MTH6115 Cryptography Exercises 6 Solutions

Q1 We consider 1001000 as the binary representation of the integer $x = 2^6 + 2^3 = 72$. We have $T_{e_B}(x) \equiv x^{e_B} \pmod{77}$. Since $e_B = 23 = 2^4 + 2^2 + 2^1 + 2^0$ we may calculate $x^{23} \pmod{77}$ by calculating x^{2^i} for all $0 \leq i \leq 4$. We have $72^2 \equiv 25 \pmod{77}$, $72^{2^2} \equiv 25^2 \equiv 9 \pmod{77}$, $72^{2^3} \equiv 9^2 \equiv 4 \pmod{77}$, and $72^{2^4} \equiv 4^2 \equiv 16 \pmod{77}$. Hence

$$\begin{aligned} 72^{23} &= 72^{2^4+2^2+2+1} = 72^{2^4} \times 72^{2^2} \times 72^{2^1} \times 72^{2^0} \\ &\equiv 16 \times 9 \times 25 \times 72 \equiv 67 \times 25 \times 72 \equiv 58 \times 72 \equiv 18 \pmod{77} \end{aligned}$$

Thus $T_{e_B}(x) = 18$. We obtain the ciphertext by taking the binary expansion of 18. Since $18 = 2^4 + 2^1$ the ciphertext is 0010010. [20]

(b) Since $N_B = 77 = 7 \times 11$ we have $p_B = 7$ and $q_B = 11$. Thus $\lambda(77) = \text{lcm}(6, 10) = 30$. We next calculate d_B, the inverse of $e_B = 23$ in $\mathbb{Z}_{30}$ by Euclid's algorithm. We have $30 = 23 + 7$, $23 = 3 \times 7 + 2$, and $7 = 3 \times 2 + 1$. Hence

$$\begin{aligned} 1 &= 7 - 3 \times 2 = 7 - 3 \times (23 - 3 \times 7) = 10 \times 7 - 3 \times 23 \\ &= 10 \times (30 - 23) - 3 \times 23 = 10 \times 30 - 13 \times 23 \end{aligned}$$

So $d_b \equiv -13 \equiv 17 \pmod{30}$. The ciphertext 0100011 is a binary representation of $T_{e_B}(x)$. Thus $T_{e_B}(x) = 2^5 + 2^1 + 2^0 = 35$. Hence

$$x = T_{d_B}(T_{e_B}(x)) = T_{d_B}(35) \equiv 35^{17} \pmod{77}$$

Since $d_B = 17 = 2^4 + 2^0$ we may calculate $35^{17} \pmod{77}$ by calculating 35^{2^i} for all $0 \leq i \leq 4$. We have $35^2 \equiv 70 \pmod{77}$, $35^{2^2} \equiv 70^2 \equiv 49 \pmod{77}$, $35^{2^3} \equiv 49^2 \equiv 14 \pmod{77}$, and $35^{2^4} \equiv 14^2 \equiv 42 \pmod{77}$. Hence

$$35^{17} = 35^{2^4+1} = 35^{2^4} \times 35 \equiv 42 \times 35 \equiv 7 \pmod{77}$$

Thus $x = 7$. The plaintext is obtained by taking the binary representation of x. Since $7 = 2^2 + 2 + 1$, the plaintext is 0000111. [20]

Eve can determine the plaintext easily because N_B is so small that the prime factorization of N_B is obvious. [5]

Q2 Let $n = 3589$ and suppose that $n = pq$ is the prime factorization of n where $p > q$. We know that $\lambda(n) = 288$. Hence $2\lambda(n) = 576$ and $n \equiv 133 \pmod{576}$. From lectures we know that $2\lambda(n) = 2\mathrm{lcm}(p-1, q-1)$ divides $\phi(n) = (p-1)(q-1)$. Thus $n - \phi(n) \equiv 133 \pmod{576}$. Since

$$n-\phi(n) = pq-(p-1)(q-1) = p+q-1 < 2(p-1) \leq 2\mathrm{lcm}(p-1, q-1) = 2\lambda(n)$$

this implies that $n - \phi(n) = 133$. Thus $p + q - 1 = 133$. Since $pq = 3589$ we have $q = 3589/p$ and hence $p + 3589/p = 133 + 1 = 134$. Thus $p^2 - 134p + 3589 = 0$. We may solve this quadratic to obtain $p = 37$ or $p = 97$. We now check that $3589 = 37 \times 97$ is indeed the prime factorization of n. [15]

Q3 (a) Suppose xy has order k in $\mathbb{Z}_n$. We have

$$(xy)^{st} = x^{st}y^{st} = (x^s)^t(y^t)^s \equiv 1 \pmod{n}$$

since x has order s and y has order t. Using a lemma from lecture notes, we deduce that k divides st. On the other hand, since xy has order k and x has order s,

$$1 \equiv (xy)^{sk} = x^{sk}y^{sk} \equiv y^{sk} \pmod{n}$$

Again, by the lemma, t must divide sk. Since t and s are coprime, this implies that t divides k. Similarly s divides k. Since s and t are coprime, st must divide k. Thus $st = k$. [30]

I E-MAILED THE CLASS TO NOTIFY THEM THAT PART (b) OF THIS QUESTION IS FALSE AND THAT THE MARKS FOR PARTS (b), (c) and (d) WOULD BE TRANSFERRED TO PART (a). PLEASE GIVE 10 BONUS MARKS TO ANYONE WHO GIVES A CORRECT SOLUTION TO (c) AND/OR (d). ONE WAY TO REPAIR MY PROOF WOULD BE USE THE FOLLOWING MODIFICATION OF (b).

(b*) Let $d = \gcd(s, t)$. We show that $\mathbb{Z}_n$ has an element of order $st/d = \mathrm{lcm}(s, t)$.

Using the prime factorisations of s and t, it can be seen that there exists a divisor s' of s and a divisor t' of t such that $\gcd(s', t') = 1$ and $st/d = s't'$. Now let $p = s/s'$ and $q = t/t'$ and consider $x^p y^q$. We have x^p has order s' and y^q has order t', so by (a), $x^p y^q$ has order $s't' = st/d$.

(c) By (b*), $\mathbb{Z}_n$ has an element of order st/d. The choice of y now implies that $st/d \leq t$. Since d divides s, we must have $d = s$. Thus s divides t.

(d) Suppose y is chosen to have maximum order in $\mathbb{Z}_n$. By (c), s divides t and hence $x^t \equiv 1 \pmod{n}$. Since this holds for all $x \in \mathbb{Z}_n$ which are coprime to n, we have $\lambda(n) \leq t$. On the other hand y has order t so $y^i \not\equiv 1 \pmod{n}$ for all $1 \leq i \leq t-1$. Thus $\lambda(n) \geq t$. Hence $\lambda(n) = t$ and y is an element of $\mathbb{Z}_n$ of order $\lambda(n)$.

Q4 Bob takes $N_B = p_B q_B$. He then chooses his exponent e_B to be coprime to $L = \operatorname{lcm}(p_B - 1, q_B - 1)$ and chooses d_B to be the inverse of e_B in $\mathbb{Z}_L$. If p_B were not prime then we may not have $\lambda(N_B) = L$. Hence we could not be sure that that the encryption map T_{e_B} was invertible and that T_{d_B} was its inverse. Thus Bob's decryption of received messages may not be correct. [10]