TMA4160 Cryptography – Fall 2010 – answers

Note: Several gcd-computations are omitted.

Problem 1

a. We compute

$$7k_1 + 4k_1^2 + 11k_1^3 + 15k_1^4 + k_2 \equiv 21 + 36 + 297 + 1215 + 21 \equiv 24 \pmod{29},$$
$$14k_1 + 10k_1^2 + k_2 \equiv 42 + 90 + 21 \equiv 8 \pmod{29}.$$

Alice sent the message HELP.

b. We see that $f(k_1, k_2, \text{KELP}) - f(k_1, k_2, \text{HELP}) = (10 - 7)k_1 = 3k_1 = 7 - 21 = 15$, and therefore $k_1 = 5$. We get

$$k_2 = 21 - (7k_1 + 4k_1^2 + 11k_1^3 + 15k_1^4) = 11.$$

Finally,

$$t \equiv 14k_1 + 10k_1^2 + k_2 \equiv 70 + 250 + 11 \equiv 12.$$

Problem 2.

a. We compute

$$\begin{aligned}
\left(\frac{650}{1829}\right) &= \left(\frac{2}{1829}\right)\left(\frac{325}{1829}\right) = -\left(\frac{325}{1829}\right) \\
&= -\left(\frac{1829}{325}\right) = -\left(\frac{204}{325}\right) = -\left(\frac{51}{325}\right) \\
&= -\left(\frac{325}{51}\right) = -\left(\frac{19}{51}\right) \\
&= \left(\frac{51}{19}\right) = \left(\frac{13}{19}\right) \\
&= \left(\frac{19}{13}\right) = \left(\frac{6}{13}\right) = -\left(\frac{3}{13}\right) \\
&= -\left(\frac{13}{3}\right) = -\left(\frac{1}{3}\right) = -1,
\end{aligned}$$

and then because $650^2 \equiv 1 \pmod{1829}$,

$$650^{(1829-1)/2} = 650^{2^9} 650^{2^8} 650^{2^7} 650^{2^4} 650^2 = 1,$$

so 1829 is composite.

b. Following the algorithm in Stinson, we get:

$x_0 = 2$	$x'_0 = 2^2 + 1 = 5$	$\gcd(5-2, 1829) = 1$
$x_1 = 5$	$x'_1 = (5^2+1)^2 + 1 = 677$	$\gcd(677-5, 1829) = 1$
$x_2 = 26$	$x'_2 = (677^2+1)^2 + 1 = 1080$	$\gcd(1080-26, 1829) = 31$

c. We multiply the three relations to get

$$(807 \cdot 1656 \cdot 1150)^2 = 5^4 \cdot 7^2 \cdot 19^2.$$

We get the square roots

$$\begin{aligned} &807 \cdot 1656 \cdot 1150 \equiv 628 \pmod{1829} \text{ and} \\ &5^2 \cdot 7 \cdot 19 \equiv 1496 \pmod{1829}, \end{aligned}$$

and $\gcd(1496 - 628, 1829) = 31$.

Problem 3

a. We compute

$$\begin{aligned} g^m = (1+n)^m + \langle n^2 \rangle &= \sum_{i=0}^{m} \binom{m}{i} 1^i n^{m-i} + \langle n^2 \rangle \\ &= 1 + \binom{m}{1} n + \langle n^2 \rangle = 1 + mn + \langle n^2 \rangle, \end{aligned}$$

since $\binom{m}{1} = m$. From this, it is clear that g has order n since $1 + n^2 + \langle n^2 \rangle = 1 + \langle n^2 \rangle$.

b. Let $x, y \in H$, so that for some $x_0, y_0 \in \mathbb{Z}^*_{n^2}$, $x = x_0^n$ and $y = y_0^n$.
It is clear that $1 \in H$. We have

$$xy = (x_0^n)(y_0^n) = (x_0 y_0)^n \in H,$$

and

$$x^{-1} = (x_0^n)^{-1} = (x_0^{-1})^n \in H.$$

Hence, H is a subgroup.

Let $x \in H$ and suppose $x = x_0^n$, $x_0 = a + \langle n^2 \rangle$. Then $x = (a + \langle n^2 \rangle)^n = a^n + \langle n^2 \rangle$ and $\phi(a + \langle n \rangle) = a^n + \langle n^2 \rangle = x$. Also, for any c relatively prime to n, $\phi(c + \langle n \rangle) = c^n + \langle n^2 \rangle = (c + \langle n^2 \rangle)^n \in H$. Hence, the image of ϕ is H.

c. Since H is the image of ϕ, we only need to show that it is an injective homomorphism. It is an homomorphism because

$$\begin{aligned}\phi((a+\langle n\rangle)(b+\langle n\rangle)) = \phi(ab+\langle n\rangle) = (ab)^n + \langle n^2\rangle = (a^n + \langle n^2\rangle)(b^n + \langle n^2\rangle) \\ = \phi(a+\langle n\rangle)\phi(b+\langle n\rangle).\end{aligned}$$

It is injective because if $\phi(a+\langle n\rangle) = \phi(b+\langle n\rangle)$, then

$$a^n + \langle n^2\rangle = b^n + \langle n^2\rangle \Rightarrow a^n + \langle n\rangle \equiv b^n + \langle n\rangle \Rightarrow a + \langle n\rangle = b + \langle n\rangle,$$

which is true because n is invertible modulo $(p-1)(q-1)$.

d. Exponentiation by un is the identity on $\mathbb{Z}_n^*$, hence it is the identity on H, because H is isomorphic to $\mathbb{Z}_n^*$. We compute

$$(xg^m)^{un} = x^{un}(g^n)^{mu} = x.$$

e. Let $c = \phi(r)g^m$. Then $c/c^{un} = \phi(r)g^m\phi(r)^{-1} = g^m$, and using the fact that $g^m = 1 + mn + \langle n^2\rangle$, we can easily recover m.