Hand in: until monday 06.11.2023, before the lecture starts

Website: `http://reh.math.uni-duesseldorf.de/~khalupczok/krypto/`

Exercise 3: Fiat–Shamir's protocol

Let n be a natural number that is known to Alice and Bob. It is known that n is a product of two primes $p \neq q$, but these factors are unknown and so big that no-one can factorize n in reasonable time. Alice chooses a secret element s of $\mathbb{Z}_n^\times$.
She would like to convince Bob, that she knows the secret s, but without ever sharing it with others.
For this, Alice computes $v \equiv s^2 \bmod n$. She keeps s secret and makes v publically available, v is especially known to Bob. One could imagine that the data set n, v are availble on a public server.

One round of the protocol:

> Alice chooses a random element r of $\mathbb{Z}_n^\times$, keeps it secret and sends the square $x \equiv r^2 \bmod n$ to Bob. Bob chooses randomly a bit $b \in \{0, 1\}$, say by coin flip, and sends it to Alice. If $b = 0$, then Alice sends the value $y := r$ to Bob, otherwise the value $y :\equiv rs \bmod n$.
> Bob verifies her answer: He checks the correctness of $y^2 \equiv xv^b \bmod n$. If this is not correct, Bob would not acknowledge that Alice knows the secret s.

Since Alice knows the secret s, she can give the correct answer in both cases, since $y^2 \equiv (rs^b)^2 \equiv r^2 s^{2b} \equiv r^2 v^b \equiv xv^b \bmod n$.

• Show that a scammer Eve who pretends to be Alice, can answer correctly to exactly one of the questions $b = 0$ of $b = 1$ of Bob, by justifying the following claims.

(a) If Eve could answer both questions correctly by y_0 resp. y_1, she would know a square root of $v \bmod n$.

(b) If Eve assumes that Bob will send the bit b, she prepares her answer as follows: She sends $x \equiv r^2 v^{-b} \bmod n$ to Bob and then $y = r$. In such a way, Bob will not suspect anything in the case when Bob sends b, otherwise the verification will fail.

Due to (a), Eve can scam Bob with probability $\leq 1/2$, and due to (b), also with probability at least $1/2$. After t many rounds, the probabilty that Eve scams Bob is only $1/2^t$.

• Answer and justify:

(c) Assuming Eve knows the prime factors of n, can she answer correctly in each round and scam Bob like this?

(d) Who is allowed to know the prime factors of n, Alice or Bob?

• Choose conrete numbers p, q, r and perform one round of the protocol by explicit calculations.