23 Kryptografie, šifrování, kódování. Vysvětli pojmy kryptografie, šifrování, kódování, steganografie, kryptoanalýza, symetrické šifrování, asymetrické šifrování, klíč, hash… a jejich praktické použití.

Kódování
- převod informace se známým zpětným postupem
- neslouží primárně k utajení dat, jen k jejich lepšímu zápisu (morseovka)

Šifrování
- převod informace, je třeba znát tajný klíč
- slouží k utajení informace

Kryptologie
- věda zabývající se tvorbou a prolomováním šifer
- studium kódů, z pohledu utajení i prolomení

Kryptografie
- věda zabývající se vytvářením šifer i zabezpečováním zprávy

Kryptoanalýza
- věda zabývající se pronikáním do šifer, hledá slabiny
- získává zašifrovaná data bez toho, aby měla klíč

Steganografie
- věda zabývající se utajením komunikace
- skrývání samotné existence zprávy

Ciphertext
- zašifrovaný text

Plaintext
- prostý, jednoduchý text

Key
- v kryptografii – řetězec čísel nebo písmen sloužící ke kódování, dekódování¨

Keyspace
- kompletní množina všech možných klíčů

Základní principy bezpečnosti informací

Confidentiality (důvěryhodnost)

- pouze oprávněné osoby mají přístup k datům

Integrity (celistvost)

- chrání před jakoukoliv neoprávněnou změnou informací
- to zaručuje přesnost a správnost dat, jestli nebyli změněny při přenosu
- musíme kontrolovat přístup na daných úrovních v systému, ale i aby lidi měli přístup k datům, která můžou

Autenticity

- slouží k zjištění o tom, že komunikujeme s tím, s kým chceme

Symetrické šifrování

- má 1 klíč – stejný pro zašifrování i rozšifrování
- dobrá k zašifrování vlastních dat
- nevhodný pro šifrovanou komunikaci – problém, když šifra unikne
- dělení – Proudová, Bloková

Proudová

- šifrujeme postupně bit po bitu
- streamy
- **RC4** – protokoly SSL, VEP, VPA
- **CHACHA20**

Bloková

- data rozsekáme na bloky stejné velikosti
- šifrujeme celé bloky najednou
- pokud nemají bloky stejnou velikost, tak se udělá padding – dopočtení

DES – Data Encryption Standard

- starší šifra, 64bitové bloky
- klíč – 56 bitů – zbylých 8 = parita
- dnes není doporučený – dnes se lehce prolomí
- odvádí se 16 kol šifrování

AES – Advanced Encryption Standard

- 128bitové bloky, velikost klíče – 128, 192, 256 bitů
- podle velikosti klíče se odvádí kola šifrování – 10, 12, 14
- bezpečnější, náročnější na výpočty, čas
- efektivní na HW i SW

3DES
- zpětně kompatibilní s DES
- pomalejší než AES
- 56bitové klíče
- zůstává v aplikacích, kde by bylo složité přejít na AES

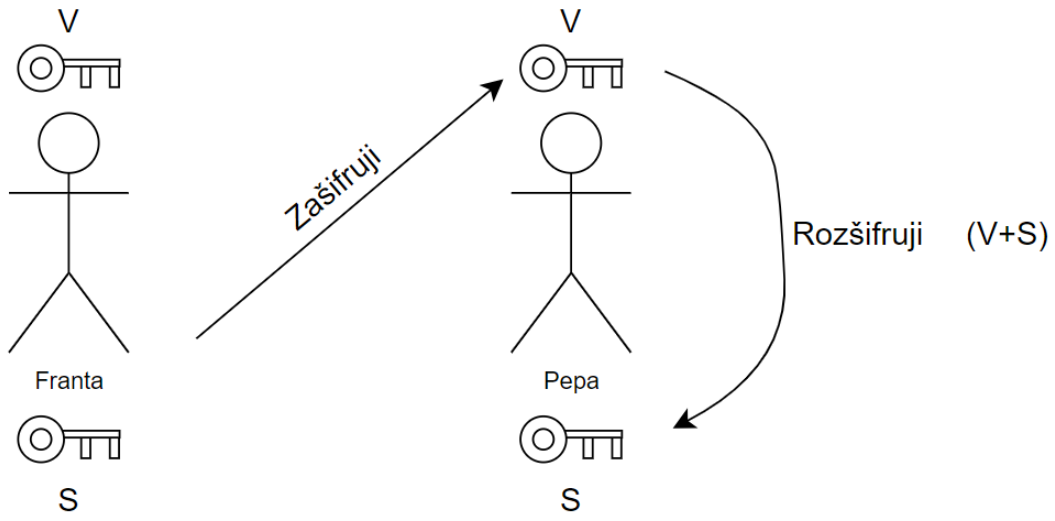
Blowfish
- rychlá a efektivní v SW implementacích
- 64bitové bloky
- variabilní délka klíče – 32-448 bitů

Twofish
- 128bitové bloky
- klíče až do 256 bitů

Serpent

Kuznyechik
- ruský, 2015

Asymetrické šifrování



- každý má 2 klíče – Veřejný a Soukromý
- zašifrujeme cizím veřejným klíčem (Franta zašifruje Pepovo veřejným klíčem)
- Pepa rozšifruje pomocí svého veřejného a soukromého klíče (jsou matematicky propojeni)
- já už zpátky nerozšifruji, protože nemám jeho soukromý klíč
- veřejný klíč můžeme klidně dát na internet – dokud nemají soukromý klíč, tak jim je samotný veřejný k ničemu

RSA – Rivesta Shamir Adelman
- první algoritmus, který byl vhodný jak pro šifrování, tak pro podepisování
- nejvíce rozšířený algoritmus
- délka klíče – 2048 bitů – nejmenší velikost, běžné používání
  – 3072 bitů
  – 4096 bitů – nejbezpečnější – pomalejší

DSA – Digital Signature Algoritm
- ideální pro elektronické podpisy

ElGamal
- používaný v PGP – Pretty Good Privacy
- pro elektronické podpisy, v e-mailech

Hash
- matematická funkce – převádí zprávu na kód
- pro stejný vstup je vždy stejný hash
- nezáleží na velikost dat – hash bude mít stejnou velikost
- skoro nemožné získat data zpět
- malé změny ve vstupních datech vedou k velkým změnám v hash hodnotě
- využití – ukládání hesel, digitální podpisy, kontrola integrity dat, rainbow tables, …

CRC kód – Cyclic Redundancy Check
- vychází z hashe
- jednoduchý způsob kontrolního součtu
- zkontroluje hash na začátku a na konci
- používá se k detekci chyb během přenosu, či k ukládání dat