Symetrické šifrování

12.03.2025

Operační systémy
IV. ročník

Bc. Lukáš Pospíšil

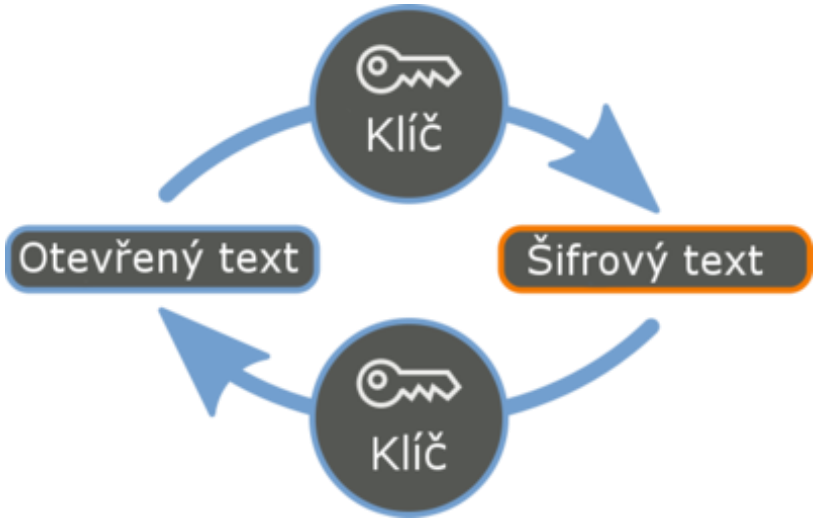
MěSOŠ
Klobouky u Brna

Cíl tématu

- **Znám** pojmy:
  - symetrické šifrování, šifrovací klíč, dešifrování, blokové a proudové šifry.
- **Popíšu** a **vyjmenuju:**
  - základní princip symetrického šifrování
  - výhody a nevýhody tohoto typu šifrování
  - nejznámější symetrické šifry (AES, DES)
- **Umím:**
  - vysvětlit průběh šifrování a dešifrování symetrickými algoritmy
  - vysvětlit problém sdílení klíče

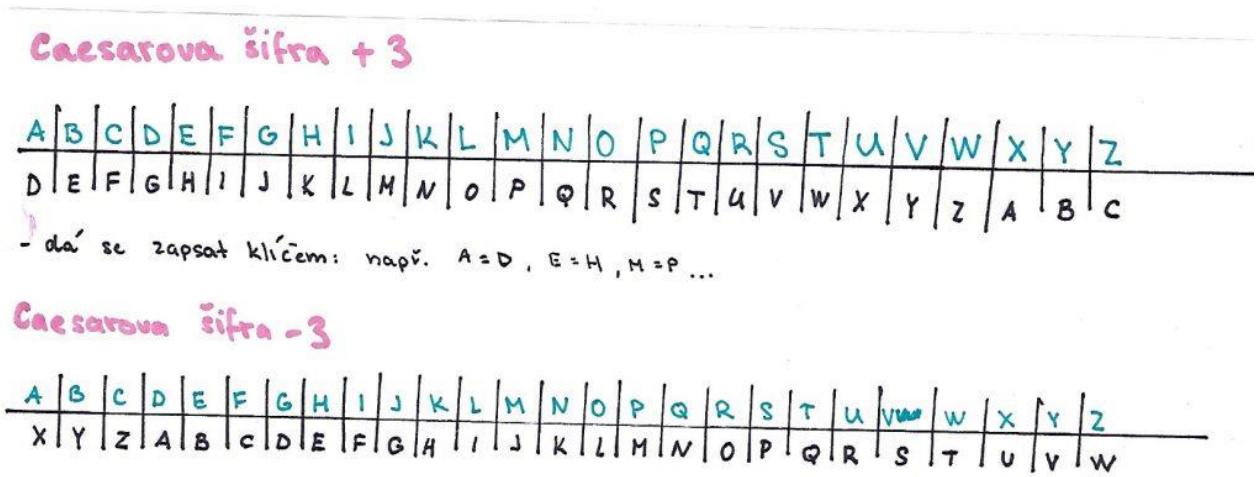
Symetrické šifrování

- **Používá stejný klíč k šifrování, ale i k dešifrování**
- Každý, kdo chce zprávu přečíst – musí znát klíč
- Otevřený text → **Šifrovací algoritmus + klíč** → Šifrovaný text
- Šifrovaný text → **Dešifrovací algoritmus + stejný klíč** → Otevřený text



Symetrické šifrování v historii

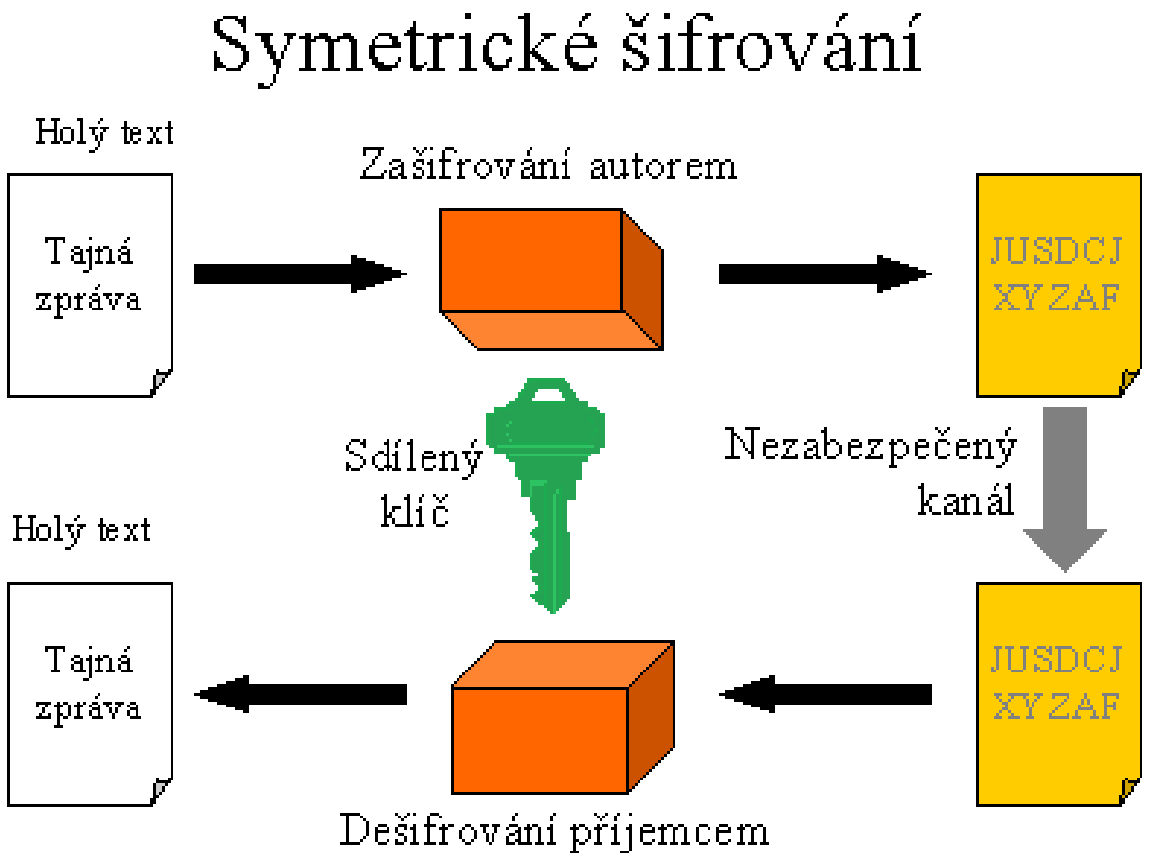
- **Caesarova šifra**
  - algortimus – posun čísel
  - klíč – hodnota posunu
- **Vigenèrova šifra**
  - klíčové slovo
- **Enigma**
  - rotory



Jak funguje

- Otevřený text „AHOJ“
- Použije se klíč + algoritmus pro šifrování
  - po zašifrování – např. X8Gh$%1h2kL
- Pošle se zašifrovaný text
- Stejným klíče se zpráva dešifruje
  - „AHOJ“
- Problém – jak předat klíč?

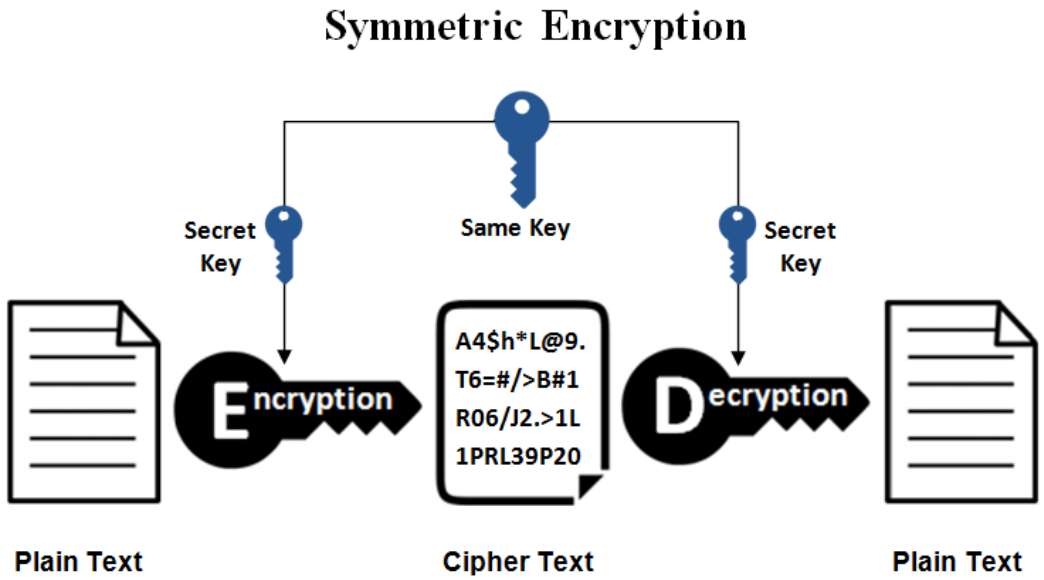
Jak funguje



MěSOŠ Klobouky u Brna

Největší problém – sdílení klíče

- Pokud se někdo **dostane ke klíči**
  - může **zprávu dešifrovat**
  - může **šifrovat falešné zprávy**
- **Problém distribuce klíčů**



MěSOŠ Klobouky u Brna

Předání klíče – řešení?

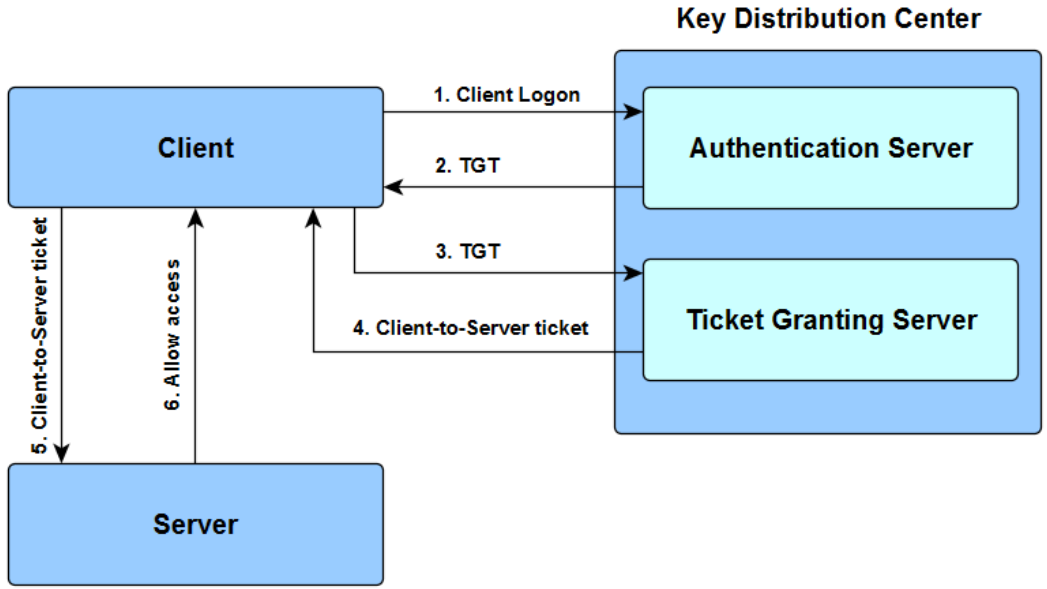
- **Osobní předání** – z ruky do ruky
  - pro malé skupiny (**tajná služba**, vojenské operace)
  - **nelze pro internetovou komunikaci**

Předání klíče – řešení?

- **Jiný zabezpečený kanál**
  - zašifrovaný e-mail, VPN tunel, šifrovaný messenger
  - **už máme kanál – proč přes něj nekomunikujeme?**
  - lze ho prolomit

Předání klíče – řešení?

- **Centrální server**
  - podnikové sítě (Kerberos)
  - může být napaden
  - funguje **jen ve vnitřních sítích**



MěSOŠ Klobouky u Brna

Předání klíče – skutečné řešení

- Skutečné řešení – **asymetrické šifrování**
  - dva klíče – veřejný a soukromý
  - veřejný – můžeme sdílet (šifrování)
  - soukromý – pouze pro nás (k dešifrování)
- Nemusíme posílat soukromý klíč
- Zachycení veřejného klíče – nelze dešifrovat

MODERNÍ SYMETRICKÉ ŠIFRY

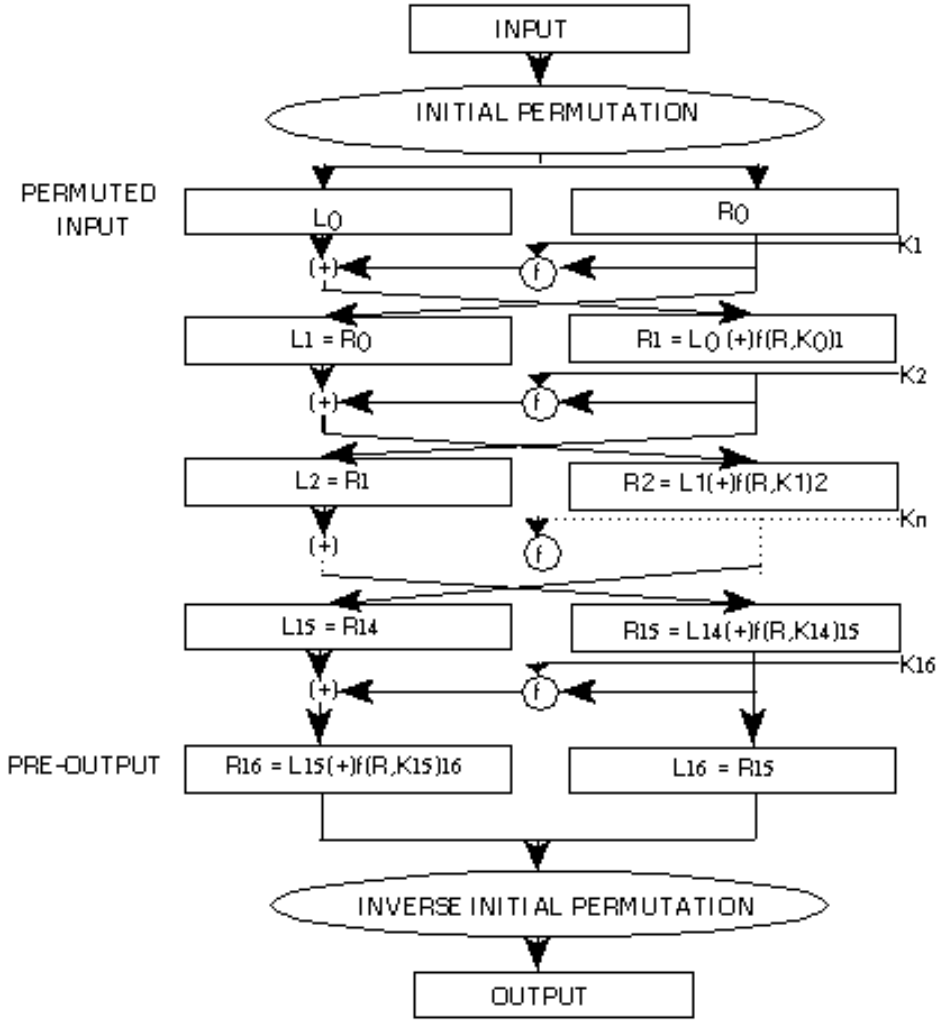
DES

- Data Encryption Standard
- **První oficiálně uznávaná počítačová šifra**
- Rok 1977 – schváleno vládou USA
- Využivá algoritmus – **Feistelova šifra**

DES – Feistelova šifra

- **opakovaná aplikace jednoduchých transformací na vstupní data**
- Jak funguje
  - rozdělení zprávy na bloky po 64 bitech (8 bajtů)
  - využití 56bit. šifrovacího klíče
  - šestnáct kol matematických operací
    - XOR, permutace, substituce…
  - výsledek – zašifrovaný text

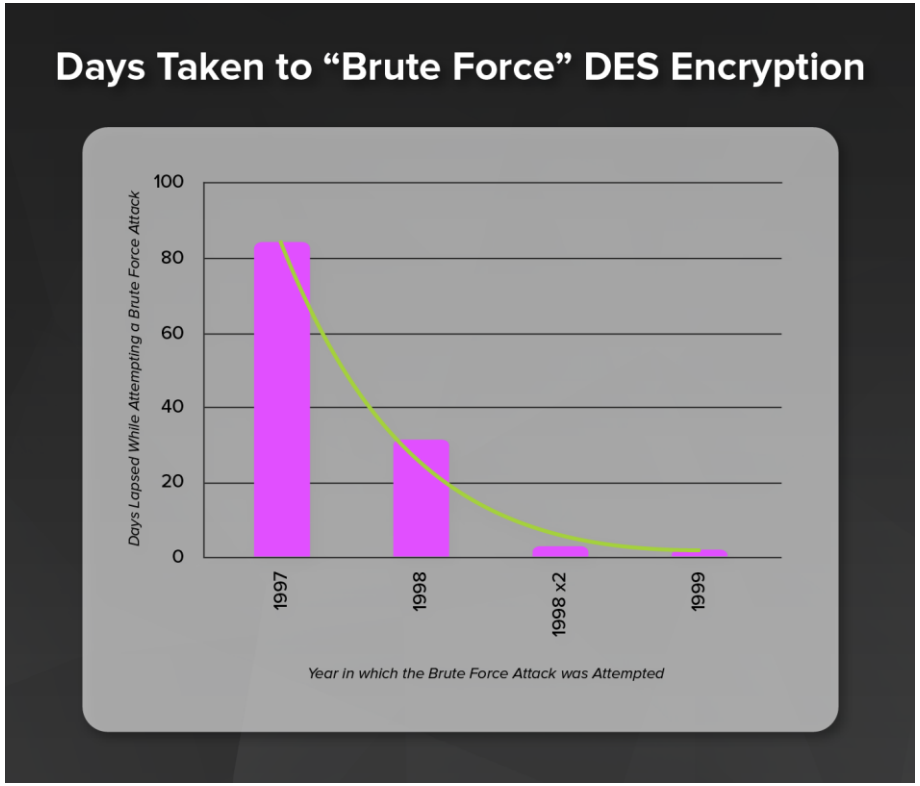
DES – algoritmus



MěSOŠ Klobouky u Brna

DES v dnešních dobách

- **Klíč v délce 56 bitů – příliš krátký**
- **Dnes prolomitelný**
- Brute-force útok
  - lze prolomit za méně než den
- Matematické slabiny
- V roce 2002 **nahrazen AES**



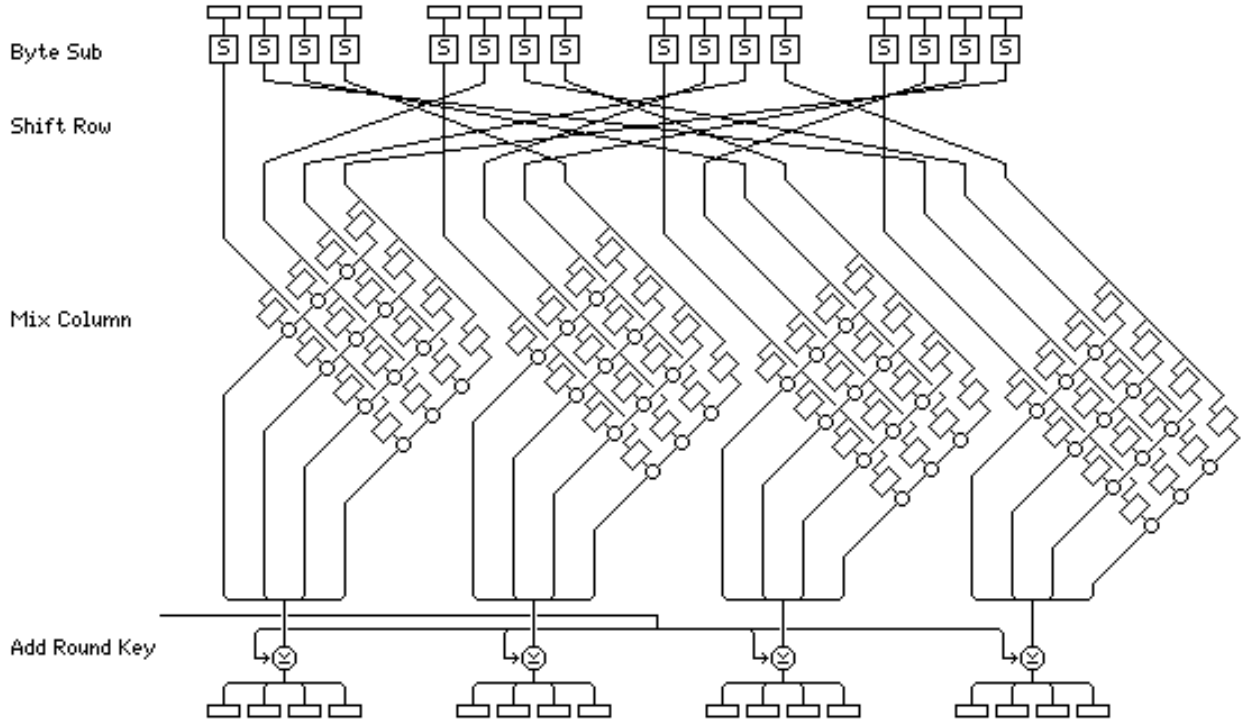
MěSOŠ Klobouky u Brna

AES

- **Nejpoužívanější symetrická šifra** na světě
- Využívána od roku 2001
- Podporuje **delší klíče** – 128 bitů, 192 bitů a **256 bitů**
- Algoritmus – **Rijindael**
  - vznik - Belgie

AES – princip

- Využívá **princip substituční-permutační sítě**
  - zpráva se opakovatelně transformuje v několika kolech



AES – princip

- Zpráva se rozdělí na bloky po 128 bitů
- Každý blok projde několika koly operací
  - substitace bajtů, posunutí řádků, mixování sloupců (zamíchání dat), přidání klíče
- V posledním kole – šifrovaný text
- **Dnes – neprolomitelné**

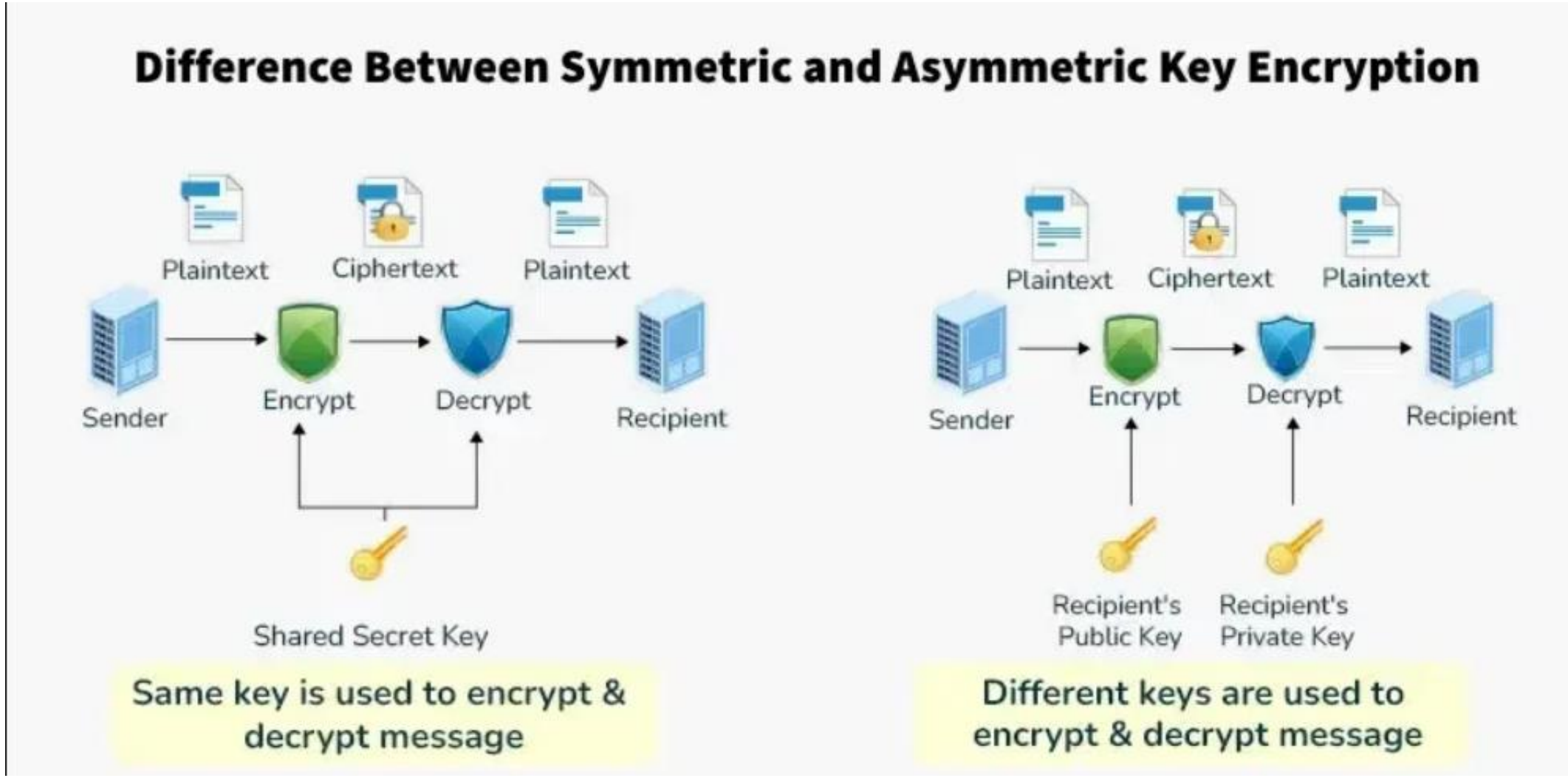
Výhody symetrického šifrování

- **Rychlost**
  - rychlejší než asymetrické
- **Vhodné pro velká data**
  - šifrování disků

Nevýhoda

- **Problém s distribucí klíče**
  - **prozrazení klíče = prolomení šifry**
  - kdo zná klíč může zprávu přečíst, ale i padělat
- Dnes se využívá **kombinace symetrického a asymetrického šifrování**

Rozdíl symetrické a asymetrické šifrování

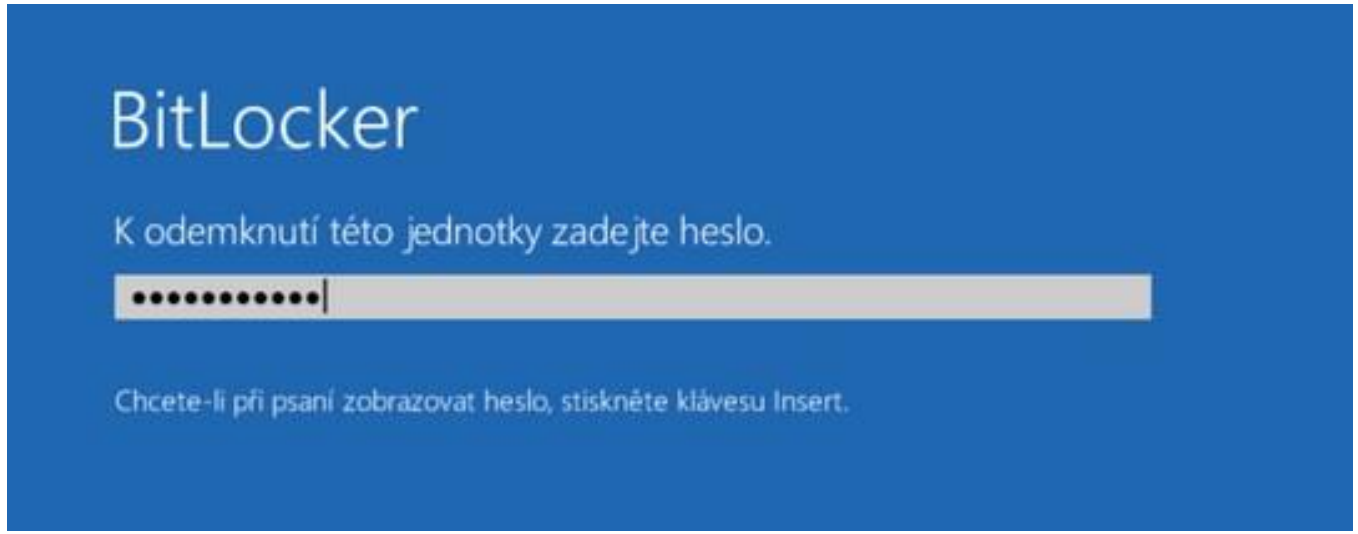


MěSOŠ Klobouky u Brna

VYUŽITÍ SYMETRICKÉHO ŠIFROVÁNÍ

Šifrování disků, souborů

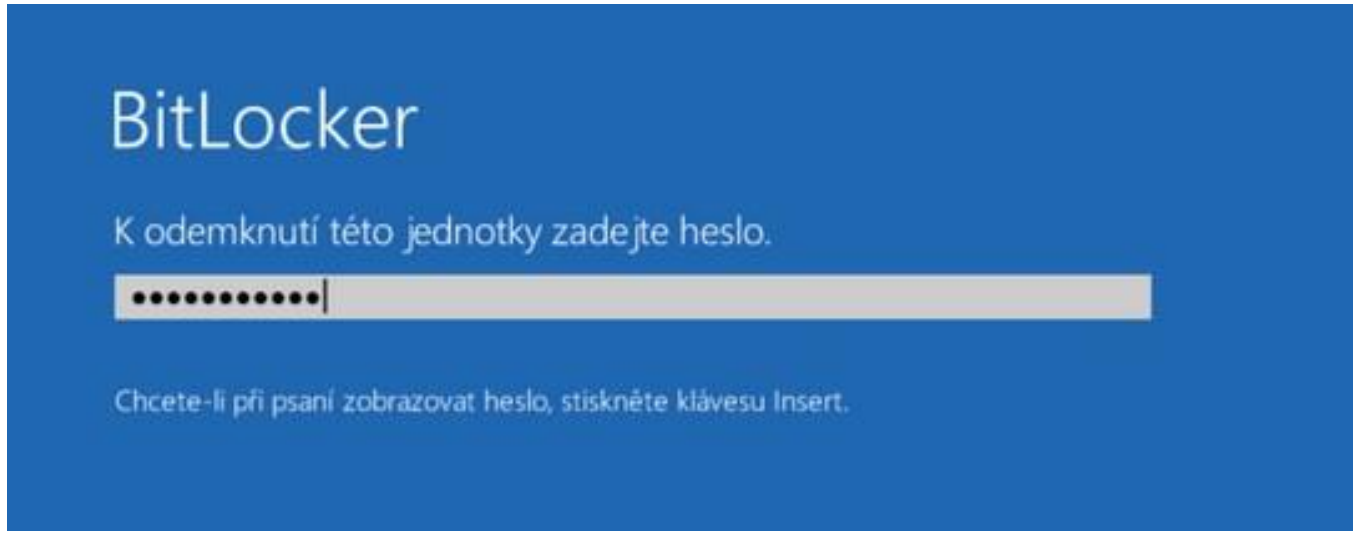
- **Data jsou šifrovaná**
- **Nelze bez klíče přečíst**
  - dešifrace pouze se správným heslem nebo klíčem
- **Bitlocker** – Windows
- **FileVault** – MacOS
- LUKS – Linux



MěSOŠ Klobouky u Brna

Šifrování disků, souborů

- **Data jsou šifrovaná**
- **Nelze bez klíče přečíst**
  - dešifrace pouze se správným heslem nebo klíčem
- **Bitlocker** – Windows
- **FileVault** – MacOS
- LUKS – Linux



MěSOŠ Klobouky u Brna

Ochrana komunikace v sítích

- Psaní e-mailu, přihlášení na web, posílání souborů
  - data putují mezi zařízením(i) a serverem
- Nešifrovaná data
  - každý po cestě může **měnit nebo odposlouchávat**
- Šifrovací protokoly – VPN, HTTPS, TLS
  - chrání komunikaci

VPN

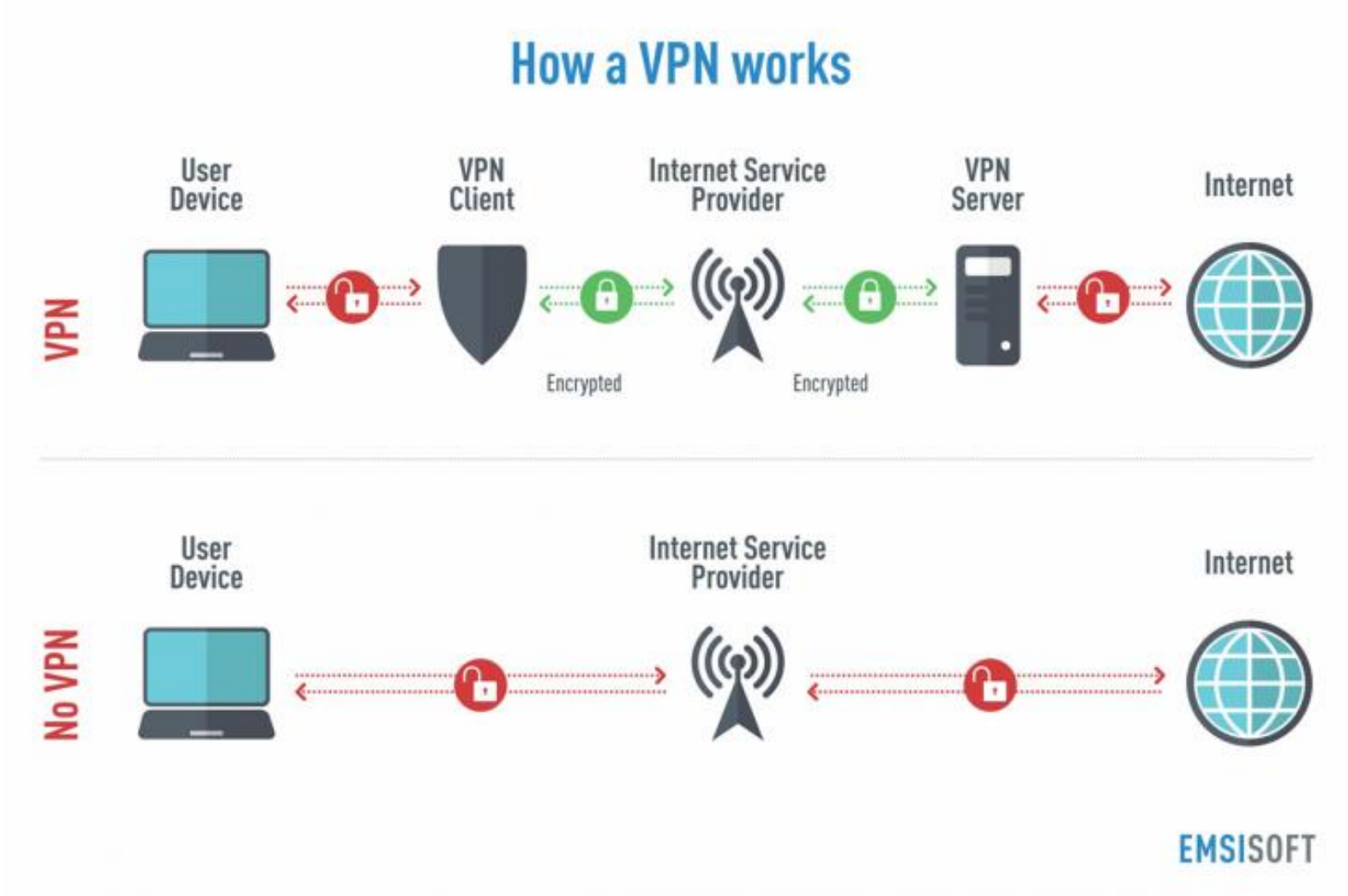
- Virtual Private Network
- Vytváří **šifrovaný tunel mezi tvým zařízením a cílovým serverem**
- Posílaná data – šifrovaná

BEZ VPN	S VPN
Když se připojíš k veřejné Wi-Fi, může kdokoliv v okolí odposlouchávat tvůj provoz	Veškerá komunikace je zašifrovaná – ani poskytovatel internetu ji nemůže přečíst
Poskytovatel internetu (ISP) vidí všechny weby, které navštěvuješ	Můžeš obejít geografická omezení a přistupovat k blokovanému obsahu
Stát nebo zaměstnavatel může blokovat přístup k určitým stránkám	Tvoje IP adresa je skrytá, takže weby nevidí tvoji skutečnou polohu

VPN – jak funguje

- Připojení k **VPN serveru**
  - **prostředník mezi tebou a internetem**
  - data se zašifrují (**AES-256**)
  - **změní se IP adresa** (weby vidí IP serveru)
  - poskytovatel vidí pouze komunikaci s VPN serverem
- Nevýhody
  - **pomalejší připojení**
  - neověřená VPN – může sbírat data

VPN

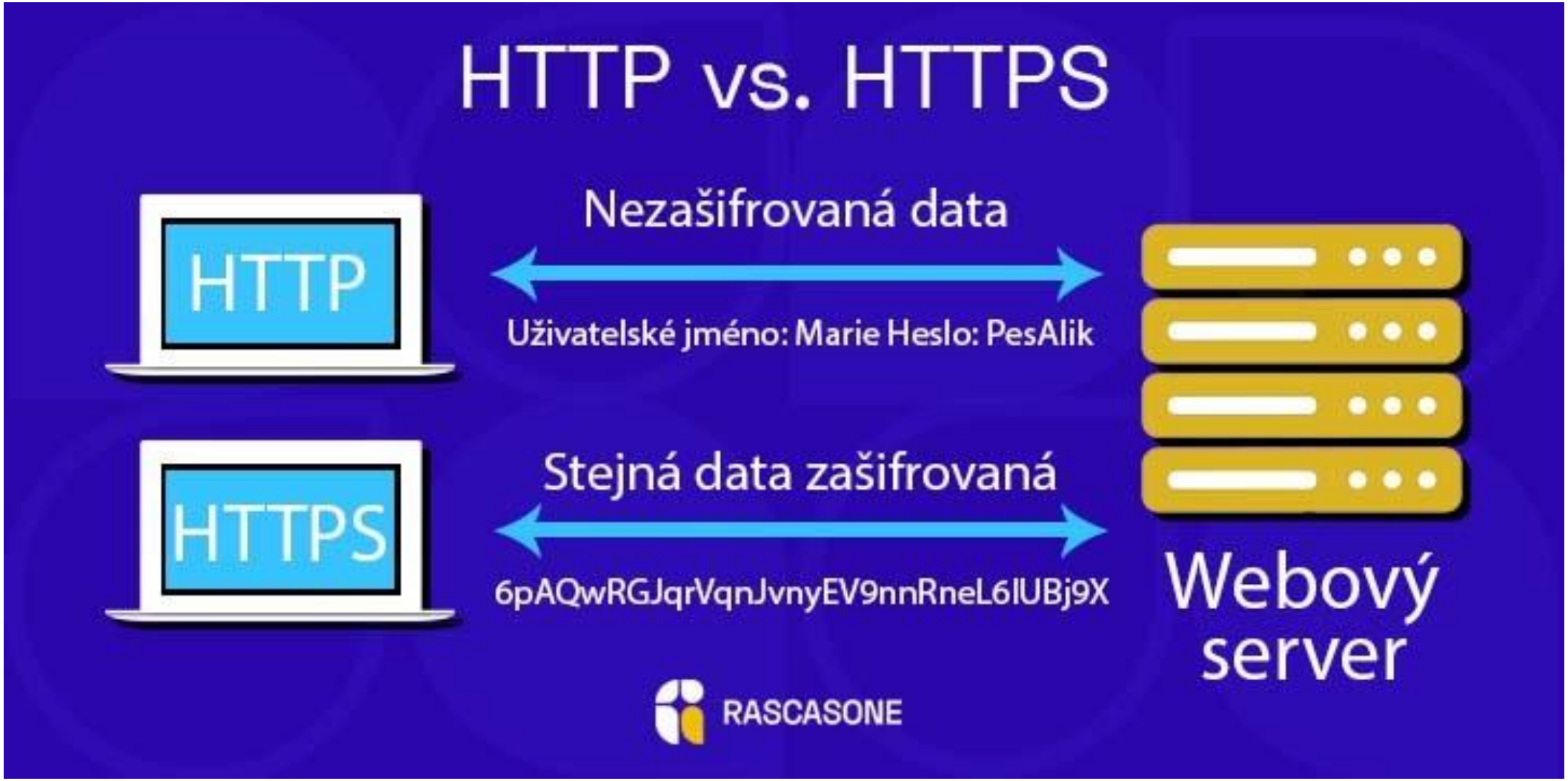


MěSOŠ Klobouky u Brna

HTTPS

- **Šifrovaná verze HTTP**
  - zabraňuje odposlechu a podvrhu dat
- **Chrání přihlašovací údaje**
  - šifrované heslo
- **Chrání před MITM útokem**
  - nelze podvrhnout falešné stránky

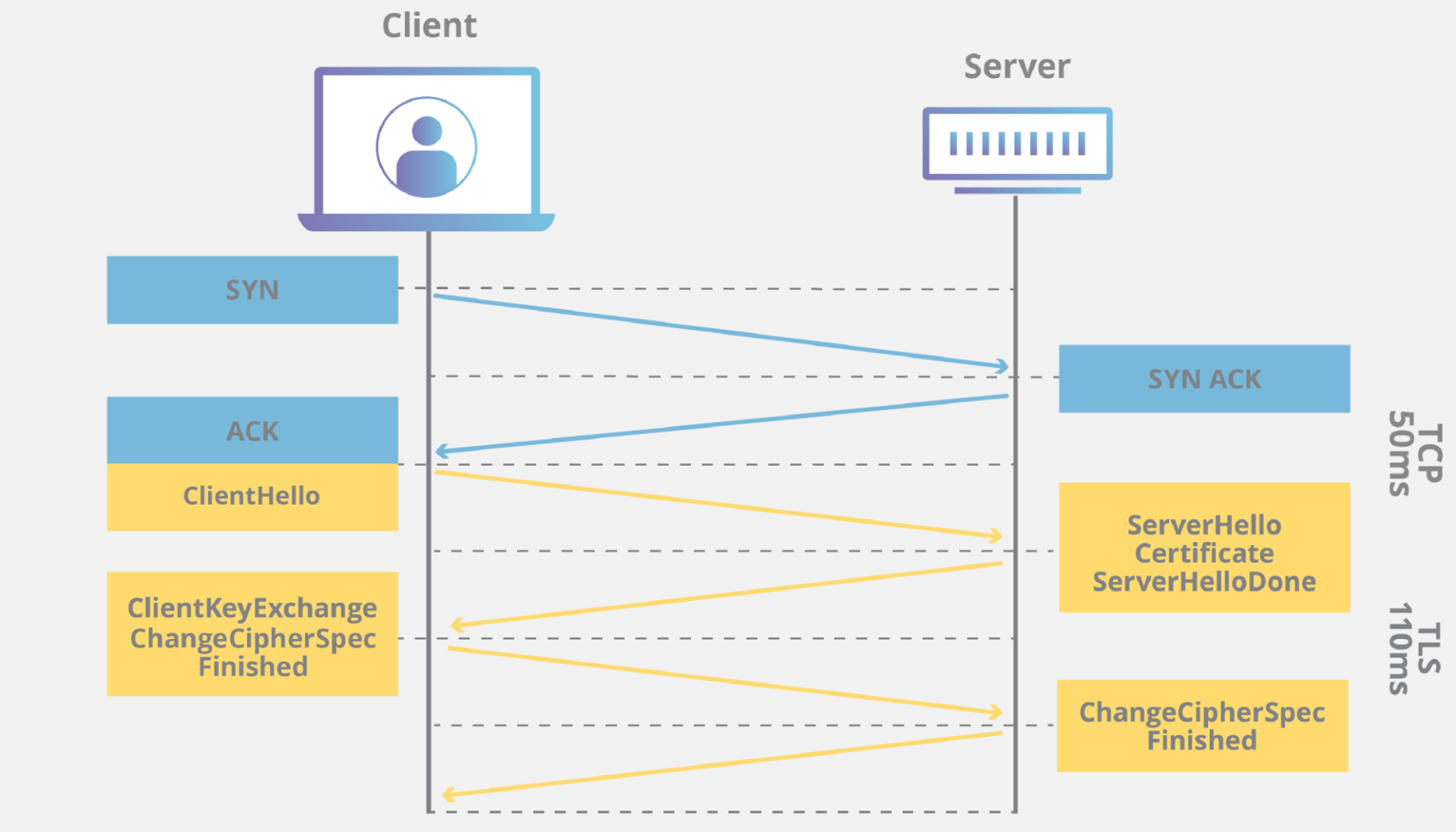
HTTPS


HTTP vs. HTTPS
HTTP
Nezašifrovaná data
Uživatelské jméno: Marie Heslo: PesAlik
HTTPS
Stejná data zašifrovaná
6pAQwRGJqrVqnJvnyEV9nnRneL6IUBj9X
Webový server
RASCASONE

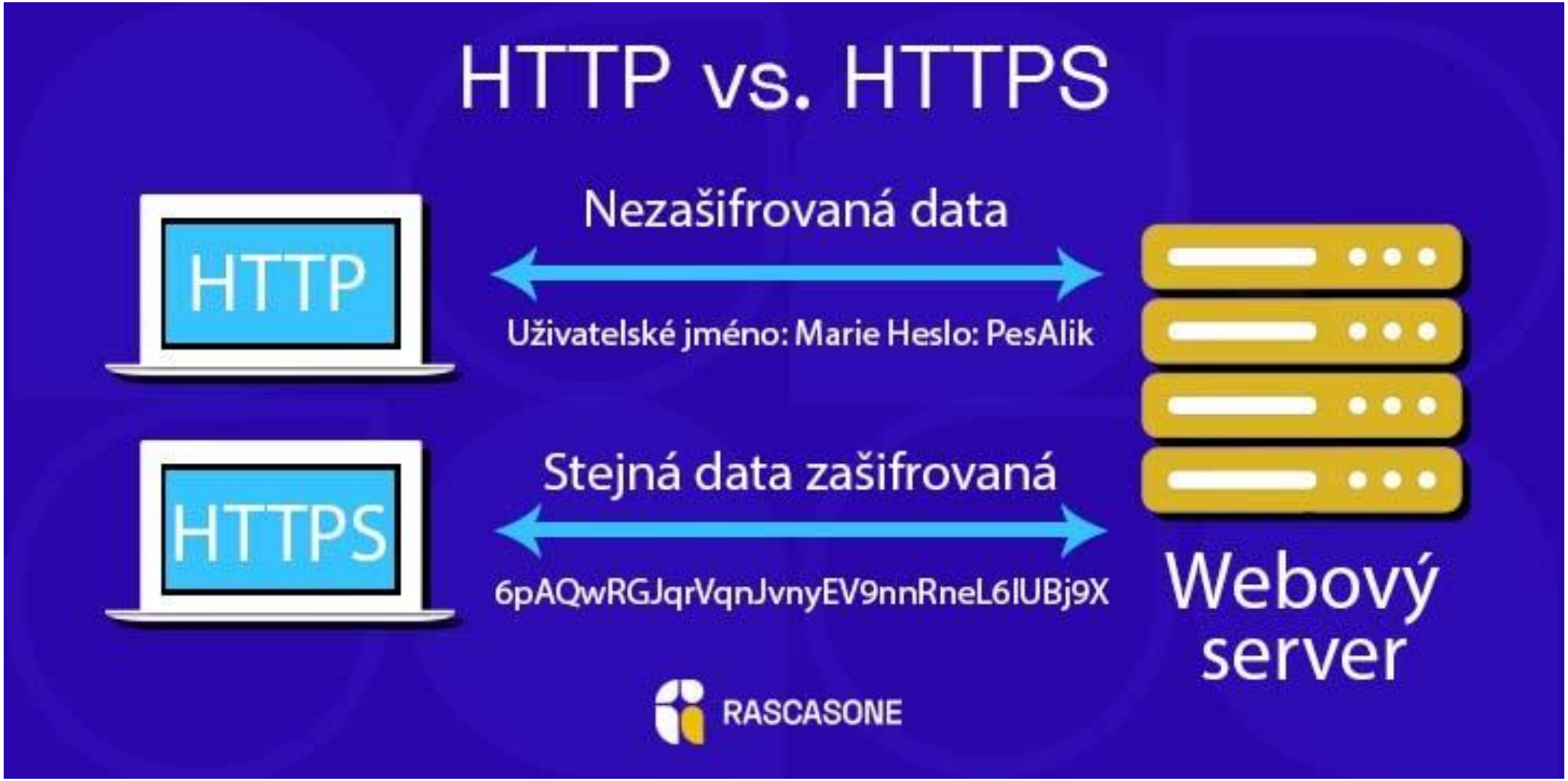
TLS

- Transport Layer Security
- **Protokol šifrující síťovou komunikaci**
- Využití
  - e-maily, VOIP hovory, přenos souborů
- Nahrazuje SSL

TLS


Client
Server
SYN
SYN ACK
ACK
ClientHello
ServerHello
Certificate
ServerHelloDone
ClientKeyExchange
ChangeCipherSpec
Finished
ChangeCipherSpec
Finished
TCP
50ms
TLS
110ms

HTTPS


HTTP vs. HTTPS
HTTP
Nezašifrovaná data
Uživatelské jméno: Marie Heslo: PesAlik
HTTPS
Stejná data zašifrovaná
6pAQwRGJqrVqnJvnyEV9nnRneL6IUBj9X
Webový server
RASCASONE

Anotace

Tato prezentace slouží k seznámení se s principy symetrického šifrování a jeho využitím v kybernetické bezpečnosti. Zaměřuje se na základní pojmy, výhody a nevýhody symetrických šifer a jejich praktické použití. Žáci se naučí, jak fungují symetrické šifrovací algoritmy, jaké mají slabiny a v jakých situacích se využívají. Hlavním cílem je, aby žáci porozuměli základům symetrického šifrování a dokázali identifikovat jeho roli v zabezpečení dat.

Hlavním cílem je, aby žáci porozuměli různým metodám správy serverových služeb v Linuxu a dokázali je efektivně využít v praxi.

Užité zdroje

- https://vyuka.mesosdev.cz/kb/operacni-systemy/kryptografie/symetricke-sifry/

Autor: Bc. Lukáš Pospíšil

Předmět: Operační systémy

Ročník: 4.

Rok vytvoření: 2025

Poslední aktualizace: 2025

MěSOŠ Klobouky u Brna