Cryptography and Security 2017

Exercise Sheet 4

Exercise 1 Captain's Age

1. The aim of this exercise is to find the very secret age of the Captain. The only information we know is that one year ago, his age was a multiple of 3, in 2 years it will be a multiple of 5, and in 4 years it will be a multiple of 7. Deduce the Captain's age.
   Hint: Maybe the Captain is Chinese...

2. Solve the following system of congruence equations:

$$\begin{aligned} 3x &\equiv 4 \bmod 7 \\ 2x &\equiv 10 \bmod 26 \\ 4x &\equiv 12 \bmod 20 \end{aligned}$$

Exercise 2 Ambiguous Power

We let $n = pq$ be the product of two different prime numbers p and q. We assume that $\frac{p-1}{2}$ and $\frac{q-1}{2}$ are odd and coprime.

1. Show that there exists $z \in \mathbb{N}$ such that $z \equiv 3 \pmod{p}$ and $z \equiv 5 \pmod{q}$ and give a method to compute it.

2. Explain how to find some exponent $e \in \mathbb{N}$ such that for every $x \in \mathbf{Z}_n^*$, we have $x^e \equiv x^3 \pmod{p}$ and $x^e \equiv x^5 \pmod{q}$.

   NOTE: we do expect a complete mathematical proof for this question.

3. Application: find such e for $p = 7$ and $q = 11$.

4. More generally, under which condition on $e_p \in \mathbb{N}$ and $e_q \in \mathbb{N}$ does some $e \in \mathbb{N}$ exist such that $x^e \equiv x^{e_p} \pmod{p}$ and $x^e \equiv x^{e_q} \pmod{q}$ for all $x \in \mathbf{Z}_n^*$?

Exercise 3 RSA with exponent 3

In this exercise we consider an RSA modulus $n = pq$ where p and q are large prime numbers (here, by large we mean at least equal to 5). We consider a valid RSA exponent e for RSA.

1. Show that neither ($p \bmod 3$) nor ($q \bmod 3$) can be equal to 0.

2. Under which condition e is a valid exponent for a modulus n?

3. From now on, we will assume that $e = 3$. Show that neither $p - 1$ nor $q - 1$ can be multiples of 3.

4. Deduce that $p \bmod 3 = q \bmod 3 = 2$.

5. What is the value of $n \bmod 3$?

6. For any digits $d_0, ..., d_{\ell-1}$, show that

$$\left(\sum_{i=0}^{\ell-1} d_i 10^i\right) \bmod 3 = \left(\sum_{i=0}^{\ell-1} (d_i \bmod 3)\right) \bmod 3$$

7. Show that $e = 3$ is not a valid RSA exponent for the following RSA modulus:

$$n = 777575993$$