5. Protokół identyfikacji Firsta-Shamina

I) Certyfikat ($x, Id_A, x=t^2 \bmod n$)

Protokół:

1. A losuje s i oblicza $y=s^2 \pmod n$, które przekazuje do B wraz z certyfikatem
2. B losuje $b \in \{0,1\}$
3. A odpowiada wartością $s*t^b \pmod n$
4. B sprawdza czy $(s*t)^2=y*x^b \pmod n$
5. Powtarzamy kroki I-IV k-krotnie (jak tak to prawdopodobieństwo uwierzytelnienia $A <= 0.5^k$

Zad 1.

Przeprowadzić protokół uwierzytelniania:

$n=3*11$

Cert=$(33, Id_A, x=7^2=16 \bmod 33)$

1) $s=5$ $y=25 \bmod 33$
2) $b=1$
3) $5*7 \pmod{33}=2$
4) $2^2=?=25*16 \pmod{33}$
   $P=(-8*2^4)=(-1)(-1)*2^2 \bmod 33 = 4$
   $b=0$, $y=25$
5) $7*5 \bmod 33$
6) $5^2=?=25 \pmod{33}$
   TAK