Application Security

Exercise Set 6, Grizzlies

1. Find and present a zero-knowledge identification or authentication protocol. Check *Feige-Fiat-Shamir zero-knowledge protocol* and *Secure Remote Password*. How those are related to scheme based on digital certificates?

Potentially useful reading:

- `http://perso.crans.org/~raffo/papers/dc-and-ffs.pdf`
- `https://www.sans.org/reading-room/whitepapers/vpns/identification-zero-knowledge-protocols-719`
- `http://srp.stanford.edu/`
- `http://ojs.pythonpapers.org/index.php/tppm/article/view/155`

[10p]

Paweł Rajba