Asymetrické šifrování

12.03.2025

Operační systémy
IV. ročník

Bc. Lukáš Pospíšil

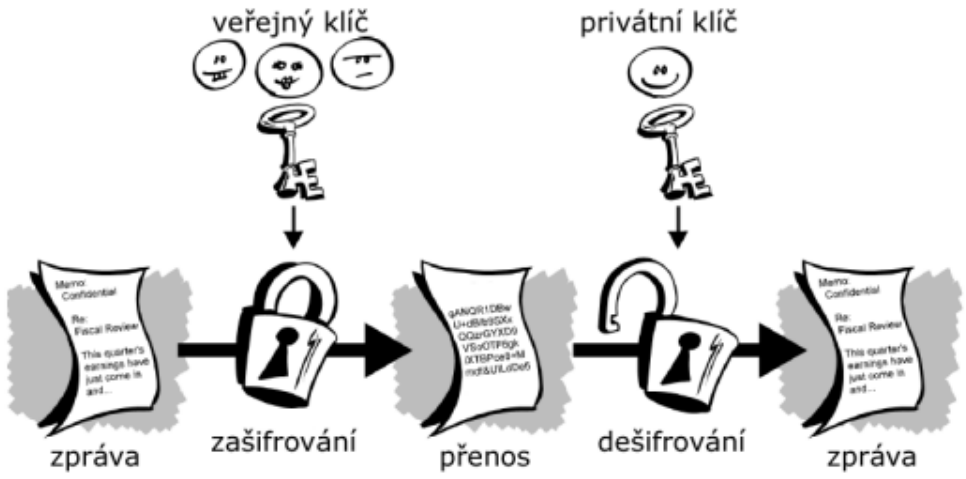
MěSOŠ
Klobouky u Brna

Cíl tématu

- **Znám** pojmy:
  - asymetrické šifrování, veřejný a soukromý klíč, RSA, digitální podpis, certifikační autorita
- **Popíšu** a **vyjmenuju:**
  - princip asymetrického šifrování
  - proces šifrování a dešifrování pomocí klíčového páru
  - využití asymetrické kryptografie v praxi
- **Umím:**
  - vysvětlit, proč je asymetrické šifrování bezpečnější pro přenos dat než symetrické šifrování, uvést reálné příklady jeho použití

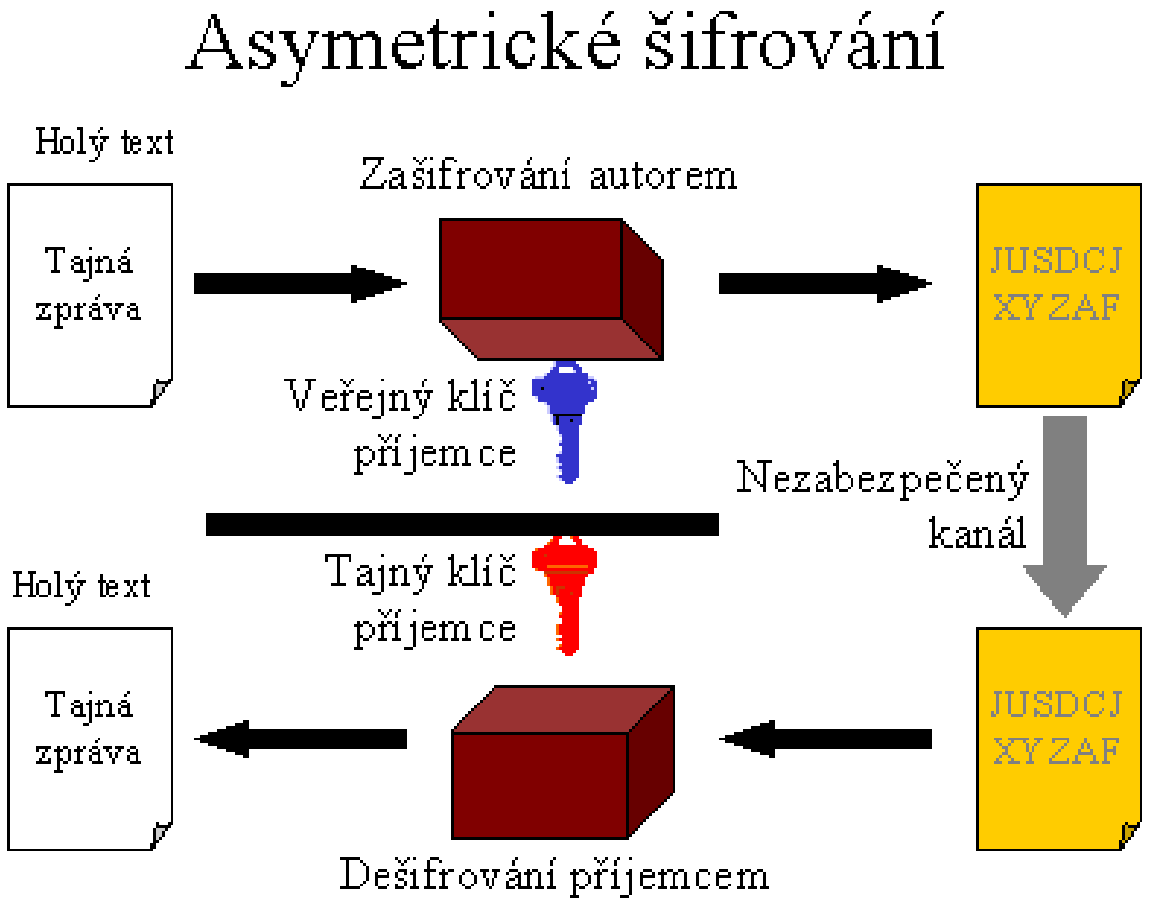
Asymetrické šifrování

- **Nepotřebuje sdílet tajný klíč**
- Místo jednoho klíče – **dva klíče**
  - **veřejný** – lze sdílet s kýmkoliv
    - **slouží pouze k šifrování**
  - **soukromý** – musí se držet v tajnosti
    - **slouží k dešifrování**
- **Řeší problém distribuce klíčů**
  - není potřeba **tajně posílat klíč**



MěSOŠ Klobouky u Brna

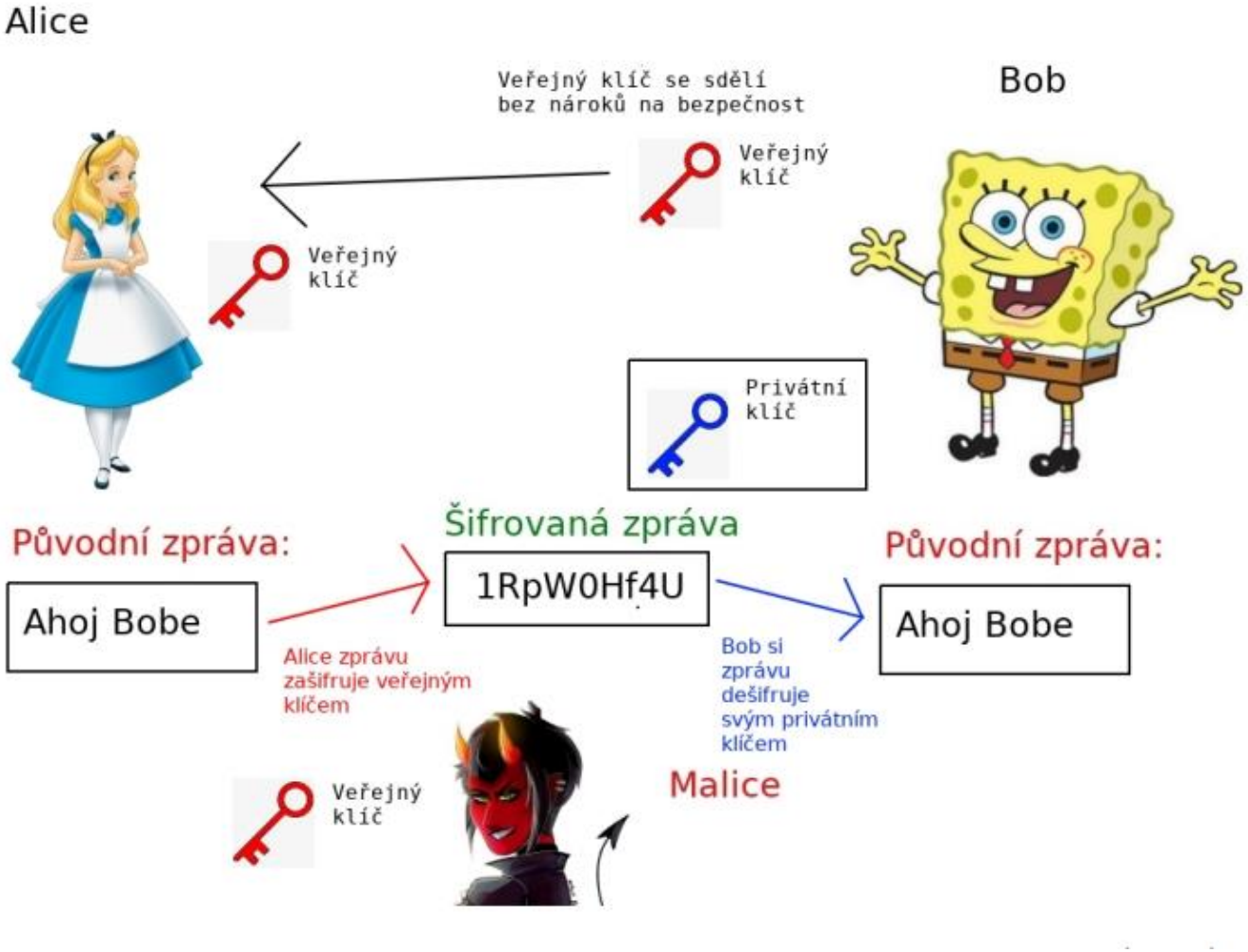
Asymetrické šifrování



Asymetrické šifrování – jak funguje

- Příjemce vygeneruje pár klíčů
  - veřejný – sdílí s kýmkoliv (XYZ123)
  - soukromý – s nikým nesídlí (ABC456)
- Odesílatel použije veřejný klíč příjemce (XYZ123)
  - zašifruje jím zprávu
- Příjemce dešifruje zprávu svým soukromým klíčem (ABC456)
- **Útočník nemá soukromý klíč → nemůže zprávu přečíst**
- **Pouze příjemce dešifruje zprávu**

Asymetrické šifrování

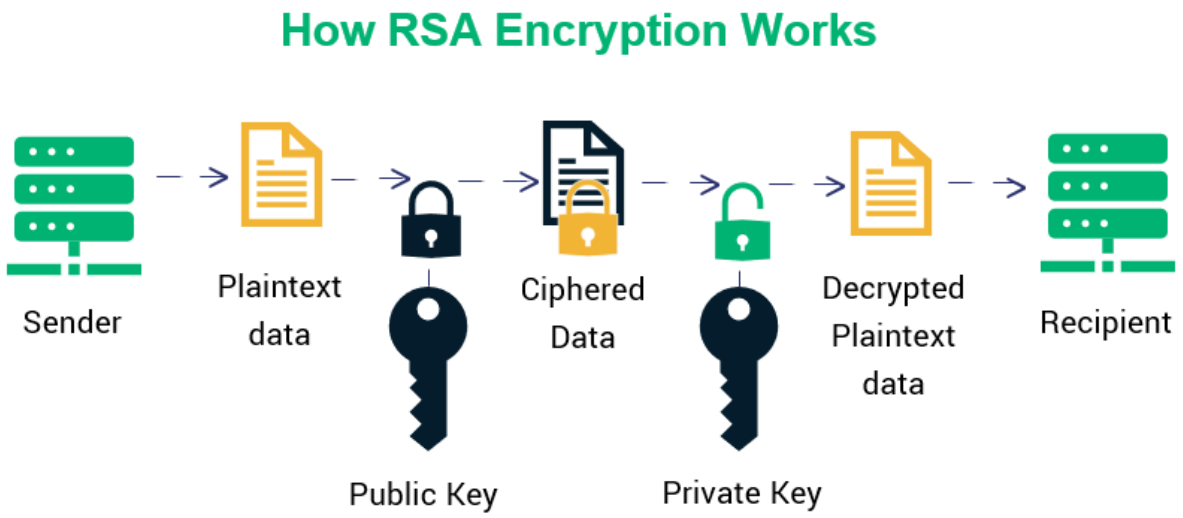


MěSOŠ Klobouky u Brna

RSA

RSA

- **Nejpoužívanější asymetrická šifra**
- Základ kybernetické bezpečnosti
- Používáme všichni
  - přihlášení do banky, podpis e-mailu, HTTPS



MěSOŠ Klobouky u Brna

RSA

- Založena na **matematickém problému faktorizace velkých čísel**
  - je lehké vynásobit dvě velká prvočísla
    - 61 * 53 = 3233
  - jak zpětně zjistit, která prvočísla byla vynásobena?
  - u malých čísel snadné
  - u obrovských (stovky číslic) – nemožné
- **Princip – prvočíselná faktorizace**
  - k vytvoření veřejného a soukromého klíče
  - dešifrování bez soukromého – nemožné

RSA

- Založena na **matematickém problému faktorizace velkých čísel**
  - je lehké vynásobit dvě velká prvočísla
    - 61 * 53 = 3233
  - jak zpětně zjistit, která prvočísla byla vynásobena?
  - u malých čísel snadné
  - u obrovských (stovky číslic) – nemožné
- **Princip – prvočíselná faktorizace**
  - k vytvoření veřejného a soukromého klíče
  - dešifrování bez soukromého – nemožné

Jak funguje

- Srdce šifry RSA – matematika – teorie čísel
- Nepočítáme běžně s celými čísly
  - využíváme **modulo** (zbytek po dělení)
- RSA využívá 3 kroky
  - generování klíčů
  - zašifrování zprávy
  - dešifrování zprávy

Generování

- Uživatel vygeneruje **pár klíčů**
  - veřejný a soukromý
- Vyberou se dvě velká prvočísla
  - ty se vynásobí
- Vypočítá se **Eulerova funkce**
- Vybere se veřejný exponent (65537)
- Výsledek
  - veřejný klíč {3233, 17}
  - soukromý klíč {3233, 2753)

Šifrování

- **Otevřený text s použitím veřejného klíče příjemce**
  - {n, e}
- Zašifrování podle vzorce
  - $c=m^e \bmod n$
    - m = původní zpráva
    - e = veřejný exponent příjemce
    - n = součást veřejného klíče

Šifrování

- Například
  - příjemcův veřejný klíč {3233, 17}
  - odesílatel chce poslat zprávu „65“ (znak v ASCII)
  - znak zašifruje
    - $c = 65^{17} \bmod 3233$
    - $c = 2970$
  - zašifrovaná zpráva = 2970

Dešifrování

- Příjemce obdrží šifrovanou zprávu (např. 2790)
- Použije
  - soukromý klíč {n, d}
  - dešifrovací vzorec $m=c^d \bmod n$
    - c = zašifrovaná zpráva (např. 2790)
    - d = soukromý exponent příjemce (2753)
    - n = součást klíče (3233)
  - $m=2790^{2753} \bmod 3233$
  - m=65
- Původní zpráva – 65 (znak v ASCII), takže písmeno A

Bezpečnost

- Dešifrování **vyžaduje faktorizaci velkého čísla n**
- Prolomení RSA znamená rozložení n na původní prvočísla
  - pro 2048 bitová čísla prakticky **nemožné**
- Současné počítače neumí faktorizovat velká čísla v rozumném čase
- RSA bezpečný s využitím dostatečně velkého klíče
- **Doporučená délka klíče: 2048 bitů a více**

Využití

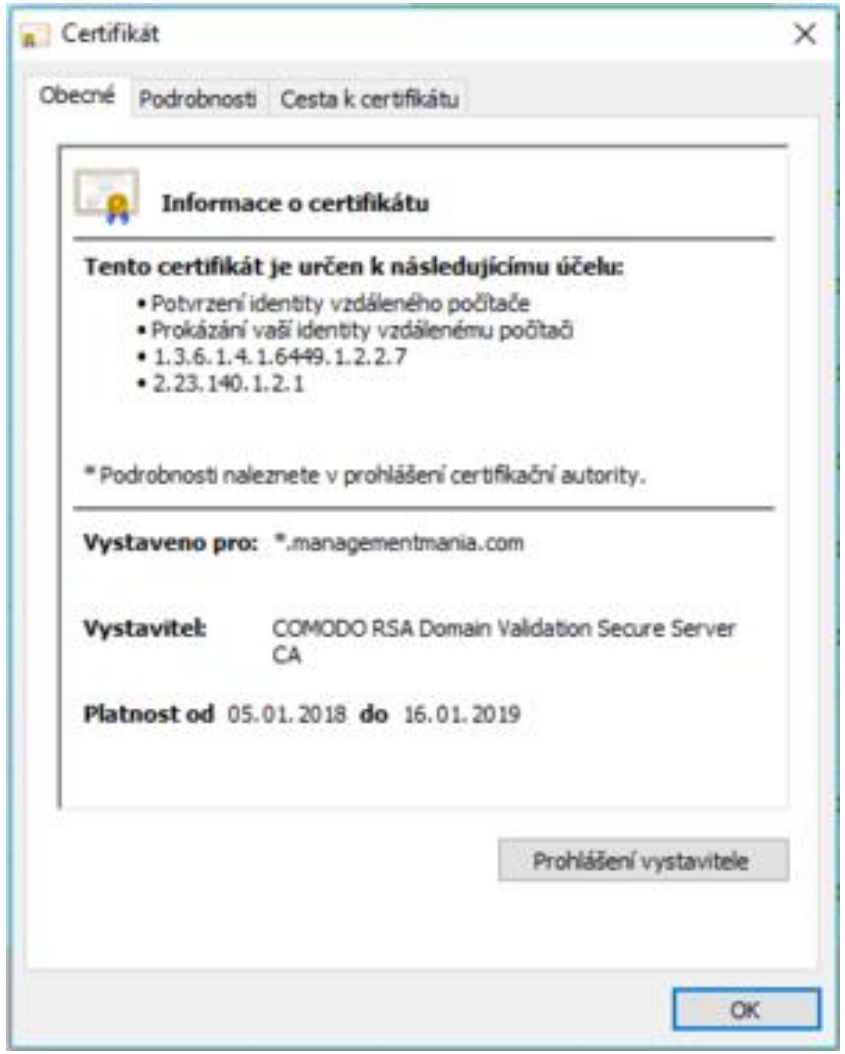
- HTTPS – zabezpečené webové stránky
- Elektronický podpis – ověření autora a integrity dokumentů
- Digitální certifikáty, certifikační autority
- E-mailová bezpečnost – šifrované zprávy (S/MIME)
- **Výměna klíčů v sítích**
  - **TLS, SSH, VPN…**

CERTIFIKÁTY
CERTIFIKAČNÍ AUTORITY

Digitální certifikát

- **Potvrzuje identitu serveru**
  - „občanský průkaz pro webové stránky a servery“
- **Obsahuje veřejný klíč**
  - slouží k šifrování komunikace

Digitální certifikát



MěSOŠ Klobouky u Brna

Digitální certifikát - obsah

- jméno vlastníka (např. mojebanka.cz)
- veřejný klíč
- platnost certifikátu (od-do)
- certifikační autoritu (kdo certifikát vydal)
- digitální podpis certifikační autority

Certifikační autorita

- **Organizace, které vydávají certifikáty a garantují jejich pravost**
- **Ověřují identitu uživatele**
  - vše v pořádku – vydají certifikát
  - podepsaný jejím soukromým klíčem
  - podpis se ověří veřejným klíčem CA uložený v systému
- Nejznámější CA – **Let‘s Encrypt**
- Ověřuje, že **server je skutečný**
- Obsahuje **veřejný klíč k šifrování komunikace**
- **Zabraňuje podvodníkům** ve vydávání se za jiné servery

Využití

- HTTPS – šifrování komunikace, ověření identity serveru
- E-maily – ověření odesílate e-mailu, šifrování zpráv (S/MIME)
- Elektronický podpis – ověření identity podepisujícího

Zneužití

- Falešný certifikát
- Typy zneužití
  - **zkompromitovaná** CA
    - napadnutí CA a zisk pravého cert. pro falešnou doménu
  - **podvržená** zprostředkující CA
    - vytvoření falešného cert. pro podřízenou autoritu
  - **předstíraná** CA v lokální síti
    - podvrh cert. a donucení prohlížeče ho akceptovat

Zneužití v historii

- **DigiNotar** (2011)
  - útočníci napadli nizozemskou CA DigiNotar
  - získali falešné certifikáty pro Google, Yahoo a další weby
  - certifikáty použity v Íránu k odposlechu Gmailu
    - umožnění vládě sledovat komunikaci disidentů
  - DigiNotar přišel o důvěru a zkrachoval

Zneužití v historii

- **Stuxnet** (2010)
  - počítačový virus, který napadl íránský jaderný program
  - použil ukradené certifikáty, aby se jevil jako legitimní software
- **Falešné certifikáty pro Google v Číně** (2015)
  - neznámá CA vydala falešný certifikát pro Google
  - uživatelé v Číně přesměrováni na falešný Google
    - jejich hesla byla odchycena

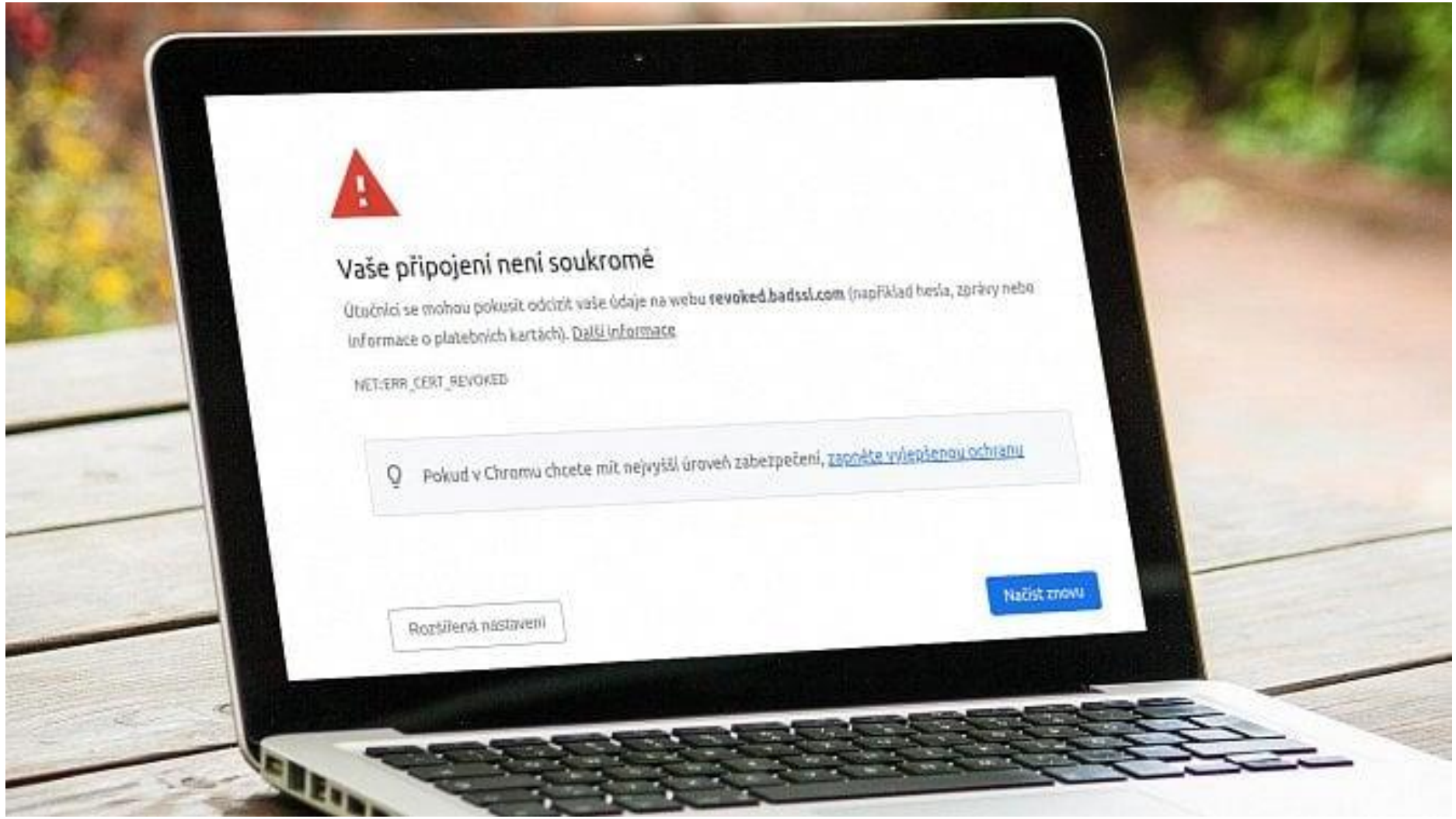
Obrana proti falešným certifikátům

- Databáze všech vydaných certifikátů
- HSTS – prohlížeč si řekne pouze o HTTPS s platnými certifikáty
- Prohlížeč ověřuje, zda je cert. platný
- Velké firmy spravují seznamy důvěryhodných certifikátů
  - v případě incidentu okamžitě zablokují kompromitované cert.

Platnost

- Každý certifikát má **platnost jen na určitou dobu**
  - 90 dní až 2 roky
- Ochrana před zneužitím, minimalizace chyb
- Webové stránky upozorňují na vypršení
  - prohlížeče často odmítají připojení
  - uživatelé mohou být zmatení a stránce přestanou důvěřovat

Platnost


Vaše připojení není soukromé
Útočníci se mohou pokusit odcizit vaše údaje na webu revoked.badssl.com (například hesla, zprávy nebo informace o platebních kartách). Další informace
NET::ERR_CERT_REVOKED
Pokud v Chromu chcete mít nejvyšší úroveň zabezpečení, zapněte vylepšenou ochranu
Načíst znovu
Rozšířená nastavení

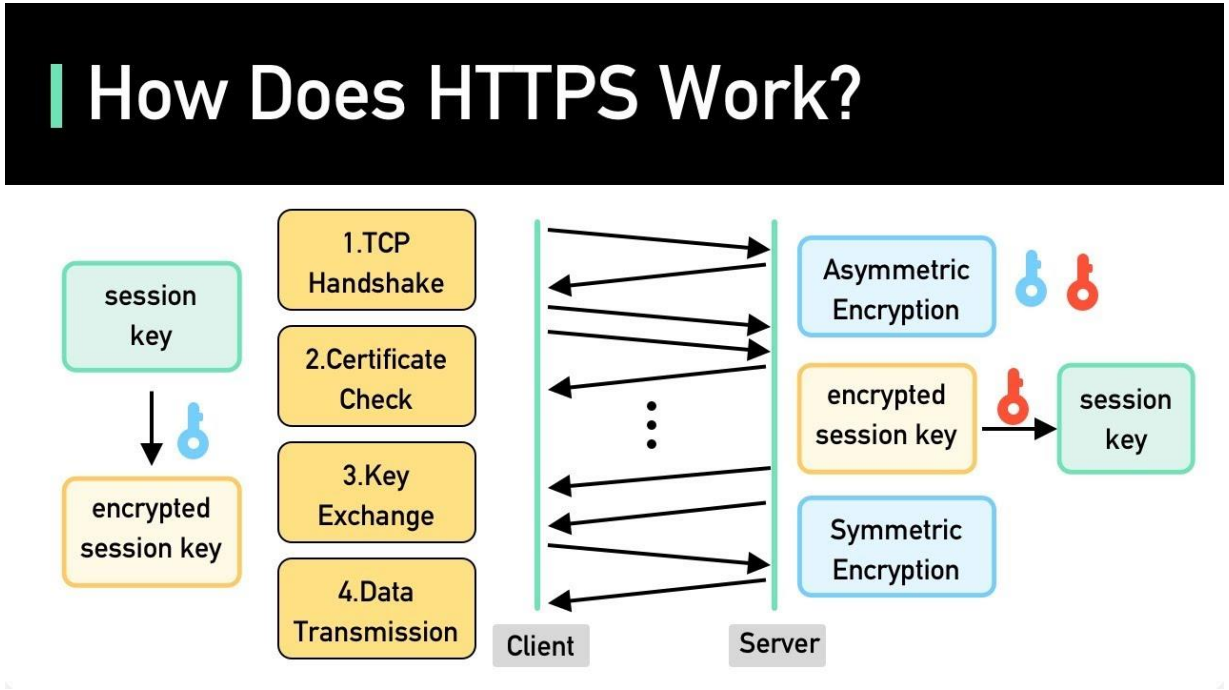
Obsah certifikátu

- **Držitel** certifikátu (Subject) – pro koho byl vydán
- **Vydavatel** (Issuer) – certifikační autorita
- **Sériové číslo** certifikátu
- **Platnost** certifikátu
- Veřejn**ý klíč** – používá se pro šifrování a ověřování komunikace
- **Digitální podpis CA** – ověřuje pravost certifikátu.
- **Algoritmus šifrování** – např. RSA, ECC nebo ECDSA.
- Rozšíření certifikátu – další informace, jako je např. podporovaná doména, použití certifikátu atd.

TYPY CERTIFIKÁTŮ

SSL/TLS

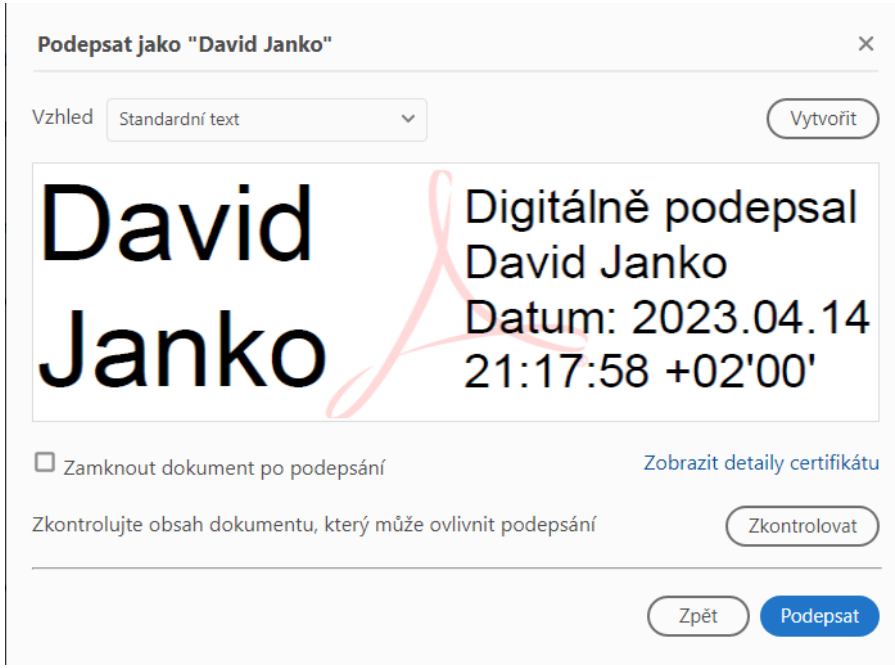
- **Šifrují komunikaci** mezi webovým prohlížečem a serverem
- Chrání před odposlechem dat
- Ověřují identitu stránky
- Zabraňuje útokům MITM



MěSOŠ Klobouky u Brna

Elektronický podpis

- **Ověřují totožnost osoby**
- **Umožňují digitálně podepsat dokument**
- Právně závazný
- Potvrzuje neměnnost dokumentu



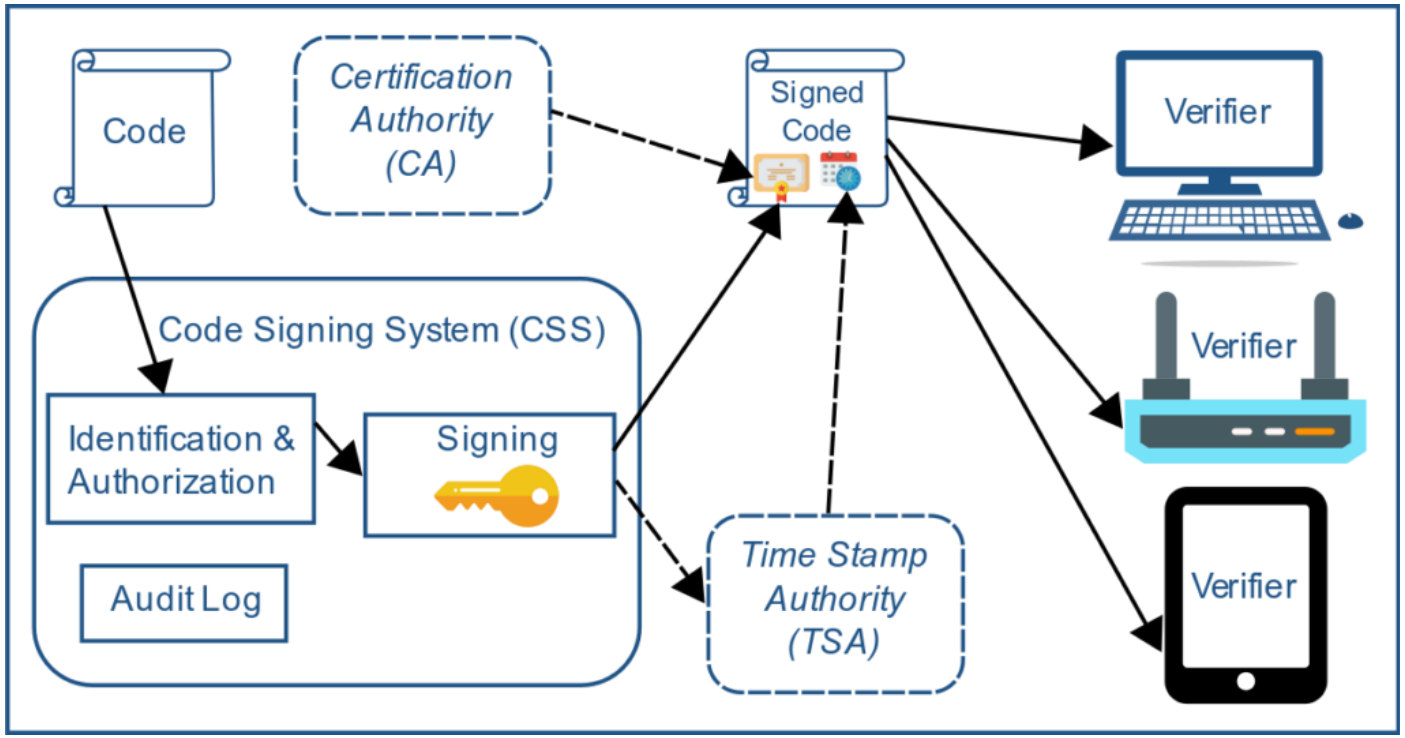
MěSOŠ Klobouky u Brna

Klientské

- **Ověřují identitu konkrétního uživatele nebo zařízení**
- Uživatel se přihlásí do systému bez hesla
- VPN připojení, firewall…

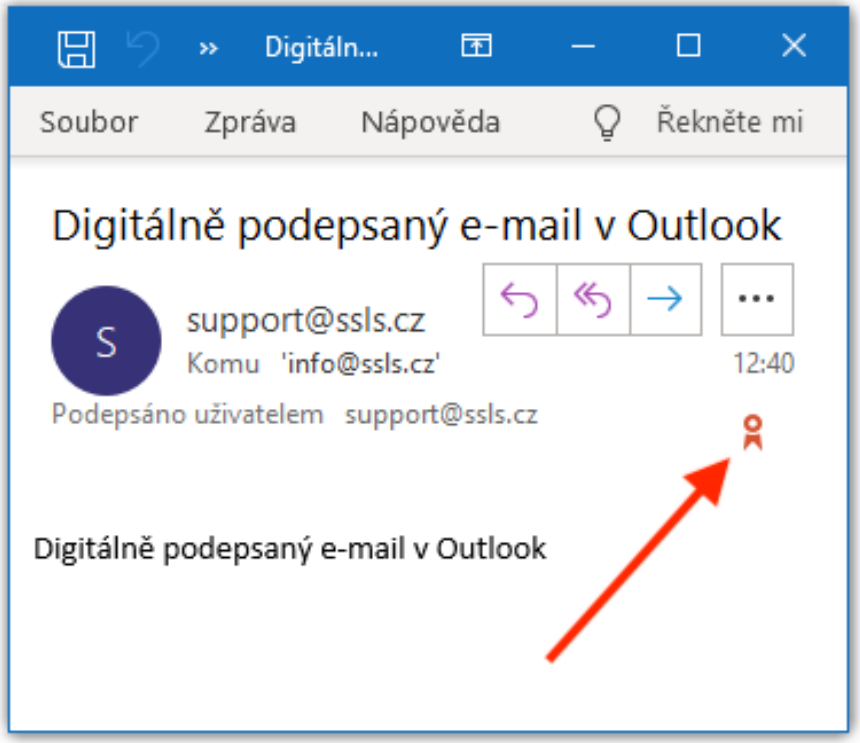
Podpis softwaru

- **Zajišťují původ důvěryhodného vývojáře a neměnnost softwaru**
- Chrání před malware



Zabezpečení e-mailu

- **Šifrují e-maily a zajišťují jejich autenticitu**
- Zabraňují odposlechu
- Kontrola identity odesílatele



MěSOŠ Klobouky u Brna

Anotace

Tato prezentace slouží k seznámení se s principy asymetrického šifrování a jeho využitím v kybernetické bezpečnosti. Zaměřuje se na základní pojmy, jako jsou veřejný a soukromý klíč, proces šifrování a dešifrování, princip RSA a role certifikačních autorit. Žáci se naučí, jak asymetrická kryptografie řeší problém distribuce klíčů a kde se v praxi používá – například v HTTPS, digitálních podpisech či zabezpečené e-mailové komunikaci.

Hlavním cílem je, aby žáci porozuměli výhodám a omezením asymetrického šifrování, pochopili jeho fungování a dokázali rozpoznat jeho využití v běžném životě.

Užité zdroje

- https://vyuka.mesosdev.cz/kb/operacni-systemy/kryptografie/asymetricke-sifrovani/

Autor: Bc. Lukáš Pospíšil

Předmět: Operační systémy

Ročník: 4.

Rok vytvoření: 2025

Poslední aktualizace: 2025

MěSOŠ Klobouky u Brna