ECS 127: Cryptography MT.1
UC Davis — Phillip Rogaway May 10, 2024

ECS 127 — Midterm 1 — Spring 2024

Instructions: The exam has this cover page then four more pages. Fill in the boxes below and write your name lightly on the back of each page. Other than that, please write on the front side of pages only. Make sure all your writing is neat and clear.

A reminder that you may not sit next to any partner or friend (meaning: immediately to the left, right, rear, or diagonal).

Occasionally I've included a hint in tiny letters. You can ignore these if you prefer; they're never necessary to answer the question.

Anticipated grading (subject to change): 10 points each for problems 1–9; 40 points for problem 10 (with 5 points for each correct response after the eighth).

Name:

Student ID:

Signature:

Seat (eg, D15):

1. For *Diffie-Hellman secret-key exchange* we fixed a large prime number p and a generator g for $\mathbb{Z}_p^*$ (the multiplicative group of integers mod p). What follows is then done in that group:

   Alice selects $a \twoheadleftarrow \{1, 2, \ldots, p-1\}$ and computes $A = g^a$. She sends A to Bob.

   Bob selects $b \twoheadleftarrow \{1, 2, \ldots, p-1\}$ and computes $B = g^b$. He sends B to Alice.

   The parties will share $K = g^{ab}$, which Alice learns by computing □

   and Bob learns by computing □ .

2. Suppose Alice encrypts a message $M \in \{0, 1, \ldots, 99\}$ to a ciphertext $C = M + K \pmod{100}$ using a uniformly random key $K \in \{0, 1, \ldots, 127\}$. This is the only message ever sent using the key K.

   The method □ ← **does** or **doesn't**

   achieve perfect privacy.

   For example, $\Pr[C = 0 \mid M = 0] =$ □

   and $\Pr[C = 0 \mid M = 42] =$ □ .

3. In our class, $R \twoheadleftarrow S$ means □

   while $\mathcal{A}(R) \Rightarrow 1$ means □ .

   $\mathcal{A}$ is an adversary and R is a string.

4. Recall the DES algorithm, DES: $\{0,1\}^{56} \times \{0,1\}^{64} \to \{0,1\}^{64}$. Name two of its **undesirable** characteristics and, for each, explain *why* the attribute is undesirable.

   a.

   b.

5. Define a blockcipher $E\colon \{0,1\}^{256} \times \{0,1\}^{128} \to \{0,1\}^{128}$ that does a great job of concealing the key—no adversary can do well at guessing it—yet E is, nonetheless, totally insecure in the ind-sense.

   $$E_K(X) =$$

6. The number of permutations on $\{0,1\}^{128}$ is $|\mathrm{Perm}(128)| = \boxed{}$.

   The number of cycles on $\{0,1\}^{128}$ is $|\mathrm{Cycl}(128)| = \boxed{}$.

   Recall from a problem set that a permutation $C \in \mathrm{Perm}(n)$ is a cycle if $0^n,\ C(0^n),\ C(C(0^n)),\ \ldots$ is all the points of $\{0,1\}^n$.

7. You are working in GF(2^8), the finite field with 2^8 points, representing points using the irreducible polynomial $g(\mathtt{x}) = \mathtt{x}^8 + \mathtt{x}^4 + \mathtt{x}^3 + \mathtt{x} + 1$.

   What point will you get if you square $s = \mathtt{00010000} = \mathtt{x}^4$? Write it in binary.

8. Let $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a blockcipher. Suppose you design a PRG $G\colon \{0,1\}^k \to \{0,1\}^\infty$ that depends on E. You want to prove that

   if E is a secure PRP then G is a secure PRG.

   To do this you would need to provide a *reduction*. The reduction will start with an

   adversary A that attacks □ ←scheme

   and will transform it into an adversary B that attacks □ ←scheme

   You'll then prove that if □ ←number, advantage

   is large then □ ←number, advantage is large, too.

9. In a homework solution we applied Shamir secret-sharing byte-wise to a message $M = M_1 \cdots M_m$, each $M_i \in \{0,1\}^8$. In what way was that approach better than just applying Shamir's scheme directly to M?

   Sketch an alternative method to secret-share $M = M_1 \cdots M_m$ that requires the dealer to only use Shamir secret-sharing on a 32-byte string. The dealer ...

10. **Mark the box** if the statement is **True**. Leave it empty if the statement is False.

1) □ In an ind-secure symmetric encryption scheme, an encryption of `Hello` and an encryption of `mom` might be easy for an adversary to tell apart.

2) □ In an ind-secure symmetric encryption scheme, ciphertexts might always start with the word `ciphertext`.

3) □ Parties A, B, and C securely compute their average salary s. Then A will necessarily learn, in addition to s, the average salary s_{BC} of parties B and C.

4) □ ind-security implies ind$-security (indistinguishability from random bits).

5) □ Perfect privacy, discussed near the beginning of our class, is the strongest possible notion of encryption-scheme security.

6) □ If an encryption scheme's key space is smaller than its message space, it can't achieve perfect privacy.

7) □ ChaCha20 has been proven secure: we know that reasonable adversaries have small prp-advantage in attacking it.

8) □ If an asymptotically secure PRG exists than P≠NP.

9) □ DES would remain invertible even if each S-box were replaced by the function $S(x_1x_2x_3x_4x_5x_6) = (x_1 + 2x_2 + 3x_3 + 5x_4 + 7x_5 + 11x_6) \bmod 16$ (treated as a 4-bit string).

10) □ On a homework we saw that, experimentally, RC4's output *is* distinguishable from truly random bits.

11) □ If $E : \{0,1\}^{256} \times \{0,1\}^{256} \to \{0,1\}^{256}$ has good security as a PRP then it has good security as a PRF.

12) □ CBC-mode encryption with a counter IV is ind-secure if its underlying blockcipher is prp-secure.

13) □ Adversary $\mathcal{A}$ queries a random function $f \twoheadleftarrow \{0,1\}^{128}$ at 2^{80} different points. The answers returned are probably all distinct (different from one another).

14) □ An *oracle* $\mathcal{O}$ computes some deterministic function f of the query X it is asked; it immediately returns $f(X)$.

15) □ The following exemplifies a *hybrid argument*: Let $\Pr[A^{\mathcal{O}_1} \Rightarrow 1] - \Pr[A^{\mathcal{O}_0} \Rightarrow 1] = \delta$. Then for any oracle $\mathcal{O}$ you devise, either $\Pr[A^{\mathcal{O}_1} \Rightarrow 1] - \Pr[A^{\mathcal{O}} \Rightarrow 1] \geq \delta/2$ or $\Pr[A^{\mathcal{O}} \Rightarrow 1] - \Pr[A^{\mathcal{O}_0} \Rightarrow 1] \geq \delta/2$.

16) □ CTR mode encryption and CBC mode encryption are both *malleable*.