Šifrování a elektronický podpis

Některé informace, které jsou uloženy v počítačových systémech nebo jsou jimi posílány po síti, jsou tajné nebo citlivé a nikdo nepovolaný by neměl mít možnost si je přečíst. Narušil by tak základní prvek bezpečnosti - důvěrnost dat.

Největší nebezpečí hrozí během přenosu počítačovou sítí nebo při krádeži zařízení obsahujícího data. Ke znečitelnění informací jsou proto používány různé způsoby šifrování.

Často je třeba mít jistotu, kdo vytvořil nebo potvrdil obsah nějakého dokumentu. Takovou identifikací a potvrzením je v běžném životě podpis. Analogicky k podpisu papírových dokumentů vznikl ve světě počítačů podpis elektronický.

Šifrování

Šifrování je přeměna srozumitelného textu (dat obecně) na nesrozumitelný text určitým postupem, algoritmem. Opačný postup se nazývá dešifrování.

Algoritmus je v obou případech ovlivněn tajným parametrem, který se nazývá (de)šifrovací klíč. Pouze ten, kdo zná klíč, se může dostat k původní zprávě.

Šifra musí být odolná vůči pokusům o dešifrování bez znalosti klíče (prolomení). Kyberzločinci používají výkonné počítače a metody, ale pokud je šifra kvalitní, pak její prolomení trvá tak dlouho, že se nevyplatí to zkoušet.

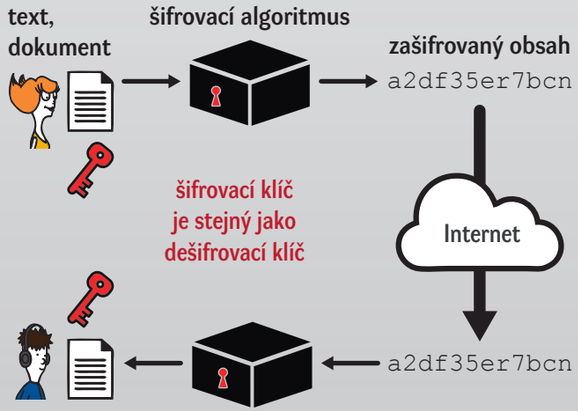
Šifrování dělíme na symetrické a asymetrické.

Symetrické šifrování

Při symetrickém šifrování oba účastnící komunikace používají tentýž společný klíč, kterým provádí šifrování i dešifrování.

Každý pár účastníků má tedy svůj společný šifrovací klíč. Před zahájením komunikace si obě strany musí dohodnutý klíč bezpečným způsobem předat.

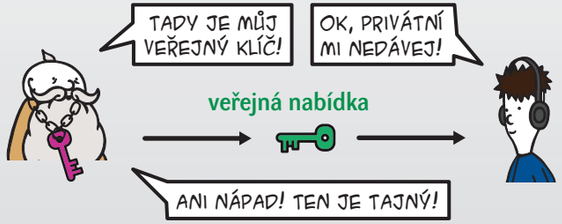
Výhodou symetrického šifrování je rychlost jeho algoritmů. Nevýhodou je nutnost bezpečného předání šifrovacího klíče. Také počet klíčů při rostoucím množství účastníků komunikace je neúměrně vysoký.



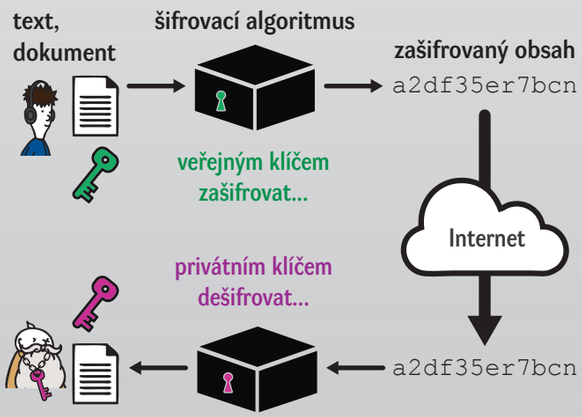
Asymetrické šifrování

Asymetrické šifrování je založeno na použití dvou šifrovacích klíčů, privátního (soukromého) a veřejného. Veřejný klíč musí být k dispozici všem zájemcům o šifrovanou komunikaci.

V případě odesílání šifrovaného dokumentu cizí osobě je nutné získat nejprve její veřejně dostupný klíč a dokument jím zašifrovat. Následně dokument může dešifrovat pouze daná osoba svým privátním klíčem.

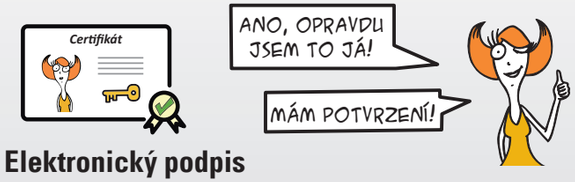


Při asymetrickém šifrování odpadá nutnost bezpečného předání šifrovacích klíčů. Počet klíčů při rostoucím množství účastníků komunikace je mnohem nižší. Nevýhodou jsou ale pomelejší algoritmy než u symetrického šifrování.



Ověření vlastníka klíče

Vlastnictví veřejného klíče danou osobou prokazuje tzv. certifikát, který vydává certifikační autorita. Ta svým mechanismem ověří, že daný veřejný klíč skutečně patří konkrétní osobě (případně webové stránce apod.). Pokud důvěřujeme certifikační autoritě, lze s jistotou pomocí certifikátu zjistit, komu patří veřejný klíč.



Elektronický podpis

Elektronický podpis znamená v kybernetickém světě to samé, co v reálném světě znamená razítko, pečeť nebo podpis vlastní rukou. Stvrzujeme jím, že jsme dokument vytvořili nebo s jeho obsahem souhlasíme.

Elektronický podpis umožňuje ověřit:

- **Autenticitu** - identitu podepisujícího
- **Integritu** - data jsou ve stejné podobě, jako v době podepsání
- **Nepopiratelnost** - podepsat lze pouze privátním klíčem a ověřit platnost lze pouze odpovídajícím veřejným klíčem, jehož příslušnost ověřuje certifikační autorita a potvrzuje ji certifikátem
- **Časové ukotvení** - elektronický podpis může obsahovat časové razítko, které prokazuje datum a čas podepsání

Jsem leták ke školení IT bezpečnosti uživatelů sítě ZČU. Školení má 10 témat. Mě, ostatní letáky, brožury a prezentace najdete na https://bezpecnost.zcu.cz.

Naší almou mater je Západočeská univerzita v Plzni a na svět jsme přišly také díky podpoře Fondu rozvoje CESNET, z.s.p.o.