ECS 189A Final — Cryptography — Spring 2011

Hints for success: Good luck on the exam. I don't think it's all that hard (I do believe I could answer everything!). Please read the questions carefully, and think before you answer. make your response **legible**, **logical**, and **succinct**. Nothing here needs more than 2–3 sentences.

Final grades should be ready around Tuesday. You should be able to retrieve them from my.ucdavis.edu in the usual way.

Hope to see some of you next year. (If you're brave enough to take another Rogaway class, I'm scheduled to teach **ecs188** (Ethics) in Fall, and **ecs120** (Theory of Computation) and **ecs227** (Cryptography) in Spring.)

Phillip Rogaway

Name:

Signature:

On problem	you got	out of
1		
2		
3		
4		
5		
6		
7		
Σ		

1 Ciphers

1. Draw a picture showing **two rounds** of a **Feistel network**. Denote the round functions for the two rounds as $F^1,\ F^2\colon\ \mathcal{K} \times \{\texttt{0},\texttt{1}\}^n \to \{\texttt{0},\texttt{1}\}^n$ where $\mathcal{K}$ is the key space.

2. **True** or **False**, and briefly **explain:** DES would remain invertible—it would still be a blockcipher—even if its S-boxes were arbitrarily changed (the number of input and output bits remaining the same).

3. **True** or **False**, and briefly **explain:** AES would remain invertible—it would still be a blockcipher—even if its S-boxes were arbitrarily changed (the number of input and output bits remaining the same).

4. In a couple of sentences, give me a quick synopsis of **Trivium**.

5. Let $E\colon \mathcal{K}\times\{\mathtt{0},\mathtt{1}\}^n \to \{\mathtt{0},\mathtt{1}\}^n$ be a blockcipher and let A be an adversary. Carefully define $\mathbf{Adv}_E^{\mathrm{prp}}(A)$, the advantage that an adversary A gets in attacking the blockcipher E. Use notation following that used in class. Then, in a paragraph, carefully **explain** what the notation means.

   $\mathbf{Adv}_E^{\mathrm{prp}}(A) \ =$

   Explanation:

6. **True** or **false**, and **explain**: For a blockcipher like $E = \mathrm{AES}$, we *know* that $\mathbf{Adv}_E^{\mathrm{prp}}(A)$ is "small" for any reasonable adversary A—cryptographers have proven good upper bounds.

2 Attacks

1. Suppose you have a blockcipher with a 40-bit key: $E\colon \{\mathtt{0},\mathtt{1}\}^{40} \times \{\mathtt{0},\mathtt{1}\}^{128} \to \{\mathtt{0},\mathtt{1}\}^{128}$. Construct from E the blockcipher $F\colon \{\mathtt{0},\mathtt{1}\}^{80} \times \{\mathtt{0},\mathtt{1}\}^{128} \to \{\mathtt{0},\mathtt{1}\}^{128}$ by saying that

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

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

An adversary A has a single plaintext/ciphertext pair $(X, Y) = (X, F_{K_1 K_2}(X))$ for a random and secret key $K = K_1 K_2$. **Describe a reasonably efficient attack** that will, most of the time, recover (K_1, K_2). By "reasonably efficient" I mean *far fewer than* 2^{80} *times steps* (with one time step being the amount of time to compute one E_K value). **What is this attack called?**

2. Don proposes a 128-bit blockcipher E that works like this. It has 16 S-boxes, $S_1, \ldots, S_{16}$, each a permutation mapping 8-bits to 8-bits. It uses a 128-bit key that gets mapped into 32 subkeys, $K_1, \ldots, K_{32}$, each 128 bits. To encrypt an input block X, for each of 32 rounds i:

    1. Replace X by $X \oplus K_i$;
    2. Replace the j-th byte of X, $X[j]$, by $S_j[X[j]]$ (for each $1 \le j \le 16$);
    3. Circularly rotate X by one byte position to the left.

When the above is complete, the ciphertext block is the final value of X.

What queries should you ask—no more than a few hundred—to allow you to completely and efficiently break this cipher?

3 Math

1. How many **permutations** are there on the space of 128-bit strings?

2. An adversary A asks an n-bit to n-bit (uniform) random **permutation** π for the values of $\pi(x_1), \ldots, \pi(x_q)$ for distinct values $x_1, \ldots, x_q$. Then A outputs a pair (x, y). The probability that this is a good *forgery* (that is, that x is none of $x_1, \ldots, x_q$ and yet $\pi(x) = y$) is *at most* $\boxed{\qquad\qquad}$. (Give a tight value.)

3. The product of bytes

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

   and

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

   in $\mathrm{GF}(2^8)$ is $\boxed{\qquad\qquad}$. Assume here that field elements are represented using the primitive polynomial

   $g(\mathtt{x}) = \mathtt{x}^8 + \mathtt{x}^4 + \mathtt{x}^3 + \mathtt{x} + 1.$

   and show your work below.

4. If $n = pq$ is the product of distinct primes, $|\mathbb{Z}_n^*| = \phi(n) = \boxed{\qquad\qquad}$.

5. For large n, there are roughly this many primes less than n: $\boxed{\qquad\qquad}$.

4 Encryption

1. Alice would like to private send a single bit $M \in \{0,1\}$ to Bob. An adversary should get *no* information about M. Alice and Bob share a uniformly random key $K \in \{0,1,2\}$. How can Alice securely send her bit to Bob? Give a formula for the ciphertext C:

   $$C = \mathcal{E}_K(M) =$$

2. Let $\mathcal{E}$ be the encryption algorithm of a symmetric encryption scheme. Recall that we define the ind-security of $\mathcal{E}$ to be

   $$\mathbf{Adv}^{\mathrm{ind}}_{\mathcal{E}}(A) = \Pr[A^{\mathcal{E}_K(\cdot)} \Rightarrow 1] - \Pr[A^{\mathcal{E}_K(\$^{|\cdot|})} \Rightarrow 1]$$

   A secure blockcipher E (secure in the prp-sense) will

   always / **sometimes** / **never**

   (*circle one*) be a secure encryption method $\mathcal{E}$ (in the ind-sense).

3. The **decisional Diffie-Hellman assumption** is the assumption that:[1]

4. Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a public-key encryption scheme. Can it be IND-secure[2] if the encryption of a plaintext P leaks the identity of the key pk with which it is encrypted? **Yes** or **No** (choose one).

5. Fix a cyclic $\mathbb{G}$ of order p (that is, $|\mathbb{G}| = p$) generated by $g \in \mathbb{G}$ (that is, $\langle g \rangle = \mathbb{G}$). Alice has a public key of $A = g^a$ and a secret key a. If Bob wants to encrypt a message $m \in \mathbb{G}$ to Alice using **ElGamal encryption**, he should choose a random $b \in \boxed{}$ and send Alice a ciphertext $\mathcal{E}_A(m) = \boxed{}$.

[1] The correct answer is that *something* is computationally indistinguishable from *something*.

[2] I refer here to the definition given in class—that $\mathbf{Adv}^{\mathrm{IND}}_{\Pi}(A) = \Pr[A^{\mathcal{E}_{pk}(\cdot)}(pk) \Rightarrow 1] - \Pr[A^{\mathcal{E}_{pk}(\$^{|\cdot|})}(pk) \Rightarrow 1]$ is "small" for all "reasonable" A.

5 Message authentication and digital signatures

1. Draw a picture that illustrates the **CBC MAC** of a message $P = P_1P_2P_3$ where $|P_i| = n$. The underlying blockcipher is $E\colon \mathcal{K} \times \{\mathtt{0},\mathtt{1}\}^n \to \{\mathtt{0},\mathtt{1}\}^n$. Make sure it is clear from your picture what string is the MAC, and how it depends on E, K, and P.

2. We have seen that the CBC MAC is not secure across strings of varying lengths. Describe a simple way to "fix" it (changing the CBC MAC as little as possible) so that it will (under reasonable assumptions) be secure across strings of varying lengths.

3. Consider signing with "raw" RSA: the signature of a message $m \in \mathbb{Z}_n^*$ is $m^d \pmod{n}$ (where $e \in \mathbb{Z}_{\phi(n)}^*$ and $ed \equiv 1 \pmod{\phi(n)}$). **True** or **False**, and briefly **explain**: we showed that this signature scheme is correct (it is existentially unforgeable under an adaptive chosen-message attack) if RSA is a secure *trapdoor permutation.*

6 Hash functions, authenticated encryption, and esoterica

1. Briefly describe a **theorem** we covered that helps justify the use of the **Merkle-Damgård** construction in schemes like SHA1.

2. Describe a correct algorithm or approach we discussed for making an **authenticated encryption scheme**—a symmetric encryption scheme that achieves both privacy and authenticity.

3. Describe what is a 1-out-of-2 **oblivious transfer**.

4. Recall that in the problem **2-party Secure Function Evaluation**, Alice, has a private input of $a_1 a_2 \cdots a_n$ (each a_i a bit) and Bob has a private input of string $b_1 b_2 \cdots b_m$ (each b_j a bit). Bob should learn $C(a_1, a_2, \cdots, a_n, b_1, \ldots, b_m)$, and Alice should learn nothing, where C is some fixed a boolean circuit. In solving this problem, we used 1-out-of-2 oblivious transfer. Please explain how.

7 A reduction

We argued in class that every **pseudorandom function** is also a good **message authentication code** (MAC). Formalize and prove this result.