University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Problem Set 6

Due at *beginning* of class on Dec. 13

1. We saw in class that one suggestion for signing using RSA (with public exponent 3) is to first *encode* the message and then sign using "textbook" RSA. More precisely, the public key consists of a modulus N for which $\gcd(3, \varphi(N)) = 1$. The secret key consists of an exponent d such that $3d = 1 \bmod \varphi(N)$. To sign message m, compute $(\mathsf{enc}(m))^d \bmod N$, where enc is some deterministic, publicly-known encoding procedure.

   (a) How is signature verification performed in this scheme?

   We showed in class that setting $\mathsf{enc}(m) = H(m)$ was secure when H was modeled as a random oracle. Here, we investigate other possibilities for enc. Assume $|N| = 1024$.

   (b) Consider the function $\mathsf{enc}(m) = 0|m|0^{99}$ (where $|m| = 924$ and $m \neq 0^{924}$). Show that this is insecure. (*Hint*: ask for one signature and then forge a signature on some different message.)

   (c) **For graduate students, or for extra credit.** Consider the function $\mathsf{enc}(m) = 0m|0m$ (where $|m| = 511$) and $m \neq 0^{511}$). Show that this is insecure. (*Hint*: ask for one signature and then forge a signature on some different message.)

2. We improve (slightly) on the Lamport one-time signature scheme we gave in class. Recall that the Lamport scheme requires a public key consisting of 2ℓ elements in order to sign messages ℓ bits long. Since signing ℓ-bit messages can also be viewed as signing one message out of 2^ℓ possible messages, we can view the efficiency of the Lamport scheme in the following equivalent way: if there are n elements in the public key, we can sign one message out of $2^{n/2}$ possible messages.

   We now show one way to improve this. Consider the following scheme which allows signing one message out of 6 possible messages: the public key consists of four elements (y_1, y_2, y_3, y_4). The secret key consists of their inverses $(x_1 = f^{-1}(y_1), \ldots)$. We assume the 6 possible messages are ordered in advance in some publicly known way (i.e., lexicographically). To sign message 1, send the pair (x_1, x_2); to sign message 2, send the pair (x_1, x_3); $\ldots$; to sign message 6, send the pair (x_3, x_4). Each signature consists of a pair of elements. Verification is done in the obvious way.

   (a) Prove the security of the above scheme for signing one of a possible 6 messages. How does the security reduction you obtain here compare to what was obtained in class for the Lamport scheme?

   (b) Sketch the generalization of the above scheme for when you have n elements in the public key (no proof of security is necessary).

(c) What is the complexity of this generalization? In other words, given a public key containing n elements, how large is the space of possible messages you can sign? Try to generalize the scheme so as to obtain the best possible result.

3. In class we have mentioned three kinds of hash functions: collision-resistant hash functions, universal one-way hash functions, and random oracles. Here, we investigate the relationship among these. Let $H : \{0,1\}^{10k} \rightarrow \{0,1\}^k$.

   (a) Show that if H is (t, ϵ)-collision resistant then it is also (t, ϵ)-universal one-way.

   (b) Show that if H is a random oracle, then H is (t, ϵ)-collision resistant. Express ϵ in terms of the output length k.

   (c) **For graduate students, or for extra credit.** Show that H can be universal one-way without being collision-resistant. Namely, give an *explicit* construction of a function which is (t, ϵ)-universal one-way (for some small ϵ) but not $(t, 1/2)$-collision resistant. For your construction, you may assume a collision-resistant hash function H' and/or a random oracle. You may give convincing arguments instead of rigorous proofs.