Cryptography - Tutorial

Computer Security
School of Informatics
University of Edinburgh

In this second tutorial for the Introduction to Computer Security course we cover Cryptography. The tutorial consists of questions from past years exams.

You are free to discuss these questions and their solutions with fellow students also taking the course, and also to discuss in the course forum. Bear in mind that if other people simply tell you the answers directly, you may not learn as much as you would by solving the problems for yourself; also, it may be harder for you to assess your progress with the course material.

1 Hash functions

Let $\mathcal{M} = \{0,1\}^*$ and $\mathcal{T} = \{0,1\}^n$ for some integer n.

1. Explain what does it mean for a hash function $h : \mathcal{M} \to \mathcal{T}$ to be one-way.
2. Explain what does it mean for a hash function $h : \mathcal{M} \to \mathcal{T}$ to be collision resistant.
3. Suppose $h : \mathcal{M} \to \mathcal{T}$ is collision resistant. Is h also one-way? If so, explain why. If not, give an example of a collision resistant function that is not one-way.
4. Suppose $h : \mathcal{M} \to \mathcal{T}$ is one-way. Is h also collision resistant? If so, explain why. If not, give an example of a one-way function that is not collision resistant. Suppose the DLOG assumption is true.
5. Bob is on an under cover mission for a week and wants to prove to Alice that he is alive each day of that week. He has chosen a secret random number, s, which he told to no one (not even Alice). But he did tell her the value $H = h(h(h(h(h(h(h(s)))))))$, where h is a cryptographic hash function. During that week Bob will have access to a broadcast channel, so he knows any message he sends to Alice will be received by Alice. Unfortunately Bob knows that Eve was able to intercept message H. Explain how Bob can broadcast a single message everyday that will prove to Alice that he is still alive. Note that your solution should not allow anyone (and in particular Eve) to replay any previous message from Bob as a (false) proof that he still is alive.

2 Symmetric encryption

Let $(\mathcal{E}_{32}, \mathcal{D}_{32})$ be a secure (deterministic) block cipher with 32-bits key size and 32-bits message size. We want to use this cipher to build a new (deterministic) block cipher $(\mathcal{E}_{64}, \mathcal{D}_{64})$ that will encrypt 64-bits messages under 64-bits keys. We consider the following encryption algorithm. To encrypt a message M under a key K, we split M into two parts M_1 and M_2, and we also split K into two parts K_1 and K_2. The ciphertext C is then computed as $\mathcal{E}_{32}(K_1, M_1)||\mathcal{E}_{32}(K_2, M_2)$. In other words we concatenate the encryption of M_1 under K_1 using $\mathcal{E}_{32}$, with the encryption of M_2 under K_2 using $\mathcal{E}_{32}$.

1. What is the corresponding decryption algorithm? To justify your answer prove that the consistency property is satisfied.

2. Consider the following game.

   - In the first phase, the attacker chooses a few 64-bit plaintext messages $M_1, \ldots, M_n$ and gets back from an encryption oracle the corresponding ciphertexts $C_1, \ldots, C_n$ under some key K that he does not know. The attacker gets to know that C_i is the ciphertext corresponding to M_i for all $i \in \{1, \ldots, n\}$.
   - In the second phase the attacker builds two 64-bit messages M_A and M_B and gets back C which is the encryption under K either of M_A or M_B. But now, the attacker doesn't know if the plaintext underlying C is M_A or M_B and has to guess it.

   Informally, a symmetric cipher is said to be vulnerable to a chosen plaintext attack if the attacker can guess (with high probability) which of M_A or M_B is the plaintext corresponding to C. Show that the new cipher $(\mathcal{E}_{64}, \mathcal{D}_{64})$ is subject to a chosen plaintext attack even though $(\mathcal{E}_{32}, \mathcal{D}_{32})$ is not.

3. A symmetric cipher is said to be vulnerable to a known plaintext attack if given a plaintext message M and its corresponding ciphertext C under some key K not known to the attacker, the attacker can recover the key K in a reasonable amount of time (that is significantly less than by a brute force-attack). Show that $(\mathcal{E}_{64}, \mathcal{D}_{64})$ is vulnerable to a known plaintext attack.

3 Cryptographic Proofs

1. Prove that in a classroom of 23 students the probability that any two students have the same birthday is over 50%, a.k.a the Birthday Paradox. Suppose birthdays are distributed uniformly over the 365 days of the year.

2. Prove that, given a collision-resistant one-way compression function, the Merkle-Dåmgard construction builds a collision resistant hash function.

3. Prove that the RSA encryption scheme is consistent: Given a public - secret keypair $(n, e), d$, it is
$$Dec_{RSA}\left(d, Enc_{RSA}\left((n, e), m\right)\right) = m \pmod{n} \ .$$
   Hint: Use Euler's theorem.