Solution Sheet 4

Cryptography and Security 2022

Solution 1 Capitain's Age

1.
$$\begin{array}{lcl} x \equiv 1 \bmod 3 & & x \equiv 1 \bmod 3 \\ x \equiv -2 \bmod 5 & \Rightarrow & x \equiv 3 \bmod 5 \\ x \equiv -4 \bmod 7 & & x \equiv 3 \bmod 7 \end{array}$$

$$\begin{array}{l} M = 105 \\ M_1 = 35 \rightarrow M_1' = 35^{-1} \bmod 3 = 2 \\ M_2 = 21 \rightarrow M_2' = 21^{-1} \bmod 5 = 1 \\ M_3 = 15 \rightarrow M_3' = 15^{-1} \bmod 7 = 1 \end{array}$$

so,

$$x \equiv 1 * 35 * 2 + 3 * 21 * 1 + 3 * 15 * 1 \bmod 105 \rightarrow x \equiv 73 \bmod 105$$

As a result, $x = 73$.

2.
$$\begin{array}{lcl} 3x \equiv 4 \bmod 7 & & x \equiv 6 \bmod 7 \\ 2x \equiv 10 \bmod 26 & \Rightarrow & x \equiv 5 \bmod 13 \\ 4x \equiv 12 \bmod 20 & & x \equiv 3 \bmod 5 \end{array}$$

so, we have

$$\begin{array}{l} M = 455 \\ M_1 = 65 \rightarrow M_1' = 65^{-1} \bmod 7 = 4 \\ M_2 = 35 \rightarrow M_2' = 35^{-1} \bmod 13 = 3 \\ M_3 = 91 \rightarrow M_3' = 91^{-1} \bmod 5 = 1 \end{array}$$

As a result,

$$x \equiv 6 * 65 * 4 + 5 * 35 * 3 + 3 * 91 * 1 \bmod 455 \rightarrow x \equiv 83 \bmod 455$$

Solution 2 Ambiguous Power

1. Since p and q are different prime numbers, they are coprime. So, we can use the Chinese remainder theorem. Let $\alpha = q(q^{-1} \bmod p)$ and $\beta = p(p^{-1} \bmod q)$. The number $z = 3\alpha + 5\beta$ is such that $z \bmod p = 3$ and $z \bmod q = 5$.

2. Since $\frac{p-1}{2}$ and $\frac{q-1}{2}$ are odd and coprime, 2, $\frac{p-1}{2}$, and $\frac{q-1}{2}$ are coprime. So, we can use the Chinese remainder theorem and find e such that $e \bmod 2 = 1$, $e \bmod \frac{p-1}{2} = 3$ and $e \bmod \frac{q-1}{2} = 5$. Clearly, e and 3 are equal modulo 2 and modulo $\frac{p-1}{2}$, so they are equal modulo $p-1$. Similarly, e and 5 are equal modulo 2 and modulo $\frac{q-1}{2}$, so they are equal modulo $q-1$. So, $x^e \equiv x^{e \bmod (p-1)} \equiv x^3 \pmod p$ and $x^e \equiv x^{e \bmod (q-1)} \equiv x^5 \pmod q$.

3. Let $\alpha = 15$, $\beta = 10$, and $\gamma = 6$. We take $e = \alpha + 0\beta + 0\gamma = 15$ and obtain $e \bmod 2 = 1$, $e \bmod 3 = 3 \bmod 3$, and $e \bmod 5 = 5 \bmod 5$. We can check that $e \bmod 6 = 3$ and $e \bmod 10 = 5$.

4. For such e to exist, it is necessary that $e \equiv e_p \pmod{p-1}$ and $e \equiv e_q \pmod{q-1}$. Since both $p-1$ and $q-1$ are even, it is necessary that $e \equiv e_p \pmod 2$ and $e \equiv e_q \pmod 2$. So, it is necessary that $e_p \equiv e_q \pmod 2$.

   This condition is also sufficient: if $e_p \equiv e_q \pmod 2$, we construct using the Chinese remainder theorem e such that $e \equiv e_p \pmod 2$ (so, we also have $e \equiv e_q \pmod 2$), $e \equiv e_p \pmod{\frac{p-1}{2}}$, and $e \equiv e_q \pmod{\frac{q-1}{2}}$. Since $e \equiv e_p \pmod 2$ and $e \equiv e_p \pmod{\frac{p-1}{2}}$, we deduce $e \equiv e_p \pmod{p-1}$. So, $x^e \equiv x^{e_p} \pmod p$. Similarly, we have $e \equiv e_q \pmod{q-1}$. So, $x^e \equiv x^{e_q} \pmod q$.

Solution 3 RSA with exponent 3

1. p, q are prime numbers more than 3, so it is clear than can not be multiple of 3.
2. $gcd(e, \phi(n)) = 1$.
3. $gcd(e, \phi(n)) = 1$, so $gcd(e, (p-1)(q-1)) = 1$, if $p-1$ or $q-1$ is a multiple of 3, then $gcd(e, (p-1)(q-1)) = 3$, which is a contradiction.
4. $3 \nmid p$ and $3 \nmid p-1$, so $3 \mid p-2$, the same applies to q.
5. $p = 3k+2$ and $q = 3k'+2$, so $n \bmod 3 = pq \bmod 3 = 1$.
6. Simply as a result of $10 \bmod 3 = 1$.
7. $n \bmod 3$ should be 1, while for the given n, we have $n \bmod 3 = 2$.

Solution 4 Find my B'day

In 2010, January 1st was a Friday. My birthday that Spring was a Monday. If every months had 30 days, it would have been the 5th day of a month. When was it?
Assign 0 to Friday, 1 to Saturday, 2 to Sunday, 3 to Monday and so on. Also number every day of the year starting with 0 for January 1st. Let x be the number of my birthday. Since it was a Monday, we have $x \bmod 7 = 3$. Since it was the 5th of a month in a calendar with 30 days per month, we have $x \bmod 30 = 4$. We observe that 7 and 30 are coprime. Thanks to the Chinese Remainder Theorem, we can compute $x \bmod 210$. We obtain

$$x \equiv 3 \cdot 30 \cdot (30^{-1} \bmod 7) + 4 \cdot 7 \cdot (7^{-1} \bmod 30) \pmod{210}$$

Since $30 \bmod 7 = 2$ and $2 \times 4 \bmod 7 = 1$, we have $30^{-1} \bmod 7 = 4$. Similarly, since $13 \times 7 = 91$ and $91 \bmod 30 = 1$ we have $7^{-1} \bmod 30 = 13$. Now, we compute

$$x \equiv 3 \cdot 30 \cdot 4 + 4 \cdot 7 \cdot 13 \pmod{210}$$

so $x = 724 \bmod 210 = 94$. Since there are 365 days in a year, we have $0 \leq x < 365$ and $x \bmod 210 = 94$, we have $x = 94$ or $x = 304$. That is, the birthday can either be the 95th or 305th day of the year, which is either April 5th or October 31st. We know that it was in Spring, so it is April 5th.