MACM 498/CMPT 881/MATH 800
Assignment 6, Fall 2004

Michael Monagan

This, last, assignment is to be handed in to me by 4pm Tuesday December 7th.
Late penalty: 10% off for each day late.

Chapter 4: Cryptographic Hash Functions

Exercises 4.6, 4.7, 4.9(a), 4.12.

Chapter 7: Digital Signatures

Exercises 7.1, 7.2, 7.3.

Additional question: Let $p = 14747$, $q = 101$, and $\alpha = 4789$. Note $q|p-1$ and α is an element of order q in $\mathbb{Z}_p$. Let $\beta = 3430$. Solve $\beta \equiv \alpha^a \bmod p$ for a.

Using the Schnorr Signature algorithm (page 286) with the above values for p, q, α, β, and the secret value a you computed, together with $k = 11$ and $h(x||\alpha^k) = (x + \alpha) \bmod p$, compute the signature for $x = 1234$ and verify it using the verification formula.

Note: to compute discrete logarithms in Maple you may use the `numtheory[mlog]` command.

Bonus Question

Let $n = pq$ where $p \equiv q \equiv 3 \bmod 4$. Recall that the map $x \to x^2 \bmod n$ partitions $QR(n)$ into simple cycles. For $n = 192649 = 383 \times 503$ I found 1 cycle of length 1, 5 cycles of length 50, 2 of length 95 and 50 of length 950.

(a) (40 marks) Explain where the cycle periods 1, 50, 95, 950 come from. Hint: if $x \in QR(n)$ is on a cycle of period π then $x^{2^\pi} \equiv x \bmod p$. Hence determine a way to ensure that seed of the BBS generator, s_0, can be selected from $QR(n)$ by a user who does not know p nor q in such a way as to guarantee a long cycle. Note: you are allowed to specify how the primes p and q should be chosen and how the seed s_0 should be chosen.

(b) (40 marks) Simulate the Monte Carlo algorithm in figure 12.8 on page 375 of chapter 12 for solving the quadratic residue problem using $n = 192649 = 383 \times 503$. You will need to implement the BBS Generator in figure 12.6 (easy) and to simulate the ϵ previous bit predictor B_0 used in figure 12.7 (hard). For this purpose you can use as much time as you need to compute B_0. Try it on enough problems so you can measure how good your B_0 is.