ECS 127: Cryptography — Handout M
UC Davis — Phillip Rogaway — Feb 15, 2019

ECS 127 Midterm — Cryptography — Winter 2019

Instructions: Your exam has this cover page and then four pages, numbered 1 to 4.

Please write neatly. If we can't easily read your writing, it is wrong. Problems might not be weighted equally.

Do not sit next to a partner or friend. The full text of an academic misconduct warning is below.

Name:

Student ID:

Signature:

Seat, as in D15:

Academic misconduct reminder: Any device that can be powered off must be. 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. If you see anything inappropriate during an exam, please report it right away. Please remember my policy about academic conduct, that any incident of academic misconduct will result in getting an "F" in the course.

1. The **key-recovery** (kr) security for a blockcipher $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ defined an adversary A's advantage as

$$\mathbf{Adv}_E^{\mathrm{kr}}(A) = \Pr[K \twoheadleftarrow \{0,1\}^k;\ K' \leftarrow A^{E_K(\cdot)}\colon\ K = K'] \,.$$

Let $E_K(X)=X$ and let A be a best adversary for attacking E in the kr-sense. Then $\mathbf{Adv}_E^{\mathrm{kr}}(A) = \boxed{}$.

2. Prof. Rogaway claimed that several aspects of DES algorithm embodied *political* choices. The most important political choice within the DES algorithm was, in Rogaway's view,

$\boxed{}$ ←something about keys

3. How many functions are there from 10 bits to 10 bits? $\boxed{}$

4. Together, Alice and Bob roll a fair die two times, getting a first random number in [1..6] and then a second random number in [1..6]. What's the *longest* bit string (that is, how many bits) that Alice can subsequently communicate to Bob with perfect privacy? Show how you computed the number.

5. Suppose that AES : $\{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$ is a secure PRP. Define a secure AES-based PRG $G : \{0,1\}^{128} \to \{0,1\}^{512}$. Keep your construction as simple and efficient as you can

6. Formally define the **syntax** of an n-bit PRP E.

Now define the **prp-advantage** $\mathbf{Adv}_E^{\mathrm{prp}}(A)$ of an adversary A attacking E.

7. Give a qualitative but clear description of the **PRP/PRF switching lemma**.

8. On PS #1 you were asked to construct a random cycle $C \twoheadleftarrow \mathrm{Cycl}(n)$ from a random permutation $\pi \twoheadleftarrow \mathrm{Perm}(n)$ and its inverse π^{-1}. Give a formula for such a $C(X)$ in terms of π, π^{-1}, Inc, and X. Here $\mathrm{Inc}\colon \{0,1\}^n \to \{0,1\}^n$ is an arbitrary cycle.

9. Define a blockcipher DBL: $\{0,1\}^{128} \times \{0,1\}^{256} \to \{0,1\}^{256}$ by

$$\mathrm{DBL}_K(X_1 X_2) = \mathrm{AES}_K(X_1) \parallel \mathrm{AES}_K(X_2)\ .$$

Show that DBL is an insecure PRP by exhibiting an adversary A^E (the superscript is the oracle) that gets good prp-advantage against DBL. There's an attack that employs only one query.

10. Suppose you'd like to break a message $M \in \{0,1\}^{100}$ into into two shares, S_1 and S_2, so that with *both* shares someone can recover M, but with only one share, they have no information about M beyond it's length. Then here's a simple and concrete way to select S_1 and S_2:

11. CBC-encryption of a long message M is often much slower than CTR-encryption of it. Why?

12. For each of the following claims, darken the left box if the statement is false and the right box if the statement is true. This problem will count more than others.

(a) F □ □ T One of the solutions to the "dating problem" described in the first problem-set solution involved the opening of eyes.

(b) F □ □ T A blockcipher $E\colon \{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$ can be secure as a PRP even if $E_K(X)$ doesn't depend on half the bits K.

(c) F □ □ T A blockcipher $E\colon \{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$ can be secure as a PRP even if $E_K(K) = K$.

(d) F □ □ T In the context of symmetric encryption, ind-security and ind\$-security turn out to be equivalent.

(e) F □ □ T The number of permutations on $\{0,1\}^{128}$ is 128!, the number of ways to reorder the bits $x_1, \ldots, x_{128}$ of a string $x_1 \cdots x_{128}$

(f) F □ □ T If E is an ideal PRP (denoted P in one proof we did in class), then CTR encryption with it will achieve perfect privacy.

(g) F □ □ T If its key space is larger than its message space, an encryption scheme will achieve perfect privacy.

(h) F □ □ T DES would remain invertible even if its S-boxes were arbitrarily changed.

(i) F □ □ T CTR encryption is nonmalleable.

(j) F □ □ T While the second byte of RC4 is slightly biased, this does not impact its security as a PRG.