Úvod do kryptológie

Rasťo Oľhava

Úvod

Ľudia sa už od nepamäti snažili uchovať svoje tajomstvá. Problémy však nastávajú ak sa chceme s niekým so svojími tajomstvami podeliť, ale tak aby sa o nich ostatné nežiadúce osoby nedozvedeli. Tento problém sprevádza ľudstvo už mnohé stáročia a dokonca podmienil vznik novej vedy *kryptológie*. Počas tejto prednášky si objasníme základne pojmy z tohto oboru a vyskúšame si spôsoby riešenia na konkrétnych príkladoch.

Základné pojmy

otvorený text. pôvodný text, ktorý ideme zašifrovať

šifrový text. zašifrovaný otvorený text

kryptografia. veda zaoberajúca sa šifrovaním t.j. zmenou vzhľadu textu tak aby bol obsah textu skrytý

kryptoanalýza. veda zaobeajúca sa dešifrovaním t.j. odhalením obsahu šifrového textu

kryptológia. vedná disciplína skladajúca sa z kryptoanalýzy a kryptografie

monogram. jedno písmeno

bigram, trigram, ... , polygram. skupina susediacich písmen v používanej abecede, napr. pentagram PRASE

šifrový systém (alebo algoritmus). akýkoľvek systém, ktorý vieme použiť na zašifrovanie otvoreného textu

Poznámka. Zistilo sa, že utajovanie šifrového systému je vo viacerých prípadoch nemožné, a preto je vo väčšine prípadov kryptoanalytikom šifrový systém známi. Ako je teda možné, že ak poznajú spôsob utajenia, nie je ich úloha už vyriešená? Odpoveďou je veľkosť množiny kľúčov. Aj pri použití rovnakého šifrového systému sa zmenou *kľúča dostáva* pred codebreakra (z ang. kryptoanalytik) úplne nová úloha. A teda čím väčšia je množina kľúčov, tým ťažšie je „odskúšať všetky možnosti(kľúče)“. Teda jedným zo znakov dobrej šifry je aby veľkosť množiny kľúčov presiahla možnosti výpočetnej kapacity aj tých najrýchlejších počítačov.

Klasické šifry

Najstaršie, a teda aj najjednoduchšie šifry delíme na dve základne typy: *substitučné* a *transpozičné*. Princípom substitučných šifier je nahradenie znaku z otvoreného textu iným (nie nutne iným) znakom, podľa určitého pravidla. Pričom pri transpozičných šifrách zameníme len poradie znakov v texte.

Modulárna aritmetika

Ešte pred uvedením jednotlivých šifier by sme mali vedieť čo je modulárna aritmetika. Zjednodušene je to aritmetika v ktorej počítame len na obmedzenej množine čísel napr. my budeme počítať na množine $0, 1, \ldots, 25$, pretože budeme používať anglickú abecedu, ktorá obsahuje 26 písmen. V praxi to bude vyzerať tak, že ak posunieme napr. písmeno Y ($A = 1$, $B = 2$, ...) o písmeno E, získame písmeno D, pretože $Y = 25$, $E = 5$ a $25 + 5 = 30$, lenže počítame len na množine zvyškov po delení 26, kde sa číslo 30 nenachádza. A tak číslo 30 reprezentuje také písmeno aké reprezentuje jeho zvyšok po delení 26, čo je $4 = D$.

Prehľad šifier

Caesarova šifra. Šifrový text vznikne z otvoreného posunutím každého znaku o k znakov. Číslo k je v tomto prípade rovnaké vo všetkých prípadoch. Nevýhodou je, že počet možných kľúčov (hodnôt čísla k) je obmedzený počtom znakov, ktoré používame (označím si ho ako n), a teda nie je problémov ich všetky odskúšať.

Jednoduchá zámena. Každý znak je nahradený nie nutne, ale väčšinou iným znakom z abecedy, ktorú používame. Takže kľúčom je konkrétna permutácia znakov abecedy, ktorú používame. Veľkosť množiny kľúčov sa nám teda rapídne zvýšila $(n!)$.

Vigenerova šifra. Je podobná ako Caesarova šifra s tým rozdielom, že počet znakov o koľko posúvam abecedu nie je rovnaký pre všetky znaky v otvorenom texte, ale len pre každý s-tý znak. To znamená, že kľúčom je reťazec znakov odĺžky s, v ktorom každý jeho znak reprezentuje príslušný posun.

Vernamova šifra. Zatiaľ jediná dokazateľne absolútne bezpečná šifra. S otvoreným textom sčítame náhodný reťazec - kľúč. Nevýhodou je potreba predania kľúča adresátovi. Na to môžeme použiť len cesty aké máme a tie nie sú bezpečné, pretože by sme nimi potom mohli posielať priamo otvorený text bez nutnosti zašifrovať ho.

Transpozičné šifry. Ako je už vyššie uvedené ich princípom je zmena poradia písmen v otvorenom texte. Ich použitie vieme ľahko rospoznať podľa toho, že v šifrovom texte je rovnaký výskyt znakov ako v bežnom jazyku.

Príklad 1. Vieme, že nasledujúci text bol vytvorený jednoduchou zámenou z anglického textu, a ďalej vieme, že medzery v pôvodnom texte boli pred zašifrovaním nahradené písmenom Z. Nájdite otvorený text.

MJZYB LGESE CNCMQ YGXYS PYZDZ PMYGI IRLLC PAYCK YKGWZ MCWZK YFRCM ZYVCX XZLZP MYXLG WYMJS MYGPZ YWCAJ MYCWS ACPZY XGLYZ HSWBN ZYXZT YTGRN VYMJC POYMJ SMYCX YMJZL ZYSLZ YMTZP MQYMJ LZZYB ZGBNZ YCPYS YLGGW YMJZP YMJZL ZYCKY SPYZD ZPKYI JSPIZ YMJSM YMJZL ZYSLZ YMTGY GXYMJ ZWYTC MJYMJ ZYKSW ZYECL MJVSQ YERMY MJCKY CKYKG

Príklad 2. Nasledujúci šifrový text vznikol z anglického textu, v ktorom boli medzery nahradené písmenom Z, pomocou Vigenerovej šifry. Zistite dĺžku kľúča, kľúč a pôvodný otvorený text.

HQEOT FNMKP ELTEL UEZSI KTFYG STNME GNDGL PUJCH QWFEX FEEPR PGKZY EHHQV PSRGN YGYSL EDBRX LWKPE ZMYPU EWLFG LESVR PGJLY QJGNY GYSLE XVWYP SRGFY KECVF XGFMV ZEGKT LQOZE LUIKS FYLXK HQWGI LF

Záver

Týmto chcem poďakovať Martinovi Dunglovi, ktorého príspevok o šifrách mi poskytol značnú inšpiráciu a niektoré úseky jeho príspevku sú až na poslovenčenie priamo použité v mojom.

Zdroje

`http://www.karlin.mff.cuni.cz/~tuma/nciphers.html`