

## Exercise sheet 5, 12 December 2024

For this exercise sheet you should not use your computer for more functions than a pocket calculator offers you (though with more digits) – unless explicitly stated. In particular the last exercises have numbers too big for your calculator. But, be mindful of your computer and do reduce when you can, not only at the end of a big calculation.

At the end there are some practice exercises to check up on your algebra and number theory knowledge. Skip these if you are confident in how to solve them – or keep them as a self test if you still need to (re-)learn the material.

1. RSA-encrypt the message 23 to a user with public key  $(e, n) = (17, 11584115749)$ . Document how you compute the exponentiation.

Note that in the exam you do not have a calculator that can compute  $m^e \bmod n$  but only multiplications, divisions, and additions.

2. Bob uses public key  $(n, e) = (443507, 11)$  and secret key  $d = 241187$ . He receives ciphertext  $c = 64649$ . Decrypt the ciphertext.
3. Users  $A, B$ , and  $C$  are friends of  $S$ . They have public keys  $(n_A, e_A) = (58483, 3)$ ,  $(n_B, e_B) = (50629, 3)$ , and  $(n_C, e_C) = (54253, 3)$ . You know that  $S$  sends the same message to all of them and you observe the ciphertexts  $c_A = 52106$ ,  $c_B = 7516$ , and  $c_C = 4649$ . What was the message?
4. Users  $X, Y$ , and  $Z$  are friends of  $P$ . They have public keys  $(n_X, e_X) = (680671, 3)$ ,  $(n_Y, e_Y) = (449341, 3)$ , and  $(n_Z, e_Z) = (499153, 3)$ . You know that  $P$  sends the same message to all of them and you observe the ciphertexts  $c_X = 132574$ ,  $c_Y = 185850$ , and  $c_Z = 18349$ . What was the message?

You are able to solve this exercise without asking your computer to factor a modulus; note that there is something weird about the moduli.

5. The m-RSA system is a multiplicative variant of RSA. To generate her keys, Alice picks integers  $a, b \in \mathbb{Z}$ , computes  $M = a \cdot b - 1$ , picks two more random integers  $a', b' \in \mathbb{Z}$ , and computes  $e = a' \cdot M + a$ ,  $d = b' \cdot M + b$ , and  $n = (e \cdot d - 1)/M$ . Her public key is  $(n, e)$  and her secret key is  $(n, d)$ .

If Bob wants to encrypt a message  $m$  to Alice, he looks up her public key  $(n, e)$  and computes  $c \equiv e \cdot m \pmod n$ .

Alice decrypts ciphertext  $c$  by computing  $m' \equiv c \cdot d \pmod n$ .

- (a) Show that  $n$  is an integer.
- (b) Show that  $m' \equiv m \pmod n$ .
- (c) Break the system.

6. For this exercise you should use a computer algebra system for all computation steps. Do not use it to factor the modulus.

Systems engineer Steve is tasked with setting up a new access control system for building access. The old system used DES with 56-bit keys and each user  $U$  already has a smart card which holds their personal access secret  $u$ . These per-user secrets are registered with the central computer.

Steve is concerned about Eve sniffing the connection and has learned that DES is outdated. The smart card offers support for RSA encryption, so he lets the server generate an RSA key pair  $(n, e)$  and  $(n, d)$  and puts  $(n, e)$  on the smart card along with the personal access secret  $u$  per user.

Because the smart card is a small computation device he chooses  $e = 3$  to make the encryption computation fast. He knows that short messages are risky with such a small exponent, so he devises a padding scheme. Finally he is concerned about Eve simply replaying a message, so he chooses to vary the padding.

Steve's scheme assumes that the smart card and the server can keep track of how many messages have been sent. He constructs the  $i$ -th message for user  $U$  with secret  $u$  as  $m_i = u \cdot 2^{123} + i$ , where  $u$  is taken as a 56-bit integer.

The server key is  $(n, e) = (1353040922319896710729948440742113526140662069124237571, 3)$ .

- (a) You are Bob. Your user secret is  $b = 13061228670230523$ . Compute  $m_i$  for  $i = 816$  and encrypt this plaintext to the server key.

- (b) You are Eve and observe three consecutive accesses by Victor. Find an attack to obtain Victor's user secret  $v$  given the consecutive ciphertexts

$$c_j = 817868348751031642943497115011670318530495923133069516,$$

$$c_{j+1} = 1202831025053489838135544835894714600198996260256957916,$$

and

$$c_{j+2} = 821851203597152318356997216923287395542225538689517412.$$

Explain how and why your attack works and use it to obtain  $v$ .

Hint: explore the algebraic relations between the ciphertexts knowing that they are consecutive and using the same  $v$ .

Note that you do not know  $j$  but it is significantly below  $2^{123}$  so  $v$  will be the top 56 bits of the plaintext you recover.

7. Read about the ROBOT attack <https://robotattack.org/>.

#### Practice exercises

1. Compute  $11^9 \bmod 35$  in two different ways: First compute  $11^9$  and then reduce modulo 35 and then compute it reducing modulo 35 whenever useful. Observe the time the computation takes you.

For the exponentiation with reduction you should use the *square-and-multiply method*.

2. State all elements in  $(\mathbb{Z}/12)^\times$ .
3. State all elements in  $(\mathbb{Z}/21)^\times$ .
4. Execute the RSA key generation where  $p = 239$ ,  $q = 433$ , and  $e = 23441$ .
5. Use the Chinese Remainder Theorem (see [video](#)) to find the smallest positive integer  $x$  satisfying the following system of congruences, should such a solution exist.

$$x \equiv 0 \pmod{3}$$

$$x \equiv 1 \pmod{5}$$

$$x \equiv 2 \pmod{8}$$