CRYPTOLAB - KRYPTOGRAFICKÁ KNIHOVNA PRO MATLAB

P. Šoustek, R. Matoušek, P. Minář, J. Prehradná

Ústav automatizace a informatiky, Fakulta strojního inženýrství, Vysoké učení technické v Brně

Abstrakt

V rámci tohoto článku je popsána knihovna CryptoLab, která obsahuje vybrané kryptografické algoritmy a to jak historické, tak i moderní symetrické šifry. Tato knihovna je určena pro podporu předmětu Teorie informací a kódování, který je vyučován na Ústavu automatizace a informatiky, FSI, VUT v Brně. CryptoLab je tvořena ze dvou částí. První část tvoří dll knihovna vytvořená v jazyce C++, druhá část sestává z obslužných funkcí pro systém Matlab, které zajišťují uživatelské rozhraní a interface s výkonnou dll knihovnou.

1 Úvod

Historie kryptografie sahá hluboko do minulosti, ale až v dnešní době Internetu se s kryptografií můžeme setkávat každodenně. Ať již při zabezpečení přístupu k internetu, emailové korespondenci, nebo jen při prohlížení webových stránek. S praktickým použitím kryptografie se tak v podstatě setkáváme na každém kroku. Proto je důležité, aby měli lidé tvořící software a hardware, alespoň základní podvědomí o jejich principech a možnostech. I z tohoto důvodu se na Ústavu automatizace a informatiky, FSI, VUT v Brně vyučuje předmět Teorie informací a kódování. V části tohoto předmětu, která se věnuje kryptografii, se studenti seznámí nejen s historickými metodami šifrování a kryptoanalýzy, ale i s moderními metodami symetrické a asymetrické kryptografie. Software Matlab, slouží jako výkonná pomůcka při praktickém použití a prezentaci nabytých znalostí v průběhu cvičení tohoto předmětu. Z tohoto důvodu byl systém Matlab skrze vytvořenou knihovnu doplněn o potřebné algoritmy pro demonstraci kryptografických metod. Vlastní knihovna je popsána v kapitole číslo tři.

2 Přehled kryptografických metod

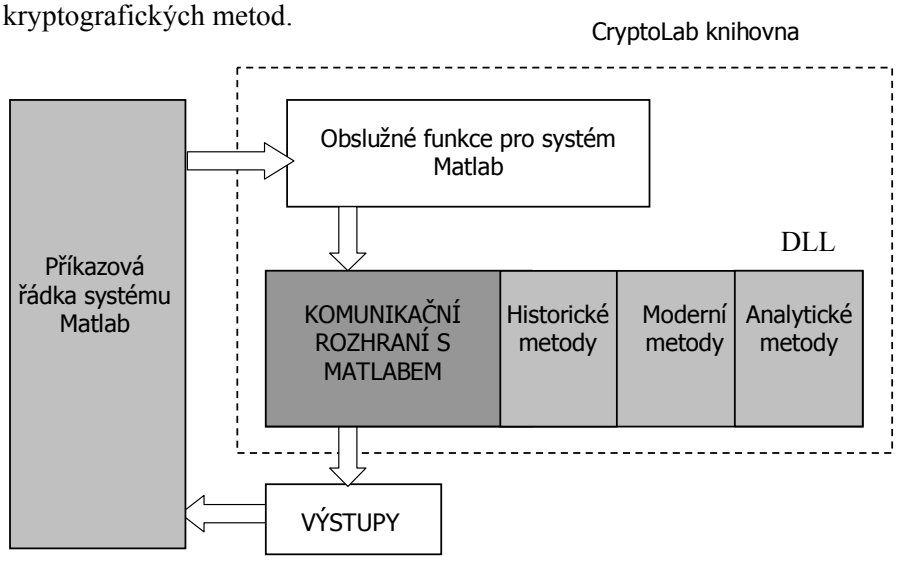
Jak je zřejmé, historie kryptografie sahá hluboko do minulosti. Mezi obecně nejznámější historické metody šifrování patří jednoduchá substituční šifra, označovaná také jako Césarova šifra. Substituční šifry jsou právě takové šifry, kde každý znak otevřené abecedy (abeceda nezašifrovaného textu) je zaměněn znakem z šifrové abecedy. Příjemce takové zprávy pro její dešifrování použije opačný postup tj. v tomto případě inverzní substituci. Mezi další historické metody, které používají substituci patří například Vigenerova šifra nebo Vernamova šifra [1]. Dalším přístupem je využití tzv. transpozice, tedy systému, kdy znaky otevřeného textu podle jistých pravidel popřehazujeme. Transpoziční šifry tedy pracují s otevřeným textem. Pochopitelně lze transpoziční i substituční přístup kombinovat. Příkladem jednoduché transpoziční šifry je sloupková šifra. U sloupkové šifry se otevřený text píše do řádků o n znacích, čímž nám vznikne pole o velikosti $m \times n$ znaků. Šifrovaný text získáme postupným zápisem znaků z jednotlivých sloupců. K dalším představitelům patří například Rail Fence šifra a Route šifra. Jak transpozice tak substituce mohou být vícenásobné. Kryptografické metody, které se užívaly do dob než došlo k masivnímu využívání elektronických počítačů, jsou často označovány jako historické metody. U těchto metod je navíc jedním ze základních pilířů ochrany i utajení šifrovacího/dešifrovacího algoritmu. Milníkem v kryptografii se stal rok 1976, který započal éru moderní kryptografie. Tehdy byl po tříletém standardizačním procesu ustanoven první státní šifrovací standard, symetrická šifra DES (*Data Encryption Standard*) [2]. V tomto kontextu byla významná práce *New Directions in Cryptography* [3] Whitfielda Diffieho a Martina Hellmana, která položila základy asymetrické kryptografie. Skupinu moderních šifer rozdělujeme na symetrické a asymetrické šifry. Symetrické šifrování je založeno na principu použití jednoho klíče, pomocí kterého se zpráva šifruje i dešifruje. Mezi tyto metody patří právě šifra DES, která sloužila po dobu 26 let a až v roce 2002 byla nahrazena novým standardem AES (*Advanced Encryption Standard*). Asymetrické šifry lze označit jako šifry s veřejným klíčem. Při asymetrickém šifrování má každý uživatel svůj veřejný a soukromý klíč. Veřejným klíčem se provádí zašifrování pro daného uživatele a tajným klíčem se provádí dešifrování přijatých zpráv.

3 Koncepce CryptoLab knihovny

Vzhledem k tomu, že systém Matlab neobsahuje kryptografické metody ani oficielní kryptografický toolbox, bylo rozhodnuto vytvořit vlastní knihovnu těchto metod. Knihovnu, která bude obsahovat základní historické šifry spolu s moderními symetrickými šiframi. Samotná knihovna označená jako CryptoLab je tvořena dvěma částmi. Dynamicky linkované knihovny DLL pro operační systém Windows napsané v jazyce C++ a obslužných funkcí pro systém Matlab vhodných pro uživatelskou práci. Softwarová implementace knihovny je navržena na co maximální obecnost a možnost rozšiřitelnosti o další kryptografické metody. Jednou z možností jak rozšířit knihovnu o další metody je pochopitelně využití dalších kryptografických knihoven a vytvoření příslušného interface, například dle vzoru CryptoLab. Příkladem kryptografických knihoven je Botan [4] nebo Crypto++ [5], které poskytují kryptografické metody i hašovací funkce. Podobně lze také použit referenční implementace nových metod, které jsou nejčastěji napsány v jazyce C. Díky tomu lze do knihovny CryptoLab velmi rychle zařadit nové kryptografické metody bez nutnosti kompletní re-implementace v systému Matlab. Další výhodou navrženého řešení je samotná rychlost šifrování, která je důležitá při šifrování velkých souborů pomocí symetrických šifer. Na Obr. 1 je naznačeno celkové blokové schéma knihovny CryptoLab. Jak je ze schématu patrné, celá knihovna je rozdělena na několik částí, kde obslužné funkce zajišťují propojení systému Matlab s DLL knihovnou. Dále komunikační rozhraní tvoří systém vhodně navržených funkcí, které obsluhují požadavky systému Matlab. Tyto funkce komunikují s výkonným jádrem DLL knihovny a tak zpracovávají uživatelské požadavky. Kromě obslužných funkcí pro systém Matlab jsou vytvořena dvě jednoduchá grafická rozhraní, které zjednodušují použití těchto funkcí a také slouží pro demonstraci jednotlivých šifer. Samotné výkonné jádro DLL knihovny je rozděleno do několika samostatných bloků. Blok historických metod tak zastřešuje jednotlivé implementované historické šifry. Sada metod pro kryptoanalýzu těchto historických šifer je implementována v bloku analytických metod. Moderní symetrické šifry jako je například šifra AES je obsažena v bloku moderních metod.

Rozdělení knihovny CryptoLab:

- obslužné metody pro systém Matlab,
- komunikační rozhraní DLL knihovny,
- sada kryptografických metod.



Obr. 1: Blokové schéma knihovny CryptoLab

V současné podobě knihovny jsou implementovány ve skupině historických metod následující šifry:

- Césarova šifra,
- Césarova šifra s klíčovým slovem,
- Monoalfabetická sloupková transpoziční šifra,
- Monoalfabetická transpoziční šifra s numerickým výběrem,

- Vigènerova šifra,
- Vernamova šifra (One time pad).

Dále jsou implementovány základní metody pro kryptoanalýzu historických šifer:

- Frekvenční analýza,
- Kasiského test,
- Index koincidence,

a skupina moderních metod obsahuje blokové šifry:

- Blowfish,
- CAST-128,
- CAST-256,
- AES/Rijndael.

Každá šifrovací metoda má svoji šifrovací/dešifrovací funkci s několika vstupními parametry (klíč, iv, mód) a s jednou výstupní hodnotou, kterou je šifrový/otevřený text. V následujících tabulkách 1 a 2 je uvedena ukázka dvou těchto funkcí spolu s jejich parametry, které jsou obsaženy v knihovně. V případě moderních symetrických šifer lze použít nejznámější módy šifrování jako je například ECB (Electronic Codebook), CBC, CFB, OFB, CTR [6]. Dále jsou implementovány pomocné funkce pro práci jak s otevřeným, tak i šifrovým textem, dalším příkladem je kódování do BASE64 kódu nebo rozdělení šifrového textu do skupin po pěti znacích.

Funkce	[ctext]= **caesarEncStr**(key, ptext, varargin)		
Popis	Šifruje daný otevřený text pomocí Césarovy šifry, znaky mimo Anglickou abecedu jsou nešifrovány		
Parametry	Parametr	Popis	Možné hodnoty
	key	Znak který vyjadřuje posunutí každého znaku v abecedě	Znak, {A..Z}
	ptext	Otevřený text	pole znaků
	varagin	- Nepovinný parametr **true** – odstraní se nealfabetické znaky z otevřeného textu	true
	ctext	Šifrový text	pole znaků

Tab. 1: Funkce pro šifrování pomocí Césarovy šifry

Funkce	[ctext]= **aesEncStr** (key, ptext, mode, iv)		
Popis	Šifruje daný otevřený text šifrou AES, vysledek je zakódován do kódu Base64		
Parametry	Parametr	Popis	Možné hodnoty
	key	Klíč o velikosti minimálně 128 bitů a maximálně 256 bitů	pole znaků {A..Z}
	ptext	Otevřený text	pole znaků
	mode	Mód šifrování (ECB, CBC, CFB, OFB, CTR)	int {0,1,2,3,4}
	iv	Inicializační vektor	int vektor 1x16
	ctext	Šifrový text	pole znaků

Tab. 2: Funkce pro šifrování pomocí šifry AES

4 Příklady použití

Využití knihovny CryptoLab v systému Matlab je realizováno pomocí připravených funkcí, skrze které lze jednoduše volat dané kryptografické metody. Dále lze použít grafické rozhraní, které je vytvořeno ve dvou variantách, a to jak pro šifrování řetězců textu tak i šifrování souborů. Ukázky použití CryptoLab knihovny, jsou zobrazeny na následujících obrazcích 2 až 4.

```
ptext = 'invade england'; % otevřený text
key   = 'white';        ; % heslo
% šifrový text
ctext = columnTransEncStr(key, ptext);
% dešifrovaný text
text = columnTransDecStr(key, ctext);
% rozdělení textu do skupin po pěti znacích
ctext = tfilter(ctext, 'group')
```

Obr. 2: Skript šifrující a dešifrující textový řetězec pomocí monoalfabetické substituční řádkové transpozice

```
key = 'security';        % heslo
iv  = [1,2,3,4,5,6,7,8]; % init vektor
mode= 2;                 % šifrovací mód
% otevřený text
ptext = 'applied cryptography';
% šifrový text
ctext = BlowfishEncStr(key, ptext, mode, iv)
% dešifrovaný text
text = BlowfishDecStr(key, ctext, mode, iv)
```

Obr. 3: Skript šifrující textový řetězec pomocí šifry Blowfish

```
key = 'password';                  % heslo
iv  = [1918,68,98,108,48,38,18,58]; % inicializační vektor
mode= 1;                           % šifrovací mód CBC
infile = 'c:\file.dat';            % vstupní soubor
outfile= 'c:\file.cry';            % výstupní soubor
decfile= 'c:\decrypted.dat'; % dešifrovaný soubor
% šifrování souboru
cast128EncFile(key, infile, outfile, mode, iv);
% dešifrování souboaru
cast128DecFile(key, infile, decfile, mode, iv);
```

Obr. 4: Skript šifrující a dešifrující zvolený soubor pomocí šifry CAST-128

5 Závěr

V článku byla představena kryptografická knihovna CryptoLab, jejímž cílem je rozšířit možnosti systému Matlab o kryptografické metody. Samotná knihovna CryptoLab je složená z obslužných funkcí pro systém Matlab a knihovny DLL, která obsahuje jednotlivé kryptografické metody a to jak pro šifrování textových řetězců, tak i souborů. Toto řešení, pomocí DLL knihovny, se ukázalo jako velmi výhodné pro implementované kryptografické metody, a to díky výhodám, které nabízí programovací jazyk použitý pro implementaci. Realizované metody mohou být využity jak z příkazové řádky, tak i vkládány do samostatných skriptů. Funkčnost knihovny byla ověřena v několika verzích systému Matlab. Realizované rozšíření systému Matlab v podobě knihovny CryptoLab je používáno pro demonstrační účely v rámci výuky a pro širší veřejnost je dostupné prostřednictvím Matlab exchange.

Poděkování

Článek vznikl za podpory projektu FSI-J-12-1810 „*Inteligentní řídicí systémy*“.

References

[1] D. Kahn. *Cryptography The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet.* Scribner, 1996.

[2] E. Biham, A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, Berlin, ISBN : 0-387-97930-1.

[3] W. Diffie, M. Hellman. *New Direction in Cryptography*. IEEE Transaction on Information Theory. Vol. 22, No. 6.

[4] Botan. [online]. [cit. 2012-10-20]. Dostupné z: http://botan.randombit.net/

[5] Crypto++. [online]. [cit. 2012-10-20]. Dostupné z: http://www.cryptopp.com/

[6] N. Ferguson, B. Shneier, T. Kohno. *Cryptography Engineering: Design Principles and Practical Applications*. Wiley, 1 edition, 2010.