MACM 442/CMPT 800/MATH 800
Assignment 5, Fall 2006

Michael Monagan

This assignment is to be handed in on Tuesday November 21st at the beginning of class. Late penalty: 10% off for each day late.

Chapter 6.

1: Suppose Bob wants to construct an ElGamal cryptosystem based on the finite field with 2^{128} elements, i.e. the group in which ElGamal is run will have $n = 2^{128} - 1$ elements. The security of the discrete logarithm problem depends on the largest prime dividing n. What is the largest prime dividing n? Using Maple, find an polynomial $f(x)$ of degree 128 in $\mathbb{Z}_2[x]$ that is irreducible over $\mathbb{Z}_2$. Then we have $F = \mathbb{Z}_2[x]/(f)$ is a finite field with 2^{128} elements. Determine the first primitive element in F, i.e., the first element in the sequence $0, 1, x, x+1, x^2, x^2+1, x^2+x+1, x^3, ...$ that has order n.

2: Using Maple, find all irreducible polynomials of the form $f = x^5+c_4x^4+c_3x^3+c_2x^2+c_1x+1$ in $\mathbb{Z}_2[x]$. For each polynomial, determine the order of the element x in the finite field $\mathbb{Z}_2[x]/f$ and hence identify which polynomials are primitive.

For each polynomial you found, verify that the period of the sequence defined by

$$z_{i+5} = z_i + c_1 z_{i+1} + c_2 z_{i+2} + c_3 z_{i+3} + c_4 z_{i+4} \bmod 2$$

with $z_0 z_1, z_2, z_3, z_4, z_5 = 10001$ is $2^5 - 1 = 31$ only for the primitive polynomials. What period do you get for the non-primitive irreducible polynomials?

3: Let $f(z) \in \mathbb{Z}_p[z]$ have degree greater than 0. Consider the finite ring $R = \mathbb{Z}_p[z]/f$. Let $[u] \in R$ be non-zero, i.e., $u \in \mathbb{Z}_p[z]$ and $u \not\equiv 0 \bmod f$. Prove that $[u]$ is invertible in R if and only if $\gcd(u, f)$=1. Hence conclude that R is a field if and only if f is irreducible over $\mathbb{Z}_p$.

4: Find an isomorphism between the group G = $(\mathbb{Z}_7^*, \times)$ and H = $(\mathbb{Z}_6, +)$.
Hint: Discrete Logarithms.

5: For CMPT 881 and MATH 800 students: Implement Algorithm 6.6 and use it to answer exercise 6.20. You will have to "simulate" an oracle for computing $L_2(\beta)$.

Chapter 2

6: For the One-Time-Pad, to encrypt one bit, let $K \in 0, 1$ be the key. Show that if the $\Pr(K = 0) \neq 1/2$ then the One-Time-Pad does NOT have perfect secrecy.

Chapter 8

7: Exercise 8.5

8: Exercise 8.9

9: Consider the linear congruential generator based on the finite field GF(2^k) with 2^k elements. Let α be a primitive element from $GF(2^k)$ and let $s_0 \in GF(2^k)^*$ be the seed. Compute

$$s_i = \alpha s_{i-1} \quad \text{for} \quad i = 1, 2, ..., m$$

and convert each s_i to a k bit bit-string: If $s_i = a_0 + a_1 y + ... + a_{k-1} y^{k-1}$ then the bit-string is $a_0 a_1 ... a_{k-1}$. This will produce a bit string of length km and thus it can be viewed as a (k, l)-Pseudo Random Bit Generator with seed s_0.

Implement this generator for $GF(2^{16})$. To construct the field you need to find an irreducible polynomial $f(y)$ of degree 16 in $\mathbb{Z}_2[y]$. Use the `Nextprime` command in Maple to find one. Now choose a random primitive element $\alpha \in \text{GF}(2^{16}) = \mathbb{Z}_2[y]/f(y)$. Now compute $s_1, ..., s_{16}$ and convert each s_i to a bit-string. This will produce a bit string of length 256.

Now explain why (k, l)-PRBGs constructed in this way are not secure for cryptographic purposes. Demonstrate this by showing how to compute f, α, s_0 from $s_1, s_2, ..., s_{16}$.

9: Consider the example of the BBS Generator on page 337 of Chapter 8 with $n = 192649 = 383 \times 503$ and $s_0 = 101355^2 = 20749 \bmod n$. Implement the BBS generator and reproduce the 20 bit bit-string 11001110000100111010. The BBS algorithm requires that $s_0 \in QR(n)$. The map $x \rightarrow x^2 \bmod n$ partitions QR(n) into a set of cycles $C_1, C_2, ...,$. Compute these cycles and their cardinality for $n = 192649$ and display the data in a reasonable format. Hence determine (i) the period for $s_0 = 20749$ and (ii) the other possible periods for this BBS generator.