Cryptography HW 4

2) Zero Knowledge Proof

$p = 23 \quad \alpha = 5 \quad a = 7 \quad \beta \equiv \alpha^a \pmod p \qquad 7^5$

p, α, β are public

$2^4 = 16 \iff \log_2(16) = 4$

$5^7 = 78125 \qquad \log_5(78125) = 7$ → finding 7 (the secret exponent) requires solving discrete log problem

$5^7 \pmod{23} = 17 \qquad 17 \equiv 5^7 \pmod{23}$

PROOF: ($23-1=22$)

1) P picks a r in $[1 \dots p-1]$, sends $d = \alpha^r \bmod p \Rightarrow d = 5^r \pmod{23}$ (commit)
2) V sends a random challenge e in $[1 \dots 2^q]$ (challenge)
3) P sends $y = r - ea \pmod q \Rightarrow y = r - e7 \pmod{22}$, a is the secret P claims to know (response)
4) V verifies if $d = g^y c^e \bmod p$
5) Repeat steps 1-5 until V is convinced