VE475 Homework 6

Liu Yihao 515370910207

Ex. 1 — Application of the DLP

1. (a) For Alice, she knows that

$$\gamma \equiv \alpha^r \bmod p$$

If Bob replies

$$b \equiv r \bmod p-1 \text{ or } b \equiv x+r \bmod p-1$$

She can get

$$\alpha^{p-1} \equiv 1 \bmod p$$

$$\alpha^r \equiv \alpha^b \equiv \gamma \bmod p \text{ or } \alpha^r \equiv \alpha^{b-x} \equiv \gamma \bmod p$$

So after calculating $\alpha^b \bmod p$ or $\alpha^{b-x} \bmod p$ and compare it with γ, she can prove Bob's identity if he replies the correct b.

(b) For Bob, he doesn't know r, but he can compute $b = \log_\alpha \gamma$ or $b = \log_\alpha \gamma + x$ so that $b \equiv r \bmod p-1$. If he can't do so, it becomes a DLP problem which is very difficult to solve, so he can prove his identity.

2. (a)

(b)

3. It is Digital Signature Protocol.