Crypto-World

Informační sešit GCUCMP
ISSN 1801-2140

Ročník 16, číslo 4-5/2014 **15. květen**

4 - 5/2014

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info/
(1395 registrovaných odběratelů)

Obsah : str.

Příloha: CFP_MKB2014.pdf
http://crypto-world.info/casop16/CFP_MKB2014.pdf

A. Definice Off-The-Record (OTR) protokolu a jeho využití

Lukáš Langhammer a Josef Polák, Fakulta elektrotechniky a komunikačních technologií, VUT v Brně,
xlangh01@stud.feec.vutbr.cz

Abstract – Tento článek představuje bezpečnostní Off-The-Record (OTR)Messaging protokol, jenž je použit na zabezpečení instant messaging (IM) komunikace. Jsou zde v krátkosti vysvětleny charakteristiky tohoto protokolu, jako dopředná ochrana dat, autentičnost zpráv a způsoby, jak je těchto vlastností docíleno. Dále je rozebírána otázka bezpečnosti a slabiny OTR protokolu a jakým způsobem jsou dále tyto problémy řešeny. V následující kapitole jsou představeny dva způsoby skupinové komunikace za použití OTR protokolu. Poslední kapitola se zaobírá možným použitím tohoto protokolu v různých programech sloužících pro instant messaging komunikaci

1 Úvod

Sociální komunikace za pomocí takzvaných IM (Instant messaging) systémů je v dnešní době velkou částí internetové komunikace. Jak se IM systémy stále více používají pro sociální a obchodní účely, kdy chceme, aby obsah zpráv znal pouze příjemce pro kterého je zpráva určena, vzrůstá důraz na ochranu obsahu zpráv. Nicméně většina mechanizmů užita pro IM a emailovou komunikaci, jako například PGP (Pretty Good Privacy) [1] a S/MIME (Secure/Multipurpose Internet Mail Extensions) [2] poskytují šifrování za pomocí dlouhodobých šifrovacích klíčů k zajištění bezpečnosti a digitální podpisy k ověření autentizace dat, což ovšem způsobuje nepopiratelnost odesilatele zprávy. To ovšem činí odesilatele zpráv zranitelnými v situaci, kdy třetí osoba, které může potenciálně odposlouchávat a uložit komunikaci i přesto, že ji z důvodu šifrování nemůže přečíst. Později může nastat situace, kdy dojde ke kompromitaci šifrovacího klíče. Stejně tak nebude odesilatel schopen popřít, že danou zprávu napsal.
Z tohoto důvodu byl v roce 2004 představen protokol Off-The-Record (OTR) [3]. Tento protokol používá kombinaci symetrické blokové šifry AES, výměny klíčů za pomoci Diffie-Hellmanova algoritmu, hash funkce SHA-1 a má kromě šifrování za úkol umožnit dopřednou ochranu zpráv a jejich popiratelnost [3]. Jinými slovy později po předání zpráv by mělo být nemožné, aby si kdokoli mohl dodatečně tuto zprávu přečíst. OTR dále umožňuje ověření autentičnosti zprávy během komunikace s tím, že později nebude tvůrce zprávy možné jednoznačně identifikovat.

2 Základní vlastnosti protokolu OTR

V této kapitole budou popsány základní vlastnosti protokolu OTR. Budou zde v krátkosti vysvětleny jednotlivé principy, jako dopředná bezpečnost, autentizace dat a popiratelnost a jak je jich prakticky dosaženo.

2.1 Dopředná ochrana dat

K dosažení perfektní dopředné ochrany jsou zprávy šifrovány za použití dočasných šifrovacích klíčů, které jsou po jejich užití vymazány. Jakmile jsou klíče použité na

zašifrování dané zprávy vymazány a tudíž je zamezeno, aby byly později získány, není možné danou zprávu následně rozšifrovat. Pro dosažení dopředné ochrany zpráv jsou tedy použity dočasné AES symetrické šifrovací klíče, jenž jsou sjednány na základě Diffie-Hellmanova kryptografického protokolu blíže popsaného např. v [5], který umožňuje komunikující dvojici sdílet takzvané "sdílené tajemství", jenž je pak použito na generování šifrovacích klíčů. Aby byla zaručena krátkodobost šifrovacích klíčů, je nezbytné, aby docházelo k dalším sjednávání klíčů a mazání použitých soukromých klíčů (hodnot parametrů x_A a x_B). Na základě skutečnosti, že výpočet Diffie-Hellmanova algoritmu vyžaduje pouze dvě modulární mocnění, není pro dnešní počítače problém vytvářet nový klíč pro každou zprávu [3]. Aby bylo dosaženo vyšší efektivity přenosu je sjednávání nových klíčů integrováno do klasické komunikace. To znamená, že každá zpráva obsahuje aktuální veřejný klíč, jenž je následně použit k odvození soukromého klíče užitého k šifrování následující zprávy [4]. Použité klíče ovšem nemůžou být vymazány okamžitě, protože zpráva odeslaná druhou stranou bude zašifrována za použití tohoto klíče a v případě, že by byl tento klíč vymazán z paměti, nebylo by již možné tuto zprávu číst. Jestliže by tedy docházelo ke změně klíče u každé zprávy a jedna strana komunikace by odeslala několik zpráv bez získání odpovědi, bylo by nutné si pamatovat všechny použité klíče $x_m...x_n$, poněvadž by nebylo jasné, který z klíčů bude použit pro šifrování zprávy druhé strany. Proto je změna klíče iniciována na základě odpovědi druhé strany a tak je docíleno toho, že bude nutné si v danou chvíli pamatovat maximálně 2 klíče [4].

2.2 Digitální podpisy a autentičnost

Digitální podpisy jsou známý a oblíbený způsob, jak identifikovat autora dat, zprávy atd. Nevýhoda digitálních podpisů v rámci IM komunikace je skutečnost, že kdokoli může dokázat, že konkrétní zpráva byla vytvořena danou osobou. Bavíme se tedy o takzvané nepopiratelnosti zprávy, jež je podepsána digitálním podpisem, což není v případě soukromé komunikace vždy žádoucí. Z tohoto důvodu není u protokolu OTR k autentizaci zpráv použito digitálních podpisů ale MAC funkce (Message Authentication Code). Jinými slovy digitální podpisy slouží k autentizaci šifrovacích klíčů nikoli samotných zpráv. K autentizaci druhé strany je tedy použito sdílené tajemství a tudíž pouze regulérní příjemce, který zná platný klíč může v danou chvíli ověřit autentičnost zpráv [3].
Digitální podpis je použit pouze na počáteční sjednání klíčů. Pro následující sjednávání je použito funkce MAC k autentizaci nového klíče za pomoci předchozího sdíleného tajemství, což je v [3] prezentováno následně:

$$g^{x_{i+1}}, E(M_r, k_{ij}),, \qquad (1)$$

$$MAC(\{g^{x_{i+1}}, E(M_k, k_{ij})\}, H(k_{ij})), \qquad (2)$$

kde $g^{x_{i+1}}$ je přenášená hodnota pro vytvoření sdíleného tajemství, k je veřejný klíč, $E(M, k)$ označuje šifrování za pomocí AES a H je hash funkce.
Dále v novější verzi protokolu je k vzájemné identifikaci uživatelů užito sdílené tajemství za pomoci tzv. socialist millionaire protokolu viz. kapitola 3.

2.3 Popiratelnost zpráv

Popiratelnost docílené u protokolu OTR si můžeme vysvětlit na následujícím příkladu: Řekněme, že Alice a Bob jsou členy jedné takové IM komunikace. Bob potřebuje mít jistotu, že přijaté data opravdu pochází od Alice, ale nesmí být schopen toto prokázat komukoli jinému. Z tohoto důvodu jsou použity již dříve zmíněné MAC klíče. Tyto soukromé MAC klíče, si můžeme představit jako hash funkce sdílené Alicí a Bobem. Alice použije svůj MAC klíč ve výpočtu MAC kódu její zprávy a pošle tento MAC společně se zprávou. Bob, jakožto příjemce pak ověří integritu a autentičnost dat srovnáním MAC, kterou vypočítala Alice a MAC, kterou vypočítá ze zprávy Bob za pomocí svého MAC klíče. Třetí strana tedy nemůže prokázat původce zprávy, poněvadž nezná soukromý MAC klíč. Současně s tím Bob nemůže komukoli prokázat, že zprávu poslala Alice, protože disponuje stejným MAC klíče a tudíž mohl tuto zprávu vytvořit sám. Dále aby bylo dosaženo popiratelnosti zpráv je po vymazání šifrovacího klíče zveřejněn daný MAC klíč za použití následující posílané zprávy [3]. Použitím tohoto přístupu je docíleno toho, že během regulérní komunikace je příjemce schopen identifikovat odesilatele zprávy, ale jakmile je MAC klíč zveřejněn kdokoli může vytvořit zprávu za použití toho klíče a tak je docíleno popiratelnosti zprávy a není tedy možno identifikovat jejího původce.

3 Zranitelnost systému a bezpečnostní hazardy

Možné útoky na původní protokol OTR jsou popsány v [6]. V tomto článku je zmíněna skutečnost, že daný protokol je zranitelný za použití takzvaného" identity misbinding" útoku [7] během úvodní výměny klíčů. Tento útok by umožnil třetí straně takzvaný MITM (Man In The Middle) útok. Jinými slovy by Eva navázala komunikaci jak s Alicí tak s Bobem, kdy by se Alice domnívala, že komunikuje s Bobem, kdy Bob je přesvědčen, že komunikuje s Evou. Takováto komunikace je v [6] prezentována jako:

$$A \rightarrow E : g^x, Sign_{S_A}(g^x), v_A, \quad (3)$$

$$E \rightarrow B : g^x, Sign_{s_E}(g^x), v_E, \quad (4)$$

$$B \rightarrow E : g^y, Sign_{s_B}(g^y), v_B, \quad (5)$$

$$E \rightarrow A : g^y, Sign_{s_B}(g^y), v_B, \quad (6)$$

kde *S* značí soukromý klíč a *v* je pak klíč veřejný.

Aby bylo možné se tomuto útoku vyhnout byla úvodní výměna autentizačních klíčů AKE (Authenticated Key Exchange) OTR protokolu změněna na SIGMA [8] variantu. V tomto případě dochází k autentizaci až za pomoci zašifrovaných zpráv poté, co je stanoveno sdílené tajemství. Takovýto postup je v [6] popsán následovně:

$$A \rightarrow B : g^x, \quad (7)$$

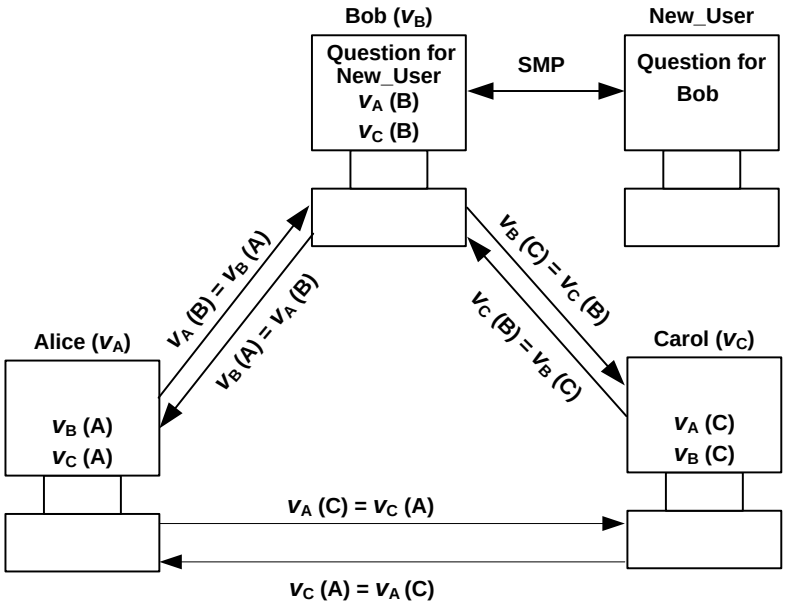
$$B \rightarrow A : g^y, \quad (8)$$

$$A \rightarrow B : A, Sign_{s_A}(g^y, g^x), MAC_{K_m}(0, A), v_A, \qquad (9)$$

$$B \rightarrow A : B, Sign_{s_B}(g^x, g^y), MAC_{K_m}(1, B), v_B, \qquad (10)$$

kde K je MAC klíč.

Dalším problémem je skutečnost, že ve výše zmíněním příkladu Alice i Bob znají veřejný klíč druhé strany než je výměna autentizačních klíčů započata. Z tohoto důvodu si protokol OTR udržuje seznam veřejných klíčů přátel dané osoby. V případě, že některý z přátel začne novou komunikaci za pomocí známého klíče, dojde k automatické autentizaci. Obecný princip komunikace s užitím protokolu OTR je na Obr. 1.



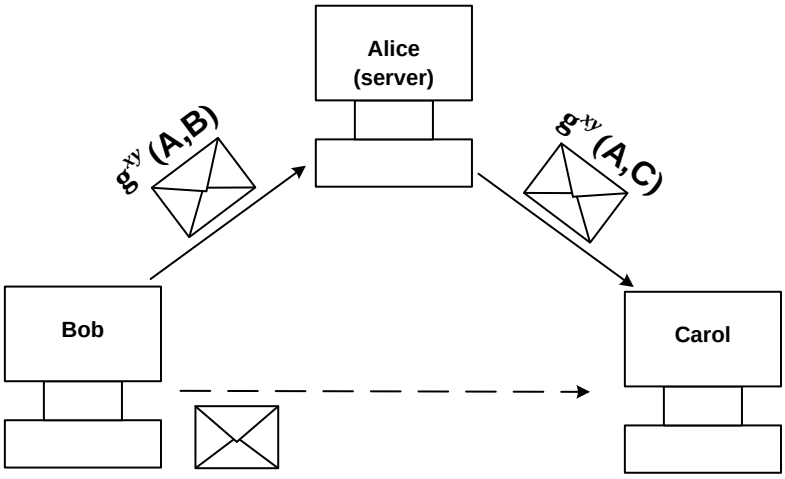
Obr. 1: Zobecněný princip komunikace za pomoci OTR protokolu

V případě, že klíč není v seznamu nalezen, například jedná-li se o první komunikaci s konkrétní osobou, je uživatel vyzván k ověření pravosti klíče. Aby byla umožněna autentizace druhé strany v tomto případě, je použit SMP (Socialist Millionaire) protokol. Koncoví uživatelé si položí otázku, na níž mohou znát odpověď pouze oni. Socialist Millionaire protokol pak slouží k porovnání těchto informaci, aniž by tyto informace byly zveřejněny. Případný MITM útočník může pouze hádat odpověď a pokud není na první pokus schopen odpovědět správně je komunikace ukončena.

4 Skupinová komunikace

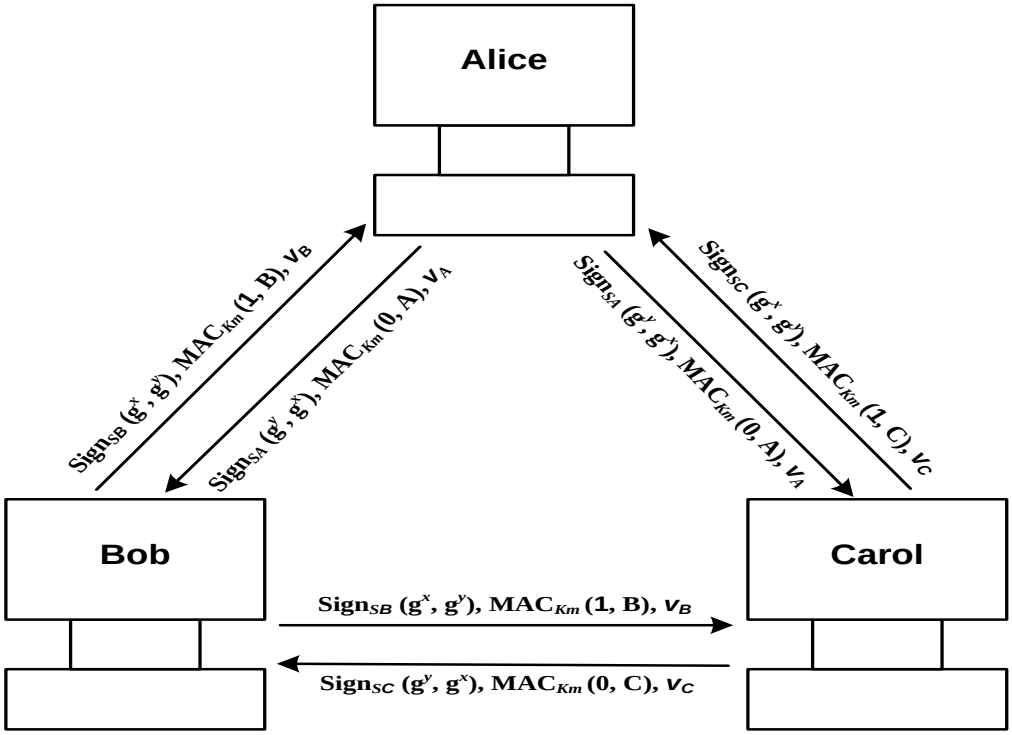
V této kapitole bude rozebrána problematika skupinové komunikace za pomocí IM systémů s použitím protokolu OTR. Vzhledem k tomu, že systémy chat místností jsou stále více užívané

nejen pro sociální komunikaci, ale i pro obchodní účely (např. obchodní diskuse, služby poskytované zákazníkům atd.) vzrůstá poptávka po zabezpečené skupinové komunikaci. Z dříve jmenovaných vlastností, které OTR protokol poskytuje, se použití OTR protokolu pro takový typ komunikace jeví jako vhodné řešení.
Z tohoto důvodu byl v [9] představen GOTR (Group OTR) protokol, jenž má poskytovat zabezpečenou skupinovou komunikaci. Princip tohoto řešení spočívá v tom, že je použit virtuální server, jímž může být kterýkoli člen skupiny. Následně tento server poskytuje výměnu klíčů se všemi ostatními účastníky stejným způsobem, jako je tomu u dvoubodového OTR spojení a takto bude mít každý člen skupiny vlastní sdílené tajemství se serverem [9]. Problém je v tom, že členové komunikace mohou přímo komunikovat jen se severem a ne mezi sebou poněvadž sdílejí svoje sdílené tajemství pouze se serverem a nebyli by tedy schopni rozšifrovat zprávy, které si mezi sebou poslali. Proto server slouží jako zprostředkovatel takovéto komunikace na základě skutečnosti, že každý člen má sdílené tajemství se serverem [9].



Obr. 2: Skupinová komunikace za použití protokolu GOTR za pomoci virtuálního serveru (Alice) v pozici prostředníka

Uveďme si příklad, kdy Bob chce komunikovat s Carol a Alice je v pozici serveru, jak je zobrazeno na Obr. 2. Zpráva je nejdříve poslána Alici, která použije sdílené tajemství, které sdílí s Bobem, aby dešifrovala zprávu a tuto zprávu následně znovu zašifruje tentokrát na základě sdíleného tajemství, jenž má s Carol.
Dále v [10] je prezentován protokol mpOTR (multi-party OTR). Za použití tohoto protokolu mohou členové komunikovat bez nutnosti centrální autority, jak je znázorněno na Obr. 3. Jinými slovy jednotliví členové nespoléhají na prostředníka, aby provedl autentizaci, ale každý člen provede svou vlastní autentizaci s každým dalším členem skupiny.Tento protokol pracuje ve třech krocích, konkrétně to jsou: nastavení komunikace, samotná komunikace a v poslední řadě její ukončení. V první fázi všichni členové komunikace vyjednávají parametry, vytváří sdílené klíče, vytvářejí a vyměňují si podpisové klíče a dochází tedy k autentizaci. Během komunikace mohou členové skupiny posílat autentizované zprávy do chat místnosti. Při ukončení konverzace jsou následně zveřejněny dočasné soukromé klíče [10].

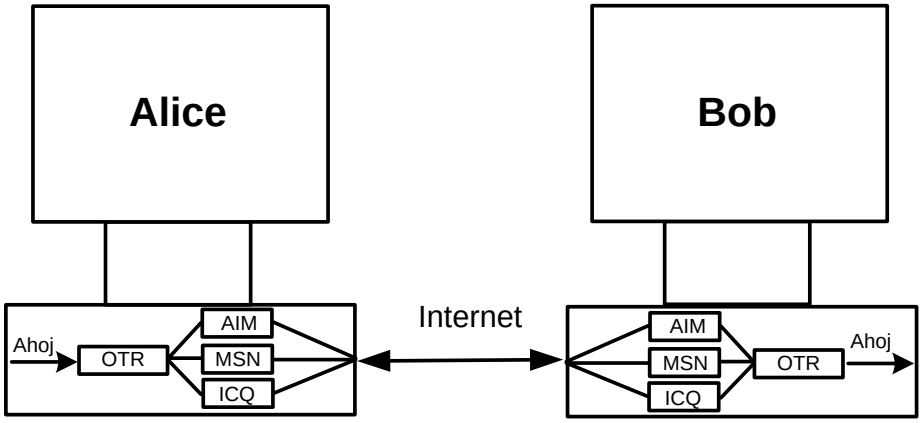


Obr. 3: Princip skupinové komunikace a autentizace u protokolu mp-OTR

5 Použití protokolu OTR

Požadavky na soukromí e-mailové komunikace nejsou nijak vysoké vzhledem k tomu, že je běžné jednotlivé maily uchovávat po dlouhou dobu. Například k většině obchodní komunikace dochází za použití e-mailů s pomocí standardních protokolu PGP a S/MIME, nicméně z pohledu protokolu OTR tyto protokoly poskytují ne vždy vhodné bezpečnostní vlastnosti. Pokud Alice pošle soukromý mail Bobovi, většinou není zamýšleno, aby Bob byl schopen dokázat komukoli dalšímu, že danou zprávu poslala Alice, přesto, že Alice potřebuje způsob, jak se Bobovi autentizovat. Za pomocí OTR protokolu toto není problém. Dále aby Alice mohla poslat svoji první zprávu, je potřeba, aby došlo k výměně klíčů. To znamená, že musí čekat, až Bob pošle svou část sdíleného tajemství, což vyžaduje, aby byl Bob online. A to nebývá v případě mailové komunikace běžné. Tento problém řeší užití takzvaných ring signatures [11].

Zvyšující se množství komunikace pomocí IM systémů, jako například AIM, MSN, ICQ ad. je dalším důvodem, proč použít OTR protokol. Tento protokol je vytvořen nad existujícími IM protokoly. Zpráva je tedy zašifrována a autentizována za použití OTR a odeslána za použití daného IM protokolu, jak prezentuje Obr. 4.



Obr. 4: Využití protokolu OTR jako pluginu pro komunikaci zajištěnou běžnými IM aplikacemi

Takto je docílena snadná integrovatelnost OTR s existujícími IM protokoly jakožto plugin, čímž se vyhneme zdvojování prvků, jako například seznamu přátel. Původně byl OTR implementován jako plugin pro linuxového IM klienta GAIM (později nazýván Pidgin) [3]. Nyní je OTR dostupné v různých podobách například pro IM klienty jako Trillian nebo Kopete. Další programy, jež mají v sobě OTR zabudován jsou např. Adjum a climm dříve známy jako mICQ [12].

V [12] je popsán experiment, jehož se zúčastnilo 8 osob a bylo testováno, jestli mezi sebou dokážou komunikovat s použitím OTR protokolu. Jsou zde popsány problémy s protokolem OTR, ke kterým během experimentu došlo a následně je navrženo, jak tyto problémy vyřešit.

6 Závěr

Se zvyšujícím se množství Instant Messaging (IM) komunikace a bezpečnostními nároky na takovýto provoz kladenými, ať už se jedná o soukromou či obchodní diskuzi, Off-The-Record (OTR) Messaging protokol se jeví jako vhodné řešení z důvodu toho, že poskytuje dopřednou ochranu dat, autentizaci druhé strany a zároveň popiratelnost zpráv, což jsou vlastnosti vhodné pro tento typ komunikace. Tento protokol využívá kombinaci symetrické blokové šifry AES, výměny klíčů za pomoci Diffie-Hellmanova algoritmu a Message Authentication Code funkce s použitím dočasných šifrovacích klíčů. Je diskutována slabost protokolu vůči útoku Man-In-The-Middle a následně řešení tohoto problému změnou úvodní výměny autentizačních klíčů (AKE) a použitím Socialist Millionaire protokolu. OTR je nejen vhodný pro komunikaci mezi dvěma uživateli, ale je zde i několik forem tohoto protokolu pro komunikaci skupinovou. Dále pak je možné protokol využít i pro e-mailovou komunikaci. V závěru je zmíněno několik IM protokolů, které využívají OTR k zabezpečené komunikaci. OTR je téže jako plugin jednoduše implementovatelný do těchto IM systémů.

Literatura

[1] J. Callas, L. Donnerhacke, H. Finney, and R. Thayer.: Open PGP message format. RFC2440, November 1998.

[2] B. Ramsdell.: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification. RFC 3851, July 2004.

[3] N. Borisov, I. Goldberg, and E. Brewer.: Off-the-record communication, or, why not to use PGP. Proceedings of the 2004 ACM workshop on Privacy in the electronic society, p. 77–84, 2004.

[4] C. Alexander and I. Goldberg.: Improved User Authentication in Off-the-Record Messaging. Proceedings of the 2007 ACM workshop on Privacy in electronic societ, p. 41–47, 2007.

[5] W. Diffie and M. Hellman.: New Directions in Cryptography. In IEEE Transactions on Information Theory, p. 74–84, June 1977.

[6] M. D. Raimondo, R. Gennaro, and H. Krawczyk.: Secure off-the-record messaging. WPES ’05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society. New York, NY, USA: ACM Press, p. 81–89, 2005.

[7] W. Diffie, P. C. V. Oorschot, and M. J. Wiener.: Authentication and authenticated key exchanges. Des. Codes Cryptography, vol. 2, no. 2, p. 107–125, 1992.

[8] H. Krawczyk.: SIGMA: The ‘SIGn-and-MAc’ Approach to Authenticated Diffie-Hellman and Its Use in IKE Protocols. In Proceedings of CRYPTO ’03, p. 400–425, 2003.

[9] J. Bian, R. Seker, and U. Topaloglu.: Off-the-Record Instant Messaging for Group Conversation. In IRI '07: Proceedings of Information Reuse and Integration, p. 79-84. IEEE Computer Society, 2007.

[10] I. Goldberg, B. Ustaoglu, M. V. Gundy, H. Chen.: Multi-party off-therecord messaging. ACM Conference on Computer and Communications Security p. 358-368, 2009.

[11] J. Ren, L. Harn.: Generalized Ring Singnatures. Transactions on Dependable and Secure Computing Vol. 5, Issue 3, p. 155-163, 2008.

[12] R. Stedman, K. Yoshida, I. Goldberg.: A user study of off-the-record messaging. SOUPS 2008: 95-104, IRI 2007: 79-84.

B. Lúštenie a analýza šifry Straddling Checkerboard

Michal Hornák, xhornakm@stuba.sk , FEI STU v Bratislave

1. Úvod

Šifra *Straddling Checkerboard* v slovenskej a českej terminológii 1- a 2-miestna zámena, je substitučná šifra zamieňajúca znaky otvorenej abecedy jedno- a dvojcifernými číslami. Otvorenou abecedou myslíme abecedu, pomocou ktorej je napísaný text pred zámenou, resp. zašifrovaním. Šifrovou abecedou myslíme abecedu zašifrovaného textu.

2. Šifrovanie

Šifrovanie sa začína zvolením si veľkosti substitučnej tabuľky, ktorú pri softwarovej implementácii môžeme reprezentovať napríklad dvojrozmerným poľom. V našom prípade budeme pre TSA používať tabuľku o veľkosti 3 × 10, s ktorou vieme substituovať najviac 28 znakov otvorenej abecedy. Následne si zvolíme číselné označenie riadkov a stĺpcov tabuľky. Označenie stĺpcov je permutáciou čísel od 0 po 9, pre označenie riadkov si zvolíme dve čísla z rozsahu od 0 po 9. Kľúč šifry checkerboard pozostáva z hesla, ktoré určuje poradie, respektíve rozloženie znakov v tabuľke, z permutácie stĺpcov a treťou súčasťou kľúča je označenie riadkov.
Pre ukážku si označíme stĺpce po poradí od 0 po 9 a riadky 1 a 3. Substitučnú tabuľku zostavujeme spôsobom, ktorý do kryptografie zaviedli už Argentíniovci. Čiže do substitučnej tabuľky vložíme najskôr znaky kľúča, pričom prípadné opakujúce sa znaky vynecháme a potom doplníme do tabuľky v kľúči nepoužité znaky otvorenej abecedy. Napríklad pre heslo HESLO, označenie stĺpcov 0-9 a riadkov 1 a 3 bude substitučná tabuľka vyzerať nasledovne:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
	H		E		S	L	O	A	B	C
1	D	F	G	I	J	K	M	N	P	Q
3	R	T	U	V	W	X	Y	Z		

V substitučnej tabuľke vždy nechávame prvý riadok neoznačený. Tento riadok predstavuje jednomiestnu zámenu, t.j. znaky z tohto riadku budú šifrované jednocifernými číslami. Taktiež v tomto riadku vynechávame stĺpce, ktorých ciframi sú označené ďalšie riadky tabuľky. V našom príklade sú to stĺpce označené číslami 1 a 3. Zvyšné dva riadky označené číslami 1 a 3 predstavujú dvojmiestnu zámenu, t.j. znaky z týchto riadkov budú šifrované dvojcifernými číslami.

Pri voľbe kľúča musíme zohľadňovať viacero faktorov, najdôležitejším kritériom je však relatívna frekvencia prvých 8 znakov. Voľbou kľúča sa budeme podrobnejšie zaoberať v časti *Ideálny kľúč* na strane 7.

Teraz už máme pripravenú substitučnú tabuľku, podľa ktorej budeme šifrovať (substituovať) otvorený text. Pre zjednodušenie a urýchlenie šifrovania si môžeme substitučnú tabuľku pre usporiadať tak, aby znaky otvorenej abecedy boli zoradené v abecednom poradí:

A	B	C	D	E	F	G	H	I	J	K	L	M
7	8	9	10	2	11	12	0	13	14	15	5	16
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
17	6	18	19	30	4	31	32	33	34	35	36	37

Pre ilustráciu si pomocou uvedenej tabuľky zašifrujeme prvé vety z knihy *Adventures of Sherlock Holmes*:

To Sherlock Holmes she is always the woman. I have seldom heard him mention her under any other name. In his eyes she eclipses and predominates the whole of her sex.

Proces šifrovania otvoreného textu je veľmi priamočiary. Každý znak otvorenej abecedy nahradíme jedno- alebo dvojciferným číslom, ktoré mu prislúcha podľa substitučnej tabuľky:

T	O	S	H	E	R	L	O	C	K	H	O	L	M	E	S	S	H	E
31	6	4	0	2	30	5	6	9	15	0	6	5	16	2	4	4	0	2
I	S	A	L	W	A	Y	S	T	H	E	W	O	M	A	N	I	H	A
13	4	7	5	34	7	36	4	31	0	2	34	6	16	7	17	13	0	7
V	E	S	E	L	D	O	M	H	E	A	R	D	H	I	M	M	E	N
33	2	4	2	5	10	6	16	0	2	7	30	10	0	13	16	16	2	17
T	I	O	N	H	E	R	U	N	D	E	R	A	N	Y	O	T	H	E
31	13	6	17	0	2	30	32	17	10	2	30	7	17	36	6	31	0	2
R	N	A	M	E	I	N	H	I	S	E	Y	E	S	S	H	E	E	C
30	17	7	16	2	13	17	0	13	4	2	36	2	4	4	0	2	2	9
L	I	P	S	E	S	A	N	D	P	R	E	D	O	M	I	N	A	T
5	13	18	4	2	4	7	17	10	18	30	2	10	6	16	13	17	7	31
E	S	T	H	E	W	H	O	L	E	O	F	H	E	R	S	E	X	
2	4	31	0	2	34	0	6	5	2	6	11	0	2	30	4	2	35	

Naším výsledkom však nebude takto rozdelený text, ak by ostal takto rozdelený išlo by iba o jednoduchú zámenu takže výsledný zatvorený text rozdelíme do pätíc

31640 23056 91506 51624 40213 47534 73643 10234 61671 71307 33242 51061 60273
01001 31616 21731 13617 02303 21710 23071 73663 10230 17716 21317 01342 36244
02295 13184 24717 10183 02106 16131 77312 43102 34065 26110 23042 35

3. Dešifrovanie šifry Straddling Checkerboard

Pre legitímneho príjemcu správy prebieha dešifrovanie podobne ako prebiehalo šifrovanie pre odosielateľa správy. Keďže legitímny príjemca správy pozná všetky súčasti kľúča a teda heslo, permutácie stĺpcov a cifry riadkov, zostaví si v prvom kroku substitučnú tabuľku. Substitučná tabuľka je vlastne prefix kód, označenie riadku je prefixom pre celý daný riadok.

V druhom kroku dešifrovania príjemca rozdelí cifry zašifrovanej správy na jedno- a dvojciferné čísla. Ak poznáme substitučnú tabuľku, tak toto delenie je jednoznačné a ľahko realizovateľné. Za našimi označeniami riadkov nasleduje cifra, ktorá určuje, o ktorý znak v danom riadku ide. Nutnou podmienkou pre správne rozdelenie na jedno a dvojciferné znaky je postupovanie zľava doprava od prvej cifry správy.

Keď už máme zašifrovanú správu rozdelenú na jedno- a dvojciferné čísla, tak v treťom kroku dešifrovania zamieňame tieto čísla za znaky otvorenej abecedy podľa substitučnej tabuľky.

V minulosti bola mienka, že človek, ktorý nepozná kľúč šifry nedokáže takto jednoducho rozdeliť cifry ZT na jedno- a dvojciferné čísla, teda znaky, pretože nepozná čísla riadkov. Bez rozdelenia ZT na znaky nie je možná ani ďalšia analýza substituovaného textu a jeho lúštenie. Tento fakt v minulosti často viedol k mylnej predstave o bezpečnosti šifry straddling checkerboard. V nasledujúcich kapitolách ukážeme, že táto šifra nie je omnoho bezpečnejšia než jednoduchá substitúcia.

4. Lúštenie šifry Straddling Checkerboard

Predpokladajme, že sme zachytili zašifrovanú správu a vieme, že bola použitá šifra Straddling Checkerboard. Ak nepoznáme substitučnú tabuľku, tak túto správu budeme musieť lúštiť pomocou frekvenčnej analýzy. Nech je zachytená správa nasledovná:

31640 23056 91506 51624 40213 47534 73643 10234 61671

71307 33242 51061 60273 01001 31616 21731 13617 02303

21710 23071 73663 10230 17716 21317 01342 36244 02295

13184 24717 10183 02106 16131 77312 43102 34065 26110

Frekvenčná analýza:

Cifra	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
Počet Výskytov	26	40	24	31	16	8	20	18	2	2
Relatívna frekvencia (%)	13,90	21,39	12,83	16,58	8,56	4,28	10,70	9,63	1,07	1,07

Už pri takto krátkom texte je jasne vidieť výchylku vo frekvenciách dvoch cifier. Najfrekventovanejšie cifry 1 a 3 spolu predstavujú až 37,97% z celého zašifrovaného textu. Tento fakt nasvedčuje tomu, že s vysokou pravdepodobnosťou sú týmito ciframi označené

riadky substitučnej tabuľky. Na základe tejto informácie vie lúštiteľ rozdeliť cifry zašifrovanej správy na jedno- a dvojciferné čísla nasledovne:

31	6	4	0	2	30	5	6	9	15	0	6	5	16	2	4
4	0	2	13	4	7	5	34	7	36	4	31	0	2	34	6
16	7	17	13	0	7	33	2	4	2	5	10	6	16	0	2
7	30	10	0	13	16	16	2	17	31	13	6	17	0	2	30
32	17	10	2	30	7	17	36	6	31	0	2	30	17	7	16
2	13	17	0	13	4	2	36	2	4	4	0	2	2	9	5
13	18	4	2	4	7	17	10	18	30	2	10	6	16	13	17
7	31	2	4	31	0	2	34	0	6	5	2	6	11	0	2
30	4	2	35												

Tieto jedno- a dvojciferné čísla predstavujú znaky otvorenej abecedy a lúštiteľ má už správu zašifrovanú iba jednoduchou zámenou. V prípade dostatočnej dĺžky textu[1] sa toto dá ľahko lúštiť či už ručne, alebo programom na lúštenie monoalfabetickej šifry (napr. program SCBSolver).

Pri ručnom lúštení využijeme frekvencie daného jazyka, v našom prípade je ním anglický jazyk. Budeme sa snažiť začať najfrekventovanejšími znakmi, v našom prípade sú to cifry 0, 2, 6 7, 4 týchto päť cifier má približne rovnakú frekvenciu výskytu takže je veľmi pravdepodobné, že tri z nich budú práve písmená E,O,A, ktoré patria k najfrekventovanejším, za predpokladu, že ide o štandardný text, nijak neupravený na vyhladenie týchto znakov. Postupnou substitúciou predpokladaných znakov dospejeme až k otvorenému textu.

Aplikačne je to zložitejšie, keďže počítač si nedokáže domýšľať ako ľudia. Preto nutné použiť nielen frekvenčnú analýzu písmen, ale aj frekvencie bigramov, trigramov a tetragramov daného jazyka. Pomocou nich vieme zistiť frekvencie rôznych slovných spojení, často sa vyskytujúcich slov.

5. Ideálny kľúč

V ukážke lúštenia bolo jasne vidieť vysoké frekvencie dvoch cifier pomocou, ktorých sa dal text rozlúštiť bez problémov. Musí tomu byť vždy tak? Ukážeme si, že pri dômyselnej voľbe šifrovacieho kľúču môžeme uvedenú vlastnosť čiastočne potlačiť alebo až úplne eliminovať. V praxi sa to, ale stáva veľmi zriedkavo, čo je sčasti spôsobené voľbou jednoduchých ľahko zapamätateľných šifrovacích kľúčov.

Ak v prvom riadku substitučnej tabuľky budeme mať písmena s najväčšou relatívnou frekvenciou pre OT daného jazyka, je o dosť pravdepodobnejšie, že cifry riadkov nebudú ani prvou ani druhou najfrekventovanejšou cifrou.

[1] Čo predpokladáme.

Pre ukážku sme pripravili tabuľku s relatívnymi frekvenciami písmen anglickej abecedy a rozložili sme ich tak, že najfrekventovanejšie písmená sú v prvom riadku a zvyšné sú rovnomerne rozložené medzi oba zvyšné riadky. Z frekvencií cifier je zjavné, že najfrekventovanejšou cifrou bude 0 nasledovaná ciframi 8 a 9.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**SUMA:**
	E	T	A	O	I	N	S	H			
Frekv.(%)	12,7	9,06	8,167	7,51	6,97	6,75	6,33	6,09			
8	R	C	Y	W	G	P	V	J	Q		
Frekv.(%)	5,99	2,78	1,97	2,36	2,02	1,93	0,98	0,15	0,10	0	18,28
9	D	L	M	F	U	B	K	X	Z		
Frekv.(%)	4,25	4,03	2,41	2,23	2,76	1,49	0,77	0,15	0,07	0	18,16
SUMA(%)	22,9	15,87	12,54	12,1	11,75	10,17	8,08	6,39	0,17		

V druhom príklade sme kľúč zvolili tak, že najfrekventovanejšou cifrou je 8 s relatívnou frekvenciou 30,9% (28,81% riadok a 2,09% stĺpec). Pričom frekvencia cifry druhého riadku je najmenšia zo všetkých s iba 7,62%.Tieto údaje sú pri relatívnej frekvencií daného jazyka a pri reálnom texte. Pri krátkych alebo špeciálne volených textoch môžu byť výchylky ešte väčšie.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**SUMA:**
	E	T	A	O	I	N	S	H			
Frekv.(%)	12,7	9,06	8,16	7,51	6,97	6,75	6,33	6,09			
8	R	D	L	C	U	M	W	F	G		
Frekv.(%)	5,9	4,25	4,03	2,78	2,76	2,41	2,36	2,23	2,02	0	28,81
9	Y	P	B	V	K	J	X	Q	Z		
Frekv.(%)	1,97	1,93	1,492	0,98	0,77	0,15	0,15	0,10	0,07	0	7,62
SUMA(%)	20,66	15,24	13,68	11,27	10,50	9,31	8,84	8,41	2,09		

V takomto prípade, keď nie je možné podľa frekvencií jasne určiť, ktoré cifry označujú riadky, by lúštenie muselo prebiehať so všetkými kombináciami prefixov. Ako si však ukážeme na konci kapitoly päť vieme si množstvo kombinácií zredukovať pomocou nami zistených intervalov ohraničujúcich minimálne a maximálne relatívne frekvencie stĺpcov a riadkov. Ak by sme neuvažovali s týmito maximálnymi relatívnymi frekvenciami museli by sme riešiť všetky možné kombinácie, ktorých je pri tabuľke veľkosti 3x10 rovných 90. Pri použití tabuľky 4x10 by ich bolo až 960.

Tak isto si to môžeme demonštrovať na tabuľke 4x10 do ktorej budem vkladať slovenskú abecedu so všetkými znakmi okrem znakov x, w, Í, ŕ, q, keďže tieto písmená sú najmenej početné v celej abecede a súčet ich relatívnych frekvencií výskytu je iba 0,064%. Hlavným dôvodom však je to, že k dispozícií máme iba 37 znakov na šifrovanie = [(4r) * (10s) – 3o], kde 4r znamená počet riadkov, 10s je náš počet stĺpcov a 3o sú označenia riadkov, ktoré z

prvého riadku . Relatívne frekvencie, ktoré využívame sú uvedené na nasledujúcej strane, keďže však obsahovali aj početnosť medzery, ktorú do tabuľky nezahŕňame, frekvenciu sme rozpočítali ku všetkým ostatným znakom podľa nasledujúceho vzťahu:

$$f(znaku)' = \frac{f(znaku)}{100\% - \text{f(medzery)}} * 100\%$$

Tabuľka relatívnych frekvencií znakov slovenské ho jazyka:

ZNAK	**S medze-rou**	**Bez med-zery**	**Znak**	**S medze-rou**	**Bez med-zery**
MEDZERA	13,489	0	B	1.124	1.139278
O	8.308	9.603403	Č	1.077	1.089243
A	7.34	8.00506	Í	0.996	1.006844
E	6.927	7.475718	Ý	0.981	0.990869
I	5.594	6.010336	Š	0.918	0.927095
N	5.185	5.492236	Ú	0.875	0.883107
T	4.294	4.528819	Ž	0.817	0.824212
V	4.057	4.239024	Ť	0.771	0.777351
S	4.051	4.222299	É	0.669	0.674198
R	3.783	3.94272	Ľ	0.307	0.309068
K	3.172	3.296715	F	0.266	0.266819
L	2.976	3.073491	G	0.222	0.222592
D	2.919	3.008534	Ď	0.141	0.141314
M	2.539	2.615342	Ň	0.139	0.139196
P	2.538	2.604119	Ô	0.128	0.128178
U	2.327	2.387597	Ó	0.075	0.075096
C	2.295	2.349677	Ä	0.06	0.060045
H	2.05	2.098153	X	0.047	0.047028
J	1.92	1.960184	W	0.011	0.011005
Z	1.811	1.846452	Ĺ	0.006	0.006001
Á	1.545	1.573496	Ŕ	0.006	0.006
Y	1.341	1.362044	Q	0	0

Následne sme vytvorili substitučnú tabuľku podobným spôsobom ako je uvedené vyššie, a teda najfrekventovanejšie znaky idú do prvého riadku, zvyšné rovnomerne do zvyšných riadkov. Existuje veľké množstvo kombinácií rozloženia znakov, toto je len jeden z mnohých.

	0	1	2	3	4	5	6	7	8	9	*SUM A*
	O	A	E	I	N	T	V				
Frekv	9.6%	8%	7.48 %	6%	5.5%	4.5%	4.2%				
7	S	L	P	H	Á	Č	Š	Ť	F	Ň	
Frekv	4.2%	3.07 %	2.6%	2.1%	1.57 %	1.09 %	0.93 %	0.78 %	0.27 %	0.14 %	17.73 %

8	R	D	U	J	Y	Í	Ú	É	G	Ô	
Frekv	3.94 %	3%	2.39 %	1.96 %	1.36 %	1%	0.88 %	0.67 %	0.22 %	0.13 %	15.96 %
9	K	M	C	Z	B	Ý	Ž	Ľ	Ď	Ó	
Frekv	3.3%	2.62 %	2.35 %	1.85 %	1.14 %	0.99 %	0.82 %	0.31 %	0.14 %	0.075 %	13.86 %
SUM A	21.04%	16.69 %	14.82 %	11.91 %	9.57 %	7.58 %	6.83 %				

Z tabuľky vidíme, že frekvencie cifier riadkov sú zamiešane medzi frekvenciami cifier stĺpcov, zapísane po poradí od najpočetnejších po najmenej početné:

0	7	1	8	2	9	3	4	5	6
Stĺpec	Riadok	Stĺpec	Riadok	Stĺpec	Riadok	Stĺpec	Stĺpec	Stĺpec	Stĺpec

V našej nasledovnej substitučnej tabuľke sme rozložil znaky abecedy v tabuľke tak aby relatívne frekvencie cifier označujúcich riadky neboli medzi najfrekventovanejšími ciframi.

	0	1	2	3	4	5	6	7	8	9	SUMA
	E	A	O	K	L	D	M				
frekv	7.48	8	9.6	3.3	3.07	3	2.62				
7	S	R	P	H	Á	Č	Š	Ť	F	Ň	
frekv	4.2	3.94	2.6	2.1	1.57	1.09	0.93	0.78	0.27	0.14	18.6
8	U	T	N	J	Y	Í	Ú	É	G	Ô	
frekv	2.39	4.5	5.5	1.96	1.36	1	0.88	0.67	0.22	0.13	19.02
9	I	V	C	Z	B	Ý	Ž	Ľ	Ď	Ó	
frekv	6	4.2	2.35	1.85	1.14	0.99	0.82	0.31	0.14	0.075	18.145
SUMA	20.07	20.64	20.05	9.21	7.14	6.08	5.25				

Z tabuľky je vidno, že ani jedna z cifier označujúcich riadok sa nenachádza medzi prvými tromi najfrekventovanejšími znakmi kde by ich lúštiteľ očakával. Keďže frekvencie prvých šiestich cifier sú približne rovnaké, hľadal by ich medzi prvými šiestimi ciframi. Pre slovenský jazyk s použitím vybraných znakov abecedy a počítaním iba s relatívnymi frekvenciami, nie je možné posunúť tieto frekvencie na ďalšie miesta. Je to zjavné, ak sa pozrieme na frekvencie cifier zvyšných stĺpcov, ktoré sú neporovnateľne menšie. Je teda na mieste uvažovať, že pri štandardnom texte v slovenskom jazyku dostatočnej dĺžky(dostatočnej na to aby bola frekvencia znakov približne porovnateľná s relatívnymi frekvenciami jazyka), môžme predpokladať, že aspoň jedna z prvých štyroch najfrekventovanejších cifier bude cifra označujúca riadok tabuľky.

Ďalším príkladom bude také rozloženie znakov v tabuľke aby relatívne frekvencie cifier označujúcich dva z troch riadkov boli čo najnižšie. Najmenej početné znaky sme umiestnili do riadkov 7,9 a stĺpcov 7 a 9, keďže nie len riadok, ale aj stĺpec s rovnakým označením ako má riadok musíme prirátavať ku frekvencií výskytu danej cifry. Ako je možné vidieť z tabuľky, cifry označujúce riadky, konkrétne 7 a 9, majú najnižšie relatívne frekvencie spomedzi všetkých cifier. Na úkor toho je však frekvencia cifry 8 (28,05%) približne dvakrát vyššia než frekvencia druhej najpočetnejšej cifry 5 (13,265%).

	0	1	2	3	4	5	6	7	8	9	SUMA
	T	A	V	I	N	O	E				
frekv	4.5	8	4.2	6	5.5	9.6	7.48				
7	H	G	J	C	Y	Ó	É	Ď	F	Ň	
frekv	2.1	0.22	1.96	2.35	1.3	0.075	0.67	0.14	0.27	0.14	10.885
8	R	D	S	M	K	P	U	Ť	L	Ľ	
frekv	3.94	3	4.2	2.62	3.3	2.6	2.39	0.78	3.07	0.31	28.05
9	Z	Č	Ú	Í	B	Ý	Š	Ž	Á	Ô	
frekv	1.85	1.09	0.88	1	1.14	0.99	0.93	0.82	1.57	0.13	10.85
SUMA	12.39	12.31	11.24	11.97	11.3	13.265	11.47				

Pri nasledujúcej substitučnej tabuľke si kľúč volíme tak, aby sme zistili akú najvyššiu relatívnu frekvenciu môže dosiahnuť stĺpec v tabuľke.

	0	1	2	3	4	5	6	7	8	9	SUMA
	O	T	S	K	R	N	V				
frekv	9.6	4.5	4.2	3.3	3.94	5.5	4.2				
7	I	Ú	Ž	G	Ň	É	Ť	Ľ	F	Ô	
frekv	6	0.88	0.82	0.22	0.14	0.67	0.78	0.31	0.27	0.13	10.435
8	A	D	L	J	Y	M	Č	Ó	Í	Á	
frekv	8	3	3.07	1.96	1.36	2.62	1.09	0.075	1	1.57	26.115
9	E	U	P	Z	B	C	Š	Ď	H	Ý	
frekv	7.48	2.39	2.6	1.85	1.14	2.35	0.93	0.14	2.1	0.99	23.67
SUMA	31.08	10.77	10.69	7.33	6.58	11.14	7				

Pri usporiadaní najfrekventovanejších cifier do jedného stĺpca označeného cifrou 0 dostávame maximálnu možnú relatívnu frekvenciu jedného stĺpca pre slovenský jazyk, ktorá je 31,08%.

Minimálnou veľkosťou jedného stĺpca pri našom výbere znakov stĺpec so znakmi ó, ô, ň, ktorých súčet nám dáva minimálnu relatívnu frekvenciu jedného stĺpca 0,345%.

Ak zrátame 12 najmenej frekventovaných písmen dostávame sa ku najnižšej relatívnej frekvencií riadku, ktorá je približne 4,501%. Takže môžeme povedať, že cifry s relatívnymi frekvenciami v rozsahu 0,485% a 4,501% sú frekvenciami stĺpcov, nie riadkov. Rovnaké ohraničenie môžeme urobiť aj zhora, konkrétne spočítaním 12 najfrekventovanejších znakov dostávame relatívnu frekvenciu 62,898%, pričom najfrekventovanejší stĺpec má relatívnu frekvenciu 31,08%, takže môžeme predpokladať, že cifry, ktorých súčet frekvencií sa nachádza v rozmedzí 31,08% a 62,898% budú s vysokou pravdepodobnosťou frekvenciami cifier označujúcich riadky. Je však nutné brať do úvahy fakt, že intervaly ku ktorým sme sa dostali, konkrétne <0,485;4,501> a <31,08;62,898> platia výhradne pre slovenský jazyk, pre ktorý sme hľadali tieto ohraničenia, čiže nie sú aplikovateľné na iné správy v inom jazyku, keďže každý jazyk má špecifické relatívne frekvencie výskytu znakov, do úvahy treba brať takisto, že tieto intervaly budú platiť iba pre tabuľku 4x10, na ktorej sme ich ziskali.

Taktiež je nutné brať do úvahy, že čím je šifrovaný text kratší tým viac sa relatívne frekvencie daného jazyka líšia od reálnych frekvencií daného textu, pre ukážku urobíme frekvenčnú analýzu jednej krátkej správy v anglickom jazyku a porovnáme ju s relatívnymi frekvenciami anglického jazyka:

Meeting will be held tomorrow at the Memorial Building in Bratislava.

Znak	A	B	C	D	E	F	G	H	I
Relatívna frekvencia(%)	8,2	1,5	2,8	4,3	12,7	2,2	2	6,1	7
Frekvencia správy(%)	8,5	5,1	0	3,4	10,2	0	3,4	3,4	11,9

Znak	J	K	L	M	N	O	P	Q	R
Relatívna frekvencia(%)	0,15	0,8	4	2,4	6,75	7,5	2	0,1	6
Frekvencia správy(%)	0	0	10,2	6,8	5,1	6,8	0	0	6,8

Znak	S	T	U	V	W	X	Y	Z
Relatívna frekvencia(%)	6,3	9,06	2,76	0,98	2,4	0,15	1,98	0,07
Frekvencia správy(%)	1,7	8,5	1,7	1,7	3,4	0	0	0

Môžeme si všimnúť, že rozdiely medzi relatívnymi a reálnymi frekvenciami pri takto krátkych správach sú príliš vysoké a neodhadnuteľné, napríklad znak S ma relatívnu frekvenciu približne 6,3% naša správa má však iba 1,7% čo je takmer 4-násobok, a teda nie je možné sa riadiť hodnotami frekvenčnej analýzy.

6. Prefix kód

Kód je vo všeobecnosti pravidlo podľa, ktorého meníme správu/informáciu, do inej po väčšinou kratšej formy. Táto forma môže byť a veľa prípadoch aj je iného typu, napríklad znaky abecedy kódujeme do čísel, Morseovho kód, svetelných alebo zvukových signálov, a iných.
Kódovanie je proces, pri ktorom sa zdrojová informácia konvertuje pomocou pravidiel daného kódovania na kód, opakom kódovania je dekódovanie, pri ktorom sa zakódovaná informácia konvertuje na zdrojovú informáciu.
Prefixový kód je typom kódu, charakteristický svojím prefixom, pre ktorý platí, že žiadne kódové slovo nie je prefixom žiadneho iného kódového slova. Ako príklad si uvedieme 2 rôzne kódové abecedy:

prvá abeceda {1,2,4,32}
druhá abeceda {1,2,3,23}

Rozdiel medzi týmito abecedami sa zdá byť minimálny, no keď si zoberieme prvú abecedu vidíme, že žiadne kódové slovo {1,2,4,32} nie je prefixom iného slova, keďže toto platí ide o prefixový kód.
Pri druhej abecede {1,2,3,23} vlastnosť, že žiadne kódové slovo nie je prefixom iného slova už neplatí. Prefixom slova 23 je slovo 2, keďže sa obidve slová nachádzajú v jednej kódovej abecede, nebolo by možné bez použitia špeciálneho znaku, ktorý by jednoznačne definoval kedy ide o jedno a kedy o dve slová, rozlíšiť či pri správe 23 ide o slovo 23 alebo dve slová 2 a 3. Z toho nám vyplýva, že táto kódová abeceda nemôže byť prefix kódom.
Jedným z najvýznamnejších prefixových kódov je Huffmanov kód, je to algoritmus, ktorý sa využíva na bezstratovú kompresiu dát, využíva sa napríklad aj pri stratových kompresiách obrázkov JPEG, audio súborov MP3, WMA, aj keď ide o stratové kompresie, časť s huffmanovým kódom je bezstratová. Pri tomto type kódovania sa ako prvé spraví frekvenčná analýza súboru a podľa nej sa vytvorí binárny strom, v ktorom najfrekventovanejšie znaky majú najkratší binárny reťazec(najfrekventovanejší znak ma dĺžku 1 bit).
Prefixový kód pri šifre checkerboard vieme skonštruovať tak, že si písmena abecedy rozdelíme do 10 skupín, ktorými sú cifry od 0 po 9 a všetkým cifrám, ktoré označujú riadky v substitučnej tabuľke priradíme cifry od 0 po 9. Uvedieme si príklad pre nasledovnú substitučnú tabuľku:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
	H		E		S	L	O	A	B	C
1	D	F	G	I	J	K	M	N	P	Q
3	R	T	U	V	W	X	Y	Z		

Je zjavné, že každé kódové slovo(v našom prípade je kódovým slovom znak abecedy) je jednoznačne definované. Taktiež, že naše kódovanie je injektívne keďže, nie je možné aby zakódovanie niekoľkých slov bolo zhodné so zakódovaním iných slov. Je to vďaka tomu, že v prvom riadku substitučnej tabuľky vynechávame stĺpce, ktorých cifry sú zároveň ciframi,

ktoré označujú riadky, ak by tomu tak nebolo stala by sa nasledovná vec:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
	H	X*	E		S	L	O	A	B	C
1	D	F	G	I	J	K	M	N	P	Q
3	R	T	U	V	W	X	Y	Z		

Ak by sme mali pri tejto tabuľke v prvom riadku v stĺpci s označením 1 znak X* potom by sme správu X*EB zakódovali ako 128, a správu GB zakódovali takisto ako 128, v takomto prípade by

$$X*EB \neq GB, \text{ ale}$$
$$K(X*EB) = K(GB)$$

Teda dané kódovanie už by nebolo jednoznačné a nešlo by už o prefixový kód.

Vďaka tomu, že ide o prefixový kód každá správa zašifrovaná šifrou checkerboard je jednoznačne dekódovateľná(resp. dešifrovateľná), v prípade že správu čítame zľava doprava od prvého prijatého znaku. Ak by sme začali správu dešifrovať až od určitej pozície, je možné, že by sme nevedeli rozlíšiť prvý znak správy, čo si ukážeme na príklade pri správe HELLOWORLD. Táto správa by podľa prvej tabuľky v kapitole Prefix kódy bola zašifrovaná nasledovne: 0255634630510. Správu by sme začali čítať až od siedmeho znaku zašifrovaného textu takže by sme zachytili správu 4630510 v takomto prípade by sme mali na výber 3 možné znaky a to konkrétne S, J a W, z ktorých by sme museli vybrať to, ktoré by najlepšie „pasovalo“ k zvyšku textu, čím väčšia tabuľka by bola použitá tým viac možných znakov by bolo na výber.

To že ide o prefix-free kód nám umožňuje dešifrovať správu postupne ešte pred prijatím celej správy čo je citeľnou výhodou hlavne pri prenose veľkej správy pomalým spojením kedy nemusíme čakať na prijatie celej správy a dešifrovaním až po prijatí celej správy.

Použitá literatúra

[1] Klasické šifry: Otokar Grošek, Milan Vojvoda, Pavol Zajac, STU v Bratislave, 2007

[2] Gentlemani nečtou cizí dopisy: Jiří Janeček, Books Bonus A, 1998

[3] Základy kryptografie: Otokar Grošek a kolektív, STU v Bratislave, 2010

[4] Základy kódovania: K.Čipková, L.Satko, STU v Bratislave, 2008

C. Nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu - eIDAS

Tak trochu v tichosti a bez nepříliš velkého zájmu médií se pomalu, ale jistě blíží účinnost právního předpisu – nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu (dále jen **eIDAS),** které umožní přeshraniční uznávání a interoperabilitu bezpečných systémů elektronické identifikace a autentizace.

Vzhledem k tomu, že jde o **nařízení**, tak tento právní předpis bude přímo aplikovatelný ve všech členských státech EU. Stojí také za upozornění, že současně **bude zrušena stávající směrnice o elektronickém podpisu 1999/93/EC**.

Stávající legislativa EU se dosud zabývala zejména úpravou oblasti využití elektronického podpisu (viz právě již zmíněná Směrnice 1999/93/EC), kdežto uvedené nařízení rozšiřuje úpravu na další zcela nové důvěryhodné služby s cílem zajistit pro potencionální uživatele digitálního světa jednoznačné právní prostředí a to již nejen pro využití různých forem elektronického podpisu, ale i nově pro autentizaci a další související důvěryhodné služby.

Toto nařízení se již připravuje poměrně dlouho (jak jsem se již v úvodu zmínil, tak v ČR bez velkého zájmu médií a odborné veřejnosti, snad s výjimkou článků J. Peterky a J. Průšy z roku 2013 uveřejněné na Lupě a odborných článků O. Felixe – např. konference ISSS).
První návrh textu nařízení Evropská komise schválila již před dvěma roky a to konkrétně 4. června 2012.

Dne 28. února 2014 byla konečně dosažena dohoda mezi reprezentanty EP, EK a Rady na znění textu tohoto dokumentu. Návrh byl následně předložen v dubnu na plenárním zasedání Evropského parlamentu (EP) a Radě ministrů bude předložen v červnu letošního roku.

Pokud vše půjde hladce (a vzhledem k dlouhému a podrobnému projednávání se to dá očekávat), tak by nařízení mohlo **vstoupit v platnost 1. července 2014** (tedy dnem, kdy se předpokládá, že nařízení bude zveřejněno v Úředním věstníku EU).

Data účinnosti jednotlivých částí budou však odložena tak, že ustanovení budou nabývat účinnosti postupně a to podle přijetí prováděcích aktů. Toto se plánuje na období 2015 – 2018. Jedna z významných povinností (vzájemné uznávání prostředků pro elektronickou identifikaci) by měla být účinná až od poloviny roku 2018. Ovšem např. dobrovolné uznávání oznámených systémů elektronické identifikace může v členském státě začít ihned po přijetí potřebných prováděcích aktů týkajících se úrovní zabezpečení a interoperability.

Co je hlavním obsahem tohoto nařízení?

Nařízení upravuje zejména následující oblasti:
1) důvěryhodnou elektronickou identitu fyzické osoby;
2) důvěryhodný elektronický podpis zaručující integritu a vazbu na identitu fyzické osoby;
3) důvěryhodné značky zajišťující integritu a vazbu na právnickou osobu;
4) důvěryhodné časové razítko zajišťující integritu a vazbu na čas;

5) důvěryhodnou službu registrovaného elektronického doručování zajišťující integritu a vazbu na odesílatele, adresáta a čas odeslání a doručení;
6) důvěryhodný dokument se zaručenou integritou;
7) důvěryhodnost webových stránek s vazbou na provozovatele.

Směrnice 1999/93/EC o elektronickém podpisu řešila z uvedených oblastí plně pouze bod 2, částečně body 1 a 6. Další vývoj využívání vynutil v EU a v ČR potřebu rozvoje souvisejících služeb a některých podpůrných prostředků.
Např. v českém zákoně o elektronickém podpisu 227/2000 Sb. se již v jeho novele v roce 2004 objevila elektronická značka (oblast 3) a časové razítko (oblast 4). Oblast 5 (částečně i 6) jsme v ČR prakticky začali budovat pomocí informačního systému datových schránek (ISDS), který vychází ze zákona č. 300/2008 Sb. Zcela nově je upravena oblast 7. Dosud byly certifikáty pro webové stránky nakupovány od „důvěryhodných certifikačních autorit" jako Verisign, Thawte atd. Hlavním měřítkem kritéria důvěryhodnosti však bylo především hlavně to, že kořenové certifikáty těchto autorit jsou k dispozici ve všech prohlížečích – právní otázka nasazení těchto certifikátů byla dosud opomíjena.

Podívejme se nejprve na oblast elektronického podpisu. Především přijetím nařízení bude **směrnice o elektronickém podpisu 1999/93/EC zrušena a to k 1. červenci 2016.**
Základní pojmy / definice „zaručený elektronický podpis" (advanced electronic signature) a kvalifikovaný certifikát (qualified certificate) zůstávají zachovány. Doplněna je definice pro „kvalifikovaný elektronický podpis" (qualified electronic signature), který je zaručeným elektronickým podpisem, založeným na kvalifikovaném certifikátu a vytvářeným pomocí kvalifikovaného zařízení pro vytváření elektronického podpisu (obdoba bezpečného podpisového prostředku SSCD ve smyslu směrnice 1999/93/EC). Tento typ podpisu není ničím novým, protože je v různých materiálech a standardech EU zmiňován již od roku 2000, ale ve Směrnici uveden není, jde tedy o jeho uznání de jure. Podstatné je, že by tento kvalifikovaný elektronický podpis měl mít stejné právní účinky jako vlastnoruční podpis a to nyní ve všech členských státech, zatímco právní účinky u ostatních typů elektronických podpisů mohou být upraveny na úrovni národního práva. To umožňuje, aby v našem právním systému mohl zůstat již „zaběhnutý" „uznávaný elektronický podpis", tak jak jej definuje §11 zákona o elektronickém podpisu č. 227/2000 Sb. (zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaným akreditovanou certifikační autoritou).

Na úrovní EU se tímto nařízením dále zavádí a definuje elektronická značka (electronic seal). Kvalifikovaná elektronická značka (elektronická značka založená na kvalifikovaném certifikátu) by měla zajistit právní domněnku, která zaručuje původ a integritu dat, s nimiž je spojena. Za důležité považuji zmínit, že existuje rozdíl mezi vymezením pojmu kvalifikovaná elektronická značka v nařízení a v našem zákonu o elektronickém podpisu. Podle našeho zákona elektronickou značkou může data označit osoba fyzická i osoba právnická. V nařízení však může data „označit" elektronickou značkou pouze právnická osoba („creator of a seal").

V přehledu oblastí uvedených v úvodu je dále pod bodem 6 uveden důvěryhodný dokument se zaručenou integritou. Dokument pocházející od právnické osoby lze označit za důvěryhodný dokument, pokud obsahuje následující prvky:
- elektronický podpis, který zaručuje identitu fyzické osoby, která je oprávněna dokumenty podepisovat;
- elektronickou značku zaručující identitu právnické osoby;
- elektronické časové razítko zaručující integritu a vazbu na čas.

Jedním z klíčových pojmů celého nařízení je definice důvěryhodných služeb. Za základní důvěryhodné služby se považuje vytváření, verifikace a validace elektronických podpisů, značek a časových razítek a certifikátů týkajících se těchto služeb. Nařízení se dále zabývá problematikou používání elektronické identifikace (eID). Nařízení ukládá povinnost uznávat systémy elektronické identifikace, které budou jednotlivými členskými státy tzv. oznámeny, za předpokladu splnění podmínek, které pro ně budou definovány. Oznámení těchto systémů není povinné, předpokládá se, že každý členský stát si zvolí, které z používaných systémů oznámí a tím umožní uznání prostředků eID vydaných v rámci tohoto systému i v ostatních státech (to platí především při přístupu ke službám poskytovaným veřejným sektorem, tj. v ČR to bude pravděpodobně přístup k registrům veřejné správy)

Ani tato oblast eID, ale není zcela nová. Této oblasti se již delší dobu (bez jasně definovaného právního zázemí) věnoval mezinárodní projekt STORK. Projekt STORK (Secure idenTity acrOss boRders linKed) je bezesporu nejvýznamnější evropský projekt v oblasti interoperability národních eID. Jeho realizace byla zahájena již v roce 2008 a zaměřuje se právě především na veřejné služby, jako je např. možnost vyřízení změny bydliště online či elektronické doručování. Na projekt STORK v současné době navazuje STORK 2.0, který se snaží se zaměřit na soukromé poskytovatele identit a dále na sběr nejrůznějších atributů (např. studované předměty na vysoké škole, informace o pověření jednat za organizaci apod.). Za Českou republiku se projektu účastní Ministerstvo vnitra ČR a sdružení CZ.NIC, které do projektu zapojilo svoji službu mojeID.

Za zmínku stojí také to, že nařízení rozšiřuje nároky na náhradu škody, které byly způsobeny nedbalostí poskytovatele důvěryhodných služeb a to v důsledku nedodržení bezpečnostních postupů.

U orgánů národního dohledu dojde k rozšíření působnosti, co se týče poskytovatelů důvěryhodných služeb i kvalifikovaných poskytovatelů důvěryhodných služeb.

Současná podoba TLS „trusted listů“ (viz aplikace certiq provozovaná MV ČR, která umožňuje ověřit, zda byl certifikát vydán jako kvalifikovaný v některém členském státu EU) dozná také rozšíření. Trusted listy by podle tohoto nařízení měly obsahovat informace o kvalifikovaných poskytovatelích všech důvěryhodných služeb (důvěryhodné služby budou nyní zahrnovat mnohem širší spektrum služeb než doposud).

Pokud jde o certifikaci zařízení pro vytváření a ověřování kvalifikovaných podpisů, tak ty by měl provádět subjekt pověřený členským státem. Tento subjekt bude svým výrokem potvrzovat, že zařízení splňuje požadavky na takováto zařízení. Seznam certifikovaných zařízení bude zveřejňovat Komise centrálně.

K realizaci daného nařízení nás tedy čeká v následujících 2-3 letech řada důležitých kroků a to včetně novelizace některých zákonů, zejména zákona o elektronickém podpisu, zákona o archivnictví, zákona o datových stránkách apod.

V neposlední řadě čeká všechny, kteří se budou podílet na realizaci tohoto nařízení v ČR důkladné seznámení s jeho obsahem, pojmy a novými možnostmi, které přináší.

D. Call for Papers
Mikulášská kryptobesídka

27. – 28. listopad 2014, Praha
http://mkb.tns.cz

Základní informace

Mikulášské kryptobesídky už letos bude dva kusy po tuctu. Je zaměřena na podporu úzké spolupráce odborníků se zájmem o teoretickou a aplikovanou kryptografii a další příbuzné oblasti informační bezpečnosti. Hlavním cílem je vytvořit prostředí pro neformální výměnu informací a nápadů z minulých, současných i budoucích projektů. Cítíme potřebu setkání expertů s jejich kolegy bez obchodních vlivů, starostí s (potenciálními) zákazníky, šéfy a dalšími rozptylujícími faktory. ;-)

Workshop se skládá ze (a) dne prezentací příspěvků, diskusí a neformálního setkání ve čtvrtek *27. listopadu* a (b) půldne prezentací příspěvků a diskusí v pátek *28. listopadu 2014*. Pro workshop jsou domluveny zvané příspěvky od:

- Joachim Posegga (Univ. Pasov, SRN).
- Gregor Leander (Ruhr-Univ. Bochum, SRN).
- Karthik Bhargavan (nezávislý výzkumník, Indie).
- Karsten Nohl (nezávislý výzkumník, SRN).

Podrobné informace, včetně pokynů k registraci, se budou průběžně objevovat na www stránkách workshopu: http://mkb.tns.cz.

Pokyny pro autory

Přijímány jsou příspěvky zaměřené především na oblasti kryptoanalýzy, aplikované kryptografie, bezpečnostních aplikací kryptografie a dalších souvisejících oblastí. **Návrhy se přijímají odděleně pro sekci KEYMAKER (studentská soutěž) a pro hlavní program workshopu.** Oba druhy návrhů mají požadovaný rozsah 5-15 stran A4 a připravenost pro anonymní hodnocení (bez jmen autorů a zjevných odkazů). Identifikační a kontaktní údaje prosím pošlete v těle e-mailu s příspěvkem jakožto přílohou a jasným označením KEYMAKER, nebo STANDARD TRACK.

Šablony pro formátování příspěvků pro Word a LaTeX lze získat na www stránkách workshopu: http://mkb.tns.cz. Příspěvky mohou být napsané v češtině, slovenštině, nebo angličtině.

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu RTF, nebo PDF a tak, aby přišly nejpozději do *30. září 2014*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2014 – navrh prispevku“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *30. října*. Příspěvek pro sborník workshopu pak musí být dodán do *11. listopadu*.

Důležité termíny

Návrhy příspěvků:	30. září 2014
Oznámení o přijetí/odmítnutí:	30. října 2014
Příspěvky pro sborník:	11. listopadu 2014
Konání MKB 2014:	27. – 28. listopadu 2014

Programový výbor

Michal Hojsík, Honeywell a MFF UK, Praha, CZ
Marek Kumpošt, NetSuite & FI MU, Brno, CZ
Vašek Matyáš, FI MU, Brno, CZ – předseda
Tomáš Rosa, Raiffeisenbank a UK, CZ
Luděk Smolík, Siegen, DE
Martin Stanek, UK, Bratislava, SK
Pavol Zajac, STU, Bratislava, SK

Mediální partneři

E. Pozvánka ke kurzu PKI (+eIDAS) Akademie CZ.NIC

Akademie CZ.NIC je vzdělávací projekt sdružení CZ.NIC, správce české domény nejvyšší úrovně. Výukové centrum, jež se pod tímto názvem skrývá, nabízí zájemcům možnost odborného vzdělávání v oblasti Internetu a internetových technologií. Kurzy jsou určeny všem, kteří se chtějí dozvědět více o vypsaných tématech, vyzkoušet si přednášenou látku v praxi, podělit se o zkušenosti s lektory, ale také s ostatními návštěvníky kurzů.

Lektory Akademie CZ.NIC jsou jak zaměstnanci sdružení, tak odborníci z praxe.

Problematika infrastruktury veřejných klíčů (PKI) ,

Kurz získal akreditaci Ministerstva vnitra České republiky č. AK/PV-856/2013 podle ustanovení § 31 odst. 5 zákona č. 312/2002 Sb., o úřednících územních samosprávných celků a o změně některých zákonů.

Kurz seznámí účastníky s principy fungování PKI z různých aspektů. Účastník se seznámí se základními principy asymetrických šifer, s definicemi a požadavky zákona o elektronickém podpisu, bude seznámen s technickým a legislativním pohledem na důvěru v certifikáty a ověření podpisu a certifikátu. **Nově je zařazena** základní **informace o** nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu - **eIDAS**. Součástí budou některé jednoduché praktické dovednosti – zejména práce s certifikáty (generování, export, import, podpis, ověření) a práce s CRL.

Jak se přihlásit

Pro přihlášení do kurzu stačí pouze vyplnit přihlašovací formulář a uhradit kurz. Pokud máte zájem o kurz, který není aktuálně vypsán, napište nám e-mail na akademie@nic.cz a budeme vás informovat o nejbližším termínu konání vybraného kurzu.

Místo konání kurzů

Akademie CZ.NIC

05.06.2014	9:00–17:00	**Brno**
12.06.2014	9:00–17:00	**Praha**

http://www.nic.cz/akademie/contact/

Možnosti slevy

Studenti mají možnost, na základě vložení kopie dokladu o studiu do přihlašovacího formuláře, **získat slevu 90 %** z dané částky kurzu.

F. O čem jsme psali v předchozích 150 číslech…

Kompletní obsah všech **150** dosud vyšlých čísel od roku 1999 je dostupný zde:
http://crypto-world.info/index2.php?vyber=obsah
http://crypto-world.info/obsah/obsah_roky.pdf

Přehled obsahu posledních vydaných čísel

Crypto-World 9-10/2013

Příloha: ukázka z knihy Aplikovaná kryptografie
http://crypto-world.info/casop15/Burda_akryptografie.pdf

Crypto-World 7-8/2013

Crypto-World 1-3/2014

G. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "***Kryptologické sekce Jednoty českých matematiků a fyziků***" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí e-ziny, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály: http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
	Jozef Krajčovič
	Jozef Martin Kollar
	Vlastimil Klíma
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jozef Martin Kollar	jmkollar@math.sk ,	
Jozef Krajčovič	kryptosvet@gmail.com ,	http://katkryptolog.blogspot.sk
Jaroslav Pinkava	jaroslav.pinkava@gmail.com ,	http://crypto-world.info/pinkava/
Pavel Vondruška	pavel.vondruska@crypto-world.info	http://crypto-world.info/vondruska/index.php
Pavel Vondruška, jr.	pavel@crypto-world.info ,	http://www.pavelvondruska.cz/