Tajemství zachování tajemství

Mája Kolovratníková
Gymnázium Na Zatlance, Praha, **maja@atrey.karlin.mff.cuni.cz**

Jan Černý
Gymnázium, Český Brod, **honzacerny@gmail.com**

Petr Čeřovský
Gymnázium J. Wolkera, Prostějov, **old_mr_grave@hotmail.com**

Tomáš Cícha
Gymnázium Vídeňská, Brno, **cicha.hrb@seznam.cz**

Abstrakt:

Cílem našeho bádání bylo seznámení se a zkoumání různých šifrovacích algoritmů z hlediska obtížnosti vytvoření kódovacího ale i dekódovacího algoritmu a časové, hardwarové i programové obtížnosti pro rozluštění daného algoritmu neznámou osobou.

1 Úvod

Tajemství je pojem, který je starý jako lidstvo samo. Charakterizovali bychom ho jako potřebu ubránit tajnou informaci před veřejností nebo nepovolanýma ušima.

Aby toto tajemství zůstalo zachováno, snaží se lidé odjakživa nalézt co nejsnazší a nejefektivnější metodu, jak informaci, kterou si předávají veřejnou oblastí (např. internetem), zašifrovat, aby jí kromě adresáta nikdo jiný nemohl získat. Zkoumáním šifrovacích algoritmů se zabývá samostatná věda zvaná **kryptologie**.

Cílem našeho bádání bylo seznámení se a zkoumání různých šifrovacích algoritmů z hlediska obtížnosti vytvoření kódovacího ale i dekódovacího algoritmu a časové, hardwarové i programové obtížnosti pro rozluštění daného algoritmu neznámou osobou.

2 Trocha teorie

Historický vývoj šifrování

Podíváme-li se na šifrování z hlediska historického vývoje, můžeme nalézt počátky šifrování již ve starověku, kdy vznikly nejprimitivnější šifry jako např. Caesarova šifra – posun v abecedě o n znaků apod. Největšího rozkvětu ale dosáhly šifry až ve 20. století během dvou světových válek, kdy byly vytvářeny složité metody zašifrování textu, aby rádiově vysílaným zprávám nepřítel nerozuměl. Nejznámějším kódovacím algoritmem z té doby je bezesporu šifrovací stroj Enigma, který byl používán Němci za 2.SV, a který prolomila trojice mladých Varšavských studentů v čele s Marianem Rejewskim.

V době virtuálního světa, kdy počítače neslouží jen ke komunikaci a počítání, není příliš efektivní používat primitivních šifrovacích algoritmů, neboť jsou v rozumném čase a na rozumném množství textu rozluštitelné. V současné době asi nejpoužívanější a nejbezpečnější metodou kódování je RSA**.** Její nevýhodou je nižší rychlost oproti klasickým algoritmům.

Kryptologie

Kryptologie je věda zkoumající podstatu šifer. **Kryptografie** je část kryptologie, která se zabývá převedením srozumitelného textu do nesrozumitelného (**encrypting**) a nazpět (**decrypting**) [1]. **Kryptoanalýza** je odvětví kryptologie zabývající se rozluštěním šifrovacího kódu na základě neuplných informací, kterými mohou být zdrojové kódy šifrovacích programů, informace o charakteru klíče či větší množství textů zašifrovaných pomocí stejného programu a klíče.

Šifrování můžeme rozdělit na **symetrické** a **asymetrické**. Symetrické šifrování je založeno na kódování a dekódování textu pomocí jednoho klíče, který mohou znát jen příjemci a odesílatelé, jelikož jde na základě znalosti tohoto klíče vytvořit jak šifrovací, tak dešifrovací program. Navíc má další nevýhodu. Lidé, kteří si chtějí takto psát si musejí nejprve klíč nějak bezpečně předat, nejčastěji se setkat. Asymetrické šifrování je založeno na kódování pomocí dvou různých klíčů. Jeden z klíčů je veřejný a majitel ho může vystavovat na internetu. Pomocí tohoto klíče odesílatel zprávu zakóduje, ale už není schopný ji zpět rozkódovat. Druhým klíčem je tzv. soukromý klíč, který zná pouze majitel (adresát), pomocí něhož může zašifrovanou zprávu přečíst. Bez znalosti soukromého klíče si zprávu nikdo nepřečte. Nevýhodou tohoto druhu šifrování je jeho časová složitost. Výhodou je naopak to, že můžeme přijímat zprávy od všech uživatelů a dekódovat je stejným algoritmem na rozdíl od symetrického šifrování, kdy musíme každému odesílateli sdělit jiný klíč, aby nám nečetl zprávy od ostatních.

Mezi symetrické šifry patří např. DES, 3DES, ČAST či IDEA. Mezi asymetrické šifry patří RSA (prvočísla) či ElGamal (diskrétní log.).

3 Naše bádání

Šifrování podle klíče

Náš program pracuje s anglickou abecedou o 27 znacích (s mezerou). V programu je matematicky převedena hodnota znaku v Ascii tabulce do intervalu <0;26>, kde **‘a‘** odpovídá nule a mezera číslu 26.

Na začátku si program načte šifrovací klíč a zjistí jeho délku. Pak načte text k zakódování a prochází ho po jednotlivých znacích s tím, že ke každé hodnotě písmena v upravené Ascii tabulce přičte hodnotu písmene příslušného znaku z klíče. Jelikož po sečtení může hodnota přetéct mimo interval <0;26>, je pro získání konečného čísla aplikováno mod 27. Program převede získanou číselnou hodnotu zpět na písmeno nebo mezeru a vypíše zakódovanou zprávu.

Zpětné dekryptování je prováděno inverzním početním způsobem k šifrovacímu a tak po zadání shodného klíče a zakódovaného textu si příjemce přečte na výstupu původní zprávu.

Maticové šifrování

I v tomto případě pracujeme s anglickou abecedou o 27 znacích a stejně jako v minulém případě používáme jejich numerickou hodnotou určenou Ascii tabulkou. Se znaky zprávy pracujeme po dvojicích. Numerickou hodnotu každé dvojice znaků, tvořící dvouprvkový vektor, násobíme kódovací maticí mod 27, a tak získáme dvojici znaků kódové zprávy. Aby bylo možné zakódovanou zprávu dešifrovat, musíme při užití maticového šifrování dodržet následující podmínku: počet znaků abecedy (v našem případě zmiňovaných 27) nesmí být soudělný (tj. největší společný dělitel je 1) s determinantem kódovací matice. Dekódování zprávy probíhá opět po dvojicích znaků, které násobíme inverzní maticí k matici kódovací, čímž získáme původní text.

4 Výsledky

Náše šifrovací programy fungují následovně:

I.A Šifrovací program

Odesílatel zadá vymyšlený klíč, pomocí něhož bude náš program šifrovat a posléze dešifrovat, pak zadá text zprávy a program mu vypíše zašifrovaný text, který může bez obav odeslat emailem.

```
M&J's encryption program:
Zadej klic: tajemstvi
Text k zakodovani: v restauraci na albertove davaji velke porce
n{{idktoztcrdzssvtue{x{mxultvjnurnztceit{ivz
Skoncit [a/n]: a
```

I.B Dešifrovací program

Příjemce zadá do dešifrovacího stejný klíč, který mu odesílatel bezpečně předal (nejlépe osobně), potom zadá zašifrovaný text a program mu vypíše původní zprávu.

```
M&J's decryption program:
Zadej klic: tajemstvi
Text k rozkodovani: n{{idktoztcrdzssvtue{x{mxultvjnurnztceit{ivz
v restauraci na albertove davaji velke porce
Skoncit [a/n]: a
```

Tento program je volně šířitelný podle pravidel GNU licence.
Zdrojové kódy si můžete stáhnout z adresy: **http://atrey.karlin.mff.cuni.cz/~maja/cipher/**

II.A Maticové šifrování

Program si nejdříve vyžádá od uživatele matici 2×2, pomocí které bude šifrovat zadaný text. Matice prochází několika ověřeními, její determinant nesmí být nulový a musí být nesoudělný s číslem 27 (počet písmen kódové abecedy). Pokud je matice použitelná, program si vyžádá na standardním vstupu onen „tajný“ text a na standardní výstup vypíše bezpečnou zašifrovanou podobu textu. Program přijímá pouze 26 znaků anglické abecedy a mezeru. Příklad výstupu je zde:

```
Zadej matici pro sifrovani.
7 5 1 13
Zadej text k zasifrovani.
jeleni jsou imunni vuci akutni hypertenzi
NUAWHWWVSYLUTPANHWBP FIIHIDKHWMWLQQWCDLAII
```

II.B Dešifrování

Funkce dešifrovacího programu je obdobná, po zadání matice a zakódovaného textu nám program vypíše opět náš starý známý „tajný“ text.

```
Zadej matici pro desifrovani.
7  5  1 13
Zadej text k desifrovani.
NUAWHWWVSYLUTPANHWBP FIIHIDKHWMWLQQWCDLAII
JELENI JSOU IMUNNI VUCI AKUTNI HYPERTENZI
```

Oba programy jsou volně dostupné na **ftp://83.240.13.177/sifra/**

5 Shrnutí

V době internetové komunikace je zabezpečení bezpečného přenosu zpráv nutností. Bezpečným šifrovacím algoritmem je zatím RSA. K jeho prolomení by do budoucna mohlo dojít pomocí kvantových počítačů, takže badání nad novými šifrovacími algoritmy má i do budoucna své opodstatnění.

6 Poděkování

Rádi bychom tímto poděkovali panu Ing. Vojtěchu Svobodovi, Csc. z FJFI ČVUT v Praze, bez kterého bychom se jen ztěží setkali a získali možnost na takovém projektu vůbec pracovat, dále bychom chtěli poděkovat panu Ing. Petru Ambrožovi rovněž z FJFI ČVUT v Praze, který nás po celou dobu akce a pomáhal nám řešit veškeré problémy (i s hladem), veškerým kolegům, kteří nás svou přítomností podpořili a v neposlední řadě veškerým profesorům a studentům FJFI ČVUT v Praze, kteří se na organizaci a přípravě této akce podíleli a umožnili nám se dozvědět řadu nových a užitečných věcí. Doufáme, že jim jejich úsilí budeme moci jednou vrátit v podobě našich vlastních příspěvků k rozvoji lidského vědění.

7 Reference:

[1] MRVA, L.: *Kryptografie a šifrování*, 2001, URL<http://home.pef.zcu.cz/mrzi/sifra.ppt>

[2] KOBLITZ, N.: *A course in number theory and cryptography,* Springer, 1994