Kryptologie

Věda, která se zabývá šifrováním ze všech úhlů pohledu. Věda o matematických technikách spojených s hledisky informační bezpečnosti, jako je důvěrnost, integrita dat, autentizace a autorizace.

Kryptografie

Věda o šifrování a dešifrování dat za pomoci matematických metod.

Kryptoanalýza

Věda zabývající se metodami zjištění původní informace ze zašifrované bez znalosti klíče. Věda o analýze slabin šifrovacích systémů.

Steganografie

Věda zabývající se utajením komunikace prostřednictvím ukrytí zprávy. Zpráva je ukryta tak, aby si pozorovatel neuvědomil, že komunikace vůbec probíhá. Nemění obsah zprávy, jen tajnou informaci maskuje.

Rozdělení šifer

- Klasické
    - Všechny jsou symetrické, používají jeden sdílený klíč
- Mechanické
    - Například kufřík na kód
- Moderní
    - Symetrické, asymetrické, hybridní

Další dělení

- Kód a kódová kniha
    - Kódová kniha je slovníkem, ve kterém jsou vybraná slova nebo věty otevřeného textu nahrazované kódy
- Transpoziční šifry
    - Přeskládání znaků zprávy jiným způsobem
    - Znalost postupu umožňuje text zpětně sestavit/dešifrovat
- Substituční šifry
    - Nahrazení znaků zprávy jinými znaky
    - Je zachována pozice písmen

Druhy substitučních šifer

Monoalfabetická (jednoduchá) substituční šifra

● Každý znak otevřeného textu je nahrazen příslušným znakem šifrovaného textu.
● Caesarova šifra, Atbash, přeházená abeceda

Homofonní substituční šifra

● Jeden znak otevřeného textu může být nahrazen jedním z několika možných znaků šifrovaného textu. Znak A může být nahrazen např. 11,17, 84 apod.
● Počet znaků zašifrovaného textu pro jeden otevřeného textu se může lišit.

Polygramová substituční šifra

● Šifrování probíhá mezi skupinami znaků . Skupina AA může být nahrazena skupinou JS, AB skupinou LM atd.
● Playfair (anglický čtverec), Bifid, Hillova šifra

Polyalfabetická substituční šifra

● Skládá se z několika jednoduchých šifer, které se pro jednotlivé znaky otevřeného textu postupně střídají.
● Vigenerův čtverec

Historie

- **Egypt** - hieroglyfy
- **Atbaš** - jednoduchá substituční šifra, posunutá abeceda
- **Scytale** - hůl, na niž se namotala páska z látky, papyru či pergamenu, na ni se napsal text. Páska se pak odeslala příjemci, jenž musel mít hůl o stejném průměru, aby namotanou pásku mohl přečíst
- **Polybiův čtverec** - převodu znaků na dvojici čísel (1-5) pomocí čtverce, do kterého se zapisují znaky abecedy
- **Caesarova šifra** - každý znak se nahradí znakem, který je v abecedě o 3 pozice za ním
- **Frekvenční analýza** - první arabská metoda kryptoanalýzy, která spočívá procentuální vyjádření výskytu písmen v daném jazyce
- **Vigenérova šifra** - používá více šifrových abeced, které se při šifrování pravidelně střídají, každé písmeno může být reprezentováno ne jedním, ale několika jinými, velké množství klíčů, které kryptoanalytik není schopen vyzkoušet
- **Morseova abeceda**
- **Vernamova šifra** - použití jednorázového náhodně vygenerovaného hesla, které má stejnou délku jako zpráva sama, zvaná též „**one-time pad**“(jednorázová tabulka)
- **Enigma** - Stroj připomínající psací stroj, Šifrovací mechanismus se skládá z prostoru, na jehož stranách jsou dvě kola, mezi která se vkládají další tři kola. Obě krajní kola mají 26 kontaktů, které odpovídají jednotlivým písmenům abecedy. Tři vnitřní kola se vybírají z pěti možných různých kol. Vždy, když je stisknuto písmeno na klávesnici, tak se první kolo otočí o jednu pozici. Poté, co se první okolo otočí 26x, otočí se druhé a nakonec třetí. Dostáváme tak celkem 26x26x26, tj. 17 576 různých stavů.

Symetrické a asymetrické šifrování

- Symetrické
    - odesílatel i příjemce používají stejný klíč
    - dešifrovací algoritmus je inverzí šifrovacího
    - jednoduchost šifrovacího a dešifrovacího algoritmu, rychlost
    - pro tajnou komunikaci je nutné si bezpečným kanálem předem předat klíč

    - Příklady:
        - Proudové
            - Zpracovávají text po jednotlivých bitech
            - FISH, RC4
        - Blokové
            - Šifrují data po blocích dané délky
            - DES, Tripple DES, AES, IDEA, BLOWFISH
- Asymetrické
    - odesílatel použije jiný klíč než příjemce (např. soukromý a veřejný klíč)
    - algoritmy šifrování a dešifrování jsou obecně různé
    - odpadá nutnost přenosu (distribuce) klíče, pro více uživatelů není potřeba tolik klíčů
    - velmi vysoké výpočetní nároky, nízká rychlost (10tis. až 100tis. krát pomalejší)
    - Příklad: RSA

Útoky proti šifrám

- Útoky přímo na šifrovací algoritmus (na jeho matematickou část)
- Znalost zašifrovaného textu
    - Máme k dispozici několik zašifrovaných textů, můžeme využívat informace - statistické rozbory, pravděpodobnost.
- Znalost otevřeného textu
    - Máme šifrované zprávy i otevřený text a chceme získat klíč, podle kterého je zpráva šifrována
- Zvolený otevřený text
    - útočník získá k libovolnému zvolenému otevřenému textu odpovídající šifrovaný text a může získat informace o klíči
- Frekvenční analýza
    - V celém šifrovaném textu se vyčíslí počet a pravděpodobnost každého znaku a seřadí se do sloupcového grafu
    - Podle vzorů jazyků určíme, jaké znaky odpovídají písmenům daného jazyka

- Útok hrubou silou
    - Útok založený na vyzkoušení všech možných kombinací daného hesla nebo textového řetězce
    - Čím delší, tím je útok více náročnější na výkon hardwaru
- Slovníkový útok
    - Vylepšený útok hrubou silou
    - Zkouší hesla z předpřipraveného slovníku
    - Spoléhá na “hloupost” uživatele, uživatel chce mít dobře zapamatovatelné heslo
- Sociometrické útoky
    - Využití metod sociálního inženýrství – využití lidského faktoru, neznalosti, manipulace

Hashovací funkce

Jsou to funkce, které umí udělat vzorek jakéhokoli souboru, aby byl závislý na všech bitech původního souboru. Hash je algoritmus, který vygeneruje digitální otisk souboru. Výstupem funkce je hash o pevné délce. Hashovací (vzorkovací) funkce jsou velmi důležité pro kryptografii a tvorbu digitálních podpisů. Obecně se hashovací funkce používají pro kontrolu zachování integrity dat, digitální podpisy, kontrolu uložených hesel a porovnávání obsahu dvou kopií dat. Nejpoužívanější hashovací funkce jsou MD5 (prolomená), SHA-1(prolomená), SHA-2(neprolomená) a bcrypt(neprolomená).

Elektronický podpis

Elektronický podpis zajišťuje několik různých věcí. První z těch důležitějších je zajištění integrity dokumentu. Pokud obdržíme elektronicky podepsaný dokument, lze ověřit, že od jeho podpisu nebyl změněn. Elektronický podpis lze použít i k tomu, aby příjemce dokázal ověřit, že odesílatel je opravdu tím, za koho se vydává.

Elektronický podpis je kousek binárních dat, který lze připojit k dokumentu. K vytvoření podpisu potřebujete podpisový klíč. Ten má dvě části − soukromou a veřejnou. Ty lze vytvořit zároveň, ale jedna z druhé nelze spočítat.