ECS 127 Midterm Solutions — Spring 2016

1. Consider the problem of achieving **privacy** in the **public-key** setting (the problem solved by *public-key encryption*). If Alice wants to send a private message M to Bob, then $\boxed{\text{Bob}}$ generates a public key Pk and a corresponding secret key Sk. Alice computes a ciphertext C for plaintext M as a function of $\boxed{M \text{ and } Pk}$.

2. Alice uses a **substitution cipher** with an alphabet Σ that consists of **32** characters. How many possible keys are there? $\boxed{32!}$.

3. The **key recovery** (kr) definition for a blockcipher $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ defines an adversary A's advantage as $\mathbf{Adv}^{\text{kr}}_E(A) = \Pr[K \stackrel{\$}{\leftarrow} \{0,1\}^k\colon A^{E_K(\cdot)} \to K]$. Let $E_K(X) = X$ (for all $K \in \{0,1\}^k$ and $X \in \{0,1\}^n$) and let A be a **best possible** adversary for attacking E in the kr-sense. Then $\mathbf{Adv}^{\text{kr}}_E(A) = \boxed{1/2^k}$.

4. Consider an **alternative key-recovery** (akr) definition for the blockcipher E having signature $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$; now A's advantage is defined by

$$\mathbf{Adv}^{\text{akr}}_E(A) = \Pr[K \stackrel{\$}{\leftarrow} \{0,1\}^k;\ K' \stackrel{\$}{\leftarrow} A^{E_K(\cdot)};\ X \stackrel{\$}{\leftarrow} \{0,1\}^n\colon E_K(X) = E_{K'}(X)]\ .$$

(In English: the probability that A finds a key that explains a random domain point.) Let $E_K(X) = X$ (for all $K \in \{0,1\}^k$ and $X \in \{0,1\}^n$) and let A be a best possible adversary for attacking E in the akr-sense. Then $\mathbf{Adv}^{\text{akr}}_E(A) = \boxed{1}$.

5. The product of bytes

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

   and

   $\texttt{00000011} \qquad (= \texttt{0x03} = \texttt{x} + 1)$

   in GF(2^8) is $\boxed{\texttt{11101010}}$. Assume here that field elements are represented using the primitive polynomial $g(\texttt{x}) = \texttt{x}^8 + \texttt{x}^4 + \texttt{x}^3 + \texttt{x} + 1$.. [[*I computed this as* $10101111 \oplus 01011110 \oplus 00011011$]]

6. **Nonmalleability** is a property that an encryption scheme might or might not have. Informally describe what it **means** to say that an encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is nonmalleable.

   It means that an adversary, given a ciphertext C, can't create a ciphertext C' different from C whose underlying plaintext M' is meaningfully related to the plaintext M underlying C.

7. Give a clear and self-contained statement of the **PRP/PRF switching lemma**.

   Let E be a blockcipher with an n-bit blocksize. Then, for any adversary A asking at most q queries, $|\mathbf{Adv}^{\text{prp}}_E(A) - \mathbf{Adv}^{\text{prf}}_E(A)| \le q^2/2^{n+1}$.
   Alternative: let A be an adversary asking at most q queries and let $n \ge 1$ be a number. Then $|Pr[\pi \stackrel{\$}{\leftarrow} \text{Perm}(n)\colon A^\pi \to 1] - Pr[\rho \stackrel{\$}{\leftarrow} \text{Func}(n)\colon A^\rho \to 1]| \le q^2/2^{n+1}$.

8. Suppose you have a blockcipher $E\colon \{0,1\}^{40} \times \{0,1\}^{128} \to \{0,1\}^{128}$ with a 40-bit key and 128-bit blocksize. You construct from E a blockcipher $F\colon \{0,1\}^{80} \times \{0,1\}^{128} \to \{0,1\}^{128}$ by saying that

$$F_{K_1K_2}(X) = E_{K_2}(E_{K_1}(X))$$

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

Suppose an adversary A gets a single plaintext/ciphertext pair $(X, Y) = (X, F_{K_1K_2}(X))$ for a random and secret key $Key = K_1K_2$. Briefly describe a reasonably efficient attack that will recover a K_1 and K_2 such that $Y = F_{K_1K_2}(X)$. By "reasonably efficient" I mean "far fewer than 2^{80} steps" (with one "step" is the amount of time to compute one $E_K(M)$ or one $E_K^{-1}(C)$ value).

For each key $K_1 \in \{0,1\}^{40}$, compute $E(K_1, X)$. Save these values, associating each to its K_1 value. Now, for each key $K_2 \in \{0,1\}^{40}$, test if $E^{-1}(K_2, Y)$ is among the saved values. As soon as you find one, answer with the corresponding (K_1, K_2).

How long will your attack take? 2^{41} steps .

About **how much storage** will your attack take? About 2^{43} bytes.

Is the attack **practical**? It's practical, although you might need to go buy a bigger disk drive.

What's the **name** of this kind of attack? meet-in-the-middle

9. We described a **PRG** (pseudorandom generator) as a map $G\colon \{0,1\}^n \to \{0,1\}^N$ with n and N positive integer constants, $n < N$. We measured the advantage an adversary A got in attacking a PRG G by

$$\mathbf{Adv}_G^{\mathrm{prg}}(A) = \Pr[A^G \to 1] - \Pr[A^\$ \to 1]$$

where the first oracle responds to any oracle query by returning $G(x)$, for a freshly sampled $x \xleftarrow{\$} \{0,1\}^n$, and the second oracle responds to any query by returning R, for a freshly sampled $R \xleftarrow{\$} \{0,1\}^N$. (This is the *multi-query* version of PRG security.)

Later, Prof. Rogaway described the **asymptotic approach** to dealing with cryptography, using an **asymptotic PRG** as our example. Rogaway began by describing the **syntax** of a (length-doubling) PRG G and, afterward, he provided a definition for when an asymptotic PRG is **secure**. Follow the same course, describing the syntax and then the security definition for an asymptotically defined PRG.

An (asymptotic, length-doubling) PRG is a map $G\colon \{0,1\}^* \to \{0,1\}^*$ where $|G(x)| = 2|x|$ for all x. Let $\mathbf{Adv}_G^{\mathrm{prg}}(A, k) = \Pr[x \xleftarrow{\$} \{0,1\}^k\colon A(G(x)) \to 1] - \Pr[y \xleftarrow{\$} \{0,1\}^{2k}\colon A(y) \to 1]$. Then G is **secure** if for all PPT algorithms A, $\mathbf{Adv}_G^{\mathrm{prg}}(A, k)$ is negligible. (Alternatively, we can give A an oracle that either samples $G(x)$ values, for a random k-bit x, or else random $2k$-bit strings.)

10. Let $E\colon \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a blockcipher and let M_1M_2 be a message, $M_1, M_2 \in \{0,1\}^n$. Write a **formula** for the CBC MAC, F, of the message $M = M_1M_2$ under key K: $F_K(M_1M_2) = \boxed{E_K(E_K(M_1) \oplus M_2)}$. Draw a clear **picture** for the CBC MAC of this same message, $M = M_1M_2$, under key K. Too lazy to draw it — you know what it looks like!

11. Why did we develop the notion of **authenticated encryption**? That is, what **purpose** does this notion serve?

We wanted a **stronger** notion of encryption—one that would guarantee CCA security, nonmalleability, and authenticity. We wanted something that would be easier to correctly use / less likely to misuse.

12. For each of the following claims, darken the **correct** answer. (Guess if you don't know.)

    (a) **True** There is a *finite field*, GF(256), on 256 points.

    (b) **True** The AES blockcipher (Rijndael) was the winner of a competition sponsored by NIST.

    (c) **True** The size of Func(n), the set of all functions from n bits to n bits, exceeds the size of Perm(n), the set of all permutations on n bits.

    (d) **True** There's a PRP-secure blockcipher $E: \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ where the first bit of $E_K(X)$ doesn't depend on the last bit of K.

    (e) **False** There's a PRP-secure blockcipher $E: \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ where the first bit of $E_K(X)$ doesn't depend on the last bit of X.

    (f) **False** In the context of symmetric encryption, *indistinguishability from random bits* (ind$) is equivalent to *indistinguishability from the encryption of random bits* (ind1).

    (g) **False** If AES is a prp-secure blockcipher, then CBC encryption with AES and a random IV will achieve perfect privacy.

    (h) **True** If AES is a prp-secure blockcipher, then CBC encryption with AES and a random IV will achieve ind$ security.

    (i) **False** If you start with a prp-secure blockcipher E, the CBC MAC over E will be a secure (unforgeable) MAC on the message space $\mathcal{M} = (\{0,1\}^n)^+$.

    (j) **False** If we modified AES so that `SubBytes` mapped each byte $X \in \{0,1\}^8$ to the constant `0x53` = `SubBytes`(X), the resulting construction would still be invertible (it would still be a blockcipher).