

## Cryptographic Protocols

SS 2016

Handout 3

*Exercises marked (\*) or (\*\*) will be checked by tutors.*

*We encourage submissions of solutions by small groups of up to four students.*

**Exercise 1:**

Compute the solutions of  $x^2 = 16 \pmod{77}$  using the Chinese Remainder Theorem.

**Exercise 2:**

Let  $N$  be a product of  $s$  distinct odd primes  $\{p_1, \dots, p_s\}$  and  $a \in \mathbb{Z}_N^*$ . How many solutions does the equation  $x^2 = a \pmod{N}$  have? How many solutions does this equation have if  $p_1 = 2$  and  $\{p_2, \dots, p_s\}$  are distinct odd primes as before?

**Exercise 3** (4 points):

(\*\*) Let  $p$  be an odd prime,  $N = p^2$  and  $a \in \mathbb{Z}_N^*$ . How many solutions does the equation  $x^2 = a \pmod{N}$  have? How to compute these, given the square roots of  $a$  modulo  $p$ ?

*Hint:* Write  $x \in \mathbb{Z}_N$  as  $x_0 + x_1 \cdot p$  for some  $x_0, x_1 \in \mathbb{Z}_p$ .

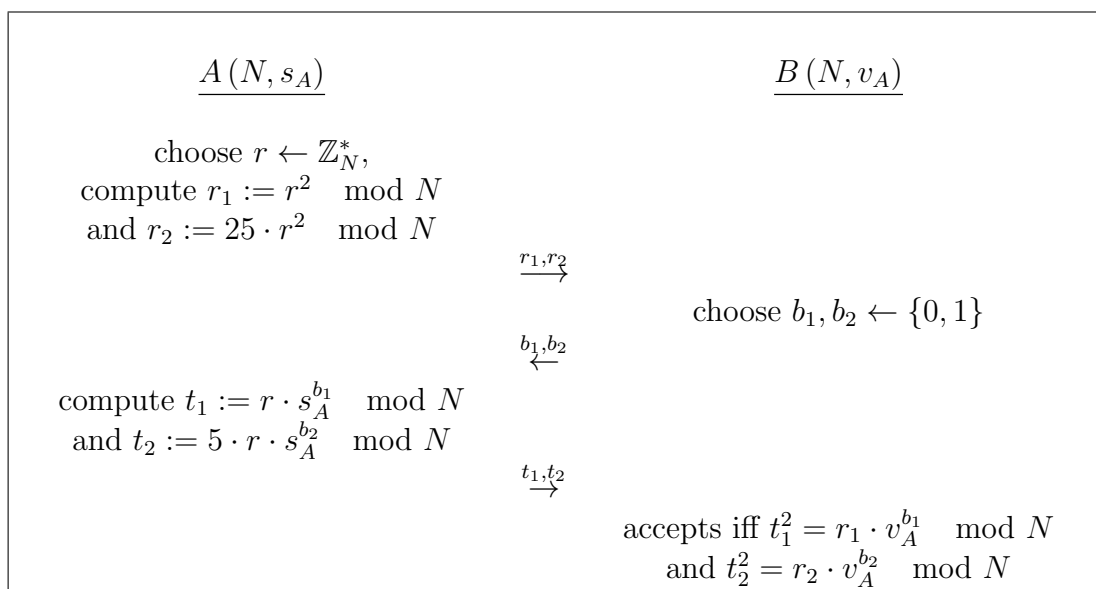
**Exercise 4:**

Consider the Fiat-Shamir identification protocol modified as follows.

**System parameters:** A trusted authority (TA) chooses RSA modulus  $N := p \cdot q$ .  $N$  is published to all participants.

**User parameters:** User  $A$  chooses a private  $s_A \leftarrow \mathbb{Z}_N^*$ . Her public key is  $v_A := s_A^2 \pmod{N}$ . (Furthermore, the TA issues a certificate that  $v_A$  really is the public key of  $A$ .)

**Protocol:** To prove the identity to  $B$ , the user  $A$  runs the following protocol:



(Furthermore, before starting the actual protocol,  $A$  sends  $v_A$  and the certificate issued by the TA to  $B$ . They only proceed if  $B$ 's verification of this certificate is successful.)

Show that:

- a) Correctness: If both  $A$  and  $B$  are honest,  $B$  will accept  $A$ 's identity.
- b) After running this protocol  $B$  can compute the secret key of  $A$  efficiently if  $B$  chooses the bits  $b_1, b_2$  appropriately.

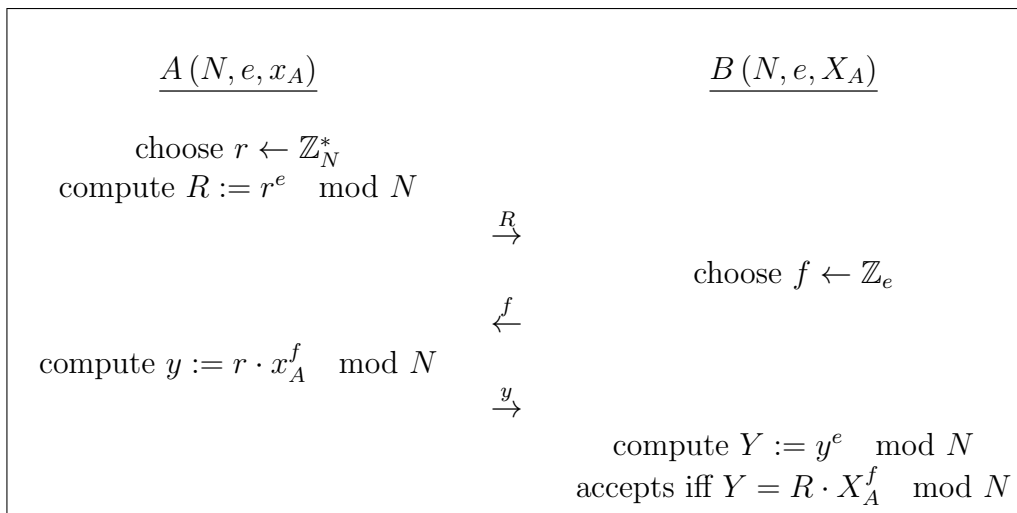
**Exercise 5** (4 points):

(\*\*) Consider the Guillou-Quisquater identification protocol which is based on RSA.

**System parameters:** A trusted authority (TA) chooses RSA parameters  $N := p \cdot q$  and some  $e \in \mathbb{Z}_{\phi(N)}^*$ . The parameters  $(N, e)$  are published to all participants.

**User parameters:** User  $A$  chooses a private  $x_A \leftarrow \mathbb{Z}_N^*$ . Her public key is  $X_A := x_A^e \pmod N$ . (Furthermore, the TA issues a certificate that  $X_A$  really is the public key of  $A$ .)

**Protocol:** To prove the identity to  $B$ , the user  $A$  runs the following protocol:



(Furthermore, before starting the actual protocol,  $A$  sends  $X_A$  and the certificate issued by the TA to  $B$ . They only proceed if  $B$ 's verification of this certificate is successful.)

Show that:

- a) Correctness: If both  $A$  and  $B$  are honest,  $B$  will accept  $A$ 's identity.
- b) Some evil  $C$  can successfully impersonate  $A$  if she can know  $B$ 's challenge  $f$  before the protocol starts. (This implies the existence of a  $1/e$ -forger which guesses  $f$  and successfully impersonates  $A$  if the guess was correct.)
- c) Analogously to the last exercise show how  $B$  can compute the secret key of  $A$ , when running the protocol twice with the same  $R$ .