Univerzita Palackého
v Olomouci

BEZIT – 10. cvičení

Příklady šifrování a bezpečného mazání dat

Karel Panchártek

18. 4. 2024

Univerzita Palackého
v Olomouci

Cryfs

- Využívá AES-256
- Šifrovaná složka, která se připojí do souborového systému
- Nelze rozpoznat původní strukturu adresářů a souborů
- Nezapomenout na odpojení ze souborového systému
- Je možná práce jak pouze CLI tak i graficky
- Nelze měnit heslo → potřeba vytvořit znovu

Univerzita Palackého
v Olomouci

7zip

- Využívá AES-256
- Vytváří archiv
- Pro práci se soubory nutné soubory „vybalit“ → Bezpečné smazání
- Přenositelné mezi OS (verze pro Windows i MacOS*)
- Je možná práce jak pouze CLI tak i graficky

* na MacOS nebyla funkčnost ověřována

Univerzita Palackého
v Olomouci

OpenSSL

- Použití primárně z CLI
- Možnost volit metodu šifrování
- Dá se použít na soubory i adresáře
- Šifování

```
openssl aes-256-cbc -in otevreny.txt -out sifrovany
```

- Dešifrování

```
openssl aes-256-cbc -d -in sifrovany -out
roundtrip.txt
```

Univerzita Palackého
v Olomouci

LibreOffice

- symetrické šifrování - využívá AES-256
- možné i asymetrické využití OpenPGP (certifikáty)
- přenositelné mezi OS (verze pro Windows i MacOS*)
- šifrování jednotlivých dokumentů (textové, tabulky a další)

* na MacOS nebyla funkčnost ověřována

Univerzita Palackého
v Olomouci

Bezpečné smazání

- pokud jsou (citlivé) soubory na disku v nešifrované podobě mohou být dostupné i po smazání
- pro klasické HDD např. nástroj Shred
- u SDD je potřeba využít příkazů pro smazání volného místa

Univerzita Palackého
v Olomouci

Úkol

1) V adresáři vytvořte v LibreOffice dokument chráněný heslem, který bude obsahovat vaše jméno a příjmení.
V tom samém adresáři zašifrujte textový soubor s vaším jménem a příjmením pomocí OpenSSL
Tento adresář zašifrujte pomocí CryFS
Adresář vzniklý pomocí CryFS zabalte do 7zip archivu chráněného heslem.
Vzniklý archiv společně s heslem pošlete na e-mail. Pro všechna šifrování použijte stejné heslo.

2) Napište jaké jiné nástroje pro šifrování znáte či používáte na svém operačním systému?

3) Napište jaké jiné nástroje pro bezpečné smazání dat znáte či používáte na svém operačním systému?