TMA4155 — Exercise 6

Kristian Gjøsteen

2006-10-05

Task 1 — Chinese Remainder Theorem

Find a solution to these equations:

$$\begin{cases} a \equiv 1 \pmod 2 \\ a \equiv 2 \pmod 3 \\ a \equiv 3 \pmod 5 \\ a \equiv 4 \pmod 7 \end{cases}$$

Can you find a solution to these equations?

$$\begin{cases} a \equiv 1 \pmod 2 \\ a \equiv 2 \pmod 3 \\ a \equiv 2 \pmod 4 \\ a \equiv 4 \pmod 5 \\ a \equiv 5 \pmod 7 \end{cases}$$

What about these?

$$\begin{cases} a \equiv 1 \pmod 2 \\ a \equiv 2 \pmod 3 \\ a \equiv 3 \pmod 4 \\ a \equiv 4 \pmod 5 \\ a \equiv 5 \pmod 7 \end{cases}$$

How many solutions can you find in the set $\{0, 1, 2, \ldots, 2 \cdot 3 \cdot 4 \cdot 5 \cdot 7 - 1\}$.

Task 2 — RSA Cryptanalysis

Alice sends the same message m to Bob, Carol and David encrypted with their RSA public keys $(n_B, 3)$, $(n_C, 3)$ and $(n_D, 3)$, respectively, getting ciphertexts c_B, c_C, and c_D.

Show how you can use the Chinese Remainder Theorem to find the message m. (You can assume that n_B, n_C and n_D are pairwise relatively prime.)

Task 3 — Exponentiation

a. Compute $z = 2^{8500} \bmod 10403$ using a standard exponentiation algorithm.

b. Notice that $10403 = 101 \cdot 103$. Show that if you know $x = 2^{8500} \bmod 101$, $y = 2^{8500} \bmod 103$, you can recover $2^{8500} \bmod 10403$ using the Chinese Remainder Theorem.

c. Use Fermat's Little Theorem and exponent arithmetic to simplify the computation of x and y.

d. Compute x, y and then z. Compare the work required for this computation with the work required in **a.**

Estimate the workloads when the modulus n satisfies $2^{2k-1} < n < 2^{2k}$, and the two factors p, q satisfy $2^{k-1} < p, q < 2^k$.

e. Show how these techniques can be used to speed up RSA decryptions if the prime factors of n are part of the secret key.

Task 4 — Exponent Arithmetic I

Compute:

a. $2^{327897432167843274891243} \bmod 11$.

b. $2^{3712907781467891624823478921 1} \bmod 101$.

Task 5 — Exponent Arithmetic II

a. Compute $x = 2^7 \bmod 11$ and then $x^5 \bmod 11$.

b. Compute $y = 2^5 \bmod 11$ and then $y^7 \bmod 11$.

c. Explain the similarity between the previous answers.