Computer Sciences, UW–Madison
CS 838: Applied Cryptography
Problem Set 1

Spring 2012
Instructor: Thomas Ristenpart
February 21, 2012

Problem Set 1

Due: Tuesday, March 6, 2012, in class.

You may discuss the problem set with classmates, but must write up problem solutions individually. If you discuss a problem with someone, indicate it clearly at the beginning of the problem's solution. I will check that you turned it in and attempted the problems.

Problem 1. Identify an Internet Request For Comments (RFC), IETF, X.509, or other standard that uses cryptography. Provide a short summary of the standard including its application domain and deployment examples (if it has been deployed). List what cryptographic primitives it uses and what security features the primitives are meant to provide. Try to answer the following questions: Do you think the standard uses the right primitives for its intended application? Can you think of security issues the standard overlooks (e.g., implementation hurdles or threats not covered by the standard)? What attacks might be possible against potential (or existing) implementations of the standard?

Problem 2. Let K be a 56-bit DES key, let L be a 64-bit string, and let M be a 64-bit plaintext. Let

$$\mathsf{DESY}(K \,\|\, L, M) \;=\; \mathsf{DES}(K, L \oplus M)$$
$$\mathsf{DESW}(K \,\|\, L, M) \;=\; L \oplus \mathsf{DES}(K, M)\ .$$

This defines block ciphers $\mathsf{DESY}, \mathsf{DESW}$: $\{0,1\}^{120} \times \{0,1\}^{64} \to \{0,1\}^{64}$.

Present the best possible key-recovery attacks that you can on these block ciphers. Your attacks should use very few input-output examples, not more than three. State the running time of your attacks.

Problem 3. Define the family of functions F: $\{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$ by $F(K, M) = \mathsf{AES}(M, K)$. Assuming AES is a secure PRF, is F a secure PRF? If so, explain why. If not, present the best attack (with analysis) that you can.

Problem 4. Let F: $\{0,1\}^k \times \{0,1\}^l \to \{0,1\}^L$ be a family of functions where $l, L \geq 128$. Consider the game G of Fig. 1.

We define

$$\mathbf{Adv}^{\mathrm{lr}}_F(B) \;=\; 2 \cdot \Pr\left[\mathrm{G}^B \Rightarrow \mathsf{true}\right] - 1\ .$$

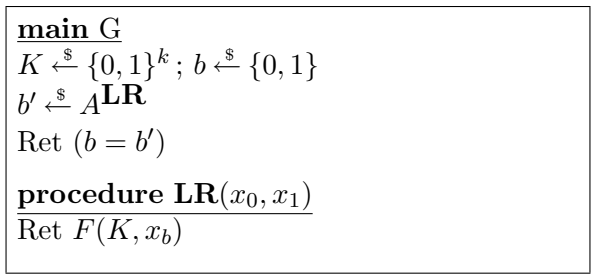

Figure 1: Game G for Problem 4.

Let $(x_0^1, x_1^1), \ldots, (x_0^q, x_1^q)$ be the queries that B makes to its oracle. (Each query is a pair of l-bit strings, and there are q queries in all.) We say that B is *legitimate* if $x_0^1, \ldots, x_0^q$ are all distinct, and also $x_1^1, \ldots, x_1^q$ are all distinct. We say that F is LR-secure if $\mathbf{Adv}_F^{\mathrm{lr}}(B)$ is "small" for every legitimate B of "practical" resources.

1. Show that the legitimacy condition is necessary for LR-security to be "interesting" by showing that if F is a block cipher then there is an efficient, illegitimate B such that $\mathbf{Adv}_F^{\mathrm{lr}}(B) = 1$. Say how may queries B uses and what is its time-complexity.

2. Let B be a legitimate lr-adversary that makes q oracle queries and has time-complexity t. Show that there exists a prf-adversary A, also making q oracle queries and having time-complexity close to t, such that

$$\mathbf{Adv}_F^{\mathrm{lr}}(B) \;\leq\; 2 \cdot \mathbf{Adv}_F^{\mathrm{prf}}(A) \; .$$

State what is the time-complexity of A. Explain why this reduction shows that if F is a secure PRF then it is LR-secure.

3. Is the converse true? Namely, if F is LR-secure, then is it a secure PRF? Answer YES or NO. If you say YES, justify this via a reduction, and, if NO, via a counter-example. (The latter means a particular family of functions F which you can prove is LR-secure but which you can show via an attack is not a PRF.)

We clarify that F above is a family of functions. It is not required to be a block cipher except in part **1.**

Extra credit

The goal of a key-search attack (such as exhaustive key search) is to find the target key, but, as discussed in the notes and in class, such an attack might find a key that is consistent with the input-output examples but is not the target key. We glossed over this, saying it "usually" does not happen. This problem gives a sense of how cryptographers arrive at this type of conclusion and estimate what "usually" means.

We use what is called the *ideal cipher model.* Let $k, n \geq 1$ be integers. Let $K = 2^k$ and $N = 2^n$ and let $T_1, \ldots, T_K$ be some enumeration of the elements of $\{0,1\}^k$. We consider a thought experiment

main EKS
$T^* \xleftarrow{\$} \{0,1\}^k$; $C^* \leftarrow E[T^*, M^*] \xleftarrow{\$} \{0,1\}^n$
Range$[T^*] \leftarrow \{C^*\}$
$T \xleftarrow{\$} A^{\mathbf{E}}(C^*)$
Return $(T = T^*)$

procedure $\mathbf{E}(T, M)$
If not $E[T, M]$ then $E[T, M] \xleftarrow{\$} \{0,1\}^n \setminus \text{Range}[T]$
Range$[T] \leftarrow$ Range$[T] \cup \{E[T, M]\}$
Return $E[T, M]$

Figure 2: Game EKS for Problem 5.

in which a block cipher is chosen at random. By this we mean that for each key T_i, we choose $E(T_i, \cdot)$ as a random permutation on $\{0,1\}^n$. Fix a message $M^* \in \{0,1\}^n$ known to the adversary, who, given a ciphertext $C^* = E(T^*, M^*)$ for a random, unknown T^* attempts to find T^*. The adversary can access E (only) as an oracle.

We formalize this via the game EKS of Fig. 2. We will use games a lot so this is a good chance to start getting familiar with them. The game maintains a table E, representing the block cipher, and assumed to initially be $\perp$ (undefined) everywhere. It also associates to each key T a set Range$[T]$ that is initially empty. The game is executed with an adversary A. As this execution continues, the tables get populated, and the block cipher gets slowly defined. First, the main procedure executes. It picks a random challenge key T^*, defines $E[T^*, M^*]$ to be a random n-bit string, and returns it to the adversary as the challenge ciphertext C^*. It then runs the adversary, which can make queries of the form T, M to procedure $\mathbf{E}$. A query T, M creates the point $E[T, M]$. It is chosen at random, but, to ensure the permutation property of a block cipher, from the set

$$\{0,1\}^n \setminus \text{Range}[T] = \{0,1\}^n \setminus \{\, E(T, M') \;:\; E(T, M') \neq \perp \,\} .$$

The test "If not $E[T, M]$" returns true iff $E[T, M]$ is undefined, meaning equal to $\perp$ rather than an n-bit string. The set Range$[T]$ contains all points $E[T, M]$ that are currently defined. When the adversary is done, it outputs its guess T for the value of T^*. Then main finishes by returning true if $T = T^*$ and false otherwise. The output of main is is called the output of the game or execution, and we let $\Pr[\text{EKS}^A]$ denote the probability that this output is true. The probability is over the random choices in the game, as well as those of the adversary, if any.

Here we are considering a very simple form of key search where there is only one input-output example.

Now, using this model, we can try to calculate the probability that an attack returns the target key, as opposed to some non-target key consistent with the input-output examples.

Problem 6. Let $k, n \geq 1$ be integers. Let $K = 2^k$ and $N = 2^n$. Fix $M^* \in \{0,1\}^n$ and let $T_1, \ldots, T_K$ be some enumeration of the elements of $\{0,1\}^k$. Consider the following adversary for game EKS:

adversary $A(C^*)$
For $i = 1, \ldots, K$ do
  If $\mathbf{E}(T_i, M^*) = C^*$ then $G \leftarrow T_i$; return G

This adversary calls the $\mathbf{E}$ oracle up to K times as shown. Let $\mathbf{Adv}^{\text{eks}}(K, N) = \Pr[\text{EKS}^A]$. This is the probability that the key G output by A in its execution with EKS equals the target key T^* chosen in main.

1. Prove that

$$\mathbf{Adv}^{\text{eks}}(K, N) \;=\; \frac{N}{K} \cdot \left[1 - \left(1 - \frac{1}{N}\right)^K\right] . \tag{1}$$

2. It is difficult to get a quantitative feel from Equation (1). We will now lower bound it via a simpler expression. To do so we first recall an inequality. Namely let x be a real number in the range $0 \le x \le 1$. Let m, l be integers such that $0 \le l \le m$ and l *is even*. Then

$$(1 - x)^m \;\le\; \sum_{i=0}^{l} \binom{m}{i} (-x)^i . \tag{2}$$

Use this and the result of **1.** above to show that

$$\mathbf{Adv}^{\text{eks}}(K, N) \;\ge\; 1 - \frac{K - 1}{2N} . \tag{3}$$

3. Let k, n be (respectively) the key-length and block-length parameters of DES. Use the result of **2.** to numerically estimate $\mathbf{Adv}^{\text{eks}}(K, N)$ in this case. Do the same when k, n are the parameters of AES.

4. What do these results tell us about the success probability of an exhaustive key-search attack on DES? What about on AES? Is DES an ideal cipher? Is AES an ideal cipher? Discuss.
