Seminár z algoritmizácie a programovania 1

Martin Bobák
Ústav informatiky
Slovenská akadémia vied

Obsah prednášky

1. **Šifrovanie**

Spätná väzba:
https://forms.gle/iKbuLdF6xDtNSEDP8

Šifrovanie

Šifrovanie

Šifrovanie predstavuje proces transformovania a utajenia správy (informácií), tak aby tieto informácie mohli byť bezpečne prenesené, a dostupné/známe len zvolenej skupine ľudí (s kľúčom).

Kryptografia: vedná oblasť zaoberajúca sa spôsobmi utajenia obsahu správy (informácií) pred nepovolanými osobami.

Kryptoanalýza: vedná oblasť zaoberajúcu sa štúdiom metód, ktoré môže útočník použiť pri snahe získať zo zašifrovaného textu ukryté informácie.

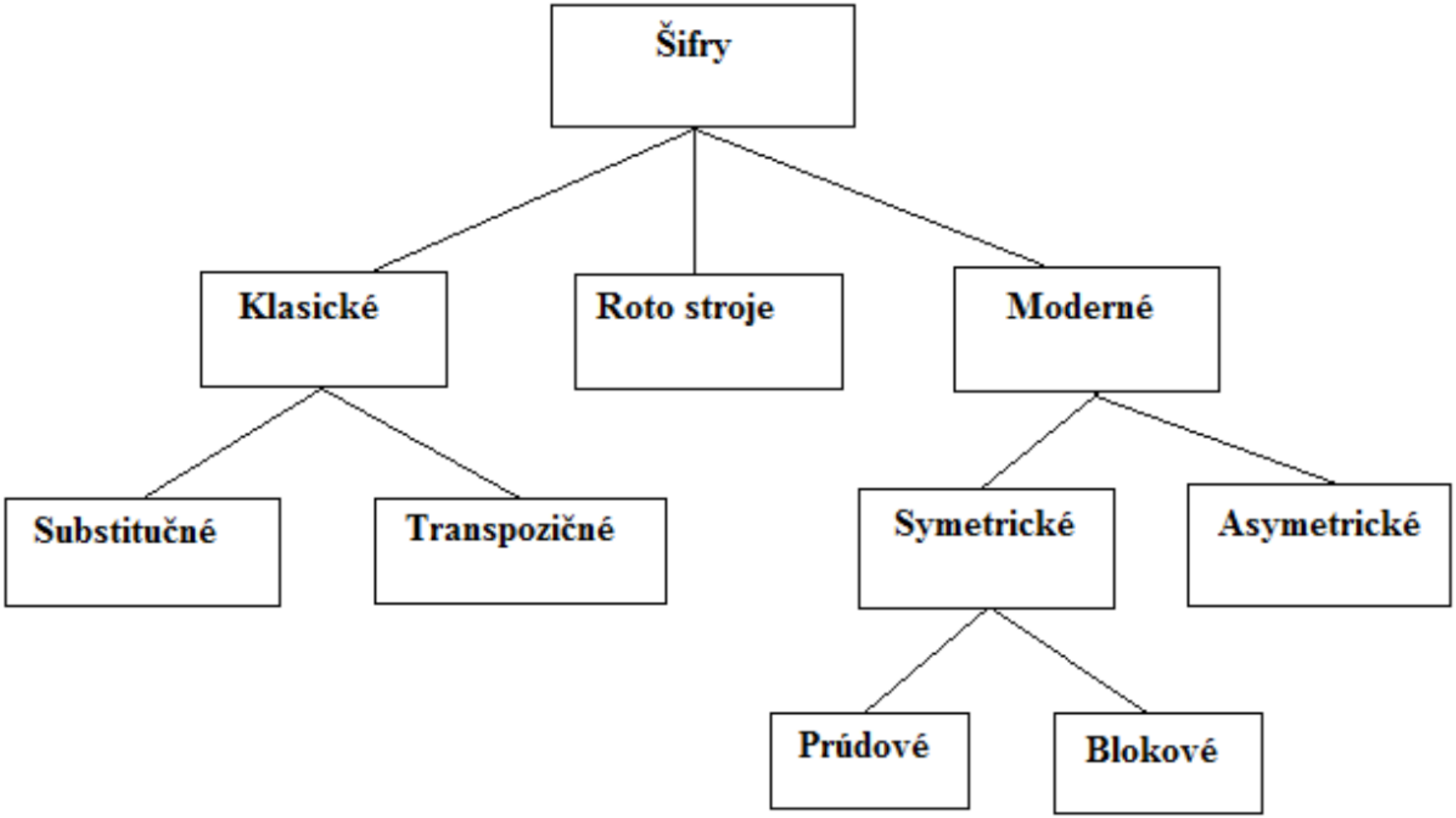
Šifrovanie

Kódovanie vyjadruje spôsob reprezentácie/štruktúry dát (napr. kódovanie obrázku použitím rozličných formátov BMP, PNG, JPG, ...), resp. reprezentácia textu použitím určitej znakovej sady. V niektorých prípadoch spolu šifrovanie – kódovanie súvisia, ale nie sú to synonymá.

- Pozor, nepliesť šifrovanie s kódovaním!

Kľúč je utajená postupnosť znakov (čísiel/bitov) používaná k zašifrovaniu, resp. dešifrovaniu prenášanej správy (informácií).

Členenie šifrovania



Cézarova šifra

Jedná sa o jeden z najjednoduchších typov substitučných šifier. Kľúčom je jediné číslo, ktoré určuje, o koľko znakov abecedy sa budú posúvať všetky písmená správy v rámci abecedy. Pri dešifrovaní dochádza k spätnému posunu písmen.

Príklad cézarovej šifry, pre kľúč = 3 (posun o 3 znaky).

Pôvodná správa: `ZLATOJESKRYTEPODSTROMOM`

Zašifrovaná správa: `CODWRMHVNUBWHSRGVWURPRP`

Vernamova šifra

Vernamova šifra štandartne vyžaduje kľúč rovnakej dĺžky ako šifrovaná správa, príp. dlhší (zostávajúce znaky/bity kľúča budú nepoužité). [Vo výnimočnom prípade, ak je kľúč kratší než správa, použije sa viacnásobne za sebou; V taktomto prípade sa však výrazne znižuje bezpečnosť.]

Výhodou Vernamovej šifry je vysoká miera bezpečnosti; nevýhodou je potreba zabezpečenia dlhého kľúča. Vysoká miera bezpečnosti je zabezpečená obzvlášť v prípade, ak je kľúč vygenerovaný náhodne (nie pseudonáhodne) a jeden kľúč sa nevyužíva na šifrovanie viacerých správ.

Vernamova šifra

Príklad šifrovania Vernamovou šifrou v bitovej reprezentácií, kde na šifrovanie / dešifrovanie je bežne používaná operácia XOR (Exclusive OR, v jazyku C je to symbol ^):

Originálna správa:	0100 0101 1110 1001 0110 1001 1010 1011
Kľúč	1011 1100 0000 0010 0011 1101 1010 0110
Zašifrovaná sp.:	1111 1001 1110 1011 0101 0100 0000 1101
Kľúč:	1011 1100 0000 0010 0011 1101 1010 0110
Dešifrovaná sp.:	0100 0101 1110 1001 0110 1001 1010 1011

Vernamova šifra

Z príkladu je vidieť že :

Zašifrovaná správa = Originálna správa XOR Kľúč
(proces šifrovania)

Originálna správa = Zašifrovaná správa XOR Kľúč
(proces dešifrovania)

V prípade pracovania s textom, môže byť použitý jednoduchý princíp, kedy kľúč pozostáva z rovnakého počtu čísiel, ako daná správa znakov. Pri šifrovaní sa tak každý znak posunie o prislúchajúci počet znakov, podľa kľúča. Dešifrovanie realizuje posun opačným smerom, podľa rovnakého kľúča.

Transpozičné šifry

Transpozičné šifry sú založené na princípe zmeny poradia znakov v správe. Obvyklým prvkom transpozičných šifier je zápis textu do určitej tabuľky / riadku / mriežky, a stanoveného spôsobu čítania tejto tabuľky (poradia čítaných znakov). Bezpečnosť takéhoto šifrovania je relatívne malá, vzhľadom na zachovanie početností jednotlivých znakov.

Transpozičné šifry

Príklad použitia jednoduchej stĺpcovej transpozičnej šifry. Šifrovanou správaou je:
POKLADJESCHOVANYVLESEPODVELKYMDUBOMTRIMETREPODZEMOU
Text správy naformátujeme do tabuľky s napr. 11 stĺpcami:

POKLADJESCH
OVANYVLESEP
ODVELKYMDUB
OMTRIMETREP
ODZEMOUXXXX

Kľúčom bude postupnosť čísiel: 5, 2, 7, 3, 11, 6, 10, 4, 9, 1, 8
Po preusporiadaní jednotlivých stĺpcov podľa stanového kľúča, bude tabuľka vyzerať nasledovne:

AOJKHDCLSPE
YVLAPVENSOE
LDYVBKUEDOM
IMETPMERROT
MDUZXOXEXOX

Zašifrovaná správa je teda:
AOJKHDCLSPEYVLAPVENSOELDYVBKUEDOMIMETPMERROTMDUZXOXEXOX

Transpozičné šifry

Kľúčom pri takejto šifre môže byť namiesto postupnosti neopakujúcich sa čísiel aj neopakujúca sa postupnosť znakov (tzv. transpozícia podľa hesla); znaky sa pri šifrovaní zoradia abecedne.

Existuje veľké množstvo rôznych transpozičných šifier, s rozličnými tvarmi základnej tabuľky, rozličným poradím čítania, a dokonca aj s doplňujúcimi náhodnými znakmi, ktoré tak predĺžia šifrovanú správu oproti pôvodnej.

Substitučné šifry

Substitučné šifry predstavujú rozsiahlu skupinu šifier, ktorých idea je založená na náhrade znaku/písmena/dvojice znakov za iný znak, podľa zvolenej šifrovacej tabuľky. Takýchto tabuliek môže byť dokonca viac, napr. pre párne pozície v reťazci jedna tabuľka, pre nepárne druhá. Táto skupina metód poskytuje výrazne vysokú variabilitu šifrovania. Nevýhodou je možnosť použitia frekvenčnej analýzy na prelomenie šifry.

Homofónna šifra

Špeciálnym typom substitučnej šifry je homofónna šifra. Nedostatok klasických monoalfabetických substitučných šifier sa snaží odstrániť tým, že každý znak má v zašifrovanom texte viacero ekvivalentov. Napr. frekvencia písmena A je v anglickom texte približne 8%. Preto tomuto znaku priradíme 8 rôznych ekvivalentov. Písmeno Z má frekvenciu výskytu cca 1% a teda mu priradíme 1 znak. K zašifrovaniu správy by sme použili každý z ekvivalentov náhodne. Frekvencia každého znaku by sa znížila na približne 1%. Ak by sme využili vyššie uvedenú frekvenčnú tabuľku a na reprezentáciu jednotlivých znakov by sme použili dvojciferné čísla, tak šifrová abeceda by mohla vyzerať napr. takto:

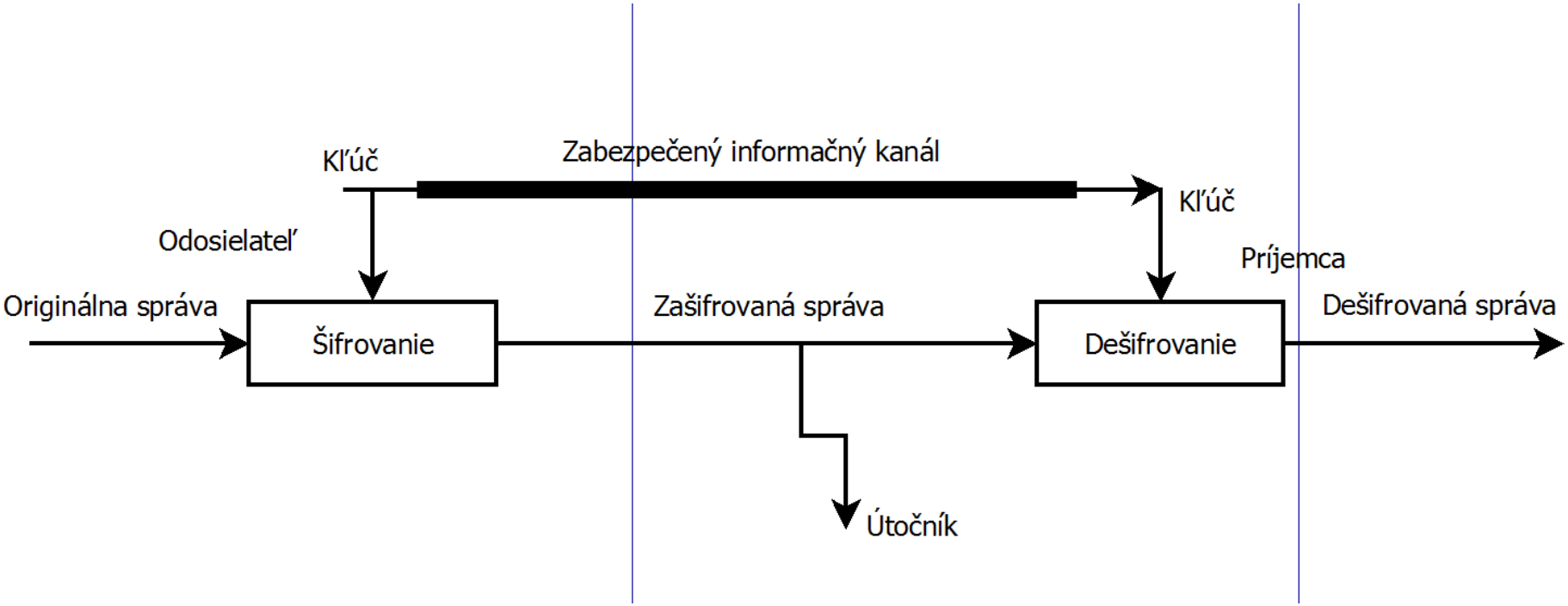
Homofónna šifra

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
77	35	30	26	03	42	00	90	07	01	04	12	58	57	15	40	21	24	47	55	13	39	19	16	37	59
50	11	25	75	79	89	71	96	17			02	10	91	53	34		78	46	83	63		62		54	
49		05	27	73			66	38			06		94	74			33	87	85	88					
76			51	82			45	31			81		95	72			80	86	69						
08				97			23	52					20	48			84	61	65						
28				67			14	29					18	56			92	70	60						
99				44										43					41						
36				22															09						
				32															68						
				93																					
				98																					
				64																					

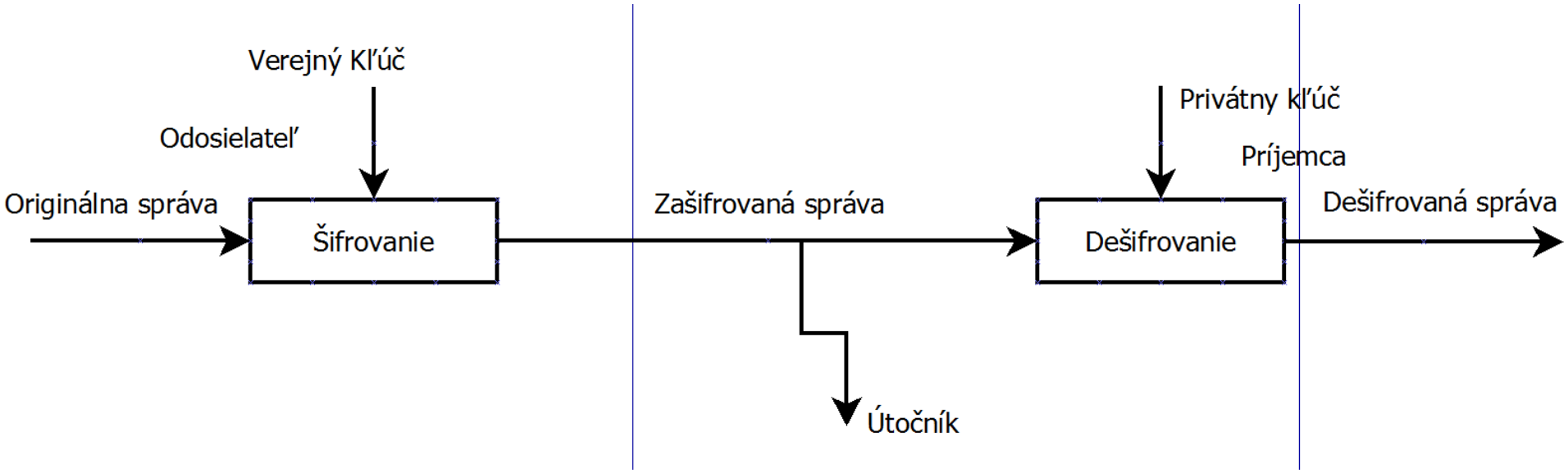
Moderné šifry

Moderné šifry, môžeme členiť na symetrické a asymetrické, podľa toho, či využívajú rovnaký kľúč na šifrovanie / dešifrovanie (symetrické), alebo používajú odlišný kľúč na šifrovanie (verejný kľúč), a iný na dešifrovanie (súkromný kľúč). Medzi symetrické šifry môžeme tiež zaradiť všetky predtým uvedené substitučné aj transpozičné šifry.

Symetrické šifrovanie



Asymetrické šifrovanie



Asymetrické šifrovanie

- Pre asymetrické šifrovanie sú typické odlišné kľúče pre proces šifrovania a dešifrovania, pričom tieto kľúče si musia vzájomne zodpovedať.
- Zjednodušene, privátny (súkromný) kľúč obsahuje obvykle 2 veľké prvočísla (p1, p2).
- Verejný kľúč obsahuje číslo Q = p1 * p2. Samotné p1 a p2 však neobsahuje. Faktorizácia čísla Q na súčin prvočísiel p1 a p2 je síce jednoznačná, avšak pre veľké čísla je extrémne časovo náročná. To je dôvod, prečo verejným kľúčom je možné správy šifrovať, avšak nie je možné dešifrovať.

Zlaté pravidlo bezpečnosti

Prostriedky, ktoré je potrebné vynaložiť na prelomenie bezpečnosti, by mali byť vyššie ako cena toho, čo je možné prelomením šifry získať.

Zdroje

[1]https://cloud5q.edupage.org/cloud/Sifrovanie.pdf?z%3AQVD4sH%2Bxg8wspsXbJ60dIiO904pzfdtdIkOHTLtRR6pBh0KvbJs87LWhWM8E1O5Y

[2]https://inventwithpython.com/cipherwheel/

[3]https://cryptii.com/pipes/caesar-cipher

[4]http://server.gphmi.sk/pages/sifry/homo.html

[5]http://server.gphmi.sk/pages/sifry/princip.html

Ďakujem vám za pozornosť!

Spätná väzba:
https://forms.gle/iKbuLdF6xDtNSEDP8