The University of Sydney
Math3024 Elementary Cryptography and Protocols

Semester 1 **Exercises for Week 12** 2004

Diffie–Hellman and Discrete Logarithms

An El Gamal cryptosystem is based on the difficulty of the Diffie–Hellman problem: Given a prime p, a primitive element a of $(\mathbb{Z}/p\mathbb{Z})^* = \{c \in Z/pZ : c \neq 0\}$, and elements $c_1 = a^x$ and $c_2 = a^y$, find the element a^{xy} in $(\mathbb{Z}/p\mathbb{Z})^*$.

1. Recall the discrete logarithm problem: Given a prime p, a primitive element a of $(\mathbb{Z}/p\mathbb{Z})^*$, and an element c of $(\mathbb{Z}/p\mathbb{Z})^*$, find an integer x such that $c = a^x$. Explain how a general solution to the discrete logarithm problem for p and a implies a solution to the Diffie–Hellman problem.

2. Fermat's little theorem tells us that $a^{p-1} = 1$ for all a in $(\mathbb{Z}/p\mathbb{Z})^*$. Recall that a primitive element a has the property that $\mathbb{Z}/(p-1)\mathbb{Z} \rightarrow (\mathbb{Z}/p\mathbb{Z})^*$ given by $x \mapsto a^x$ is a bijection.

a. Show that a is primitive if and only if $a^x = 1$ only when $p-1$ divides x.

b. Let p be prime $2^{32} + 15$. Show that $a = 3$ is a primitive element of $(\mathbb{Z}/p\mathbb{Z})^*$. Use the `Magma` function `Log` to compute discrete logarithms of elements of `FiniteField(p)` with respect to a.

c. Let p be the prime $2^{32} + 61$. Show that the element $a = 2$ is a primitive element for $(\mathbb{Z}/p\mathbb{Z})^*$. Use the `Magma` function `Log` to compute discrete logarithms of elements of `FiniteField(p)` with respect to a.

3. Compare the times to compute discrete logarithms in the previous exercise. Now factor $p-1$ for each p. What difference do you note? Explain the timings in terms of the Chinese remainder theorem for $\mathbb{Z}/(p-1)\mathbb{Z}$.

4. Let p be the prime $2^{131} + 1883$ and verify the factorization

$$p - 1 = 2 \cdot 3 \cdot 5 \cdot 37 \cdot 634466267339108669 \cdot 3865430919824322067.$$

Let $a = 109$ and $c = 1014452131230551128319928312434869768346$ and set

$$n_5 = (p-1) \text{ div } 634466267339108669$$
$$n_6 = (p-1) \text{ div } 3865430919824322067.$$

Then verify that $c^{n_5} = a^{129 n_5}$ and $c^{n_6} = a^{127 n_6}$. Find similar relations for

$$n_1 = (p-1) \text{ div } 2 \quad n_3 = (p-1) \text{ div } 5,$$
$$n_2 = (p-1) \text{ div } 3 \quad n_4 = (p-1) \text{ div } 37.$$

and use this information to find the discrete logarithm of c with respect to a.