ŠIFROVÁNÍ A OCHRANA DAT

Principem šifrování je převod čitelných dat na nečitelná data. Zpětný převod z nečitelných dat na čitelná data se nazývá dešifrování.

- **Kryptologie** = věda zabývající se utajováním obsahu zpráv (= šiframi)
- **Kryptografie** = věda zkoumající metody šifrování smyslu zpráv, které budou čitelné jen se speciální znalostí (= klíč); zabývá se rozvojem algoritmů, konstrukcí klíčů a snaží se udržet zprávu zašifrovanou i v situacích, kdy jí zachytí třetí strana
- **Kryptoanalýza** = věda zkoumající metody luštění šifrovaných informací; kryptoanalytici se snaží proniknout do kryptografických systémů, aby získali otevřený text (= opak skryté zprávy)
- **Steganografie** = věda zkoumající metody zakrytí existence zprávy; nemusí být nutně šifrována, ale úkolem je, aby třetí strana nevěděla, že je zpráva předávána. Tajná zpráva může být zakódována například do šumu v souboru se zvukem, obrázkem nebo videem. Zachycení zprávy ale znamená i její prolomení. Pokud je soubor chráněn podle autorského práva, stejná metoda se využívá pro vložení informace o copyrightu (= watermark).

Historie

První zmínky o utajování obsahu písma se objevovaly již ve starém Egyptě, Mezopotámii a Indii. Jednalo se o mechanické ukrytí utajovaných zpráv (překrytí zprávy vyryté do dřevěné destičky voskem).

Caesarova šifra

- každé písmeno tajné zprávy je posunuto v abecedě o pevný počet pozic
- málo možných klíčů, je dnes považována za velmi snadlo luštitelnou
- Julius Caesar ji používal při svých vojenských taženích a zvolil si posun o 3 místa

Historii kryptografie lze rozdělit do dvou částí. První je klasická kryptografie, která se vyznačovala tím, že k šifrování stačila pouze tužka a papír. Během 1. poloviny 20. století začaly vznikat různé přístroje, které umožňovaly složitější postup při šifrování. Tím začíná druhá část, které se říká moderní kryptografie. Započal ji Claude Shannon, který se považuje i za otce matematické kryptografie. V dnešní době se k šifrování používají místo speciálně vytvořených strojů především počítače a jedná se o široce dostupný a běžně využívaný nástroj.

Enigma

- mechanický stroj používaný Němci za 2. světové války k utajování zpráv
- složena z klávesnice, sady rotujících disků a reflektorů

- po stisku klávesy se uzavře elektrický obvod; proud projde sestavou rotorů, přes reflektor a zpět
- původně vybavena sadou 5 rotorů (později až 8), z nichž se vybíraly 3
- rozluštěna skupinou Ultra vedenou Alanem M. Turingem

Vernamova šifra

- jednorázová tabulková šifra
- každý znak zprávy se posune o náhodně zvolený počet míst v abecedě
- bez znalosti klíče v principu nerozluštitelná

Symetrické šifrování

- stejný klíč se používá jak pro šifrování, tak i pro dešifrování
- historicky starší
- výhodou je nízká výpočetní náročnost - rychlejší šifrování a dešifrování
- nevýhodou je nutnost sdílení tajného klíče
- **Blokové šifry** – pracuje se s bloky pevně stanovené délky (většinou 64 bitů a víc), šifrovaný text bude mít stejnou velikost jako text otevřený
    - DES (Data Encryption Standard) – jedna z prvních blokových šifer, původně určena pro šifrování dat v civilních státních organizacích USA, považována za nespolehlivou
    - AES (Advanced Encryption Standard) – používána pro bezdrátové Wi-Fi sítě
- **Proudové šifry** – pracují s proudy textu a šifrují text po jednom bitu, rychlejší, náchylnější k útokům

Asymetrické šifrování

- odesílatel požádá příjemce o jeho šifrovací klíč (= **veřejný klíč**), tímto klíčem zašifruje zprávu a odešle ji
- příjemce si pak zprávu svým dešifrovacím klíčem (= **soukromý klíč**) dešifruje
- **klíčový pár** = veřejný + soukromý klíč

- symetrické a asymetrické šifrování lze použít současně
- po navázání komunikace si pomocí asymetrického šifrování vyměníme klíč pro symetrické šifrování a další přenos probíhá pomocí něho (díky asymetrickému šifrování se vyhneme nutnosti riskantní výměny klíčů a díky následnému přechodu na symetrické šifrování pak probíhá celý proces mnohem rychleji)
- HTTPS

Ochrana dat

= proces zabezpečení digitálních informací, aby nedošlo ke ztrátě či zneužití

Způsoby zničení dat:

- **technická porucha pevného disku**
- **výpadek proudu** – pokud v tu chvíli počítač zapisuje na disk
- **smazání dat** – při vysypání koše se data fyzicky nesmažou, ale místo se označí za volné a příští stažený soubor je nahradí, pak by už nebylo možné data zachránit
- **ztráta klíče** k dešifrování dat

Způsoby ochrany:

- **ukládání** – průběžné ukládání rozpracované práce
- **zálohování** – ukládáno alespoň na dvou místech, aktivní informace, cloud či lokální úložiště, využíváno pro obnovení v případě ztráty dat
- **archivace** – uchovávání starých či neaktuálních dat:
    - **pevný disk počítače** - kopírujeme důležité soubory, mohou být prosté nebo komprimované
    - **externí pevný disk**
    - **USB disky** - výhodou je rychlá záloha a jednoduchý přenos dat
    - **datová centra** - zálohují na pásky o velikostech v GB
    - **CD a DVD** - dlouhodobější záloha dat
- **šifrování** – zajištění nečitelnosti uložených nebo zasílaných dat pro nepovolané uživatele

Zálohovat musíme pravidelně a kvalitně, funkčnost každé zálohy je potřeba ověřit

Malware:

- **Počítačový vir**
    - připojuje se k jiným programům a dále se šíří
    - může přepisovat systémové oblasti disku nebo dokonce odstranit celý obsah pevného disku
- **Počítačový červ**
    - většina červů začíná jako e-mailová příloha, která při otevření nakazí počítač
    - červ hledá soubory obsahující e-mailové adresy a tyto adresy použije k rozesílání nakažených e-mailových zpráv a často napodobuje adresu odesílatele v těchto e-mailových zprávách tak, aby to vypadalo, že je odesílatelem někdo, koho uživatel zná
- **Trojský kůň**
    - skrývá se uvnitř ostatních programů.
    - do operačního systému vloží kód, který hackerům umožní přístup k nakaženému počítači
    - jsou rozšiřovány prostřednictvím virů, červů nebo staženého softwaru
- **Spyware**
    - většinou shromažďují reklamní data a osobní údaje

Zdroje:

https://cs.wikipedia.org/wiki/Kryptografie

https://wikisofia.cz/wiki/Z%C3%A1kladn%C3%AD_rozd%C4%9Blen%C3%AD_kryptologie

https://www.napocitaci.cz/33/symetricke-a-asymetricke-sifrovani-uniqueidqOkE4NvrWuNY54vrLeM677jX7sp3Lu-ZpLpGVMy1prAV

https://studijni-svet.cz/ochrana-dat-informatika/

http://www.ivt.mzf.cz/seminar/3-bezpecnost-dat/

https://sifrovani.fd.cvut.cz/index.html

https://cs.m.wikipedia.org/wiki/Bloková_šifra

https://cs.m.wikipedia.org/wiki/Proudová_šifra

https://www.zebra.cz/zalohovani-nebo-archivace/