The University of Sydney
Math3925 Public Key Cryptography

Semester 2	**Assignment 2**	2004

This assignment will be due on Friday 24 September, should be submitted at 638 Carslaw by 5PM, and is worth 10% of the assessment for this course.

1. Let n be the integer 228618946967762521. Explain how 3-torsion elements in $\mathbb{Z}/n\mathbb{Z}^*$ can be used to factor n, and demonstrate this with $x = 90208952368431523$.

2. **a.** Find the discrete logarithm x of 2 with respect to the base 3 in $\mathbb{F}_p^*$, where $p = 1234621183$. Use the Pollig-Hellman reduction, noting that $p - 1 = 2 \cdot 3 \cdot 83 \cdot 383 \cdot 6473$, and give the values you determine for $x \bmod 2, x \bmod 3$, etc.

b. Now determine the discrete logarithm $\log_3(2)$ in $\mathbb{F}_p^*$, where $p = 65537$, expressing the result in base 2.

3. Verify that the ring $\mathbb{Z}[\tau]/(13)$, where $\tau^3 - \tau + 1 = 0$ is a field, that 61 divides the order of $\mathbb{Z}[\tau]/(13)^*$, and that $x = \tau + 6$ and $y = \tau + 10$ have exact order 61.

a. Partition $\mathbb{F}_{13^3}$ into disjoint sets

$$
\begin{aligned}
S_1 &= \{a + b\tau + c\tau^2 \in \mathbb{F}_{13^3} : 0 \le a \le 4\}, \\
S_2 &= \{a + b\tau + c\tau^2 \in \mathbb{F}_{13^3} : 5 \le a \le 8\}, \\
S_3 &= \{a + b\tau + c\tau^2 \in \mathbb{F}_{13^3} : 9 \le a\},
\end{aligned}
$$

and use these to determine four cycles and tails in the Pollard ρ method beginning with an initial value of the form $x^n y^m$. Give both the elements $x^{n_i} y^{m_i}$ and the exponents (n_i, m_i) in the sequence. Use your cycles to determine the discrete logarithm $\log_x(y)$.

b. Find the complete set of relations between the elements

$$-1, \tau, 2, 3, \tau^2 + 1, \tau^2 + \tau + 1, -2\tau - 1, x, y$$

of $\mathbb{F}_{13^3}$, and demonstrate how to use these to determine $\log_x(y)$.