TMA4160 Cryptography - Exam 2011 Sample Solutions

Problem 1. a) Let $p = 138547$. For Bob's exponent to be invertible it has to be coprime to $p-1$ and thus odd (this holds for any prime p). As a result, 26 is not suitable. Since 5 does not divide $p-1$, choosing $e = 25$ is a suitable choice. By the extended Euclidean algorithm,

$$\begin{aligned} 21 = & \quad (p-1) & -5541 \cdot e \ , \\ 4 = & -(p-1) & +5542 \cdot e \text{ and} \\ 1 = & \ 6 \cdot (p-1) & -(5541 + 5 \cdot 5542) \cdot e \ , \end{aligned}$$

hence $d \equiv -(5541 + 5 \cdot 5542) \equiv -33251 \mod p-1$.

b) Since x_0 is a Q.R. it means that $x_0^{\frac{p-1}{2}} \equiv 1$ and so $(x_0^e)^{\frac{p-1}{2}} \equiv \left(x_0^{\frac{p-1}{2}}\right)^e \equiv (1)^e \equiv 1 \mod p$. Thus the encryption of x_0 is also a Q.R.. Similarly, x_1 is a Q.n.R. means that $x_1^{\frac{p-1}{2}} \equiv -1$ and so $(x_0^e)^{\frac{p-1}{2}} \equiv \left(x_0^{\frac{p-1}{2}}\right)^e \equiv (-1)^e \equiv -1 \mod p$, since e is odd. Thus the encryption of x_1 is also a Q.n.R.. Now, using the properties of the Legendre/Jacobi symbol,

$$\begin{aligned} \left(\tfrac{y_0}{p}\right) &= \left(\tfrac{45826}{138547}\right) = \left(\tfrac{2}{138547}\right)\left(\tfrac{22913}{138547}\right) = -\left(\tfrac{22913}{138547}\right) = -\left(\tfrac{138547}{22913}\right) \\ &= -\left(\tfrac{1069}{22913}\right) = -\left(\tfrac{22913}{1069}\right) = -\left(\tfrac{464}{1069}\right) = -\left(\tfrac{2}{1069}\right)^4\left(\tfrac{29}{1069}\right) \\ &= -\left(\tfrac{29}{1069}\right) = -\left(\tfrac{1069}{29}\right) = -\left(\tfrac{25}{29}\right) = -\left(\tfrac{5}{29}\right)^2 \\ &= -\left(\tfrac{29}{5}\right)^2 = -\left(\tfrac{4}{5}\right)^2 = -\left(\tfrac{2}{5}\right)^4 = -1 \end{aligned}$$

so y_0 is a Q.n.R. and thus must be the encryption of x_1 (since Bob is assumed to be honest). Hence Alice should pick y_1 to win.

c) If computing discrete logarithms modulo p is feasible, then Alice can determine Bob's encryption exponent e (and thus the correspondance between x_i and y_i) as follows: When Alice receives y_0, y_1, she computes $\alpha = \log_{x_0} y_0 \mod p-1$. If α exists and $x_1^\alpha \equiv y_1 \mod p$ then $e = \alpha$. Otherwise, $e = \log_{x_0} y_1 \mod p-1$. □

Problem 2. a) Let $b = (1,1,0,0,1,0,1,0)$. Then $b(x) = x^7 + x^6 + x^3 + x$ and we need to find $b^{-1}(x) \in \mathbb{Z}_2[x]/[f(x)]$ for $f(x) = x^8 + x^4 + x^3 + x + 1$. By the extended Euclidean algorithm,

$$\begin{aligned} x^6 + x^2 + 1 = & \quad f(x) & + & \quad (x+1)b(x) \\ x^2 + 1 = & \quad (x+1)f(x) & + & \quad x^2 b(x) \quad \text{and} \\ 1 = & \ (x^5 + x^4 + x^3 + x^2 + 1)f(x) & + & \ (x^6 + x^4 + x + 1)b(x) \ . \end{aligned}$$

Hence $b^{-1}(x) \equiv (x^6 + x^4 + x + 1) \mod f(x)$ so $b_*(x) = x^6 + x^4 + x + 1 \in \mathbb{Z}_2[x]$. Now we can compute

$$\begin{aligned} \sigma(b) &= (x^4 + x^3 + x^2 + x + 1) \cdot (x^6 + x^4 + x + 1) + (x^6 + x^5 + x + 1) \\ &= x^{10} + x^9 + x^6 + x^5 + x^4 + x \\ &\equiv x^2 + x + x^6 + x^5 + x^4 + x \equiv x^6 + x^5 + x^4 + x^2 \mod (x^8 + 1) \end{aligned} \ .$$

Taking the coefficients gives $c = (0,1,1,1,0,1,0,0)$.

b) Let $g(x) = x^8 + x^4 + x^3 + 1$. $g(1) \equiv 0 \mod 2$ so $g(x)$ is reducible over $\mathbb{Z}_2$ with $(x+1)$ as a factor. This means that the ring $\mathbb{Z}_2[x]/[g(x)]$ is not a field and as a result, $b(x)$ is not invertible for all bytes b as required for encryption. □

Problem 3. a) Let $n = 151187$. Bob's uncertainty is not justified as the primality test never identifies a prime as composite (on the contrary, it might pass a composite as a prime for some base). Using Pollard's $p-1$ with $B = 6$ means computing $\gcd\left(2^{6!} - 1 \mod n, n\right)$ which gives a factor of n.

$$\begin{aligned}
2^{6!} &\equiv \left(\left(\left(4^3\right)^4\right)^5\right)^6 &&\equiv \left(\left(64^4\right)^5\right)^6 &&\equiv \left(16777216^5\right)^6 \\
&\equiv \left(146646^5\right)^6 &&\equiv \left(\left(146646^2\right)^2 \cdot 146646\right)^6 &&\equiv \left(\left(4541^2\right)^2 \cdot 146646\right)^6 \\
&\equiv \left(59249^2 \cdot 146646\right)^6 &&\equiv \left(33048 \cdot 146646\right)^6 &&\equiv 57723^6 \\
&\equiv \left(57723^2 \cdot 57723\right)^2 &&\equiv \left(85623 \cdot 57723\right)^2 &&\equiv 113399^2 \\
&\equiv 37788^2 &&\equiv 122916 \mod n
\end{aligned}$$

and $\gcd(122915, n) = 31$. Hence $n = 31 \cdot 4877$.

b) Let $p = 151189$, $h = 82935$ and $g = 7$. From congruences (2) and (3) we deduce that 293 and 43 must be prime divisors of $p - 1 = 151188$ so we get $\frac{151188}{293 \cdot 43} = 12 = 2^2 \cdot 3$. Therefore, we need to obtain two more congruences using Pohlig-Hellman, one mod 3 and one mod 4:

<u>modulo 3:</u> Let $\alpha \equiv \alpha_0 \mod 3$. $h' = h^{\frac{p-1}{3}} = h^{50396}$ and $g' = g^{50396}$. $h' \equiv g'^{\alpha_0} \mod p$ and since $g' \not\equiv g'^2 \equiv h' \mod p$ we have

$$\alpha \equiv 2 \mod 3 \ . \qquad (8)$$

<u>modulo 4:</u> Let $\alpha \equiv \alpha_0 + \alpha_1 \cdot 2 \mod 4$. $h' = h^{\frac{p-1}{2}} = h^{75594}$ and $g' = g^{75594}$ and by congruence (5) we have $\alpha_0 = 1$. Next, $h'' = \left(h \cdot g^{-\alpha_0}\right)^{\frac{p-1}{4}} \equiv (82935 \cdot 7^{-1})^{37797} \equiv (82935 \cdot 43197)^{37797} \equiv 3582543195^{37797} \equiv 119840^{37797} \mod p$ (from congruence (7), $7^{p-2} \equiv 7^{-1} \equiv 43197 \mod p$). Now, $h'' \equiv g'^{\alpha_1} \mod p$ and by congruence (5), $\alpha_1 = 1$. So,

$$\alpha \equiv 3 \mod 4 \ . \qquad (9)$$

Finally, to combine congruences (1), (3), (8) and (9) using the Chinese remainder theorem, we need $516^{-1} \mod 293$ and $3516^{-1} \mod 43$ ($37797^{-1} \equiv 1 \mod 4$ and $50396^{-1} \equiv 2^{-1} \equiv 2 \mod 3$).

From congruence (1) we get $516^{-1} \equiv 223^{-1} \equiv 113 \mod 293$ and from congruence (4) we get $3516^{-1} \equiv 33^{-1} \equiv 30 \mod 43$. Therefore,

$\alpha = 270 \cdot 516 \cdot 113 + 4 \cdot 3516 \cdot 30 + 3 \cdot 37797 \cdot 1 + 2 \cdot 50396 \cdot 2 \equiv 563 \mod p - 1$. □

Problem 4. a) Since textbook RSA is not randomized, anyone can encrypt "Yes" and "No" to learn the corresponding ciphertexts and thus what Alice sends to Bob, even if the decryption exponent is unconditionaly secret. ElGamal, on the other hand, is randomized and even if the message space is as small as {Yes,No}, if computing discrete logarithms is intractable modulo the prime used, the previous approach cannot be applied. Hence Alice's choice could be appropriate.

b) Given an unsigned ElGamal ciphertext $(y_1, y_2) = (g^r, mg^{\alpha r})$, due to its homomorphic property, an adversary can modify it by multiplying the second component by anything. For example, $(y_1, cy_2) = (g^r, cmg^{\alpha r})$ would decrypt to cm. Another way is to raise both components to some power. For example $(y_1^x, y_2^x) = (g^{xr}, m^x g^{\alpha x r})$ would decrypt to m^x.

Let's consider the first approach. What Eve is looking for is for a c such that $cY \equiv N \mod p$ and $cN \equiv Y \mod p$, where Y and N are the encodings of "Yes" and "No" respectively. Combining the two congruences gives $c^2Y \equiv Y \mod p$ i.e. $c^2 \equiv 1 \mod p$ which means $c \equiv \pm 1 \mod p$. The non-trivial case is $c \equiv -1 \mod p$ which further implies $N \equiv -Y \mod p$. Since the encoding chosen satisfies this ($17173 + 6546 = p$), Eve will achieve her goal by sending $(5844, -1279 \mod p) = (5844, 22440)$.

In the second approach Eve would be looking for an exponent x such that $Y^x \equiv N \mod p$ and $N^x \equiv Y \mod p$. Combining them we get $Y^{x^2} \equiv Y \mod p$ implying $x^2 \equiv 1 \mod p - 1$, i.e. $x \equiv \pm 1 \mod p - 1$. The non-trivial case is $x \equiv -1 \mod p - 1$ in which case $Y^{-1} \equiv N \mod p$. This is not the case with the encoding used here. □