MTH6115 **Cryptography**

Solutions 9

---

1 By Question 7 we have $\lambda(256)|64$. To prove the equality, we find an odd number a such that $a^{32} \not\equiv 1 \pmod{256}$. The following calculation shows that $a = 5$ has this property:

$$5^1 \equiv 5, \quad 5^2 \equiv 25, \quad 5^4 \equiv 625 \equiv 113, \quad 5^8 \equiv 113^2 \equiv 12769 \equiv -31,$$
$$5^{16} \equiv (-31)^2 \equiv 961 \equiv -63, \quad 5^{32} \equiv (-63)^2 \equiv 3969 \equiv -127 \not\equiv 1.$$

2 $\lambda(1000000) = \text{lcm}(\lambda(2^6), \lambda(5^6)) = \text{lcm}(2^4, 4 \cdot 5^5) = 2^4 \times 5^5 = 50000$. The other values are given below.

n	120	121	122	123	124	125	126	127	128	129	130
$\lambda(n)$	4	110	60	40	30	100	6	126	32	42	12

Some sample calculations are $\lambda(120) = \text{lcm}(\lambda(2^3), \lambda(3), \lambda(5)) = \text{lcm}(2, 2, 4) = 4$ amd $\lambda(126) = \text{lcm}(\lambda(2), \lambda(3^2), \lambda(7)) = \text{lcm}(1, 6, 6) = 6$.

3 We have $\lambda(130) = 12$. So we have to solve $7d \equiv 1 \pmod{12}$. The answer is $d \equiv 7 \pmod{12}$, i.e. T_7 is its own inverse mod 130.

4 We have $N = pq = 7571$ and $\phi(N) = (p-1)(q-1) = pq - p - q + 1 = 7392$. Therefore $p + q = 7571 - 7392 + 1 = 180$. So p and q are solutions of the equation

$$x^2 - 180x + 7571 = 0$$

Solving this we find $p, q = 67, 113$. It is easy to check that $67 \cdot 113 = 7571$.

5 We have $N = 713057 = pq$ where $2 < p < q$ primes, and $\lambda(N) = 88920 = \text{lcm}(p-1, q-1)$. The residue of division of $N = 713057$ by $2 \cdot \lambda(N) = 177840$ is $r = 1697$. So p and q are solutions of the equation

$$x^2 - 1698x + 713057 = 0$$

Solving this we find $p, q = 761, 937$. It is easy to check that $761 \cdot 937 = 713057$.

6 We have $de - 1 = 132 = 4 \cdot 33$. Apply the algorithm with $x = 2$. We have $\gcd(2, 299) = 1$. Let $y = 70 \equiv 2^{33} \pmod{299}$. (Note that $2^{33} \pmod{299}$ is easy to calculate because $33 = 2^5 + 1$.) Then $z = 70^2 \equiv 116 \pmod{229}$ has the property that $z^2 \equiv 1 \pmod{299}$. So 299 divides $116^2 - 1 = 115 \cdot 117$. From this we find the factors of 299 to be $\gcd(115, 299) = 23$ and $\gcd(117, 299) = 13$. So, $299 = 13 \cdot 23$.

7 a) Let $m = q\lambda(N) + r$, where $0 \leqslant r < \lambda(N)$ is the residue of the division of m by $\lambda(N)$. For every a coprime to N we have

$$a^r \equiv a^{m-q\lambda(N)} \equiv (a^m)(a^{\lambda(N)})^{-q} \equiv 1 \cdot 1 \equiv 1 \pmod{N}.$$

Since $\lambda(N)$ is the smallest positive integer with this property, we must have $r = 0$, that is, $\lambda(N)|m$.

b) First we prove the case $n = 3$. We have $a^2 - 1 = (a-1)(a+1)$. Both factors are even, so $a^2 - 1$ is divisible by 4. In fact, one of $a-1$ and $a+1$ is divisible by 4 (why?), so $a^2 - 1$ is divisible by 8, as desired. Now suppose $a^{2^{n-2}} - 1$ is divisible by 2^n. We have

$$a^{2^{n-1}} - 1 = (a^{2^{n-2}} - 1)(a^{2^{n-2}} + 1).$$

By the induction hypothesis, the first factor is divisible by 2^n. The second factor is even. Therefore, $a^{2^{n-1}} - 1$ is divisible by 2^{n+1}. This complete the induction step.

It follows from Part (a) that $\lambda(n)|2^{n-2}$.