

# Identifikácia a autentifikácia

6. januára 2003

## Protokol pre identifikáciu užívateľa

- jedná sa o systém typu výzva odpoveď
1. Bob pošle Alici náhodný reťazec
  2. Alica pošle Bobovi výsledok z ich spoločnej funkcie  $f$  (kde použila ich spoločný kľúč  $k$ )
  3. Bob si spočíta tú istú funkciu a overí, že Alica je tá pravá (a zoberie si ju)

## Autentifikácia správy

- spočíta sa charakteristika správy a zakóduje sa kľúčom
- spolu so správou je charakteristika odoslaná Bobovi a ten si overí, že sa jedná o správnu správu výpočtom charakteristiky
- pri veľkých blokoch sa prevádza xor a bloky sa počítajú postupne

## Fiat-Shamir

- verejný kľúč:  $v$  a súkromný kľúč (Alicin):  $s^2 = v$
1. Alica si vyberie náhodné  $r < n$
  2. spočíta  $a = r^2 \bmod n$  a pošle  $a$  Bobovi
  3. Bob si vyberie náhodný bit  $z$  a pošle ho Alici
  4. Alica pošle Bobovi  $y = rs^z$
  5. Bob si overí, že:  $y^2 = av^z \bmod n$
- schéma sa dá rozšíriť podobne ako pri podpisovaní - namiesto  $s, b, v$  zoberieme vektory
1. Alica si vyberie náhodné  $r < n$
  2. spočíta  $a = r^2 \bmod n$  a pošle  $a$  Bobovi
  3. Bob si vyberie náhodný bitový reťazec  $z$  a pošle ho Alici
  4. Alica pošle Bobovi  $y = r \prod_{i=1}^k s_i^{z_i} \bmod n$
  5. Bob akceptuje, ak platí:  $y^2 = a \prod_{i=1}^k v_i^{z_i} \bmod n$
- tak ako pri podpisovacom algoritme, aj tu je bezpečnosť:  $2^{-kt}$

### Schnorrova identifikačná schéma

- najkôr je nutné dohodnúť sa s TA a tá zverejní: prvočísla  $p, q$ , a  $\alpha \in \mathbb{Z}_p$ ,  $2^t < q$
  - Alica si vymyslí náhodné  $a$ :  $0 \leq a \leq q - 1$
  - hodnotu:  $v = \alpha^{-a} \bmod p$  pošle TA
1. Alica si vyberie náhodné  $0 \leq k < q$
  2. spočíta:  $\gamma = \alpha^k \bmod p$
  3. Alica pošle certifikát  $C(Alica) = (ID(Alica), v, s)$  a  $\gamma$  Bobovi
  4. Bob si u autority overí  $ver_{TA}(C(Alica))$
  5. Bob si vyberie náhodné číslo:  $1 \leq r \leq 2^{lg q}$  a pošle ho Alici
  6. Alica spočíta:  $y = (k + ar) \bmod q$
  7. Bob checkne:  $\gamma \equiv \alpha^y v^r \bmod p$
- neexistuje dôkaz o bezpečnosti