Šifrovanie údajov – zadanie

- **Úloha 1:**
  - Vytvorte vlastný pár kľúčov použiteľný pre šifrovanie aj pre podpisovanie dokumentov
    - zvoľte maximálnu možnú veľkosť kľúča
    - pár by mal stratiť platnosť po 3 mesiacoch od vytvorenia
    - Exportujte svoj verejný kľúč a vymente si exportovaný kľúč s kolegom
    - Importujte si kľúč od kolegu do vašej kľúčenky
    - Overte odtlačok importovaného kľúča vo vašej kľúčenke s odtlačkom kolegu a podpíšte daný kľúč
- **Úloha 2:**
  - Zašifrujte a podpíšte bežný súbor asymetrickou šifrou.
    - Zašifrujte súbor tak, aby si jeho obsah dokázal prečítať kolega i Vy.
    - Správa a podpis by mali byť v jednom súbore.
  - Vymente si zašifrovaný súbor s kolegom, ktorého kľúč bol použitý na zašifrovanie súboru.
  - Dešifrujte obdržaný súbor a overte jeho obsah a podpis.
- Hodnotenie: 0,5 b za každú úlohu.

Šifrovanie komunikácie - zadanie

- **Úloha:**
  - Aktivujte na vašom stroji webovú konzolu ‘cockpit’.
  - Vytvorte tunel ktorý umožní cez verejne dostupný server na ktorý máte prístup (napr. 'student.fiit.stuba.sk') , urobiť spojenie z vonkajšej siete (napr. z domu) na webovú konzolu na vašom virtuálnom stroji (ktorý je za NAT a nemá verejnú IP adresu).
- Napríklad:
  - Spojenie na 'student.fiit.stuba.sk:9090' (alebo aspoň 'localhost:9090' na stroji 'student') bude presmerované na port, na ktorom počúva ‘cockpit’ vášho virtuálneho stroja.
- Demonštrujte správnu funkčnosť tunelu.
- Detailne vysvetlite fungovanie a význam takéhoto presmerovania.
- Hodnotenie: 1b

Zdroje

- man gpg
- https://www.gnupg.org/gph/en/manual.html
- http://www.spywarewarrior.com/uiuc/gpg/gpg-com-4.htm
- https://futureboy.us/pgp.html
- man ssh
- man sshd
- man ssh_config
- https://cockpit-project.org/
- man curl, wget, lynx