DUM 8 téma: Kryptografie

ze sady: 3 **tematický okruh sady:** III. Ostatní služby internetu
ze šablony: 8 – Internet **určeno pro:** 4. ročník
vzdělávací obor: 18-20-M/01 Informační technologie
vzdělávací oblast: odborné vzdělávání
metodický list/anotace: viz VY_32_INOVACE_08308ml.pdf

Ochrana dat

Obsah informační systémů – data v nich uložené – jsou mnohdy největším majetkem firmy a jejich poškození nebo vyzrazení pro ni může mít katastrofální následky. Často používaným nástrojem pro ochranu takových dat jsou kryptografické metody.

Kryptografii v tomto kontextu chápeme jako vědeckou disciplínu – obor – vytvářející metody převodu zpráv a dat z podoby kýmkoliv čitelné (tzv. „otevřený text“) do podoby jiné, ze které případný útočník obsah zprávy nezjistí.

Pro tento úkol používá řady algoritmů, metod a matematických postupů – pod souhrnným názvem šifry.

Substituční šifra

Nejjednodušším způsobem utajení textu, je záměna symbolů použitých ve zprávě za jiné, útočníkovi neznámé. Takovou „šifru“ lze vyzkoušet i v běžném kancelářském programu, pouhou změnou písma:

Běžná zpráva: AGENT PRIJEDE V SEST NA HLAVNI NADRAZI

Zapsaná nezvyklým písmem:

✌☜☠❄ ☞☼☝☺☜☟☜ ✞♦☜♦❄ ☠✌ ☟☹✌✞☠☝ ☠✌☟☼✌☪☝

Samozřejmě nebude pro většinu čtenářů problémem ani překvapením.

Samostatný úkol: Zkuste dešifrovat následující zprávu…

♋♎□ ⌘❖●♋♎■♏ ♎♏⬧♓♐❒□❖♋♦ ♦♏■♦□ ♦♏⊠♦ □❒♓♒●♋⬧♦♏ ⬧♏ ◆ ❖♲◆♍◆♐♓♍♓♒□ □ ♌□♎ ⌘♋ ♋♋♦♓❖♓♦◆

Další variantou jsou substituční šifry s posunem, kdy se pro zápis otevřené i uzavřené verze zprávy používá stejných symbolů, jen se změněným významem. Příkladem je Caesarova šifra, kdy posuneme pořadí písmen v abecedě o předem smluvený počet symbolů (třeba 3):

Původní text	A	B	C	D	E	F	G	H	…
Uzavřená forma	D	E	F	G	H	I	J	K	…

Pro takovou šifru je často užívá název ROT3 (od rotation 3) a vyznavači GeoCachingu jistě znají variantu ROT13 (kdy se abeceda posunuje o 13 symbolů). Samozřejmě musí obě

strany vědět, jaké symboly v abecedě používají (velká/malá písmena, diakritika…). Mezera se většinou ponechává nezměněna (což je jednou ze slabin metody).

Při praktickém použití pak zprávu:

TAJNA SCHRANKA JE V DUTINE STROMU NA NAMESTI

Převedeme na:

WDMQD VFKUDQND MH Y GXWLQH VWURPX QD QDPHVWL

Kryptoanalýza

Případný útočník může na šifru zaútočit několika způsoby – například metodou hrubé síly, kdy prostě vyzkouší všech 26 možných variant posunu a předpokládá, že alespoň jedna povede na smysluplný text. V našem případě by získal varianty například:

Posun zpět o 2:

UBKOB TDISBOLB KF W EVUJOF TUSPNV OB OBNFTUJ

Posun zpět o 5:

RYHLY QAFPYLIY HC T BSRGLC QRPMKS LY LYKCQRG

A konečně posun zpět o 3:

TAJNA SCHRANKA JE V DUTINE STROMU NA NAMESTI

Kdy je zřejmé, která variant je „ta správná“.

Samostatný úkol: Metodou hrubé síly zkuste dešifrovat zprávu:

VDUCRMRBLRYURWJAWR XKXA TAHYCXPAJORN YANMYXTUJMJ MXKAXD IWJUXBC VJCNVJCRTH

Další možností je aplikace principů frekvenční analýzy. Ta využívá znalosti četnosti znaků v jednotlivých jazycích, kdy lze následně v šifrovaném textu vyhledávat symboly s podobnou četností a přímo tak určit jaký symbol odpovídá kterému. U šifer typu ROT dokonce stačí určit několik prvních znaků, z nich odvodit směr a velikost posunu a zbytek symbolů už přímo dešifrovat. Například v češtině je pořadí nejčastějších symbolů O, E, N, A, T… (1)

Metodu vyzkoušíme na příkladu (frekvenční analýza potřebuje poněkud delší texty):

WVUVIRCEZ JYIFDRQUVEZ ER QRBCRUV ERMIYL TVJBV ERIFUEZ IRUP R JCFMVEJBV ERIFUEZ IRUP, LQERMRAZT EVGFILJZKVCEFJK GIZIFQVEPTY GIRM TCFMVBR, GIRM FSTRER R JMITYFMREFJK QRBFER, ERMRQLAZT ER FSVTEV JUZCVEV YFUEFKP CZUJKMZ R ER UVDFBIRKZTBV R JRDFJGIRMEV KIRUZTV ERJZTY ERIFUL, GRDVKCZMF KIGBPTY QBLJVEFJKZ Q UFS, BUP CZUJBR GIRMR R QRBCRUEZ JMFSFUP SPCP M ERJZ MCRJKZ GFKCRTFMREP, MBCRURAZT ERUVAV UF QRSVQGVTVEZ KVTYKF GIRM JGFCVTEPD LJZCZD MJVTY JMFSFUEPTY ERIFUL, MPTYRQVAZT Q GIRMR TVJBVYF ERIFUR R JCFMVEJBVYF ERIFUR ER JVSVLITVEZ, GIZGFDZERAZT JZ JMLA UZC FUGFMVUEFJKZ MLTZ SLUFLTZD XVEVIRTZD QR FJLU MVJBVIVYF CZUJKMR ER QVDZ R MPARUILAZT MLCZ, RSP JV TVJBR R JCFMVEJBR WVUVIRKZMEZ IVGLSCZBR ULJKFAEV QRIRUZCR DVQZ JKRKP, AVQ KPKF YFUEFKP TKZ, LJEVJCF JV ER KVKF CZJKZEV QRBCRUEZTY GIRM R JMFSFU

U kterého spočítáme četnost symbolů (například nástrojem http://www.asecuritysite.com/security/Coding/freq):

a	b	c	d	e	f	g	h	i	j	k	l	m
11 [1.6%]	20 [2.9%]	26 [3.8%]	11 [1.6%]	51 [7.5%]	52 [7.6%]	18 [2.6%]	0 [0.0%]	33 [4.8%]	44 [6.4%]	27 [4.0%]	19 [2.8%]	35 [5.1%]
n	o	p	q	r	s	t	u	v	w	x	y	z
0 [0.0%]	0 [0.0%]	18 [2.6%]	19 [2.8%]	82 [12.0%]	12 [1.8%]	31 [4.5%]	38 [5.6%]	58 [8.5%]	2 [0.3%]	1 [0.1%]	16 [2.3%]	48 [7.0%]

Kde nejčetnější znak je R, následovaný V, F, E, Z atd… při porovnání se známou frekvencí písmen v češtině může ukazovat na záměnu R-O (o 3 symboly), nebo V-E (17 symbolů), F-N (18 symbolů), E-A (17 symbolů). Stačí vyzkoušet získané hodnoty na první část textu:

Posun o 3: TSRSFOZBW GVFCAONRSBW BO NOYZORS…

Posun o 17: FEDERALNI SHROMAZDENI NA ZAKLADE…

A výsledek je jasný. **Samostatný úkol: Dešifrujte zbytek textu**

Další typy šifer

Složitější šifrou se substitucí je třeba Vigenèrova šifra. Princip je podobný (záměna symbolů), ovšem postup složitější a hůře prolomitelný.

Jako klíč šifry se nepoužívá pouhý počet posunutí symbolů, ale řada několika čísel – kdy první symbol textu je šifrován s posunem dle prvního čísla, druhý symbol posunut dle druhého čísla a podobně. Při dosažení konce klíče se začne používat od začátku. Každý symbol otevřené zprávy se tak může v šifrovaném textu objevit zašifrovaný do několika různých cílových symbolů.

Příklad: MATURITA SE BLIZI

Šifrovací klíč: 5, 7, 12, 6

Postup:

1. Symbol „M“ zašifrujeme s posunem 5 … tedy na „R“

2. Symbol „A“ s posunem 7 … na „H“

3. Symbol „T“ s posunem 12 … na „F“

4. Symbol „U“ s posunem 6 … na „A“

5. Symbol „R“ znovu o 5 … na „W“

… a tak dále

Výsledkem je šifrogram: **RHFAWPFG XL NRNGU**

Kde je například znak „A“ převeden nejdříve na „H“ a jeho další výskyt na „G“, symbol „I“ je v původním textu dokonce 3x – v šifrogramu pak jako „P“, „N“ a „U“. Čímž je použití frekvenční analýzy ztíženo, zůstává ale stále patrná struktura textu z předložek, spojek a mezer mezi slovy.

Pro jednodušší zapamatování šifrovacího klíče můžeme místo jednotlivých číslic uvádět písmena, která odpovídají jejich pořadí v abecedě za „A“ – v tomto případě by klíčem k šifře bylo slovo „FHMG“.

Samostatná práce:

Zašifrujte text: PREZOUVANI KONTROLUJE SKOLNIK

Pomocí klíče: SKOLA (kde „A“ zastupuje číslo 1 atd)

Samostatná práce:

Dešifrujte šifrogram: TVSIOXIGCHL VNM YLDV

S klíčem: LINUX

Zdroje:

- Archiv autora

Citovaná literatura

1. **Králík, Jan.** The Czech Language. [Online] http://www.czech-language.cz/alphabet/alph-prehled.html.