COMS W4261: Introduction to Cryptography.
Instructor: Tal Malkin

Problem Set 4

Due: Friday 11/21/2014, by 5:00pm

1. Prove that the following modification to the basic CBC-MAC does not yield a secure MAC (even for fixed-length messages): Mac outputs all blocks $t_1, \ldots, t_\ell$ rather than just $t_\ell$. (Verification only checks whether $t_\ell$ is correct).

2. Recall the encrypt-then-authenticate scheme we saw in class, assuming we have any secure MAC and CPA-secure encryption: generate independent keys for each of the underlying schemes; to encrypt, first use the encryption algorithm to get $c$, then authenticate $c$ getting a tag $t$, and output $\langle c, t \rangle$.

Prove that the scheme satisfies unforgeability (using the definition we gave in class).

Note: while you’re not required to prove so here, it is not too hard to also prove that the scheme is CCA secure if the underlying Mac algorithm is deterministic (or any strong MAC). Thus, this scheme satisfies our requirement for secure authenticated encryption.

3. Let $(\text{GEN}, H)$ be a CRHF. Define $\hat{H}^s(x) = H^s(0^n \parallel H^s(x))$.

Prove that $(\text{GEN}, \hat{H})$ is a CRHF.

4. (a) Compute by hand $78^{4,800,000,002} \pmod{35}$ (show your work).

(b) Use the extended Euclid algorithm to compute $7^{-1} \pmod{17}$ and $32^{-1} \pmod{77}$ by hand (show your work).

(c) Recall the Blum-Micali PRG candidate we saw in class (secure under the DLA assumption): on input $s$ set $x_0 = s$, and define $x_{i+1} = g^{x_i} \pmod{p}$. The $i$th output bit is 0 iff $x_i < \frac{p-1}{2}$.

Let the prime $p = 13$, and the generator $g = 2$ (you can check that this is indeed a generator). Compute the first 3 bits of the output of the Blum-Micali PRG on the seed $s = 9$.

5. Let $p > 2$ be a prime. In this problem you will work in $\mathbb{Z}_p^*$, so here are reminders of facts we saw in class. Recall that $\mathbb{Z}_p$ is a field of integers modulo $p$, and $\mathbb{Z}_p^*$ is the multiplicative group of that field (consisting of $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$). Recall Fermat’s little theorem: for all $a \in \mathbb{Z}_p^*$, $a^{p-1} \equiv 1 \pmod{p}$. Further recall that $\mathbb{Z}_p^*$ is cyclic. That is, there exists a generator $g$ such that $\mathbb{Z}_p^* = \{g^1 \pmod{p}, g^2 \pmod{p}, \ldots, g^{p-1} \pmod{p}\}$ (or, $\mathbb{Z}_p^* = \{g^0 \pmod{p}, g^1 \pmod{p}, \ldots, g^{p-2} \pmod{p}\}$). In particular, for any generator $g$ these $p-1$ powers of $g$ are all distinct elements, and we have that for any $x, y$, if $g^x \equiv g^y \pmod{p}$, then $x \equiv y \pmod{p-1}$. Finally, recall that $QR_p$ is the set of elements that have a square root modulo $p$, namely $QR_p = \{a \in \mathbb{Z}_p^* \mid \exists x \ a = x^2 \pmod{p}\}$.

We stated in class all the facts below. In this problem you are asked to prove them.

(a) Let $a = g^x \pmod{p}$ where $g$ is a generator. Prove that $a \in QR_p$ if and only if $x$ is even.
(b) Prove that for all $a \in \mathbb{Z}_p^*$, $a \in QR_p$ if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$. ( Hint: write $a = g^x \pmod{p}$ for a generator $g$.)

By the way, the value of $a^{(p-1)/2}$ is called the Legendre symbol of $a$, and is often written as $(\frac{a}{p})$ or $L_p(a)$. It turns out that for any $a$, $(\frac{a}{p})$ is always either 1 (when $a \in QR_p$), or $-1$ (when it is not).

(c) Show that if the prime $p$ satisfies $p \equiv 3 \pmod{4}$ and $a \in QR_p$, then $a^{(p+1)/4}$ is a square root of $a$ modulo $p$. 