ECS 127 Midterm Solutions — Cryptography — Winter 2019

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

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

   Let $E_K(X) = X$ and let A be a best adversary for attacking E in the kr-sense. Then $\mathbf{Adv}^{\mathrm{kr}}_E(A) = \boxed{2^{-k}}$.

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, $\boxed{\text{the short length of keys (only 56 bits)}}$ ←something about keys

3. How many functions are there from 10 bits to 10 bits? $\boxed{2^{10 \cdot 2^{10}}}$

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.

   $\boxed{5 = \lfloor \log_2(36) \rfloor \text{ bits}}$

5. Suppose that $\mathrm{AES} : \{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$ 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

   algorithm $G(K)$ // $K \in \{0,1\}^{128}$
   return $\mathrm{AES}_K(0) \,\|\, \mathrm{AES}_K(1) \,\|\, \mathrm{AES}_K(2) \,\|\, \mathrm{AES}_K(3)$

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

   A PRP is a function $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ such that for all $K \in \mathcal{K}$, the function $E(K,\cdot)$ (also written $E_K(\cdot)$) is a permutation (on $\{0,1\}^n$).

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

   $\mathbf{Adv}^{\mathrm{prp}}_E = \Pr[K \twoheadleftarrow \mathcal{K} : A^{E_K(\cdot)} \Rightarrow 1] - \Pr[\pi \twoheadleftarrow \mathrm{Perm}(n) : A^{\pi(\cdot)} \Rightarrow 1]$

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

   The PRF and PRP measures of security for an n-bit blockcipher are close as long as the number of queries remains small. It needs to stay well under $2^{n/2}$.

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.

   $C(X) = \pi^{-1}(\mathrm{Inc}(\pi(X)))$ or $C(X) = \pi(\mathrm{Inc}(\pi^{-1}(X)))$.

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

$$\mathrm{DBL}_K(X_1X_2) = \mathrm{AES}_K(X_1) \parallel \mathrm{AES}_K(X_2)\ .$$

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.

Adversary A^E
Query 0^{256} to the oracle and receive C Parse C as C_1C_2 where $\lvert C_1\rvert = \lvert C_2\rvert$ if $C_1 = C_2$ then return 1 else return 0

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:

$S_1 \twoheadleftarrow \{0,1\}^{100}$ $S_2 \leftarrow M \oplus S_1$ (Of course you will recover by $M \leftarrow S_1 \oplus S_2$)

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

CBC is inherently sequential (non-parallelizable): it needs to encipher one message block at a time because the encryption of a block depends on the previous ciphertext block. On the other hand, CTR mode is fully parallelizable.

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) **True** One of the solutions to the "dating problem" described in the first problem-set solution involved the opening of eyes.

    (b) **True** 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) **True** 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) **False** In the context of symmetric encryption, ind-security and ind$-security turn out to be equivalent.

    (e) **False** 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) **False** 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) **False** If its key space is larger than its message space, an encryption scheme will achieve perfect privacy.

(h) **True** DES would remain invertible even if its S-boxes were arbitrarily changed.

(i) **False** CTR encryption is nonmalleable.

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