Úvod do kryptografie

08.03.2025

Operační systémy
IV. ročník

Bc. Lukáš Pospíšil

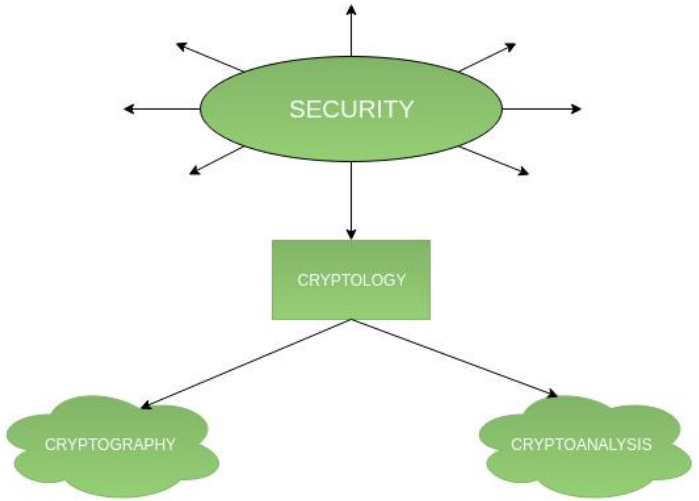
MěSOŠ
Klobouky u Brna

Cíl tématu

- **Znám** pojmy:
  - kryptografie, kryptoanalýza, šifrování, dešifrování, klíč, text, hashovací funkce, digitální podpis
- **Popíšu** a **vyjmenuju:**
  - rozdíl mezi symetrickým a asymetrickým šifrováním
  - význam a použití hashovacích funkcí a digitálních podpisů
  - historické i moderní šifrovací algoritmy
- **Umím:**
  - vysvětlit principy základních šifrovacích metod
  - identifikovat silné a slabé stránky různých šifer

Kryptologie

- Velká **věda zabývající se metodami šifrování a jejich luštěním**
- Pod kryptografii spadají disciplíny:
  - **kryptografie – vymýšlí šifry** a metody, jak skrývat zprávy
  - **kryptoanalýza** – snaží se **šifry prolomit** a najít chyby



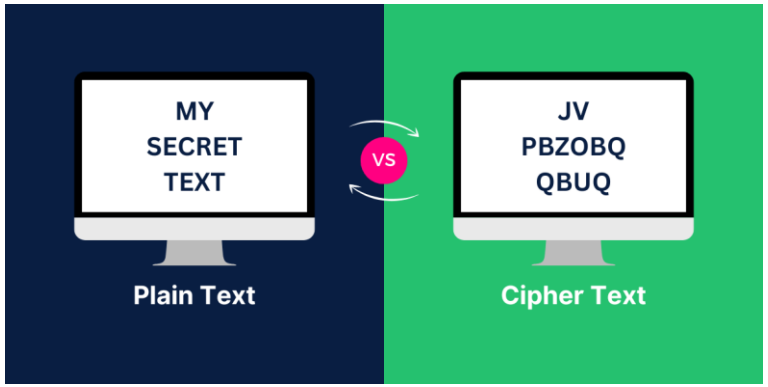
ZÁKLADNÍ POJMY

Klíč

- Tajná informace
- **Určuje, jak se zpráva zašifruje a jak ji dešifrujeme zpět**
- V šifrách:
  - Caesarova šifra – číslo posunu v abecedě
  - Vigenèrova šifra – tajné slovo
  - Moderní šifry (AES, RSA) – velké číslo se stovkami bitů
    - generují se náhodně

Text

- Každá zpráva má dvě podoby
  - **otevřený** text (plaintext)
    - normální zpráva, kterou chceme zašifrovat
  - **šifrovaný** text (ciphertext)
    - podoba zprávy po zašifrování
- **Bez klíče je šifrovaný text jen nesmyslná změť znaků**



Šifrovací algoritmus

- **Matematický postup**
  - pomocí něj se zpráva **převádí** na šifrovaný text a zase zpět
- Zašifrování zprávy
  - použít správný algoritmus a klíč
- Čím složitější algoritmus, tím bezpečnější šifra

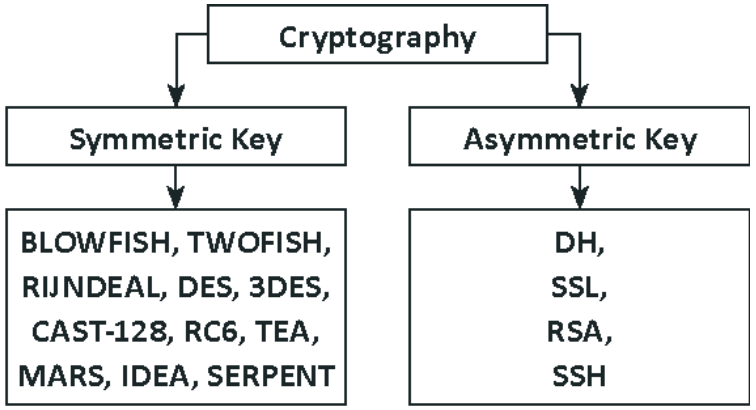
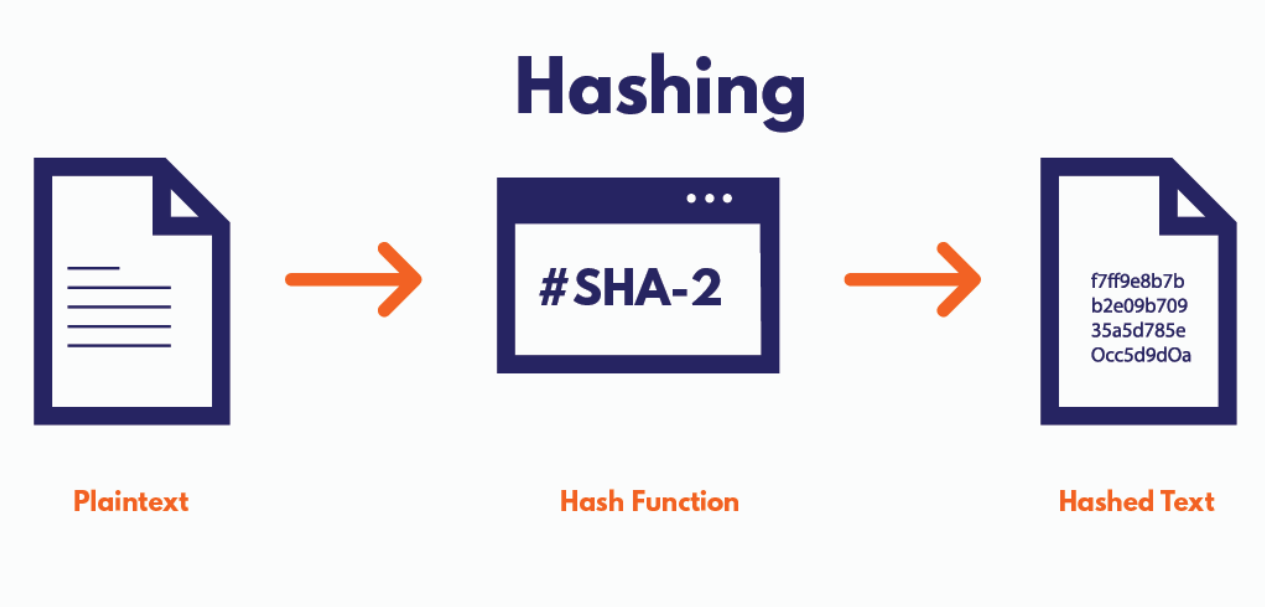


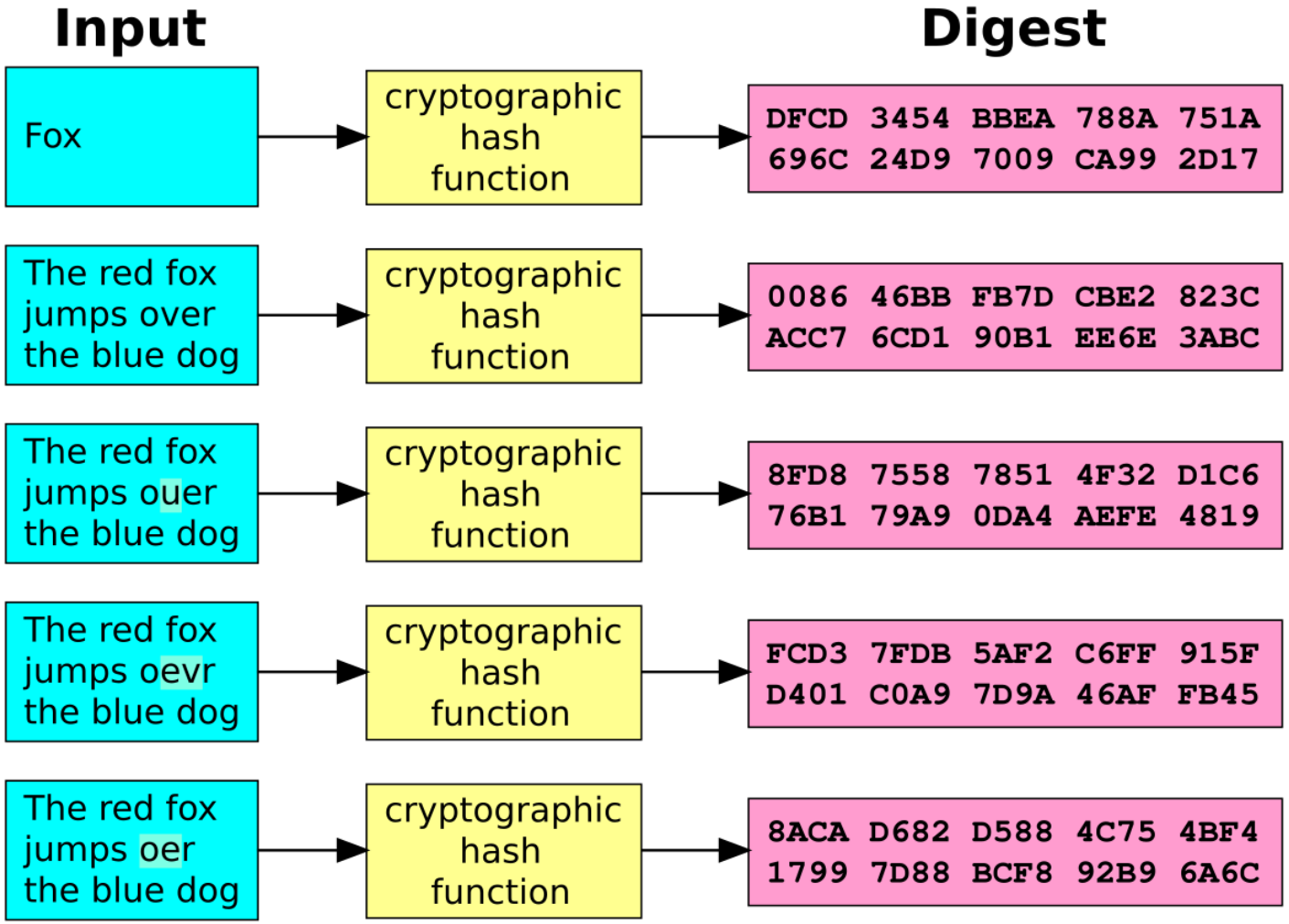
Figure 1: Classification of cryptographic algorithms [6]

Hashovací funkce

- **Nelze jej zpětně dešifrovat**
- Jedinečný řetězec znaků
- Ochrana hesel, digitální podpisy, zabezpečení souborů

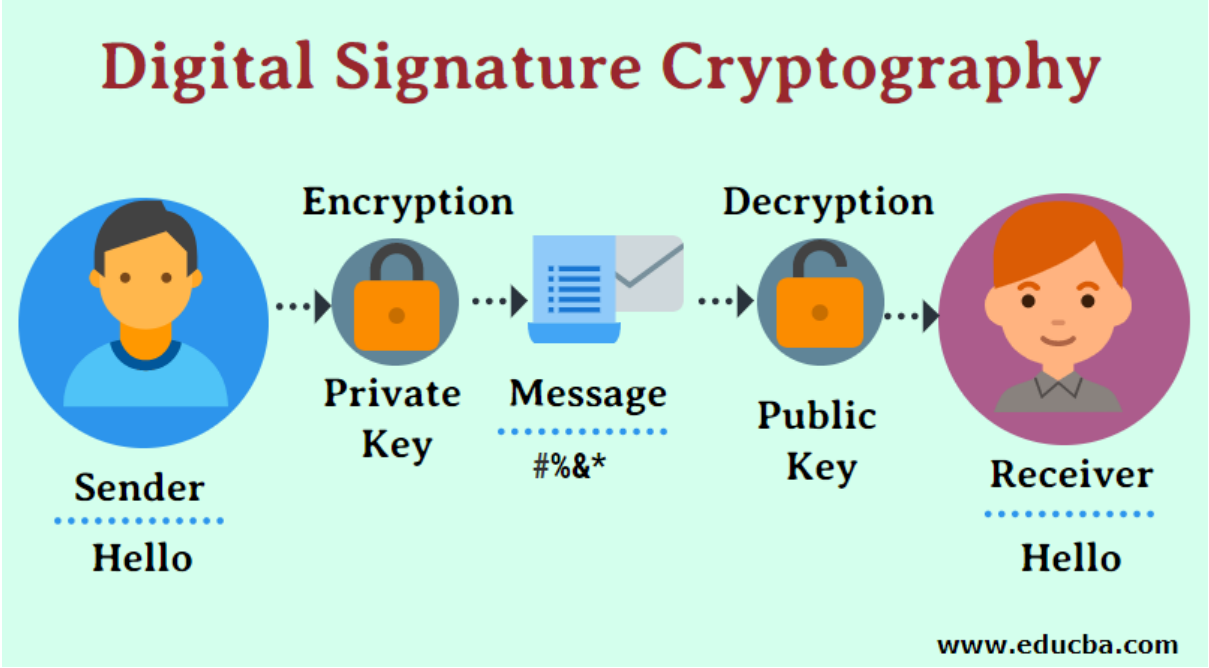


Hashovací funkce



Digitální podpis

- **Ověřuje pravost zprávy**
- Kombinuje hashování a asymetrické šifrování
- E-mailová komunikace, smlouvy, podpis software



MěSOŠ Klobouky u Brna

HISTORIE

Historie

- Jak utajit zprávu, aby jí rozuměl jen ten, kdo ji má číst?
- Šifrování se hodilo v oblastech
  - války – tajné rozkazy
  - diplomacie – aliance, intriky
  - obchod – informace o cenách zboží

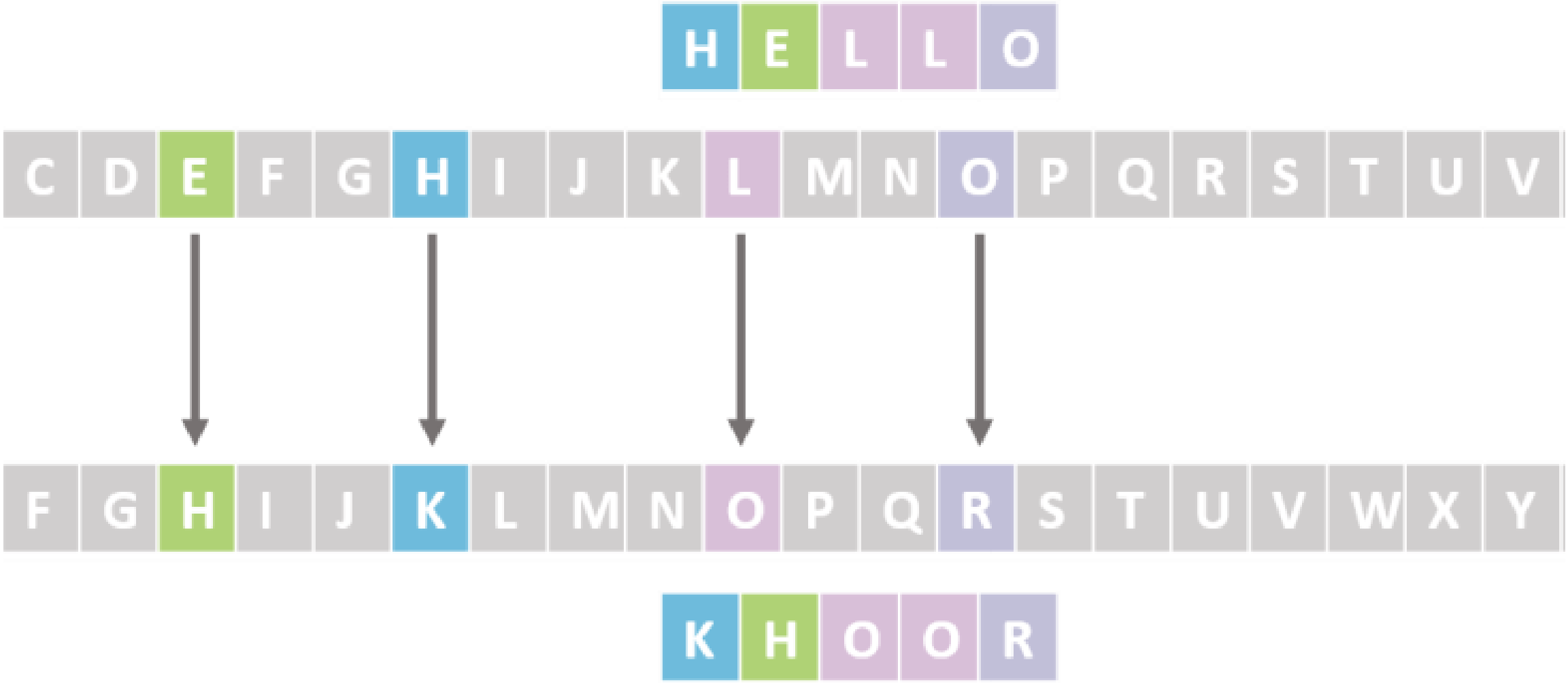
Caesarova šifra

- **Substituční šifra**
  - **každé písmeno v otevřené zprávě zaměníme za jiné písmeno podle pevně daného pravidla**
- Vytvořil Julius Gaius Caeasar pro tajné rozkazy vojakům

Caesarova šifra – jak funguje

- Každé písmeno v abecedě posuneme o určitý počet míst vpravo
- My budeme používat ASCII znaky
- Například:
  - AHOJ
  - vybereme posun 3
  - A+3 = D, H+3 = K, O+3 = R, J+3 = M
  - DKRM
  - pro dešifrování – stejný posun zpět

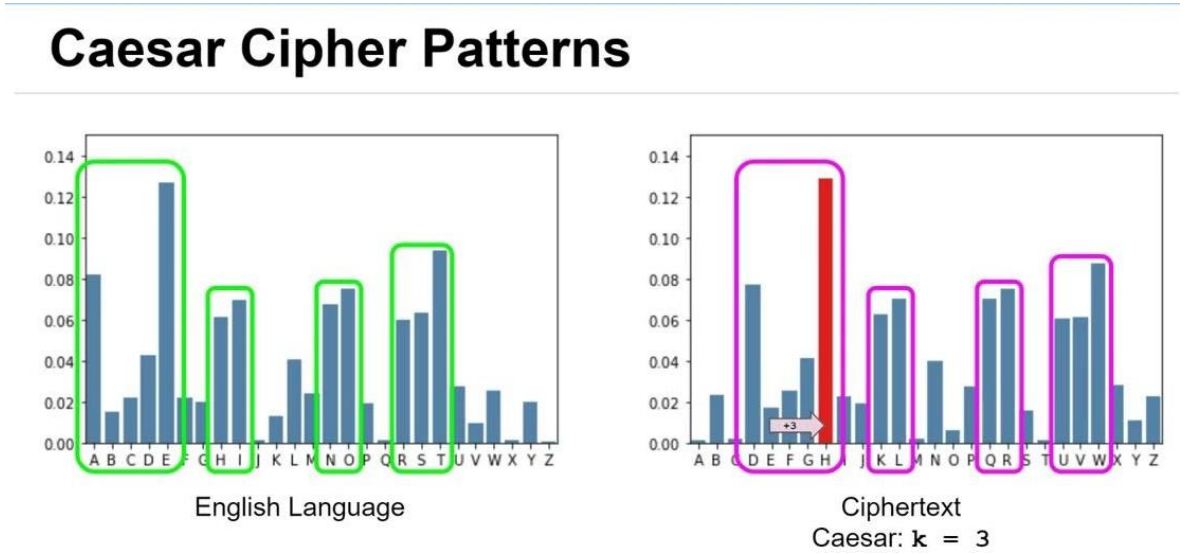
Caesarova šifra – jak funguje



MěSOŠ Klobouky u Brna

Caesarova šifra – jak funguje

- **Šifrovací klíč – posun**
- Dnes nepoužitelná – strašně jednoduchá
- Neznáme klíč – vyzkoušíme všech 25 posunů
  - abeceda má jen 26 písmen
- Delší zpráva
  - frekvenční analýza
  - lze odpočítat klíč



MěSOŠ Klobouky u Brna

Vigenèrova šifra

- **Každé písmeno šifruje jiným posunem**
- Posun (klíč) určuje
  - **tajné klíčové slovo**
- Pro dešifrování - **Vigenèrova tabulka**
  - matematická tabulka
  - kombinuje 26 Caesarových šifer

Vigenèrova šifra – jak funguje

- Vybereme klíčové slovo
  - například HESLO
  - opakuje se nad šifrovaným textem
  - čím delší klíč, tím složitější šifra
- Otevřený text TAJNAZPRAVA
- Klíč HESLOHESLOH
  - klíčové slovo opakujeme dle délky zprávy

Vigenèrova tabulka

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenèrova šifra – jak funguje

- Vybereme klíčové slovo
  - například HESLO
  - opakuje se nad šifrovaným textem
  - čím delší klíč, tím složitější šifra
- Otevřený text TAJNAZPRAVA
- Klíč HESLOHESLOH
  - **klíčové slovo opakujeme dle délky zprávy**

Vigenèrova šifra – jak funguje

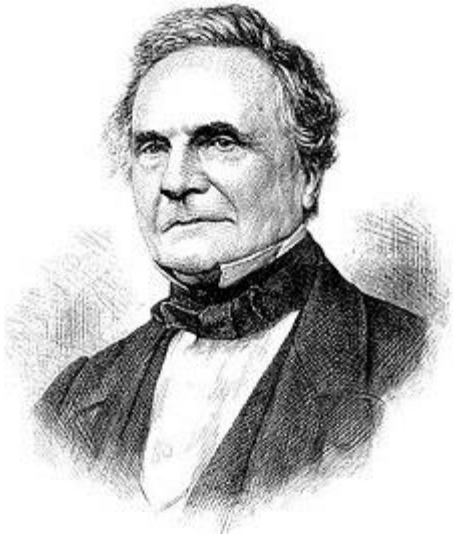
- Najdeme písmeno zprávy a písmeno v klíči
  - průnikem získáme šifrovaný znak

Původní text	T	A	J	N	A	Z	P	R	A	V	A
Klíčové slovo	H	E	S	L	O	H	E	S	L	O	H
Šifrovaný text	A	E	B	Y	O	F	T	I	L	J	H

  - šifrovaný text = AEBYOF TILJH

Vigenèrova šifra – jak funguje

- Dešifrování
  - průnik šifrovaného textu a písmena v klíči
- Prolomena pomocí **frekvenční analýzy**
  - 50. léta 19. století – **Charles Babbage**



Enigma

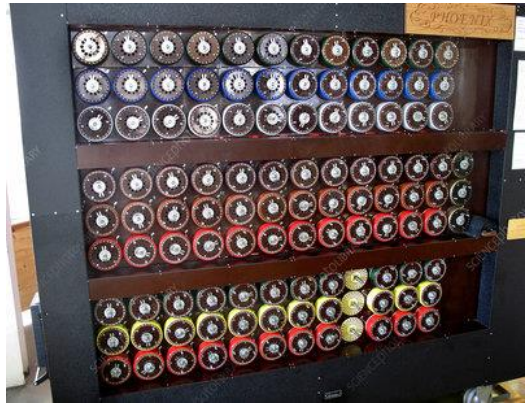
- Užívána Němci během 2. svět. Války
- **Elektromechanický šifrovací stroj**
- Každé písmeno prošlo přes **rotory** (otočné kotouče)
  - **stejné písmeno se zašifrovalo jinak**
- Navíc **zapojovací deska** pro manuální prohození písmen
- Bez znalosti nastavení rotorů a zapojovací desky – neprolomitelná
- Každý den se měnilo nastavení dle tajného kódu

Enigma

MěSOŠ Klobouky u Brna

Bombe

- Nakonec prolomena – lidskou chybou
- **Alan Turing**
  - počítač **Bombe**
  - Britové zjistili, že každá zpráva začíná např. „Drahý Adolfe…“
  - našli vzory a urychlili dešifrování



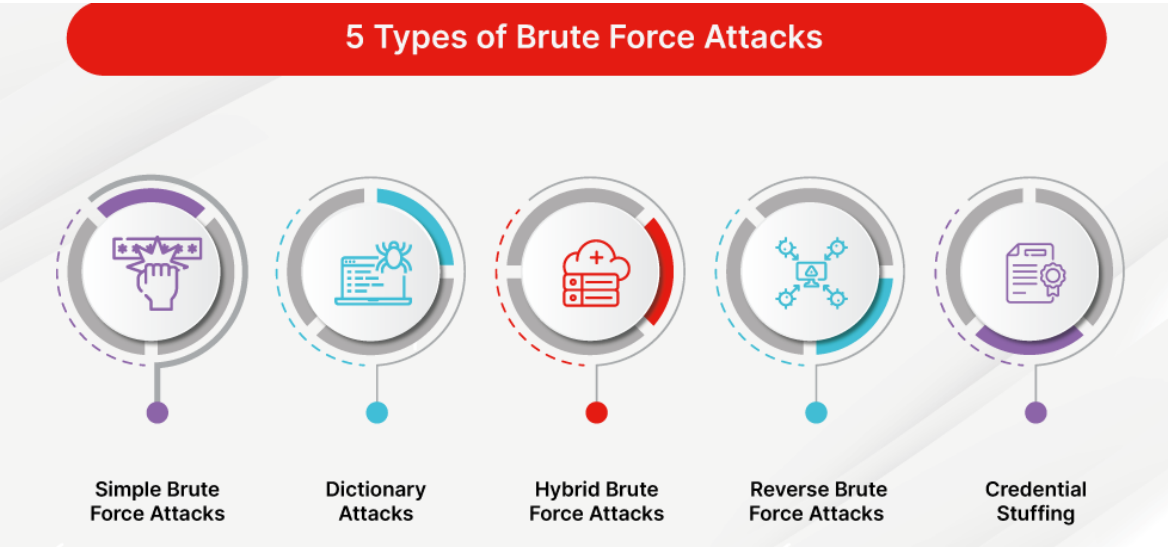
ÚTOKY NA ŠIFRY

Frekvenční analýza

- **Metoda sledující, jak často se písmena v textu opakují**
- V každém jazyce se některá písmena objevují častěji než jiná
  - čeština – „E“, „A“, „O“, „I“, „N“
- XLMW MW HVMRO JSVI XLMW TEWWI
  - M 8x, W 4x…
  - M může být původní „E“ (nejvyskytovanější)
  - M je 13. v abecedě, E je 5. v abecedě
    - posun 8 míst zpět
  - TOTO JE ZPRAVA PRO TEBE

Brute-force

- **Hrubá síla**
- Vyzkouší se všechny možné klíče, dokud se nenajde správný
- Caesarova šifra – vyzkoušíme všech 25 posunů
- Slovníky, seznamy – jednoduchá hesla – ahoj, 1234…



Matematický útok

- Moderní šifry, těžké na rozluštění
- RSA šifra – dnes neprolomitelná
- V budoucnu řeší kvantové počítače

Anotace

Tato prezentace slouží k seznámení se s principy kryptografie a jejího využití v kybernetické bezpečnosti. Zaměřuje se na základní pojmy, historické i moderní šifrovací metody, hashovací funkce a digitální podpisy. Žáci se naučí rozlišovat mezi symetrickým a asymetrickým šifrováním, pochopí význam šifrovacích algoritmů a jejich zabezpečení. Hlavním cílem je, aby žáci porozuměli základům kryptografie a dokázali identifikovat možné hrozby spojené s šifrováním a jejich řešení v praxi.

Hlavním cílem je, aby žáci porozuměli různým metodám správy serverových služeb v Linuxu a dokázali je efektivně využít v praxi.

Užité zdroje

- https://vyuka.mesosdev.cz/kb/operacni-systemy/kryptografie/uvod-do-kryptografie/

Autor: Bc. Lukáš Pospíšil

Předmět: Operační systémy

Ročník: 4.

Rok vytvoření: 2025

Poslední aktualizace: 2025

MěSOŠ Klobouky u Brna