# Bezpečnost blokových a proudových šifer

Jakub Kopecký 2023

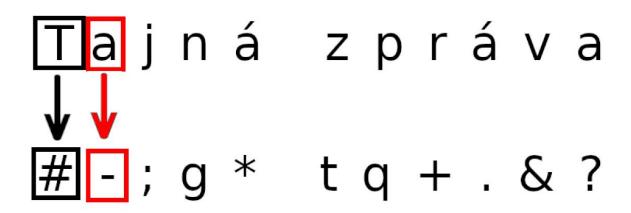
#### Co je to šifra?

 Algoritmus pro transformaci (mapování) původního otevřeného textu na šifrovaný text.



#### Proudové šifry

Šifrování otevřeného textu znak po znaku, bajt po bajtu



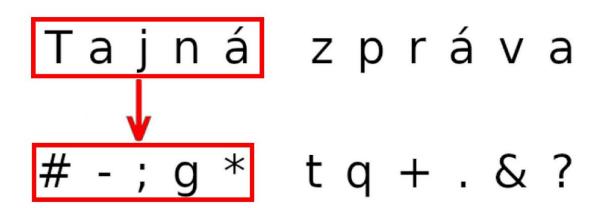
#### Proudové šifry

- Kombinují otevřený text s proudem (pseudo)náhodných znaků
- Binární operace
  - o XOR
- Keystream -(pseudo)náhodný proud znaků
  - Tajný klíč
  - (Náhodný) Inicializační vektor
  - Algoritmus
- Algoritmy
  - o RC4, Salsa20/ChaCha20, A5/1

#### Proudové šifry

- Synchronní
  - Nutnost synchronizace příjemce a odesílatele
  - Vyžadují MAC (pro ověření autenticity)
- Samosynchronní
  - Využívá šifrovaný text k vypočítání keystreamu

Šifrování otevřeného textu v pevně stanovených blocích



- Substituce a permutace
  - S-Boxy a P-Boxy
- Klíčová rozpětí
  - Tajný klíč
  - Klíčová expanze
- Algoritmy
  - o AES, DES, 3DES

- Šifrovací režimy
  - ECB (Electronic Codebook)
    - Nejzákladnější, náchylný k analýze vzorů
  - CBC (Cipher Block Chaining)
    - Každý blok je XORován s předchozím šifrovaným blokem
  - CTR (Counter)
    - Keystream generován inkrementací čítače

- Zpětná vazba (řetězování)
  - OFB (Output Feedback)
    - Generuje keystream z předchozího šifrovaného výstupu
  - CFB (Cipher Feedback)
    - Šifruje předchozí blok šifrovaného textu pro XORování s otevřeným textem

# Bezpečnost proudových šifer

- Bezpečnost závisí na keystreamu
  - Nepředvídatelnost a jedinečnost
  - Délka klíče a inicializačního vektoru
- Zásada jednorázového použití
  - Keystream nikdy nesmí být znovu použit
  - Zajistí bezpečnost a odolnost proti útokům

# Bezpečnost proudových šifer

- Slabiny a útoky
  - Korelace mezi otevřeným textem a šifrovaným textem
  - Útoky s vyčerpáním klíčů
  - Problémy s generátory (pseudo)náhodných čísel
- Opatření pro zvýšení bezpečnosti
  - Použití kryptograficky silných generátorů (pseudo)náhodných čísel
  - Řádná správa klíčů a inicializačních vektorů
  - MAC pro ověření integrity a autenticity

# Bezpečnost blokových šifer

- Bezpečnost závisí na algoritmu a klíči
  - Silný algoritmus a dostatečně dlouhý klíč
  - Řádná správa klíčů
- Výběr vhodného šifrovacího režimu
  - Odolnost proti analýze vzorů a útokům
  - Například CBC, CTR místo ECB

# Bezpečnost blokových šifer

- Slabiny a útoky
  - Útoky na základě času a paměti
  - Útoky s vyčerpáním klíčů
  - Útoky na implementaci
- Opatření pro zvýšení bezpečnosti
  - Použití doporučených algoritmů, např. AES
  - Aktualizace a revize implementace
  - MAC pro ověření integrity a autenticity

#### Názorná ukázka



#### Zdroje

- Mgr. Květuše Sýkorová materiály <u>https://en.wikipedia.org/wiki/Block\_cipher</u>
- https://en.wikipedia.org/wiki/Stream\_cipher
- https://crypto.stackexchange.com/questions/3052/are-stream-ciphers-less-secure
- https://crypto.stackexchange.com/questions/35318/cryptanalysis-of-xor-cipher-with-repeated-key-phrase