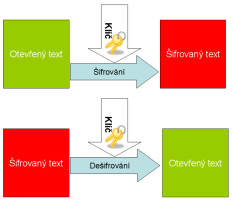
Šifrování

- princip kryptografických metod a jejich využití v praxi(symetrická, asymetrická, hybridní)
- zásada důvěrnosti
- šifrování z historického pohledu
- způsoby distribuce a uložení šifrovacích klíčů

Princip kryptografických metod a jejich využití v praxi(symetrická, asymetrická, hybridní)

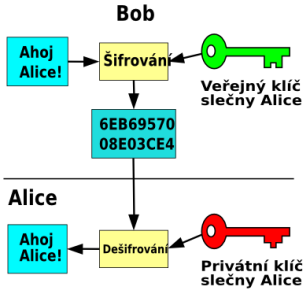
- **Symetrická**
  - vývoj od starověku po současnost
  - jeden klíč pro šifrování i dešifrování
  - většina symetrických šifrovacích algoritmů je velmi rychlá
  - síla (bezpečnost)
    - nesmí záviset na utajení algoritmu
    - síla šifer se poměřuje délkou klíče udávanou v bitech, např. 5-ti bitový klíč představuje 2^5 kombinací - tedy 32 různých klíčů (kombinací)
    - za bezpečné se dnes považují algoritmy, které používájí klíče o minimální délce 128bitů – tedy více než $3{,}4 \times 10^{38}$ kombinací



Princip fungování symetrické šifry

  - **Nevýhody**
    - nutnost sdílení tajného klíče - odesílatel a příjemce tajné zprávy se musí předem domluvit na tajném klíči
    - problém - Jak bezpečně předat klíč příjemci šifrovaných dat?
  - **Druhy**
    - **proudové šifry** - zpracovávají otevřený text po jednotlivých bitech
    - **blokové šifry** - rozdělí otevřený text na bloky stejné velikosti a doplní vhodným způsobem poslední blok na stejnou velikost
      - u většiny šifer se používá blok o 64 bitech, AES používá 128 bitů
  - algoritmy - např. DES, 3DES, CAST, IDEA, Blowfish, RC, ...
    - **DES** - algoritmus navržený pro bankovní sektor
    - RC - blokové šifry původně vyvinuté Ronaldem Rivestem a uchovávané jako obchodní tajemství firmy

- **Asymetrická**
  - používá dvojici klíčů: **veřejný** a **soukromý**
  - **veřejný klíč** může použít kdokoliv pro zašifrování zprávy
  - dešifrovat lze pouze pomocí **soukromého klíče**
  - eliminován problém s předáváním klíčů
  - algoritmy jsou výrazně (řádově 1000x) pomalejší než algoritmy symetrické
  - jelikož většina symetrických algoritmů pracuje pouze se speciálními čísly (např. prvočísly) používají se zde klíče o velikosti až 2048 bitů
  - algoritmy - např. RSA, Diffie-Hellman, DSS, ...



Princip fungování asymetrické šifry

    - **RSA** - nejznámější asymetrická šifra
        - základ většiny systému využívajících asymetrické šifrování
        - založen na problému faktorizace velkých čísel
        - faktorizace - problém rozložení čísla na součin menších čísel, v nejčastější podobě pak rozklad celého čísla na součin prvočísel (např. číslo 15 na 3×5)
    - Diffie-Hellman - systém pro výměnu kryptografických klíčů mezi dvěma stranam
        - nejedná se vlastně o šifrovací algoritmus, ale o metodu pro vyvinutí a výměnu sdíleného privátního klíče přes veřejné komunikační kanály
        - v zásadě se obě strany dohodnou na nějaké společné číselné hodnotě a pak vytvoří klíč

- **Hybridní**
    - spojuje výhody obou předchozích řešení (symetrické a asymetrické šifrování)
    - eliminuje tak jejich problémy
        - u symetrického šifrování - problém s přenosem klíče pro šifrování a dešifrování
        - u asymetrického šifrování - náročnost na výpočetní výkon
        - Princip
            - nejprve náhodně vygenerujeme klíč pro symetrickou šifru a zašifrujeme jím zprávu
            - poté klíč samotný zašifruje asymetricky
            - poté odešleme zašifrovaný klíč spolu se šifrovanou zprávou příjemci
            - ten si pomocí asymetrické šifry dešifruje klíč
            - pak pomocí klíče k symetrické šifře dešifruje i samotnou zprávu
    - bezpečnost systému je závislá na bezpečnosti obou použitých šifer
    - principy hybridního šifrování využívá např. **HTTPS** *(viz dále)*

Využití šifrování v praxi

- **HTTPS**
    - nadstavba síťového protokolu HTTP
    - umožňuje zabezpečit spojení mezi webovým prohlížečem a webovým serverem před odposloucháváním, podvržením dat a umožňuje též ověřit identitu protistrany
    - používá protokol HTTP, přenášená data jsou šifrována pomocí SSL nebo TLS, standardní port na straně serveru je **443**
    - využívá **asymetrické** šifrování (pro předání symetrického klíče) i **symetrické** šifrování (pro šifrování komunikace)
    - **Princip**
        - obě strany si před zahájením komunikace vygenerují privátní a veřejný klíč.
        - při zahájení komunikace si vymění veřejné klíče (tyto klíče by měly obě strany ověřit pomocí jiného komunikačního kanálu)
        - ověření může proběhnout kontrolou *výtahu* (otisk, hash, miniatura) veřejného klíče u protistrany
            - např. pomocí telefonu, nebo lze použít princip přenosu důvěry - protistrana předává veřejný klíč, který je digitálně podepsaný (nejlépe důvěryhodnou certifikační autoritou - VeriSign, GeoTrust, RapidSSL, ...). Digitální certifikáty jsou základním kamenem zabezpečení poskytovaného protokoly SSL/TLS.

- Šifrování je také velice důležité pro fungování **digitálního podpisu**. Digitální podpis používá pro své fungování **asymetrické šifrování**.

Zásada důvěrnosti

- Vyjadřuje potřebu uložit data tak, aby jejich obsah mohl přečíst jen ten, komu jsou určena.

Šifrování z historického pohledu

V průběhu historie se šifrování rozvíjelo, stejně tak se uplatňovaly stále složitější šifry.

- **Substituční šifry**
  - Spočívá v nahrazení každého znaku zprávy jiným znakem podle nějakého pravidla
  - **Posun písmen**
    - Každé písmeno tajné zprávy je posunuto v abecedě o pevný počet pozic. Šifra je z dnešního pohledu velmi snadno rozluštitelná, protože je jen málo možných klíčů. Ve své době ale představovala nevídanou metodu a osvědčila se velmi dobře
    - např. Caesarova šifra
  - **Tabulka záměn**
    - Šifrování pomocí tabulky záměny, které je založeno na záměně znaku za jiný bez jakékoli vnitřní souvislosti či na základě znalosti klíče

- **Steganografie**
  - Neboli ukrývání zprávy jako takové. Sem patří různé neviditelné inkousty, vyrývání zprávy do dřevěné tabulky, která se zalije voskem apod. V moderní době lze tajné texty ukrývat například do souborů s hudbou či obrázky namísto náhodného šumu.

- **Vigenèrova šifra**
  - Používá heslo, jehož znaky určují posunutí otevřeného textu

- **Vernamova šifra**
  - Jde dosud o jedinou známou šifru, o níž bylo exaktně dokázáno, že je nerozluštitelná. Podobně jako Vigenèrova šifra i tahle spočívá ve sčítání písmen otevřeného textu a hesla

- **Transpoziční šifra**
  - Spočívá ve změně pořadí znaků podle určitého pravidla. Například tak, že otevřený text je zapsán do tabulky po řádcích a šifrový text vznikne čtením sloupců téže tabulky

Způsoby distribuce a uložení šifrovacích klíčů

- **Způsoby distribuce**
  - Problémem symetrického šifrování je předávání šifrovacího klíče. Tento nedostatek řeší asymetrické šifrování. Klíč je třeba předávat zabezpečeným kanálem. Konkrétní řešení závisí na dané situaci, počtu subjektů mezi kterými je třeba klíč přenést (2 účastníci komunikace, 3 účastníci, ...), apod.

- **Uložení šifrovacích klíčů**
  - Doporučení pro uložení privátního klíče:
    - Klíč skladujte na přenosném médiu (USB flash, CD, ...)
    - Chraňte svůj privátní klíč dostatečně silným heslem pro případ, že vám někdo zcizí fyzické médium, kde jej máte uložen
    - Zálohujte klíč na jiná média uložená na bezpečných místech
    - Mějte klíč pro nejhorší scénář i vytištěný na papíře a uložený na bezpečném místě
    - Chraňte záložní klíče fyzicky (trezor) i elektronicky použitím dalších metod zabezpečení (například šifrováním celého záložního media)
    - Nezapomínejte, že elektronická média mají konečnou životnost (u DVD např. jen 2 roky)

Pojmy

- **Autentizace** - ověření identity uživatele, nejčastěji heslem, ale i otiskem prstu, předmětem atd.

- **Bezpečné heslo**
  - je takové, které není snadno zjistitelné, uhodnutelné nebo jinak snadno zneužitelné. Hesla slouží pro ochranu přístupu k nejrůznějším systémům a informacím, do kterých by se neměl dostat nikdo nepovolaný.
  - Nejbezpečnější hesla jsou tedy „nesmyslné“ kombinace znaků
  - Bezpečné heslo by mělo mít minimálně 8 znaků
  - V dobrém hesle by neměly být použité jen běžné znaky
  - Není příliš vhodné používat pouze jedno heslo jako "hlavní"

- **Jednorázové heslo** - používá se, např. když zapomenete heslo. Požádáte server o přidělení jiného, které vám bude odesláno emailem popř. sms. Toho heslo platí jen omezenou dobu.

- **Kryptografie (neboli šifrování)**- nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí
  - Šifrování může hrát významnou úlohu při každodenní komunikaci a práci s počítačem:
    - pomocí šifrování můžeme chránit informace uložené na našem počítači před neautorizovaným přístupem – a to dokonce i před lidmi, kteří jinak mají k našemu počítačovému systému přístup.
    - šifrováním můžeme chránit informace při přenosu z jednoho počítače na druhý.
    - šifrováním můžeme zabránit či detekovat náhodné nebo úmyslné změny dat.
    - pomocí šifrování je možno ověřit, zda autorem dokumentu je opravdu ten, kdo myslíme

- **Šifrovací algoritmus** - funkce sestavená na matematickém základě a provádí samotné šifrování a dešifrování dat.

- **Šifrovací klíč** - říká šifrovacímu algoritmu jak má data (de)šifrovat, podobá se počítačovým heslům, avšak neporovnává se zadaná hodnota s očekávanou, nýbrž se přímo používá a vždy tedy dostaneme nějaký výsledek, jehož správnost závisí právě na zadaném klíči.

- **Délka klíče** - ovlivňuje, kromě jiného, časovou náročnost při útoku hrubou silou – což je kryptoanalytická metoda, kdy postupně zkoušíme všechny možné hodnoty, kterých klíč může nabývat.

- **Šifra** - Kryptografický algoritmus, který převádí čitelnou zprávu neboli prostý text na její nečitelnou podobu neboli šifrový text.