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

ECS 127 Quiz — Cryptography — Spring 2016

Instructions: Please **fill in the boxes** at the top margin of this page!

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

Relax and take a breath (it's always good to remember to breathe). Good luck.

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 you 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 problem). 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. In the **dating problem**, Alice holds a bit $a \in \{0, 1\}$ and Bob holds a bit $b \in \{0, 1\}$. We intend that $a = 1$ when Alice wants to go on a date with Bob, and $b = 1$ when Bob wants to go on a date with Alice. Alice and Bob want to compute [ ] (Boolean formula involving a and b) in such a way that each party learns only this. We don't care if Alice learns b when $a = 1$, or if Bob learns a when $b = 1$, because [ ].

3. In a single sentence, describe **Kerckhoff's principle**.

   [ ]

4. Alice uses a *substitution cipher* with an alphabet Σ that consists of the 95 printable ASCII characters. How many possible keys are there? [ ] (Write a mathematical expression. Don't simplify).

5. Consider Diaconis's algorithm for breaking a substitution cipher. It assumes we have values $M[x, y]$ describing the likelihood of each bigram (x, y), where $x, y \in \Sigma$ (and so $\sum_{x,y\in\Sigma} M[x, y] = 1$). The algorithm defines the *plausibility* of a candidate plaintext $M = x_1 \cdots x_m \in \Sigma^m$ as the number $\text{Pl}(M) =$ [ ]. (Given a ciphertext $C = c_1 \cdots c_m$, the algorithm then attempts to find a permutation $f \colon \Sigma \to \Sigma$ that maximizes $\text{Pl}(f(c_1) \cdots f(c_m))$).

6. Compute the following number:

$$\Pr[X \xleftarrow{\$} \{0,1\}^{128};\ Y \xleftarrow{\$} \{0,1\}^{128} :\quad X = Y] = \boxed{}\ .$$

7. In a picture or in English text, describe some high-level aspect about the algorithm **A5/1** (a stream cipher used in cell phones).

8. We described a (classical) PRG (pseudorandom generator) as a map $G\colon \{0,1\}^n \to \{0,1\}^N$ with $n < N$. We then measured the efficacy of an adversary A attacking such a PRG G with a real number $\mathbf{Adv}_G(A)$, which Prof. Rogaway defined as

   $\mathbf{Adv}_G(A) =$

   (Give some mathematical expression)

   where

   (Explain any terms you use in the mathematical expression)

9. How many 10-character passwords are there of the form:
   nine of the characters are **lower-case English letters**, while **one** of the characters is an **upper-case English letter**. . Write a simple mathematical expression. Do not simplify.

10. **True** **False** (← Darken the correct answer)
    There is a *finite field*, GF(100), on 100 points. Now **explain**:

11. Draw a picture showing **two rounds** of a **Feistel network** (the construction used in DES). Label the input block $M = M_1 M_2$ with M_1 and M_2, where $|M_1| = |M_2|$, and call the key-dependent round functions F_1 and F_2.

12. **True** **False** DES would remain invertible—it would still be a blockcipher—even if each S-box (the eight functions $S_1, \ldots, S_8 \colon \{0,1\}^6 \to \{0,1\}^4$) were replaced by the function $S(x) = x^2 \bmod 16$. (The 6-bit x is treated as a number, then the numeric result is regarded as a 4-bit string.) Now **explain**:

13. **True** **False** Dog day didn't work out so well, as there was only one dog, and he wouldn't stop barking. *Extra credit: name the dog(s), or write a limerick about dog day.*

You leave this blank, we'll fill it in ⟶

page 1	page 2	page 3	Σ