← **Seat row‖num (eg, E12)** **First three letters of last name (eg, Rog)** →

ECS 127 Midterm — Cryptography — Spring 2016

Instructions: Please **fill in the boxes** (left **and** right) at the top margin of this page.

Throughout the exam, please write neatly. If we can't easily ready your writing, it's wrong.

Please remember the prohibition against sitting next to anyone you know. The full text of an academic misconduct warning is below.

I'm afraid I won't be able to get this exam back to you until next Monday. A little patience, please. Relax and good luck. —Phil Rogaway

---

LASTNAME, Firstname:

Signature:

Academic misconduct reminder: Please remember my rule about academic conduct (that cheating means getting an "F" in the course). The exam is closed book, closed notes, closed neighbor. Any device that can be powered off must be powered off for the duration of the exam. **You may not sit next to someone you know.** In that sentence, "next to" means to your left, right, directly behind, or diagonally behind; and "someone you know" means that they're a friend or someone you've worked with (in this class or some other) or someone with whom you have some sort of understanding concerning cheating. If you see anything inappropriate during an exam, please report it immediately by going to see me or a TA.

1. Consider the problem of achieving **privacy** in the **public-key** setting (the problem solved by *public-key encryption*). If Alice wants to send a private message M to Bob, then [ ] (Who?) generates a public key Pk and a corresponding secret key Sk.

   Alice computes a ciphertext C for plaintext M as a function of [ ] .

2. Alice uses a **substitution cipher** with an alphabet Σ that consists of **32** characters. How many possible keys are there? [ ] (Write a mathematical expression. Don't simplify).

3. The **key recovery** (kr) definition for a blockcipher $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ define an adversary A's advantage as $\mathbf{Adv}_E^{\mathrm{kr}}(A) = \Pr[K \xleftarrow{\$} \{0,1\}^k\colon A^{E_K(\cdot)} \to K]$. Let $E_K(X) = X$ (for all $K \in \{0,1\}^k$ and $X \in \{0,1\}^n$) and let A be a **best possible** adversary for attacking E in the kr-sense. Then $\mathbf{Adv}_E^{\mathrm{kr}}(A) =$ [ ] (Some formula).

4. Consider an **alternative key-recovery** (akr) definition for the blockcipher E having signature $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$; now A's advantage is defined by

   $$\mathbf{Adv}_E^{\mathrm{akr}}(A) = \Pr[K \xleftarrow{\$} \{0,1\}^k;\ K' \xleftarrow{\$} A^{E_K(\cdot)};\ X \xleftarrow{\$} \{0,1\}^n\colon E_K(X) = E_{K'}(X)]\ .$$

   (In English: the probability that A finds a key that explains a random domain point.) Let $E_K(X) = X$ (for all $K \in \{0,1\}^k$ and $X \in \{0,1\}^n$) and let A be a best possible adversary for attacking E in the akr-sense. Then $\mathbf{Adv}_E^{\mathrm{akr}}(A) =$ [ ] (Some formula).

5. The product of bytes

   $\texttt{10101111} \qquad (= \texttt{0xAF} = \mathtt{x}^7 + \mathtt{x}^5 + x^3 + x^2 + \mathtt{x} + 1)$

   and

   $\texttt{00000011} \qquad (= \texttt{0x03} = \mathtt{x} + 1)$

   in GF(2^8) is [ ] . Assume here that field elements are represented using the primitive polynomial $g(\mathtt{x}) = \mathtt{x}^8 + \mathtt{x}^4 + \mathtt{x}^3 + \mathtt{x} + 1$.

6. **Nonmalleability** is a property that an encryption scheme might or might not have. Informally describe what it **means** to say that an encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is nonmalleable. (Please don't use the word *malleability* in your description.)

   [ ]

7. Give a clear and self-contained statement of the **PRP/PRF switching lemma**.

8. Suppose you have a blockcipher $E\colon \{0,1\}^{40} \times \{0,1\}^{128} \to \{0,1\}^{128}$ with a 40-bit key and 128-bit blocksize. You construct from E a blockcipher $F\colon \{0,1\}^{80} \times \{0,1\}^{128} \to \{0,1\}^{128}$ by saying that

$$F_{K_1 K_2}(X) = E_{K_2}(E_{K_1}(X))$$

where $|K_1| = |K_2| = 40$.

Suppose an adversary A gets a single plaintext/ciphertext pair $(X, Y) = (X, F_{K_1 K_2}(X))$ for a random and secret key $Key = K_1 K_2$. Briefly describe a reasonably efficient attack that will recover a K_1 and K_2 such that $Y = F_{K_1 K_2}(X)$. By "reasonably efficient" I mean "far fewer than 2^{80} steps" (with one "step" is the amount of time to compute one $E_K(M)$ or one $E_K^{-1}(C)$ value).

How long will your attack take? (Number of *steps*). About

how much storage will your attack take? (In **bytes**).

Is the attack **practical**? (Explain).

What's the **name** of this kind of attack? .

9. We described a **PRG** (pseudorandom generator) as a map $G\colon \{0,1\}^n \to \{0,1\}^N$ with n and N positive integer constants, $n < N$. We measured the advantage an adversary A got in attacking a PRG G by

$$\mathbf{Adv}_G^{\mathrm{prg}}(A) = \Pr[A^G \to 1] - \Pr[A^{\$} \to 1]$$

where the first oracle responds to any oracle query by returning $G(x)$, for a freshly sampled $x \stackrel{\$}{\leftarrow} \{0,1\}^n$, and the second oracle responds to any query by returning R, for a freshly sampled $R \stackrel{\$}{\leftarrow} \{0,1\}^N$. (This is the *multi-query* version of PRG security.)

Later, Prof. Rogaway described the **asymptotic approach** to dealing with cryptography, using an **asymptotic PRG** as our example. Rogaway began by describing the **syntax** of a (length-doubling) PRG G and, afterward, he provided a definition for when an asymptotic PRG is **secure**. Follow the same course, describing the syntax and then the security definition for an asymptotically defined PRG. (You don't have to define terms like *probabilistic polynomial time* or a function being *negligible*, although you *should* know what these mean.)

10. Let $E\colon \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a blockcipher and let M_1M_2 be a message, $M_1, M_2 \in \{0,1\}^n$. Write a **formula** for the CBC MAC, F, of the message $M = M_1M_2$ under key K: $F_K(M_1M_2) =$ ______ . Draw a clear **picture** for the CBC MAC of this same message, $M = M_1M_2$, under key K.

11. Why did we develop the notion of **authenticated encryption**? That is, what **purpose** does this notion serve?

12. For each of the following claims, darken the **correct** answer. (Guess if you don't know.)

(a) **True** **False** There is a *finite field*, GF(256), on 256 points.

(b) **True** **False** The AES blockcipher (Rijndael) was the winner of a competition sponsored by NIST.

(c) **True** **False** The size of Func(n), the set of all functions from n bits to n bits, exceeds the size of Perm(n), the set of all permutations on n bits.

(d) **True** **False** There's a PRP-secure blockcipher $E\colon \mathcal{K}\times\{\mathtt{0},\mathtt{1}\}^n \to \{\mathtt{0},\mathtt{1}\}^n$ where the first bit of $E_K(X)$ doesn't depend on the last bit of K.

(e) **True** **False** There's a PRP-secure blockcipher $E\colon \mathcal{K}\times\{\mathtt{0},\mathtt{1}\}^n \to \{\mathtt{0},\mathtt{1}\}^n$ where the first bit of $E_K(X)$ doesn't depend on the last bit of X.

(f) **True** **False** In the context of symmetric encryption, *indistinguishability from random bits* (ind\$) is equivalent to *indistinguishability from the encryption of random bits* (ind1). (Equivalent in the sense that an encryption scheme Π is secure in one sense iff it is secure in the other.)

(g) **True** **False** If AES is a prp-secure blockcipher, then CBC encryption with AES and a random IV will achieve perfect privacy.

(h) **True** **False** If AES is a prp-secure blockcipher, then CBC encryption with AES and a random IV will achieve ind\$ security.

(i) **True** **False** If you start with a prp-secure blockcipher E, the CBC MAC over E will be a secure (unforgeable) MAC on the message space $\mathcal{M} = (\{\mathtt{0},\mathtt{1}\}^n)^+$.

(j) **True** **False** If we modified AES so that `SubBytes` mapped each byte $X \in \{\mathtt{0},\mathtt{1}\}^8$ to the constant `0x53` = `SubBytes`(X), the resulting construction would still be invertible (it would still be a blockcipher).

page 1	page 2	page 3	page 4	Σ