Kryptologie - technický obor zabývající se ochranou přenosu informace
Kryptografie - zabývá se konstrukcí šifrovacích klíčů, tedy nástrojů napomáhající k šifrování zpráv
Steganografie - hlavním úkolem je zakrýt existenci zprávy
Kryptoanalýza - dala by se označit za protiklad kryptografie. Zkoumá vlastnosti otevřeného textu, šifrovaného textu

Symetrické šifry (k zašifrování se používá klíč, který je nutná sdílet s příjemcem, který ho díky tomuto klíči dešifruje)

- Jeden klíč (symetrický, konvenční) je použit pro obě operace – šifrování i dešifrování
- Nutnost sdílet klíč
- **Blokové šifry** - pro šifrování datových souborů **(AES, DES)**
  - **Režimy činnosti** - způsoby řetězení dat z výstupu na vstup, aby se nešifrovali stejné bloky (CBC, ECB)
- **Proudové šifry** - (bit po bitu) aplikace pro přenos telekomunikací/datastream. **(RC4)**

S-Box (substituční) a P-Box (permutační) - Základním stavebním blokem algoritmu **DES** je jednoduchá kombinace těchto technik (tj. substituce, následovaná permutací), která je modifikována hodnotou klíče

Asymetrické šifry (RSA, Diffie-H., DSA) (odesílatel si vyžádá příjemcův **public key** a tím zprávu zašifruje, jediný, kdo může potom zprávu dešifrovat je příjemce s jeho **private key**. Kdyby to udělal někdo jiný, dešifruje se nesmysl).

- Asymetrický klíčový pár (privátní, veřejný)
- Odpadá nutnost sdílení klíče před inicializací komunikace
- Vysoké výpočetní nároky
- Nutnost dobře zabezpečit a kontrolovat veřejný klíč

Jednocestné funkce - Jednocestné funkce - operace, které lze snadno provést pouze v jednom směru (ze vstupu lze snadno spočítat výstup, z výstupu je však velmi obtížné nalézt vstup.) *(Poštovní schránka, míchání barev)*

Hybridní šifry - data se šifrují symetricky, klíč se pošle pomocí asymetrických klíčů

Substituce (nahrazení) - znaky jsou nahrazeny za jiné, pořadí znaků zůstane zachované
Transpozice - přeskupení znaků

Diffie-Hellman

- Cílem je přes nezabezpečený kanál vytvořit mezi stranami šifrované spojení, bez předchozího dohodnutí šifrovacího klíč
- Cílem je sestavit sdílený symetrický klíč pro hlavní datový provoz
- je nutné aplikovat digitální podpisy a certifikáty pro autorizaci údajů (**kvůli man in the middle**)

Man-in-the-middle - funguje na principu prostředníka v komunikaci, který přeposílá a zároveň má možnost číst tok obou stran (jakoby se vydává za jednoho z nich)

- **Ochrana** - digitální podpisy a certifikáty pro autorizaci údajů

Hash Algoritmy (ideálně 160 bitů) - bCrypt knihovna

- Uložení hesel systému (aby nebyly uloženy v plain textu)
- Systém nemusí znát heslo uživatele, stačí znát hash
- Při změně jen jednoho bitu se mění i hodnota hashe
- **MD5 (prolomen), SHA, SHA-2 algoritmy**

Útoky na šifry

- Brute force (zkouším dokud to nevyjde), musím znát co hledám
- Pokus omyl
- Lineární
- Dictionary útok (nejčastější kombinace, slova…)

Ciphertext-only attack - Odvodit co nejvíce otevřených textů nebo úplně nejlépe klíč použitý k zašifrování.

Known-plaintext attack - Je k dispozici zašifrovaný text, ale i odpovídající otevřený text - hledám klíč

Chosen-plaintext attack - Je k dispozici zašifrovaný text i odpovídající otevřený text, útočník si vybírá bloky, které šifruje - hledá klíč

Brute force attack - musím znát to, co hledám a kdy mám ten algoritmus zastavit

Útok postranními kanály - útok na fyzickou realizaci (analýza možných úniků informací při elektromagnetickém vyzařování…)

Velké množství útoků pomocí sociálního inženýrství **(phishing, pharming)** nebo i fyzické napadnutí.

Kryptoanalýza monoalfabetických substitučních šifer - založena na vlastnostech jazyka

- Analýza četnosti výskytu jednotlivých znaků (frekvenční analýza)
- Vyhledávání typických shluků (poslední znaků slov, poměr souhlásek, samohlásek)

Kryptoanalýza polyalfabetických substitučních šifer - určí se počet použitých substitucí, dále dokument rozdělíme na části, šifrované stejnou substitucí a na tyto části použijeme postupy analýzy monoalfabetických šifer.

Index koincidence - dá se díky němu odhadnout, jak moc velké je klíčové slovo

Kasického metoda - odhadování pomocí společného dělitele nějakých shluků, které se vyskytují od sebe v textu

RSA

- Založen na předpokladu obtížnosti rozložit velké číslo na součin prvočísel – **faktorizace**
- **Posílání dat -** Šifruje se veřejným a dešifruje privátním
- Vypočítá se jejich součin **n = p * q.**
- Vypočte se hodnota **Eulerovy funkce: φ(n) = (p − 1)(q − 1).**
- **Veřejný klíč složen z (n -** modul**, e -** veřejný exponent**)**
- **Soukromý klíč složen z (n -** modul**, d -** dešifrovací, soukromý exponent**)**
- Šifrování **- c = m^e mod n**
- Dešifrování **- m = c^d mod n (m -** zpráva**, c -** šifra**)**

DSA

- Založen na výpočtu **diskrétního logaritmu**
- **Podepisování** - Šifruje se privátním a dešifruje veřejným

Vernamova šifra - nerozluštitelnost - nelze použít brute-force (klíč je dlouhý jako zpráva sama, je náhodný a nelze ho použít opakovaně)

Polyalfabetická šifra

- **Vigenérova šifra** - Založena na 26 monoalfabetických substitucích a využívá klíčové slovo
- V podstatě tabulka, kde je první řádek abeceda v plain textu a postupně se posune začátek o jednu
- Hledá se průsečík s klíčem

Monoalfabetická šifra

- Pevný posun **(caesarova šifra)**
- Reversní abeceda
- Lineární posun **(afinní šifra)**
- Substituce klíčovým slovem

Frekvenční analýza

- Pomocí frekvenční analýzy lze rozhodnout zda se jedná o transpoziční či substituční systém
- U transpoziční se pozná posun a u substituční s změní četnost jiných znaků
- Počítá frekvenci znaků

Statistická analýza

- Souvisí se zpracováním přirozeného jazyka (poměry souhlásek, samohlásek)
- Jaká je pravděpodobnost, který znak je na začátku slova...

Substituční šifry - Caesarova šifra, Vernamova, Playfair šifra
Transpoziční šifry - Zubatka, Transpozice v tabulce…
Hybridní -

Steganografie

- Snaha o ukrytí zprávy - nepřitahuje pozornost
- **Fyzická** - skrytí zprávy uvnitř voskových tabulek, neviditelné inkousty
- **Digitální** - ukrývání do obrázků, zvukových stop, a mm souborů
- **Lingvistická** - modifikace nosného textu, aby ukryl tajný text (každé druhé písmeno ve slově)

Least Significant Bit - nejméně významný bit - spočívá v neschopnosti lidského oka poznat rozdíl mezi dvěma barvami, které se liší právě v LSB

Nulové šifry (nezašifrované zprávy) - skutečná zpráva je obsažena v textu jiné, neškodně vypadající zprávy

Digitální vodoznak - vložení informace do digit. dokumentu tak, že je obtížné ji najít nebo odstranit. Vodoznak nelze odstranit jednoduchou úpravou.

Stegoanalýza - opakem **steganografie** - odhaluje a detekuje skryté informace

Kvantová kryptologie

- **Jev neurčitosti** - měření způsobuje změnu vlastností v kvantovém stavu - detekce narušitele
- Hlavní komunikační je symetrický na základě klíče, který se domluví kvantovýma principama
- Optický jev - (BB84) **polarizace**

Šifrování deterministickým chaosem

- Modulace (práce se signály)
- Chaotické maskování
- Chaotické klíčování
- CML Systémy

CML Systémy - Zalozený na motylím effektu (citlivost na počáteční podmínky)
- synchronizace chaotického systému na obou stranách

Eliptické křivky

- Výhoda - **kratší klíče** - efektivnější výpočty certifikátů a podpisů

Délka klíče (délka klíčového prostoru)

- Substituční - permutace **k!**
- Klasický systém **- n^k (n - abeceda, k - délka klíče)** třeba abeceda 26 znaků a délka klíče 8 > **26^8**