Kryptografia: Úvodná príručka pre stredoškolákov

Úvod

V modernej digitálnej dobe prebieha väčšina našej komunikácie a úloh online. Keď si píšeme so spolužiakmi, platíme kartou, prihlasujeme sa do sociálnych sietí alebo posielame e-maily – všetko to zahŕňa prenos údajov cez siete, ktoré nemáme plne pod kontrolou. Mohli by nastať veľké problémy, ak by niekto tento prenos odpočúval, alebo upravoval, alebo sa len tak pozeral, čo robíme.

A práve pretoje dôležité **šifrovanie**.

Čo je to šifrovanie? Neformálne povedané, **šifrovanie je spôsob, ako urobiť správu nezrozumiteľnou pre kohokoľvek, kto nemá potrebný kľúč**. Je to proces, ktorý premieňa čitateľnú informáciu na niečo, čo vyzerá ako náhodný text. Tento nezrozumiteľný text sa dá opäť previesť späť na pôvodnú formu, ale iba pomocou správneho kľúča.

Prečo je šifrovanie dôležité?

- Chráni naše súkromie (správy cez WhatsApp, na Messengeri).
- Chráni heslá a osobné údaje.
- Komplikuje útoky hackerov.
- Umožňuje bezpečné bankové transakcie.
- Je základom kyberbezpečnosti.

Bez šifrovania by internet jednoducho **nebol bezpečný**.

Cieľ a obsah tejto príručky

Cieľom tejto knihy je poskytnúť zrozumiteľný a ľudský úvod do kryptografie. Budeme sa venovať najmä **symetrickým blokovým šifrovacím metódam** a tiež jednoduchým klasickým šifrovacím technikám, ktoré pomôžu pochopiť základné princípy.

Obsahovo sa postupne dostaneme od základov až ku konkrétnym algoritmom.

---

1. Základné pojmy

Aby sme mohli rozprávať a správne pochopiť šifrovaniu, je potrebné, aby sme si najprv objasnili niektoré dôležité pojmy.

1.1 Abecedy, slová, jazyky, správy

Šifrovanie pracuje s **textom**. Text je postupnosť znakov z určitej **abecedy**.

- **Abeceda**: množina symbolov, napr. slovenská abeceda, ASCII, binárna {0,1}.
- **Slovo**: konečná postupnosť symbolov nejakej abecedy.
- **Správa**: text, ktoré chceme preniesť od odosielateľa k príjemcovi.
- **Jazyk**: množina všetkých platných slov vytvorených nad nejakou abecedou.

Príklad: Správa „AHOJ“ je jednoslovný text, v ktorom je slovo vytvorené nad abecedou slovenských veľkých písmen.

1.2 Kryptosystém

Základné rozdelenie:

Kryptografia – veda o šifrovaní.

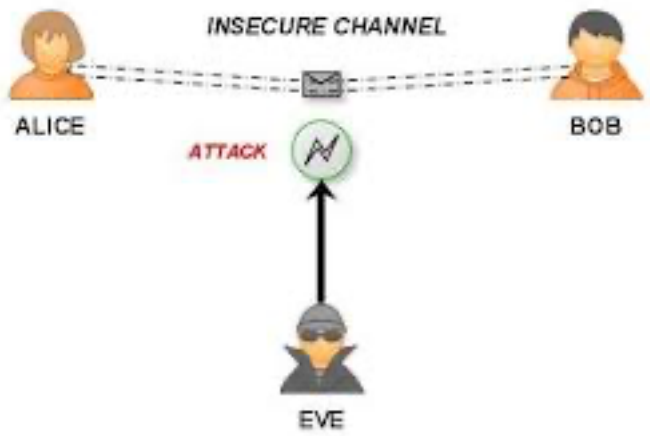
Kryptoanalýza – veda o prelomení šifier.

Kryptosystém obsahuje: - množinu správ (otvorený text), - množinu šifrovaných textov, - množinu kľúčov, - algoritmus šifrovania, - algoritmus dešifrovania.

1.3 Schéma Alica – Bob – Eva

Toto je klasická modelová situácia:

- **Alica** posiela správu.
- **Bob** je príjemca.
- **Eva** (odpočúvajúca) sa snaží správu zachytiť alebo prelomiť.



1.4 Otvorený a šifrový text

- **Otvorený text (plaintext)** – klasický text, ako ho napíše autor (čitateľná podoba).
- **Šifrový text (ciphertext)** – text po aplikovaní šifry (nezrozumiteľná podoba).

1.5 Neformálny popis šifrovania a útoku

Šifrovanie:

Autor textu alebo iná entita aplikuje na otvorený text nejakú šifru s určitým kľúčom, s cieľom spraviť text nečitateľným pre kohokoľvek, kto nepozná kľúč.

Dešifrovanie:

Príjemca textu sa snaží pomocou kľúča spätne rozlúštiť šifrový text za zisku otvoreného textu.

Útok:

Útočník získa zašifrovanú správu a aplikovaním rôznych metód sa snaží získať pôvodnú správu. Podľa vyšie spomínanej schémy Alica-Bob-Eva je tým útočníkov Eva.

Eva sa snaží určiť: - kľúč, - otvorený text, - alebo oboje.

---

2. Šifra – definícia, úloha kľúča a príklady

2.1 Definícia šifry

Šifra je metóda, ktorá pomocou kľúča premieňa otvorený text na šifrovaný text a naspäť.

2.2 Úloha kľúča

Kľúč je parameter, ktorý určuje, ako presne šifra funguje. Bez kľúča by bola šifra príliš ľahko prelomená.

---

3. Klasifikácia šifier

3.1 Symetrické šifry

- rovnaký kľúč slúži na šifrovanie aj dešifrovanie

Blokové šifry

- spracúvajú text po blokoch

Prúdové šifry

- šifrujú znak po znaku (napr. Vernamova šifra)

3.2 Asymetrické šifry

- používajú verejný a súkromný kľúč

V tejto príručke sa budeme venovať najmä:

- symetrickým šifrovacím metódam
- jednoduchým historickým šifrom

---

4. Jednoduché šifry

V tomto odseku si predstavíme niektoré zaujímavé, jednoduché šifry: Caesarova šifra, Affinná šifra, Vernamova šifra, Permutačná šifra

Každá bude obsahovať: opis, príklad, algoritmus, Python implementáciu, kryptoanalýzu??.

4.1 Caesarova šifra

4.2 Šifra Affine

4.3 Vernamova šifra

4.4 Vigenèrova šifra

---

5. Symetrické blokové šifry – prehľad

---

6. Praktická úloha – program v Pythone

TO DO

---

7. Zhrnutie

Podstata tejto príručky bolo naučiť sa čo je šifrovanie a prečo je dôležité, aké sú základné šifry, ako fungujú a ukázať si na nich ako funguje kryptoanalýza, prečo je dôležitá...

V tejto príručke sme sa naučili: čo je šifrovanie a prečo je dôležité, ako funguje kryptosystém, ako vyzerá komunikácia medzi Alicou, Bobom a Evou, - aké sú základné typy šifier, - ako fungujú jednoduché klasické šifry, - čo znamená kryptoanalýza.