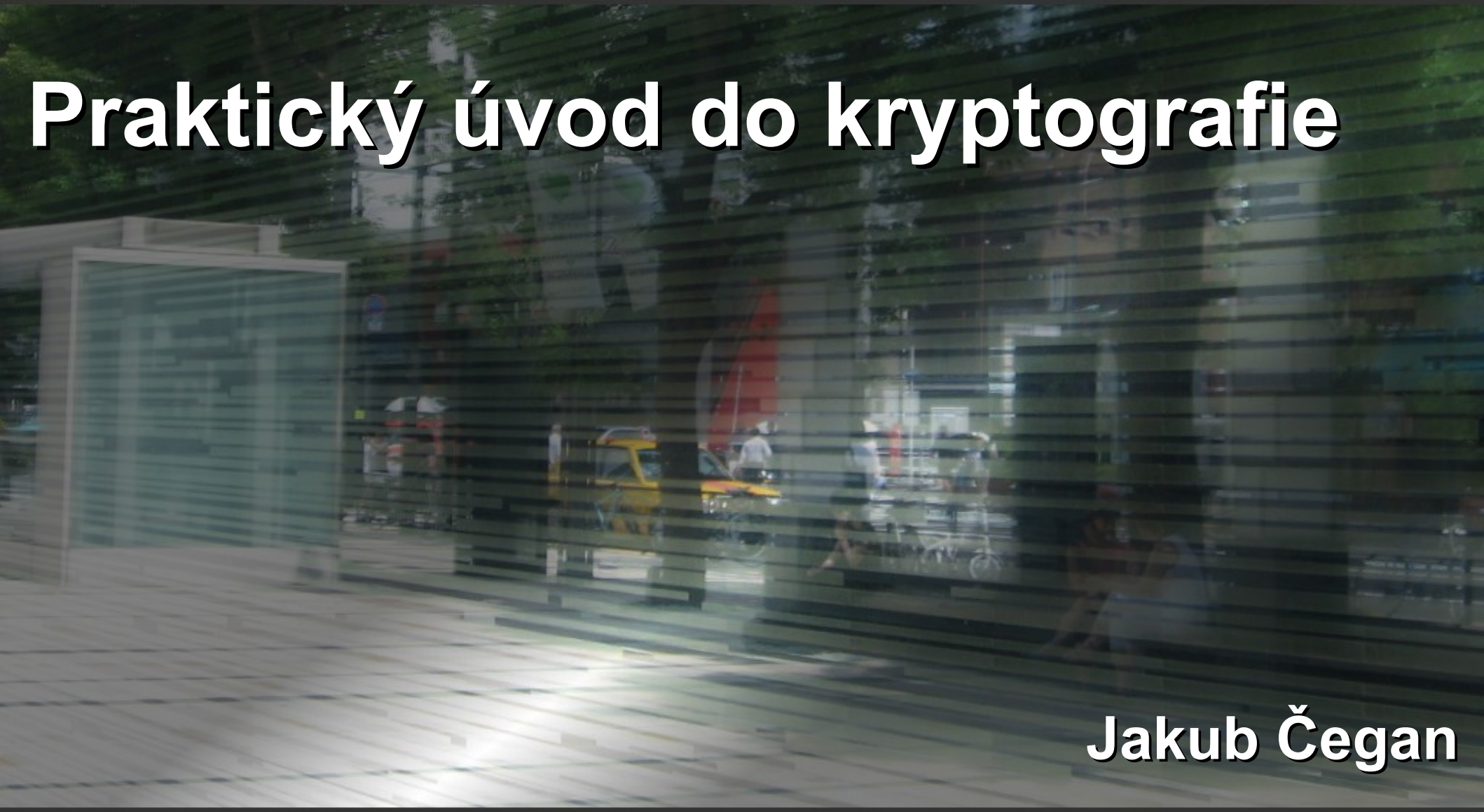
# Praktický úvod do kryptografie



Jakub Čegan

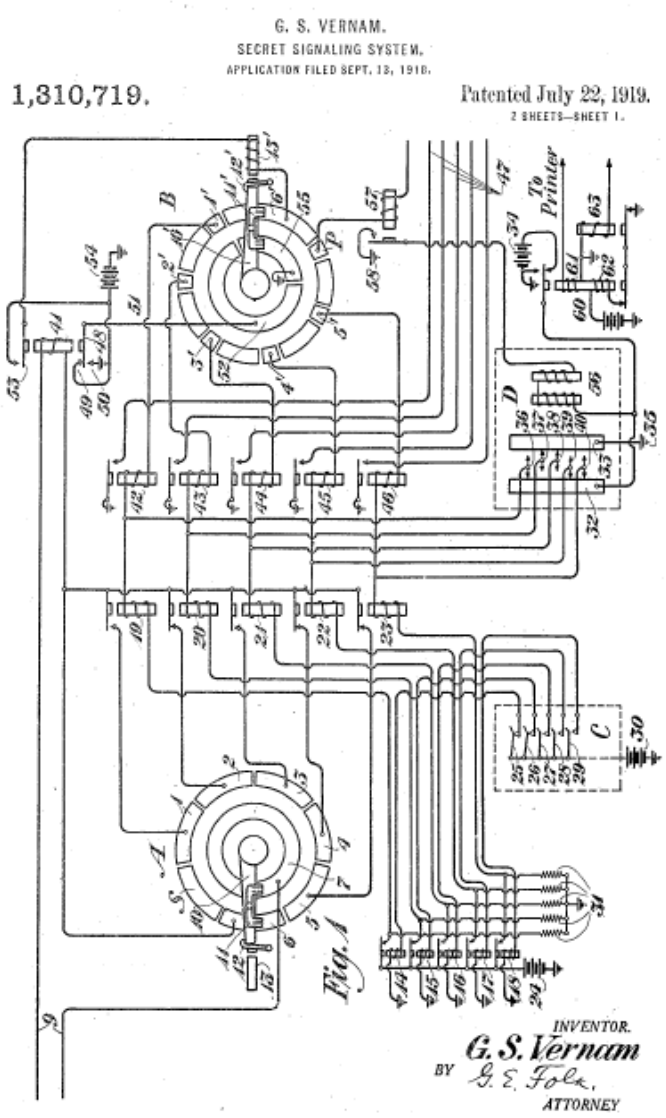
# Co nás čeká?

- Motivace
- Úvod do kryptografie
- Symetrická kryptografie
- Asymetrická kryptografie
- Zajímavosti a průšvihy

# Motivace

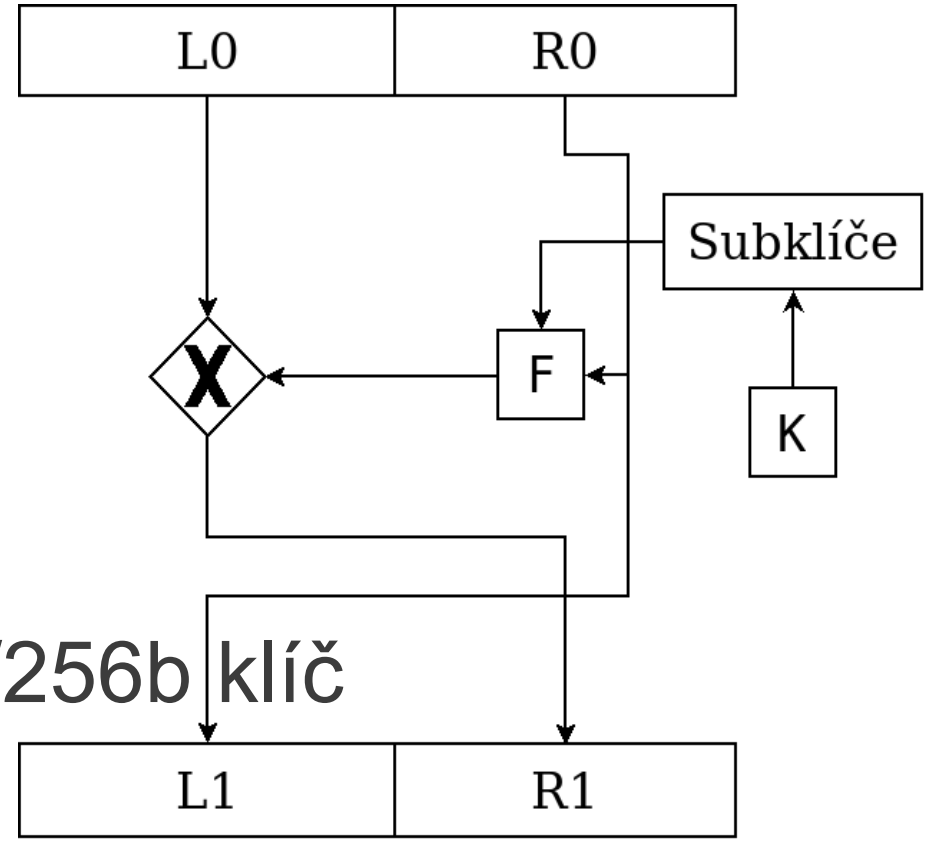
- Proč šifrovat?
  - Paranoia
  - Mám co skrývat
  - Protože chci a můžu
  - Pro jistotu
- Aplikace kryptografie
  - Certifikáty a certifikační autority
  - Elektronický podpis
  - Truecrypt
  - PGP a S/MIME
  - SSH a SSL

- Klasická kryptografie
- Moderní kryptografie
  - Důvěrnost
  - Integrita
  - Nepopiratelnost
  - Autentizace
- Kerckhoffův princip
- Vernamova šifra
- Životnost klíče a Mooreův zákon

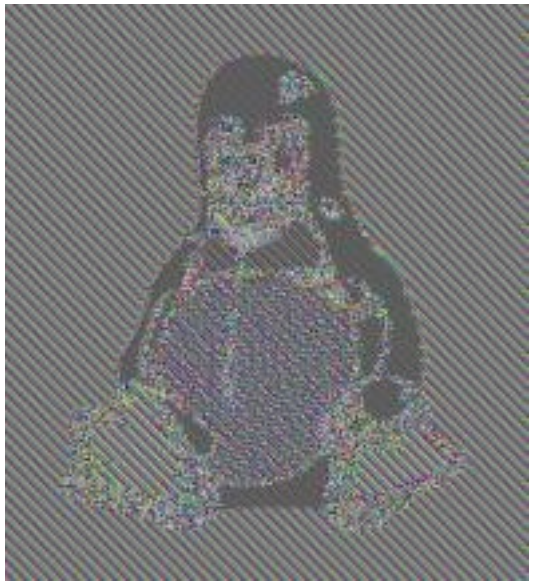

G. S. VERNAM.
SECRET SIGNALING SYSTEM.
APPLICATION FILED SEPT. 13, 1918.
1,310,719. Patented July 22, 1919.
2 SHEETS—SHEET 1.
To Printer
Fig. 1.
INVENTOR.
G. S. Vernam
BY G. E. Folk.
ATTORNEY

# Symetrická kryptografie

- Důvěrnost, Autentizace, Integrita
- Tajný klíč
- Minimální klíč: **128b**
- Slabina: **distribuce klíče**
- **DES** - 64b blok a 56b klíč
  - Feistelova šifra
  - Dočasně zesílen na 3DES
- **AES** - 128b blok a 128/192/256b klíč
  - Aktuální standard
  - Záměna bytů, prohození řádků, kombinování sloupců



- Útok hrubou silou
  - Diferenciální kryptoanalýza
  - Lineární kryptoanalýza
- ECB vs. **CBC**, **CBF**, **OFB**, **CTR**

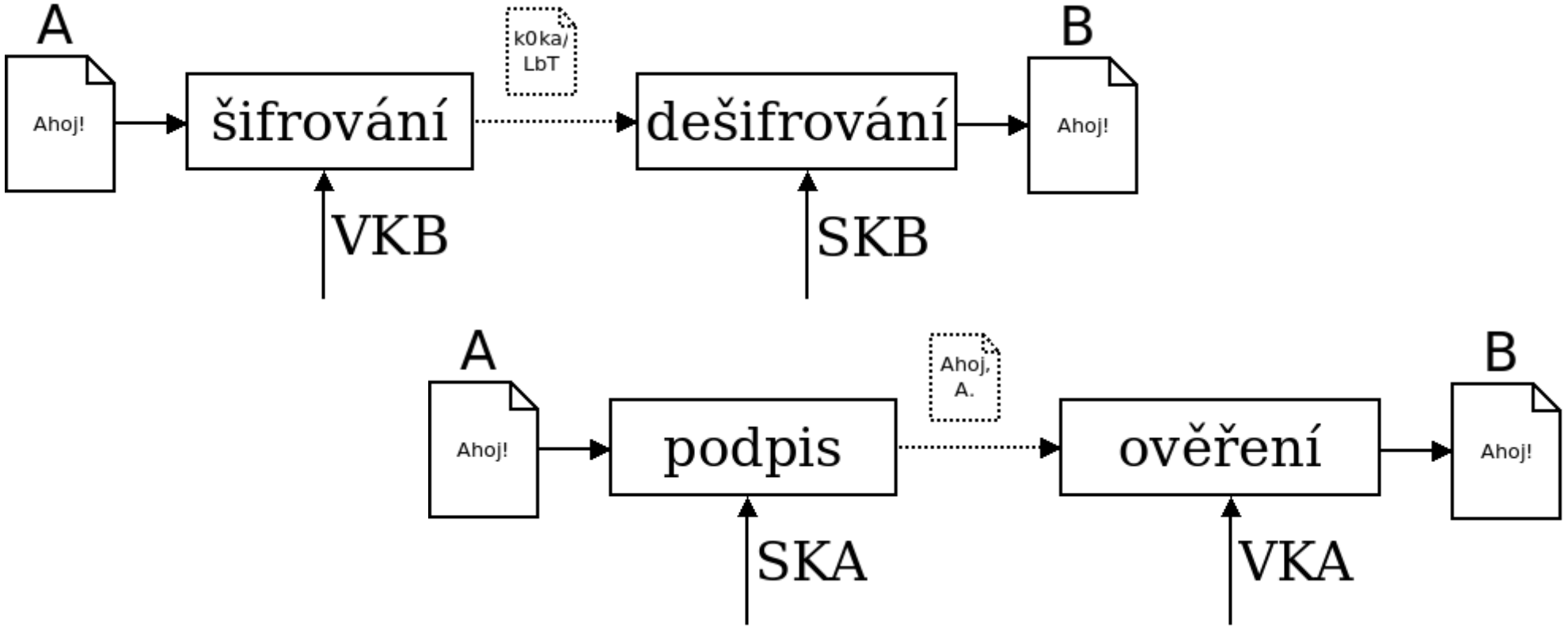


# Asymetrická kryptografie

- Autentizace, integrita, nepopiratelnost a důvěrnost
- Soukromý a veřejný klíč
- Minimální klíč: **1024b**
- Slabina: **relativní pomalost, nelze je vymyslet**
- Založeny na matematickém Voodoo
  - **Knapsack** – problém batohu
  - **RSA** – faktorizace prvočísel
  - **DSA** a **Diffie Hellman** – diskrétní logaritmus
  - **Eliptické křivky** – eliptické křivky nad tělesem Fp

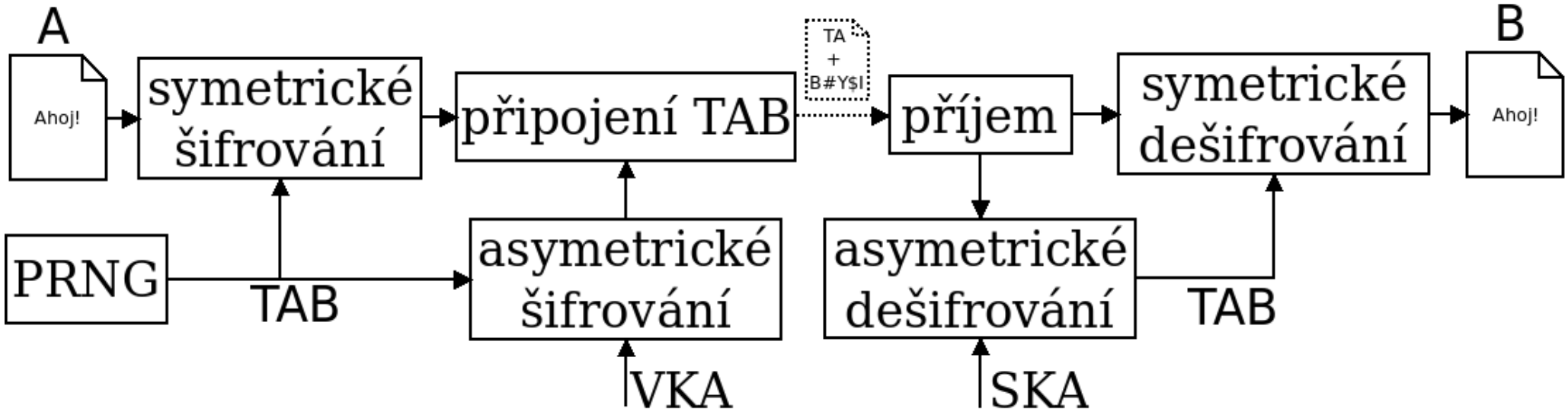
# Použití klíčů

- Šifrování a podepisování
- Napřed podepsat nebo šifrovat?



# Realita je trošku jiná

- Pseudonáhodný generátor
- Symetrické šifrování
- Asymetrické šifrování



# Zajímavosti a průšvihy

- Zoufalství jménem WPS
- Prolomení MS-CHAPv2

- Truecrypt a Enigmail
- HW šifrované flashdisky


Děkuji za pozornost.