Math 418/818
Assignment 6
Due 5 November 2015

1. (a) Let $p = 65537 = 2^{16} + 1$ and $g = 5$. You receive the message $(29095, 23846)$ which your friend composed using the ELGamal cryptosystem in $\mathbb{F}_p^\times$, using your public key $g^a$. Decipher the message, given that your secret key is $a = 13908$. (You may use a calculator or MAPLE for some of your computations. However, you should indicate clearly what you are computing and what the result is.)

(b) Assume that 3-letter words $xyz$ in the 31-symbol alphabet $\Sigma = \{0, 1, \ldots, 30\}$ are represented in $\mathbb{F}_p$ as $31^2x + 31y + z$. Interpret the message of part (a) as a text by identifying the letters A–Z with 0–25, blank = 26, . = 27, ? = 28, ! = 29, ’ = 30.

2. (a) Show that $f(x) = x^2 - 2$ is irreducible over $\mathbb{F}_{11}$.
(b) Write down the multiplication and division rule for two elements $ax + b, cx + d \in A_f = \mathbb{F}_{11}[x]/(f) \simeq \mathbb{F}_{121}$.

3. Show that if $\alpha \in \mathbb{F}_{p^2}$ is a root of the polynomial $g(x) = x^2 + aX + b$, where $a, b \in \mathbb{F}_p$, then $\alpha^p$ is also a root of $g(x)$. In addition, verify that $a = -(\alpha + \alpha^p)$ and that $b = \alpha^p + 1$, provided that $\alpha \notin \mathbb{F}_p$. Is this true if $\alpha \in \mathbb{F}_p$?

4. (a) Using the Silver-Pohlig-Hellman algorithm, find the discrete log of 103 and of 97 to the base 2 in $\mathbb{F}_{181}$.
(b)* Using the Silver-Pohlig-Hellman algorithm, find the discrete log of $x$ to the base $x + 2$ in $A_f \simeq \mathbb{F}_{49}$, where $f(x) = x^2 + 1 \in \mathbb{F}_7[x]$.

5. MAPLE problem (refer to the MAPLE instruction sheet):
   (a) Recall that the command $\text{Rem}(g, f, x) \mod p$ computes the remainder $\text{rem}(g, f)$ of two modular polynomials $f, g \in \mathbb{F}_p[x]$. If $g_1 = x^3 + 3x^2 + 1$, $g_2 := 3x^3 + 2x + 3$ and $f := x^4 + x^2 + 3$, find $\text{rem}(g_1g_2, f)$ in $\mathbb{F}_7[x]$.
   (b) Write a one-line function (program) $\text{multp}(g_1, g_2, f, p)$ which computes the product $g_1g_2$ in $A_f$ (for $g_1, g_2, f \in \mathbb{F}_p[x]$). Test your program for $g_1, g_2, f$ and $p = 7$ as in part (a).
   (c) Write a small program $\text{ordp}(g, f, p)$ which calculates the order of $g \in (A_f)^\times$. (Use your function $\text{multp}(.)$ of part (b).) For $f$ and $p$ as in part (b), find the order of $g = x + 1$ and also of $g = x^2 + 1$.
   (d) Write a program $\text{powtab}(g, f, p)$ which computes the power table of $g \in A_f$. Your program should return a list of length $\text{ord}(g)$ whose $i$-th entry is $g^{i-1}$. Test your program for $A_f$ as in part (b) and $g = x^2 + x + 1$. Check that your output list has the right number of elements.