DM534 — Øvelser Uge ??

Introduktion til Datalogi, Efterår 2021

Jonas Vistrup

---

1 I

1.1

We consider the RSA system and use the notation and algorithms from the slides. Let $N_A = 1517$ and $e_A = 13$.

- Encrypt the message m = 43. For the modular exponentiation, use the algorithm from the slides, page 30. Show all steps in your computation.
- If you had created the keys yourself, you would know that $p = 37$ and $q = 41$. From this information and $e_A = 13$, find the secret key d_A. Use the Extended Euclidean Algorithm from pages 47-48 of the RSA slides used in lectures (there, e and d are called a and s (and d also is called x at top of page 48)). Show all steps in your computation.

SVAR a:

$$
\begin{aligned}
43^{13} \mod 1517 &= 43 \cdot z_1 \mod 1517 \\
z_1 &= 43^{12} \mod 1517 = c_1 \cdot c_1 \mod 1517 \\
c_1 &= 43^{6} \mod 1517 = c_2 \cdot c_2 \mod 1517 \\
c_2 &= 43^{3} \mod 1517 = 43 \cdot z_2 \mod 1517 \\
z_2 &= 43^{2} \mod 1517 = c_3 \cdot c_3 \mod 1517 \\
c_3 &= 43 \mod 1517 = 43 \\
z_2 &= 43 \cdot 43 \mod 1517 = 332 \\
c_2 &= 43 \cdot 332 \mod 1517 = 623 \\
c_1 &= 623 \cdot 623 \mod 1517 = 1294 \\
z_1 &= 1294 \cdot 1294 \mod 1517 = 1185 \\
43^{13} \mod 1517 &= 43 \cdot 1185 \mod 1517 = 894
\end{aligned}
$$

SVAR b: Initialize

$d_0 \leftarrow (37-1)\cdot(41-1) = 1440$, $d_1 \leftarrow 13$, $s_0 \leftarrow 0$, $s_1 \leftarrow 1$, $t_0 \leftarrow 1$, $t_1 \leftarrow 0$, $n \leftarrow 1$.

Cycle 1:

$$\begin{aligned} n &= 2 \\ q_2 &= \lfloor d_0/d_1 \rfloor = \lfloor 1440/13 \rfloor = 110 \\ d_2 &= d_0 - q_2 \cdot d_1 = 1440 - 110 \cdot 13 = 10 \\ s_2 &= s_0 - q_2 s_1 = 0 - 110 \cdot 1 = -110 \\ t_2 &= t_0 - q_2 t_1 = 1 - 110 \cdot 0 = 1 \end{aligned}$$

Cycle 2:

$$\begin{aligned} n &= 3 \\ q_3 &= \lfloor d_1/d_2 \rfloor = \lfloor 13/10 \rfloor = 1 \\ d_3 &= d_1 - q_3 \cdot d_2 = 13 - 1 \cdot 10 = 3 \\ s_3 &= s_1 - q_3 s_2 = 1 - 1 \cdot -110 = 111 \\ t_3 &= t_1 - q_3 t_2 = 0 - 1 \cdot 1 = -1 \end{aligned}$$

Cycle 3:

$$\begin{aligned} n &= 4 \\ q_4 &= \lfloor d_2/d_3 \rfloor = \lfloor 10/3 \rfloor = 3 \\ d_4 &= d_2 - q_4 \cdot d_3 = 10 - 3 \cdot 3 = 1 \\ s_4 &= s_2 - q_4 s_3 = -110 - 3 \cdot 111 = -443 \\ t_4 &= t_2 - q_4 t_3 = 1 - 3 \cdot -1 = 4 \end{aligned}$$

Cycle 4:

$$\begin{aligned} n &= 5 \\ q_5 &= \lfloor d_3/d_4 \rfloor = \lfloor 3/1 \rfloor = 3 \\ d_5 &= d_3 - q_5 \cdot d_4 = 3 - 3 \cdot 1 = 0 \\ s_5 &= s_3 - q_5 s_4 = 111 - 3 \cdot -443 = 1440 \\ t_5 &= t_3 - q_5 t_4 = -1 - 3 \cdot 4 = -13 \end{aligned}$$

$s = s_{n-1} = s_4 = -443$. To make the result positive add m (1440).

$$d_A = -443 + 1440 = 997$$

1.2

Why in RSA is it necessary that $gcd(e_A, (p_A - 1)(q_A - 1)) = 1$? Find an example (that is, values e_A, p_A and q_A) where this greatest common divisor is not equal to 1.

SVAR: If $gcd(e_A, (p_A - 1)(q_A - 1)) \neq 1$, then there exist no multiplicative inverse for e_A mod $(p_A - 1)(q_A - 1)$.

1.3

Try executing the Miller-Rabin primality test on 11, 15, and 561. First, what type of numbers are they (note: 561 is known from the slides)? For each, run the Miller-Rabin test for at least one value a of your own choice, preferably for more. Use e.g. Maple or a simple Java program importing the class **BigInteger** from the Java library for executing the exponentiations (first raising to a power and then using modulus should work in reasonable time for numbers this size, hence there is no need to use the fast modular exponentiation algorithm in this exercise). Which calculations showed that the composite numbers were not prime—the first line (the Fermat test) or later lines?

SVAR: 11 is prime. 15 and 561 is composite.

With 561, be sure to try an a relatively prime to 561 (most are, 2 is a simple example). What happens differently if you try $a = 3$? Can you explain the latter?

SVAR: Siden $561 = 3 \cdot 11 \cdot 17$, så er 561 og 3 ikke relativ prime, derfor bliver den fanget af den første gennemkørsel.

1.4

Find four different square roots of 1 modulo 143, i.e., numbers which multiplied by themselves modulo 143 give 1 (and which are at least 0 and less than 143). You may consider writing a simple program for finding them.

SVAR: 1, 12, 131 og 142.

1.5

[Optional] Add two of these different square roots which are not negatives of each other modulo 143 (two where adding them together does not give 143). Find the greatest common divisor of this result and 143. Subtract these same two different square roots and find the greatest common divisor of this result and 143. Think about why you get these results. (These effects are the starting point for the math behind fast primality testing algorithms.)

$1 + 12 = 13$. $gcd(13, 143) = 13$.

$12 - 1 = 11$. $gcd(11, 143) = 11$. TODO: Spørg om fulde forklaring hvorfor.

$$a \cdot a \equiv 1(\mod p) \text{ and } b \cdot b \equiv 1(\mod p)$$
$$a^2 - b^2 \equiv 1 - 1 \equiv 0(\mod p)$$
$$(a + b)(a - b) \equiv 0(\mod p)$$
$$(a + b)(a - b) = k \cdot p$$
$$a + b < 2p$$