Applied Cryptography Mid-term Examination

Spring Semester 2022

(263-4660-00L)

K.G. Paterson

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 (Block ciphers and CTR mode).

(a) Let $\mathsf{E}\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ denote a block cipher with k-bit keys and n-bit blocks. Define what it means for E to be (q,t,ϵ)-secure as a PRP. You can use either a diagram or pseudo-code to illustrate your answer. Make sure to define the advantage $\mathbf{Adv}^{\mathrm{PRP}}_{\mathsf{E}}(\mathcal{A})$ of an adversary $\mathcal{A}$ as part of your answer. [4 marks]

(b) Explain briefly how the PRF security definition differs from the PRP security definition. [1 mark]

(c) CTR-mode is a method for using a block cipher to construct a symmetric encryption scheme with message space $\{0,1\}^*$.

1) Briefly describe the *encryption* operation of CTR-mode. You may use pseudo-code in your answer if you wish. You do not need to specify how the initial counter value is chosen. [2 marks]

2) Describe the main security requirement on counter selection in CTR-mode and explain what weakness results if this requirement is violated. [2 marks]

3) One way to select the counters in CTR-mode is to set the initial counter value to the all-zero string 0^n and use each key to encrypt only a single message. Briefly describe **two** other options for selecting the counter values used in CTR-mode. [2 marks]

(d) Suppose $\mathsf{F}\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ is an efficiently computable function. Consider CTR-mode where F is used in place of the block cipher E.

1) Explain briefly why, in terms of functionality, such an F can be used in place of E in CTR-mode. In particular, consider the requirements on E and F for correct decryption. [1 mark]

2) Let $\mathtt{SE} = (\mathtt{KGen}, \mathtt{Enc}, \mathtt{Dec})$ be a general symmetric encryption scheme. Define what it means for $\mathtt{SE}$ to be (q,t,ϵ)-IND-CPA secure. You may use either a diagram or pseudo-code to illustrate your answer. Make sure to define the advantage $\mathbf{Adv}^{\text{IND-CPA}}_{\mathtt{SE}}(\mathcal{A})$ as part of your answer. [3 marks]

3) Now assume F is a PRF. Consider the version of CTR-mode, denoted $\mathtt{CTR}[\mathsf{F}]$, in which each key K is used to encrypt only one message (of maximum block-length 2^n) and the initial counter value is set to the all-zero string 0^n. Formally prove that $\mathtt{CTR}[\mathsf{F}]$

is IND-CPA secure for the class of adversaries $\mathcal{A}$ making at most one query to the relevant oracle.

As part of your answer, for any such adversary $\mathcal{A}$, prove an equality between $\mathbf{Adv}^{\text{IND-CPA}}_{\mathtt{SE}}(\mathcal{A})$ and the advantage of a related PRF adversary $\mathcal{B}$ against F, relating the running time and resources consumed by $\mathcal{B}$ to those of $\mathcal{A}$.

(Hint: Consider a game hopping proof in which G_0 is the normal IND-CPA security game and G_1 is the game in which F is replaced by a random function f. Bound the difference in the probability that $b' = b$ in G_0 and G_1, and then compute that probability in G_1.) [8 marks]

(e) Give an attack showing that the scheme $\mathtt{CTR}[\mathsf{F}]$ does not resist IND-CCA attacks. [2 marks]

Problem 2 (CBC-MAC and its security).

(a) Recall that a MAC scheme $\mathtt{MAC}$ consists of a triple of algorithms $\mathtt{MAC} = (\mathtt{KGen}, \mathtt{Tag}, \mathtt{Vfy})$ and has three associated spaces: a key space $\mathcal{K}$, a message space $\mathcal{M}$ and a tag space $\mathcal{T}$.

Define what it means for a MAC scheme to be (q_t, t, ϵ)-SUF-CMA-secure. (Here you may assume a "no-verify-oracle" version of the security game; you may use a diagram to illustrate your answer.)
[3 marks]

CBC-MAC. $\mathtt{CBC\text{-}MAC}$ is a MAC scheme built from a block cipher E with n-bit blocks and k-bit keys. $\mathtt{CBC\text{-}MAC}$ has message space $\mathcal{M} = (\{0,1\}^n)^*$ (i.e. $\mathcal{M}$ consists of all bit-strings that are a multiple of n in bit-length) and key space $\{0,1\}^k$. Given a key $\mathsf{K} \in \{0,1\}^k$ and a value $\mathsf{IV} = 0^n$, the tag τ for a message m consisting of r many n-bit blocks $m_1, \ldots, m_r$ is computed as follows:

$$c_0 = \mathsf{IV}; \quad c_i = \mathsf{E}(\mathsf{K}, m_i \oplus c_{i-1}) \quad (1 \le i \le r); \quad \tau = c_r.$$

That is, the tag τ is the last block of the CBC-mode encryption of the message m under key K using an all-zero initialisation vector, as shown in Figure 1. Verification on input (K, m, τ') recomputes τ and compares it to τ'.

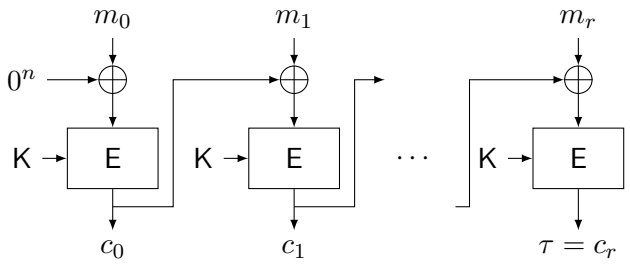

Figure 1: Tag algorithm of `CBC-MAC`.

(b) Show that `CBC-MAC` is **not** SUF-CMA secure by describing an efficient adversary that has advantage 1. Full credit will be given for an attack that makes just one query to the tag$(\cdot)$ oracle. [3 marks]

(c) Fix an integer $r \geq 1$ and let $\mathcal{M}_{n,r} := \{0,1\}^{nr}$ denote the set of bit-strings of fixed length nr. Give a **brief** argument to explain why `CBC-MAC` is SUF-CMA secure if the message space is restricted to $\mathcal{M}_{n,r}$ and E is a suitably strong block cipher. (Hint: first consider the case $r = 1$, then proceed by induction.) [4 marks]

(d) Recall that a nonce-based MAC scheme consists of a triple of algorithms $(\texttt{KGen}, \texttt{Tag}, \texttt{Vfy})$ and *four* associated sets: a key space $\mathcal{K}$, a nonce space $\mathcal{N}$, a message space $\mathcal{M}$ and a tag space $\mathcal{T}$. Recall also the definition of SUF-CMA security for "normal" (not nonce-based) MAC schemes from part (a).

Discuss the differences in the definitions of SUF-CMA security for nonce-based and normal MAC schemes. (You may again assume "no-verify-oracle" versions of the security games.) [4 marks]

(e) Fix an integer $r \geq 1$. Consider a nonce-based version of CBC-MAC for message space $\mathcal{M}_{n,r} = \{0,1\}^{nr}$ in which the nonce N has n bits and is used as the IV (previously fixed to 0^n) in the fixed-length CBC-MAC scheme introduced above. Show that this scheme is **not** SUF-CMA-secure by describing an attack and analysing its advantage and number of queries needed. Full credit will be given for an attack that has advantage 1 and makes just one query to the tag$(\cdot)$ oracle. [3 marks]

(f) Let $\texttt{MAC} = (\texttt{KGen}, \texttt{Tag}, \texttt{Vfy})$ be a normal (i.e. not nonce-based) MAC scheme for some message space of the form $\{0,1\}^n \times \mathcal{M}'$, where $\mathcal{M}'$ is some set of bit-strings. Suppose that a nonce-based scheme $\texttt{N.MAC} = (\texttt{N.KGen}, \texttt{N.Tag}, \texttt{N.Vfy})$ is built from `MAC` as follows: `N.KGen` is identical

to $\texttt{KGen}$, the message space of $\texttt{N.MAC}$ is $\mathcal{M}'$, nonces N in $\texttt{N.MAC}$ are n-bit strings, and the algorithm $\texttt{N.Tag}$ on input (K, N, m) with $m \in \mathcal{M}'$ outputs $\tau \leftarrow\!\!\$\ \texttt{Tag}(\mathsf{K}, N \,\|\, m)$.

1) Define a suitable algorithm $\texttt{N.Vfy}$ for $\texttt{N.MAC}$ and show that the resulting scheme is correct. [2 marks]
2) Formally prove that $\texttt{N.MAC}$ is SUF-CMA secure as a nonce-based MAC scheme if $\texttt{MAC}$ is SUF-CMA secure as a normal MAC scheme. Your proof should provide a concrete security analysis relating the advantage of any (q_t, t, ϵ)-SUF-CMA adversary $\mathcal{A}$ against $\texttt{N.MAC}$ to that of a related SUF-CMA adversary $\mathcal{B}$ against $\texttt{MAC}$. [6 marks]