns $m = \mathsf{D}(K, c_1) \oplus c_0$, where D denotes the inverse of block cipher E.

In the remainder of this question, you will analyse the security of CBC[E].

i) Suppose CBC[E].Enc is used to encrypt q single-block messages $m_1, m_2, \ldots, m_q$ (where the m_i are not necessarily distinct). Notice that the message input to the block cipher E for each encryption has the form $r_i := c_{i,0} \oplus m_i$ where $c_{i,0} \leftarrow_\$ \{0,1\}^n$. Let

Z denote the event that in the course of these q encryptions, a value r_i is repeated. Give a brief argument to show $\Pr[Z] \leq q^2/2^{n+1}$. [3 marks]

ii) Use the above result and the result in part b) for PRP-PRF security to **sketch** a proof of the IND-CPA security of CBC[E]. In particular you should prove a bound relating the IND-CPA advantage of any adversary $\mathcal{A}$ against CBC[E] to the PRP advantage of a related adversary $\mathcal{B}$ against E. You may make free use of the advantage rewriting and difference lemmas.

Hint 1: Use a sequence of games G_0, G_1, G_2, G_3 such that:

G_0: the IND-CPA adversary $\mathcal{A}$ plays against a challenger implementing the scheme CBC[E] as defined above.

G_1: as in G_0 but E with random key K is replaced by a random permutation π.

G_2: as in G_1 but π is replaced by a random function f.

G_3: as in G_0 but $\mathcal{A}$ plays against a challenger which returns random bit strings of length $2n$ bits in response to $\mathcal{A}$'s encryption oracle queries.

Hint 2: Define q_i to be $\Pr[b' = b]$ in game G_i. Establish a sequence of inequalities bounding the values of $|q_i - q_{i+1}|$ for $i = 0, 1, 2$ and use this to prove a bound on $|q_0 - \frac{1}{2}|$.

[10 marks]

(e) Suppose that the values c_0 used in CBC-mode (as described above) are not random but instead are predictable to the adversary. Is CBC-mode still secure? Briefly justify your answer. [1 mark]

Problem 2 (Hash functions and authenticated encryption).

(a) Give formal definitions of

1) an (unkeyed) hash function, and [2 marks]

2) an adversary against the collision resistance of a hash function H. [2 marks]

(b) What distinguishes collision resistance for unkeyed hash functions from other security definitions you have seen in this course, e.g., (t, q, ε) IND-CPA security? Why is this? [2 marks]

(c) Consider the following simplified version of the $\mathsf{SHA3}$ hash function for *single-block* unpadded message inputs of length r bits. It uses an unkeyed permutation $\mathsf{F}\colon \{0,1\}^{r+c} \to \{0,1\}^{r+c}$ over $(r+c)$-bit strings, which is constructed via some efficient and invertible bit operations.

```
$\underline{\mathsf{SHA3}(m)}$
$C \leftarrow 0^c$                     // Initial inner state
$x \leftarrow \mathsf{F}(m \,\|\, C)$   // Absorbing $m \in \{0,1\}^r$
$y \leftarrow \mathsf{F}(x)$            // Squeezing
Return $y[1..r]$                       // Output first $r$ bits of $y$
```

1) Consider a modified version $\mathsf{SHA3}'$ of the above, which outputs all of y instead of only the first r bits $y[1..r]$. Describe an attack against the pre-image resistance of $\mathsf{SHA3}'$. [2 marks]

2) Consider $\mathsf{SHA3}''\colon \{0,1\}^r \times \{0,1\}^c \to \{0,1\}^r$ which works like $\mathsf{SHA3}$ above, except that it takes as a second input the initial inner state C:

```
$\underline{\mathsf{SHA3}''(m, C)}$
$x \leftarrow \mathsf{F}(m \,\|\, C)$   // Absorbing $m \in \{0,1\}^r$, with $C \in \{0,1\}^c$ as input
$y \leftarrow \mathsf{F}(x)$            // Squeezing
Return $y[1..r]$                       // Output first $r$ bits of $y$
```

(So $\mathsf{SHA3}$ is $\mathsf{SHA3}''$ with the second input fixed to 0^{512}.)

Describe an attack against the collision resistance of $\mathsf{SHA3}''$. That is, show how to construct two values $(m_1, C_1) \neq (m_2, C_2)$ such that $\mathsf{SHA3}''(m_1, C_1) = \mathsf{SHA3}''(m_2, C_2)$. [4 marks]

(d) HMAC is a PRF built from a Merkle–Damård hash function H.

1) Define $\mathsf{HMAC}(K, m)$ in terms of H, the key K, and the input message m. For simplicity, assume K is k bits long where k is the block size of the compression function underlying H.

   Hint: Recall that K is first expanded into two keys, $K_1 \leftarrow K \oplus \mathsf{ipad}$ and $K_2 \leftarrow K \oplus \mathsf{opad}$, for defined constants ipad and opad. [1 mark]

2) From $\mathsf{SHA3}$, one can define KMAC essentially as $\mathsf{SHA3}(K \parallel m)$ for some key K and message m. KMAC can be shown to be a secure PRF.

   Briefly compare KMAC to the HMAC design: What is the main difference and why is the same approach not secure for a Merkle–Damgård hash function? [2 marks]

(e) AE security for a symmetric encryption scheme is defined as the combination of two other security notions. Name them and give a brief informal explanation of each. [3 marks]

(f) Construct a secure authenticated encryption (AE) scheme from a PRF alone, via the following steps. You may assume that, like HMAC and KMAC, the PRF can process variable-length message inputs.

1) Give a construction of an AE scheme $\mathrm{AE} = (\mathrm{KGen}, \mathrm{Enc}, \mathrm{Dec})$ from a (variable-length input) PRF F with key space $\{0,1\}^k$.

   Hint 1: You may use/refer to generic composition constructions with appropriate explanation.

   Hint 2: Recall that by the PRP-PRF switching lemma, a PRF can be used in place of a PRP whenever only the forward (encipher) operation of the PRP is needed. [4 marks]

2) Briefly argue why your construction achieves AE security if F is a secure PRF. [3 marks]