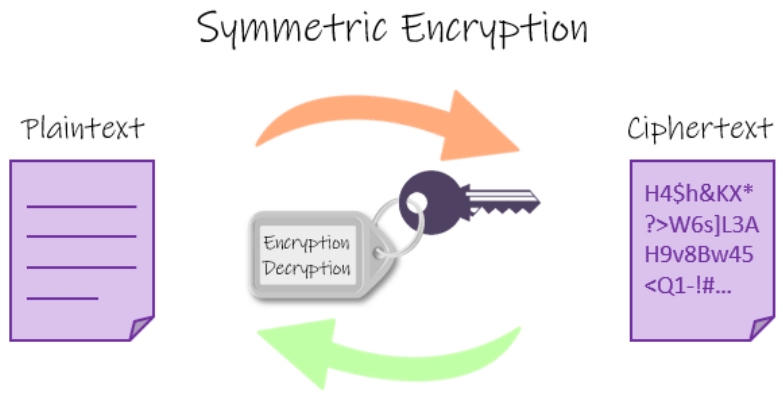
10. Zabezpečení komunikace, ACL

Kryptografie

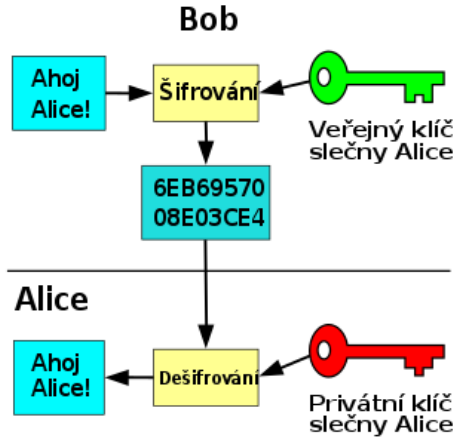
Symetrická

- K šifrování i dešifrování se používá stejný soukromý klíč
- Obě strany musí mít ke klíči přístup
- Oproti asymetrické šifře jednodušší
- Diffieho–Hellmanova výměna klíčů



Asymetrická

- Oproti symetrické není potřeba výměny klíčů
- Veřejný šifrovací klíč
  - Majitel ho uveřejní a kdokoliv jím může šifrovat jemu určené zprávy
- Soukromý dešifrovací klíč
  - Majitel jej drží v tajnosti a může jemu určené zprávy dešifrovat
- Klíče jsou matematicky svázány, z šifrovacího klíče nesmí být možno vypočítat ten dešifrovací
- Využívá se jednocestných funkcí – ze vstupu se snadno vypočítá výstup, opačný směr je velmi obtížný
- Používá se také pro elektronický podpis – možnost prokázat u dat jejich autora

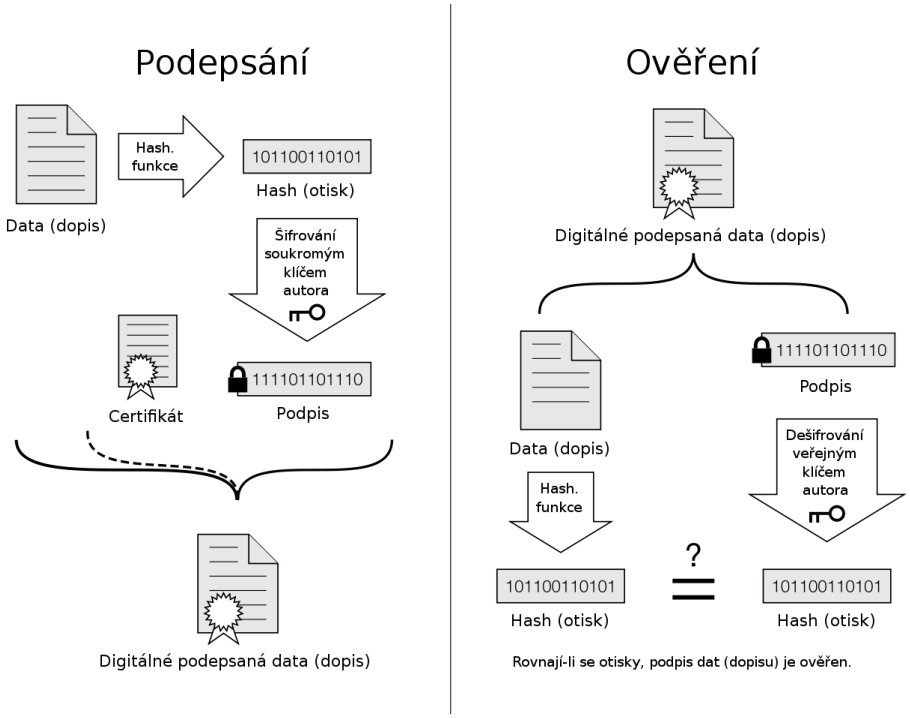


Hashování

- Funkce, která z libovolně dlouhého vstupu vytvoří vždy stejně dlouhý výstup
- Malá změna u vstupních dat vyvolá velkou změnu na výstupu
- Z hashe (otisku) je velmi obtížné zrekonstruovat původní zprávu
- Není zaručena jedinečnost hashe (množina vstupů je větší než množina výstupů)
- Použití:
    - Rychlejší prohledávání tabulek v databázi
    - Kontrola správnosti dat
    - Skladování hesel v databázi

Elektronický podpis

- Zašifrování pomocí soukromého klíče, dešifrování pomocí veřejného
- Funkce:
    - Jsou odeslány data společně s hashem dat, který je zašifrován soukromým klíčem
    - Příjemce si pomocí veřejného dešifrovacího klíče hash dešifruje (získá původní hash zprávy) a samotnou zprávu si zahashuje
    - Pokud se tyto dva hashe rovnají, je podpis validní



Digitální certifikát

- Vydáván certifikační autoritou
- Elektronicky podepsaný veřejně šifrovací klíč
- Obsahuje údaje o subjektu, jeho veřejný klíč, podpis certifikační autority, dobu platnosti, ...

Certifikační autorita

- Autorita vydávající digitální certifikáty
- Důvěryhodná třetí strana
- První certifikační autorita, Česká pošta, eldentity

VPN – Virtual Private Network

- Propojení počítačů do soukromé sítě, i když jsou na různých místech v internetu
- Veškerá komunikace přes šifrovaný tunel
- Při komunikaci se serverem vidí poskytovatel i server pouze adresu VPN serveru
- Důvěra mezi uživatelem a poskytovatelem VPN¨
- VPN se také používá pro vzdálený přístup do místní sítě nějaké firmy nebo státu

SSL – Secure Sockets Layer

- Jeho nástupce je TLS – Transport Layer Security
- Nejčastěji se používá pro šifrovanou HTTPS komunikaci
- Let's Encrypt

ACL – Access Control List

- Filtruje příchozí a odchozí pakety na základě informací v hlavičce
- Většinou je na konci zakázání veškeré komunikace, která není explicitně povolena
- Nakonfiguruje se list, který lze podle jména nebo čísla přiřadit k interface (lze specifikovat, jestli chceme příchozí nebo odchozí data)
- Standardní ACL
    - Filtruje na základě zdrojové IP adresy
    - Identifikace dle čísel 1–99, 1300-1999
    - Mělo by být umístěno co nejblíže k cíli (chceme zabránit všem adresám, ne jen adresám z konkrétní sítě)
    - `Switch(config)# access-list 5 deny host 10.5.1.10`
    - `Switch(config)# access-list 5 permit 10.5.1.10 0.0.0.255`
    - `Switch(config)# access-list 5 deny any`
    - `Switch(config-if)# ip access-group {číslo|jméno ACL} {in|out}`
- Rozšířené ACL
    - Filtruje na základě zdrojové a cílové IP adresy, protokolu, zdrojového a cílového portu…
    - Identifikace dle čísel 100-199, 2000-2699

    - Mělo by být umístěno co nejblíže ke zdroji
    -
- Jmenné ACL
    - Místo identifikačního čísla je použito jméno

Správa switche a routeru

- Telnet a SSH
- Telnet:
    - Nezabezpečený
    - Konfigurace:
        - Potřeba nakonfigurovat IP adresu
        - `Device (config)#line vty 0 4`
        - `Device (config-line)#login`
        - `Device (config-line)#password cisco`
    - Použití: `telnet adresa`
- SSH:
    - Zabezpečený
    - Konfigurace:
        - `hostname`
        - `ip domain-name`
        - `crypto key generate rsa`
        - `line vty 0 15`
        - `transport input shh`
        - `login local`
        - `ip address`
        - `username name password heslo`
    - Použití: `ssh -l name adresa`
    -