Modern Cryptography December 12, 2018

Midterm Exam – Solutions

Lecturer: Krzysztof Pietrzak, TA: Michael Walter

Put your name and student ID (if applicable) on every sheet that you hand in. Leave space in the top left corner of every sheet to allow for stapling. Any permanent pen is allowed, but text written in erasable pens (e.g. pencils) will not be considered during grading.

1. (12 points)

True or false

(a) $1/n^{\log(n)}$ is negligible (in n) **True**

(b) $1/n$ is negligible **False**

(c) $1/\log(n)$ is negligible **False**

(d) If $f(n)$ is negligible, then $f(n)^2 + \sqrt{f(n)}$ is negligible. **True**

(e) If $f(n)$ is negligible, then $2^{f(n)}$ is negligible. **False**

Solution: This is easy to see by letting $f(n) = 0$, which is clearly negligible, but $2^{f(n)} = 1$, which is not negligible. □

(f) If $f(n)$ is negligible, then $f(n) \cdot n^{\log(n)}$ is negligible. **False**

Solution: Consider $f(n) = 1/n^{\log(n)}$, which by (a) is negligible. But $f(n) \cdot n^{\log(n)} = 1$, which again is not negligible. □

2. (10 points)

In the definition of CPA secure encryption, the adversary can choose two messages m_0, m_1, and must then guess whether he received an encryption of m_0 or m_1. He must choose messages of same length, explain why.

Solution: If we change the definition of CPA security and allow the adversary to choose two messages of arbitrary different length, then this notion becomes unachievable.

To see this, let $(\mathsf{Enc}, \mathsf{Dec})$ denote the (efficient) encryption and decryption algorithms. For the security parameter n and a polynomial $p(\cdot)$, let $p(n)$ be the upper bound on the run-time of Enc when encrypting a single bit. Consequently $p(n)$ is *also* the upper bound on the size of the ciphertext for single-bit messages. Assuming that the decryption is always correct, the length of the ciphertext for a random message of length $2p(n)$ is at least $p(n)$ with overwhelming probability.

Now consider the IND-CPA game where the adversary challenges on $m_0 = 0$ and a random $2p(n)$-bit message m_1. If $b = 0$ then the ciphertext is of length at most $p(n)$; on the other hand, if $b = 1$ then almost always the length of the ciphertext is greater than $p(n)$. Thus the adversary can successfully guess the bit b with overwhelming probability. □

3. (10 points)

Rank from best to worst:

(a) Encrypt-and-authenticate

(b) Encrypt-then-authenticate

(c) Authenticate-then-encrypt

Explain (in one or two sentences) your choice for best and worst.

Solution: As discussed in Lecture 6, (b) is better than (c), which in turn is better than (a).

Encrypt-and-authenticate is clearly insecure when instantiated with a MAC scheme that leaks information of the message (say it's first bit).

Authenticate-then-encrypt, while not being totally insecure, does succumb to oracle-padding attacks and is hence not CCA-secure.

Encrypt-then-authenticate renders the decryption oracle in the CCA game useless for the adversary (since it cannot forge a valid messages) and for this reason it is better than authenticate-then-encrypt. This intuition can be formalised to show that encrypt-then-authenticate results in CCA-secure schemes if the underlying encryption scheme is CPA-secure and the MAC is strongly unforgeable. Recall that we called this notion Authenticated Encryption in class. □

4. (10 points)

Let $h : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a pairwise independent permutation. For which values X, Y are the following statements true (give the maximum value for which the statements are true). Explain (in one or two sentences) why for your choice of X, Y, the statements are no longer true for $X+1$ and $Y+1$, respectively.

(a) $\mathsf{MAC}(k,m) = h_k(m)$ is a secure X-time MAC (recall that this means the MAC is secure as long as one authenticates at most X messages).

Solution: $X = 1$. In class we proved that $\mathsf{MAC}(k,m) = h_k(m)$ is an information-theoretically secure 1-time MAC. To see why it is not necessarily secure for $X = 2$, consider as example the pairwise independent permutation $\pi : \{\mathbb{Z}_p^* \times \mathbb{Z}_p\} \times \mathbb{Z}_p \mapsto \mathbb{Z}_p$ defined as $\pi_{a,b}(m) = am + b$ (which was discussed both in class and in the homework). Once two distinct messages $m \neq m'$ are tagged using π and result in tags t, t', respectively, it is easy to recover the key a, b by solving the system of 2 equations: $t = am + b$ and $t' = am' + b$. Then a forgery can easily be obtained for any message since the key is known. □

(b) $\mathsf{ENC}(k,m) = h_k(m)$ achieves perfect secrecy if the number of encrypted messages is restricted to be at most Y.

Solution: Again, the solution is $Y = 1$. In this case we have perfect secrecy, because from the definition of pairwise independent permutation it follows (see below) that for any $m, c \in \{0,1\}^n$ we have $\Pr_k[h_k(m) = c] = \frac{1}{2^n}$. In particular, we have $\Pr_k[h_k(m) =$

$c] = \Pr_k[h_k(m') = c]$ for all m, m', c. This is one of the three equivalent definitions of perfect secrecy.

We briefly show that $\Pr_k[h_k(m) = c] = \frac{1}{2^n}$ for any m, c. Recall that by the definition of pairwise independent permutation we have $\Pr_k[h_k(m) = c \wedge h_k(m') = c'] = \frac{1}{2^n(2^n-1)}$ for any $m \neq m'$ and $c \neq c'$. So for arbitrary m, c and some $c' \neq c$:

$$\Pr_k[h_k(m) = c] = \sum_{m' \neq m} \Pr_k[h_k(m) = c \wedge h_k(m') = c'] = \sum_{m' \neq m} \frac{1}{2^n(2^n-1)} = \frac{1}{2^n}$$

$\mathsf{ENC}(k, m)$ cannot possibly be perfectly secret for $Y = 2$ messages as one can trivially distinguish the cipertexts of two equal and two distinct messages: only in the former case the ciphertexts will be identical (see also homework 2). □

5. (15 points)

Attacks

(a) Explain why encryption in CBC mode (shown below) is not a CCA secure encryption scheme (by giving an attack).

Solution: We construct an adversary $\mathcal{A}$ who breaks CCA-security. $\mathcal{A}$ chooses two equal length messages $m^{(0)} \neq m^{(1)}$ and gets back the challenge ciphertext $c^* = (IV, c_1, \ldots, c_\ell)$. Next, $\mathcal{A}$ queries the CCA-oracle on the ciphertext $c = (IV', c_1, \ldots, c_\ell) \neq c^*$, where $IV' \neq IV$. As a response, $\mathcal{A}$ gets the decryption $m = (m_1, \ldots, m_\ell)$ of c^* where $m_i = F_k^{-1}(c_i) \oplus c_{i-1}$ for $i \in \{1, \ldots, \ell\}$. Thus, $\mathcal{A}$ can decrypt c^* to $m^* = (m_1 \oplus IV' \oplus IV, m_2, \ldots, m_\ell)$. □

(b) Explain why CBC-MAC (as shown below) is not a secure MAC (by giving an attack) if the message space contains all messages whose length is a multiple of n bits.

Solution: We construct an adversary $\mathcal{A}$ who breaks the security of the CBC-MAC. First, $\mathcal{A}$ queries some arbitrary 1-block message $m_1 \in \{0,1\}^n$ to the MAC-oracle and gets back a tag $\tau = F_k(m_1)$. Then, $\mathcal{A}$ queries the oracle on the message τ and gets $\tau' = F_k(\tau)$. As a forgery, $\mathcal{A}$ outputs $((m_1, 0^n), \tau')$. To see that this is a valid forgery, note that

$$CBC - MAC_k(m_1, 0^n) = F_k(F_k(m_1) \oplus 0^n) = F_k(\tau) = \tau'.$$

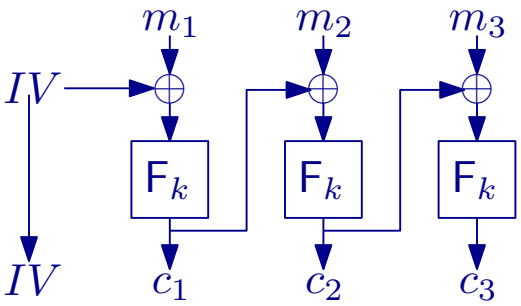
□

(c) Show that a two round Feistel network is not a pseudorandom permutation (no matter how the two round functions are).

Recall that one round of a Feistel network, instantiated with $f : \{0,1\}^n \to \{0,1\}^n$ maps $(L, R), L, R \in \{0,1\}^n$ to $(R, L \oplus f(R))$.

Solution: Let $((L_0, R_0), (L_2, R_2))$ be an input/output pair, i.e., $L_2 = L_0 \oplus f_1(R_0)$ and $R_2 = R_0 \oplus f_2(f_1(R_0) \oplus L_0)$. Then the output (L_2', R_2') of any (L_0', R_0) (with the first block being arbitrary, the second part equal to R_0) can be distinguished from random since $L_2' = L_0' \oplus f_1(R_0) = L_2 \oplus L_0 \oplus L_0'$. □

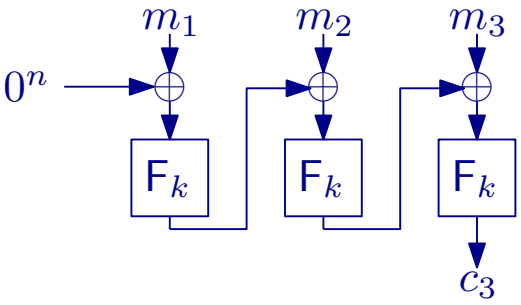
Cipher Block Chaining (CBC) Encryption



$c \leftarrow \mathsf{CBC\text{-}Enc}_k(m_1, \ldots, m_\ell)$

- random $IV \leftarrow \{0,1\}^n$
- $c_0 := IV$
  $c_i := \mathsf{F}_k(c_{i-1} \oplus m_i)$
- $c := \langle IV, c_1, \ldots, c_\ell \rangle$

CBC-MAC



$\tau \leftarrow \mathsf{CBC\text{-}MAC}_k(m_1, \ldots, m_\ell)$

- $c_0 := 0^n$
  $c_i := \mathsf{F}_k(c_{i-1} \oplus m_i)$
  $\tau := c_\ell$

One Round Feistel Network