Cipher (Šifra)

Šifra je základním nástrojem kryptografie. Na rozdíl od kódu (který nahrazuje celá slova či pojmy symboly) šifra pracuje s jednotlivými znaky nebo bity dat. Moderní šifry jsou založeny na složitých matematických operacích, které jsou bez znalosti klíče prakticky neprolomitelné.

Základní rozdělení šifer

Podle toho, jakým způsobem se pracuje s klíči, dělíme šifry do dvou hlavních kategorií:

1. Symetrické šifry (Symmetric Ciphers)

Používají **stejný klíč** pro šifrování i dešifrování. Jsou velmi rychlé a vhodné pro přenos velkých objemů dat.

- **Příklady:** AES (standard pro bankovnictví a HTTPS), ChaCha20, DES (zastaralé).
- **Výhoda:** Rychlost.
- **Nevýhoda:** Nutnost bezpečného předání klíče mezi oběma stranami.

2. Asymetrické šifry (Asymmetric Ciphers)

Používají dvojici klíčů: **veřejný klíč** (pro šifrování) a **soukromý klíč** (pro dešifrování). Jsou matematicky mnohem náročnější.

- **Příklady:** RSA, ECC (Eliptické křivky).
- **Výhoda:** Bezpečné – soukromý klíč nikdy neopustí vaše zařízení.
- **Nevýhoda:** Pomalost, nejsou vhodné pro velké soubory (používají se k předání symetrického klíče).

Typy šifer podle způsobu zpracování

Typ	Popis	Příklad
Proudové (Stream)	Šifrují data bit po bitu nebo znak po znaku. Ideální pro streamování audia/videa.	ChaCha20, RC4
Blokové (Block)	Rozdělí data na pevné bloky (např. 128 bitů) a ty šifruje jako celek.	**AES**

Historický vývoj (Od papíru k čipům)

1. **Substituční šifry:** Nahrazení znaku jiným (např. Caesarova šifra: A → D). 2. **Transpoziční šifry:** Změna pořadí znaků ve zprávě (přesmyčky). 3. **Mechanické šifry:** Legendární německý stroj **Enigma** z 2. světové války. 4. **Digitální šifry:** Moderní algoritmy využívající operace jako XOR, rotace bitů a složité substituční tabulky (S-boxy).

Co tvoří sílu šifry?

Bezpečnost moderní šifry nesmí záviset na utajení jejího mechanismu (tzv. Kerckhoffsův princip), ale pouze na **tajnosti klíče**. Síla je dána:

- **Délkou klíče:** Udává se v bitech (např. AES-256). Čím delší klíč, tím více kombinací musí útočník zkusit (Brute Force).
- **Kryptanalýzou:** Odolností algoritmu vůči matematickým trikům, které by zkrátily hledání klíče.

Praktické využití

Dnes se se šiframi setkáváte na každém kroku:

- **SSL/TLS:** Zabezpečení webových stránek.
- **End-to-End šifrování:** WhatsApp, Signal (zprávy si přečte jen odesílatel a příjemce).
- **Šifrování disku:** BitLocker nebo FileVault chrání data v notebooku při krádeži.

Související pojmy: Kryptografie, Šifrování, Klíč, AES, RSA, SSL/TLS, Hashování, Brute Force.