Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 7, číslo 11/2005 **15. listopad 2005**

11/2005

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.

Starší sešity jsou dostupné na adrese

http://crypto-world.info

(1045 registrovaných odběratelů)

Obsah : str.

A. Soutěž v luštění 2005 – přehled úkolů III. kola (P.Vondruška) 2-7
B. Hardening GNU/Linux, Komplexnější prostředky pro lokální hardening OS Linux, část 3.(J.Kadlec) 8-12
C. Může biometrie sloužit ke kryptografii? (Martin Drahanský, Filip Orság) 13-18
D. Mikulášská kryptobesídka 2005 (D.Cvrček) 19-21
E. Konference IT SECURITY GigaCon (P.Vondruška) 22
F. O čem jsme psali v listopadu 1999-2004 22-23
G. Závěrečné informace 24

A. Soutěž v luštění 2005 - přehled úkolů III. kola!

Pavel Vondruška, (pavel.vondruska@crypto-world.info)

Letošní soutěž v luštění vstoupila do závěrečné etapy 1.11.2005 večer, kdy byly zveřejněny úkoly posledního, třetího kola. Po úlohách prvého kola, které bylo věnováno šifrám/nešifrám (pracovně tak nazýváme šifrové systémy, které nebyly v praxi nikdy použity) a po úlohách druhého kola, kde byly předloženy klasické šifrové systémy, byly v tomto závěrečném kole předloženy šifrové systémy, které se skutečně používaly během prvé a druhé světové války.

V tomto čísle otiskujeme přehled všech soutěžních úloh třetího kola a úplný přehled nápověd, které byly v NEWS k těmto úkolům zveřejněny.

V následujícím čísle 12/2005, které vyjde po skončení soutěže (**soutěž končí 27. listopadu 2005 ve 20.00 hod**.), budou zveřejněny všechny otevřené texty soutěžních úloh, postupy jejich zašifrování / dešifrování, poznámky k luštění a krátké informace od soutěžících, kteří se rozhodnou s ostatními soutěžícími podělit o své zážitky, radosti a strasti z luštění.

V době přípravy tohoto přehledu je již známo obsazení prvních míst letošní soutěže. Všechny úlohy prozatím vyřešilo osm soutěžících. První je dokázal vyřešit loňský vítěz s pseudonymem Misof.

Limit patnácti bodů, který je potřebný pro zařazení do slosování o ceny (http://soutez2005.crypto-world.info/index.php?crypto=ceny) zatím splnilo 50 řešitelů (údaj platný v okamžiku psaní tohoto příspěvku). Losování proběhne 28.11.2005. Vylosovaní řešitelé budou uvedeni na stránce soutěže v sekci aktuality a budou o tom vyrozuměni e-mailem.

Průběžná statistika soutěže (15.11.2005, 10:00)

Celkem soutěžících:	**148**
Počet soutěžících, kteří vyřešili alespoň 1 úlohu:	132
Počet soutěžících, kteří splnili podmínku k zařazení do slosování o ceny:	**50**
Nejvyšší počet dosažených bodů:	75
Počet soutěžících, kteří vyřešili všechny úlohy:	8
Celkem publikovaných úloh:	26
Maximální počet bodů, které lze dosáhnout:	75

Aktuální statistika je k dispozici na stránce soutěže:
http://soutez2005.crypto-world.info/index.php?crypto=statistika

Přehled úkolů - III.kolo
Šifrové systémy prvé a druhé světové války

Nepozdvihne národ proti národu meče a nebudou se více učiti boji. (Bible)

ÚLOHA III/1 – SLOUPCOVÁ TRANSPOZICE (ÚPLNÁ TABULKA)

```
TNKUD BEOSR RTCSC UOSOS SAEJA CVCCT SUTAH NODOS SOAOE
KELIA NISPX NILAV OETOM AASAK UPABU TLNSH SVVEP ALKHT
CEDOA CDVNE SAONR JDYDN UIIOE ERTHT BUIJZ OPJRE ETVUH
YIIII ERANU TLEKE UTMRS ASIZT ACIIX ECSNE TTIRE VLNRA
KUDIM AUAAC YODDE JUOOE IDUKN AIEAN EKPAY EELZE ZIOOZ
KENFT OVAAJ CHAJE IDDNI STIED EZHLP LUBAI RNJSM RUMRV
TLOVV VEAOT EUSSY EETIE VLKTB ITRRI CAAEB OLHOA YEHYM
ITMTZ VOVOC VAUTR IZESZ MPEVU TDPDO TRMEV AEALU TYANO
KOOJA ZTOUC EISCM IZDSE AUNYX OCNSL ZIHCO OOZLO TDEPR
JIADO MZLLZ HDADR AUTID LYKVA JEROI NIPRX SADIH URCYP
DNOIR UEZZY KZZEL EUKKU EHLED NEUSI AKAIC TZAPS KJAPX
AZPLE MDEIS BZRZM IOLEL LEAVC HSJJU NOEUZ KBYJB FEUEU
YDATI ISKEA (550)
```

BODY: 3

ÚLOHA III/2 - PLAY FAIR

```
POEHL HWPKC YMBUQ TTMBU DHPXH MDHBV MHWPH XLARK VPQLR
QPDQL PWKRC RMHSB BVYBE HKROT BVIQM VOPHM FKQUQ NYMPS
ONOVE HWVCR SDCQQ OQLQO BHDXM WWZXS FKHDP IDMHB GREHH
LHEWP KCYMB USGMY NBQBD GYBKH DGQIO ULOKB EHYBU TMYEQ
FLCKO MDTQE CQXIR CFKQH HMGWP CVGHD VPRKR QGKPQ QBDFF
KOTWZ DBAGP WFWPK NTCWP CZVGQ KNUQQ HDMMT RADMV PRKFK
GKQBV HGRIK GRIQO TIQZN DGQLT IGQSH NVWFU QYHMB TUSBU
QBUUQ QIGKV NNQYB WPMDH KMTWV QGNZT DXDDO MCLGC QQOQL
QOBHD XMWNK IKTUF XFCGR IKHKK BNFRK HYMOQ TOMDF CHADE
USIEX HSQCV NTMIU NKIKT UGR (428)
```

BODY: 5

ÚLOHA III/3 - DVOJITÁ TRANSPOZICE (ÚPLNÁ TABULKA)

```
ZAEOM TAGTS IVHOR RZLYL KEDDE MSAJO FMRKL NTIYI GIJLE
LKDKE ZEIKK AAZAN SPBNI EVRKO TSBVR IEPNA OAENC IYVUZ
VTVEE ZOTAE RESSY UDMEV SCJES EKDIK AJAEP FZDIT EAPAI
CYDTP NEIKE VDAIU AAEUC NEHDV AENNR EKNTK MDEIJ ONACD
RIMZA RDECN ORGRN RZOAA PAONN JITRZ EUSOA TRIKO YNENO
```

```
CTPTA ENHIV INANO DTAAI ONSMD KUAAS RVAYI FYIDK LOOHI
OZTAK YLEIH ADOEY EVCKC AECEK AARCV KOSJY AOAEO DVAZR
IAJYC INNEH ESTDY BCISI EZSAV CAHBO EPNZL CLNAO ENVRU
RSTMU IATNA LIONO OMOTT SXKKD TENPY HAITM AASDS NENCU
TYCCV DAARA VVOPI ODPLO SCENA JOREY JEVJI EGOPN TOSVA
YKDGL BCMHT ENOPE ZCBOJ OICYA VRHDB ASOTD EUEYL VIEVS
TRASR RVBIA SHUEV MHASS DECJE INIOO EBORL PZNOT NPHIV
YIANA IBIYZ ARSHV NSTLS UANIK ITVND REAER TESEI RPZAZ
CZNKI JRVTU JNYPI RLYKA COPTA ASRMN ACYLH HOEUA SZAAX
KMIOI EDVSI YOAMH IATAE IRROA CIOIA HCNOD LRTNL OSNXD
DODNI LRLIA OHNRK PARNO AEASV SGAAN INUIB VZNAA PTCZI
OPNAE ALOSY BOJOD LEANA GUCVS RIUOT AMNRE SICKR RHOAE
THMZE SNEAO ADPEU NMNSA SLRIC JD (792)
```

BODY: 4

ÚLOHA III/4 - ÜBCHI

```
ISULA OOLPY LEAYE AMTZU CPAML OEVIO ONBVR DNTOI CROEM
NSUPY ZNOVD NAHTL ESOEH EMZIY SBOKP RSIUE RAHAI EAHAT
UONRO EIEGO PBCTL CIGZT PAMZK ETNLA OODRB VETIV ANILV
ISAOJ RAEZY CARYP LSOOO BATPL EMIIL ZRNDD YOVDK EAEOI
VOREE DTKIQ DCIII SOIUH PDATT VIHMS EUNPN FAKLP OPZNA
EABOA EEZKZ YARIV TRHAS YSVRT EEOWK NMLEU IABMI ZEEJK
JTHTC EERIA KVECN SBIOU AOILW ATAAN OYJPO ELTVZ AAKAN
UEUES TOEIE LZOYD SOYME REEIR PDMNC KVELL ILWTS IPEPV
KRRAK NRPEO SNOLU IVEEI KYENE MDIVA DTBAT DKTAK HMETC
DCOYA NICTX COSOP ABIPV VETDS AECKL PNUOC SSOPO RTOOI
TCZZE ELEOV OOYIN OKUKM OTYRA EEBCR RYSIM OONDP HAEVI
TNVTN NKSOL PMEYR RCONU YEKLC DNDDU IHJEP YNLAL BPVEO
NUEYT KZOME SUOIU VKOOA IHVNS LINJD LLPAI NCCAY NNOMK
VOKAK SVNGR NKNZO SATEA BEEDI OAECR AKADI ASPMD EKPNO
YRNJA NTNOP YENOC IYNJL SENTR LUYND VNVJN SZOEA AIUPI
RSNVO DZDSN LOZRR ANONK (695)
```

BODY: 5

ÚLOHA III/5 - ADFGX

```
AAAFA AADXG AAFFD AAAFG DDFDF ADXDD DAFAG GDAFD ADFGA
DAAAF ADDFA DFFXX ADAFD FGFXA AGGFD DADDX XAFGX GGDAF
XDDDA DAGAA GFDXA DGXDD AXGDA ADDDG ADDFX GDGAD AAGFA
GDDAA GFAAG DGAAG FXAFF XAADD AFXXX FDAAF GXFGX GFDAA
AXDDD FFFXX XAAAD ADFAG AAGAD GGGXF DDFFA AGAFF XADAD
DFADD ADDGX XDDAG FAAFF DXDGD XAAXD FGXXA XXAAD AXDAX
DXFAA FXADD AGDDA AFXXA FAFFD GFDDX DGFAA DAXDA DAGAD
AADAF AFXAD GADFD ADDXD FGAAA GDADD AXXFD AXAXA AFAAX
```

```
DAGDX AAADG DAADD ADAAD FADDD AFDFG ADFXD ADDFD DDFDD
GFDAD DAFDA ADGGA FAGFA XAAXD DDAAD GADDG DFDDA FDADX
ADADX FXDFD DDADD XDADA GFAXD AXDAA XFDDA DFXFD XXFGD
GFDDD AFDDG DXDGF DAAFF DDAAA GADAA DFFDF DFDDG DFDDA
AFXDX GDGDX FDXDF FXFGA AAAXA FFDGA GDXDD DAXAF DAAFX
DXFDD DFAGG GXGFF XDXDD ADGDA GAGGD AXXXD XXDGX DXDDG
ADFXF DDAGD AAGDF XDDDA DDADA FXADD DFDGF DFFDD GDGFA
GAXXA DFAGX DXFDF ADFGF FFXXG AAAXX AFAAX AFGDG XAGAA
DADDG AGAXA AXDGG DDDAG XFGAD AGFGX AGGDF DGADA DDDFD
DFDFA FDDGX FAAFD FDFAD AFDGA ADXDG AAAFA AXAAG DDGAA
GGAGG AXDXA AXAAD AGFGF GADAF AGGGA AAGAD AXDGA AAAAG
XAAXD DFADA ADAGD AADDA XFXAD XDADD DFXXA ADAXA GDAAX
AGGDX AFAAG FFDAF AFADG XGGFA AXDGA AXDXX AGDDX XADDG
AADXA AGGDG FXXDA DADDF AAXXD AAGGD AAADF DGAFF AXDXG
XXDAF DADAG FDAFA GDADD AXAGX GDFAX ADGDF FAGDA FGFGG
ADAAG AAGFG DGAXD FGDAA GADGA DAFFF GADAD ADXAD FAAFG
DGXAF AFDGA GDXDA GXXDD FDDFX FDGDX FDAGA GDDGD AAFFD
DDDDX DFAAX GGDDA DXFAD AGDDG FXDGG AXDAD DDDAX DAFFD
AFDDG FFXGA XXADA DFAGD DDDDA DFAFA FDDFG ADFDD DDDDF
DADXD DDDFF DDFDF GAFXA FAXFD GDDDA FDDFA AGDDD XFFDX
ADFFD DGADF DXAXX AXFDA XGAXA ADDAD FXDXD AADFX (1300)
```

BODY: 5

ÚLOHA III/6 – ENIGMA č.1

```
QRX QTC QTC = ENIGMA STN = NW QTC = CQ
CQ CQ DE CW2005 CW2005 CW2005 = ENIGMA MESSAGE =
0000 317 NUP AYT =

VZFOA UMZTT IDDIQ RVTOS BJWQQ DAWEQ UPMKA CDWHA MFOKV ZYHUF
XNOCC SPSKH VCKOQ DPGQV EGJCP ZMHSY FESPH NYLYL CQPYP UYXQC
KZHTO YADKG LIXCQ EHUYG WUTEJ XKTAI LXPDY CBDXF PMTSQ KWQPT
MLIQT GTJFZ AFTBP SMQLR TJVME JZESN NOKTO VMOSA FUVIA HOIAM
VKQAD UYLAG KDVGB SGOYG LGYYH YFGEH IOGCH VOYGP ZEVQA CDSON
PSMGD RFUSD NZJPT WYNCL MKQKO DDZRJ JWVIC CCOZU QUKAF JJVZE
XIUSX HPJYB JCZWH QV+
= RPT =
VZFOA UMZTT IDDIQ RVTOS BJWQQ DAWEQ UPMKA CDWHA MFOKV ZYHUF
XNOCC SPSKH VCKOQ DPGQV EGJCP ZMHSY FESPH NYLYL CQPYP UYXQC
KZHTO YADKG LIXCQ EHUYG WUTEJ XKTAI LXPDY CBDXF PMTSQ KWQPT
MLIQT GTJFZ AFTBP SMQLR TJVME JZESN NOKTO VMOSA FUVIA HOIAM
VKQAD UYLAG KDVGB SGOYG LGYYH YFGEH IOGCH VOYGP ZEVQA CDSON
PSMGD RFUSD NZJPT WYNCL MKQKO DDZRJ JWVIC CCOZU QUKAF JJVZE
XIUSX HPJYB JCZWH QV+
```

BODY: 4

ÚLOHA III/7 – ENIGMA č.2

```
QRX QTC QTC = ENIGMA STN = NW QTC = CQ
CQ CQ DE CW2005 CW2005 CW2005 = ENIGMA MESSAGE =

0000 420 LUK HAN =

QSGTQ UJIKK IVFZI APIHF WHFXX WKHNA PXWZJ HNAAC VAWZK IIEVV
VKIAS YUQKL IAWQO QJWFM JEOVF HSAHE SYCGH USFFT DQEND QSGDO
LVUFD CFGWM OYBSG JIZYV BXDGT DOLHV TFWZE AYNFG FIMNL ZRZZH
DTVJF TJRAQ ALHQK JJJVP XIILL RHYUR FQKNH XOAVF KIIYX AOOXF
ROPRL NOEQO YSPVD EDIHD TWSRJ TANEB BHCIA MDXRK VJHWJ GQFHM
DPRTB CCQAK ZDUIT ECHOS IXYBT JGKML GBKRN KAQKK PEVIZ OQVFD
AFLEV MQYDY MOONW TZUON UGRKS LUJCD BHKQQ HNIVV WMNOB YEQFO
WOYHL NBRRP YUYMX PSRIZ AJQBZ SNODI CPFVQ WDGFG YELCA ILJJI
ZNRPX XYMWM BVHKL QMJKJ
= RPT =
QSGTQ UJIKK IVFZI APIHF WHFXX WKHNA PXWZJ HNAAC VAWZK IIEVV
VKIAS YUQKL IAWQO QJWFM JEOVF HSAHE SYCGH USFFT DQEND QSGDO
LVUFD CFGWM OYBSG JIZYV BXDGT DOLHV TFWZE AYNFG FIMNL ZRZZH
DTVJF TJRAQ ALHQK JJJVP XIILL RHYUR FQKNH XOAVF KIIYX AOOXF
ROPRL NOEQO YSPVD EDIHD TWSRJ TANEB BHCIA MDXRK VJHWJ GQFHM
DPRTB CCQAK ZDUIT ECHOS IXYBT JGKML GBKRN KAQKK PEVIZ OQVFD
AFLEV MQYDY MOONW TZUON UGRKS LUJCD BHKQQ HNIVV WMNOB YEQFO
WOYHL NBRRP YUYMX PSRIZ AJQBZ SNODI CPFVQ WDGFG YELCA ILJJI
ZNRPX XYMWM BVHKL QMJKJ+
```

BODY: 5

Přehled zveřejněných nápověd k úlohám třetího kola

1. Soutěž 2005 - nápověda k úlohám třetího kola (!)

zveřejněno v NEWS 30.10.2005
http://crypto-world.info/news/index.php?prispevek=2180

Vážení soutěžící,
v nejbližší době budou zveřejněny úlohy třetího a posledního kola naší soutěže.
Nezapomeňte, že celkový vítěz bude ten, kdo nejen vyřeší všechny úlohy, ale vyřeší je jako první!
Informace z tohoto příspěvku je tedy možné využít k přípravě k řešení úloh třetího kola.

a. Přehled systémů, které budete ve třetím kole řešit:
III/1 Sloupcová transpozice (úplná tabulka)
III/2 Playfair
III/3 Dvojitá transpozice (úplná tabulka)
III/4 ÜBCHI
III/5 ADFGX
III/6 ENIGMA
III/7 ENIGMA

b. Popis systémů
Jednoduchá transpozice, Crypto-World 11/2000, str. 2-6
http://crypto-world.info/casop2/crypto11_00.pdf

Popis šifry PlayFair, Crypto-World 3/2005, str. 11-14
http://crypto-world.info/casop7/crypto03_05.pdf

Popis šifry ÜBCHI, http://soutez2005.crypto-world.info/images/UBCHI.pdf

Popis šifry ADFGX, http://soutez2005.crypto-world.info/images/ADFGX.pdf

Dešifrace textu zašifrovaného Enigmou, Crypto-World 78/2005, příloha
http://crypto-world.info/casop7/enigma.pdf

c. Nápověda
Klasické luštění úloh tohoto kola by bylo velmi pracné. Z tohoto důvodu se ve vašem případě bude jednat spíše o řešení / dešifraci. Obdobně jako v úloze II/9. Předložené systémy mají jeden nebo dva klíče. Je možné, že jeden z klíčů (díky řešení předchozích úloh) již znáte a teprve druhý budete muset získat (po tomto zjednodušení) vyluštěním.... V případě, že úloha má jeden klíč, je možné, že jej již také znáte ...
Dále vám prozradím, že úlohy již nepoužívají informace z řešení úkolů prvého kola. Na úkoly prvého kola můžete zcela zapomenout.

2. Soutěž 2005 - nápověda k úlohám č.III/3 a č. III/5

zveřejněno v NEWS 2.11.2005
http://crypto-world.info/news/index.php?prispevek=2204

Zjištění špióna
a) zjistil jsem, že již třem lidem se podařilo vyřešit všechny šifrové depeše !

b) III/3 Dvojitá transpozice (úplná tabulka)
1. klíč : klíč (délky 12 - neznám)
2. klíč : délky jiné než 1. klíč (již znám)

c) III/5 ADFGX
První klíč tzv. substituční určuje obsah převodové tabulky, která má 25 znaků a neobsahuje W.
Permutační klíč: (jeho délka je větší než druhý klíč u III/3 a menší než první klíč u III/3 a již ho také znám)

- - -
V e-zinu 12/2005 budou zveřejněny otevřené texty a popisy ke všem 26-ti letošním soutěžním šifrovým textům.

B. Hardening GNU/Linux, část 3.
Komplexnější prostředky pro lokální hardening OS Linux

Josef Kadlec, student FJFI ČVUT Praha, (josef.kadlec@gmail.com)

Ve třetí a závěrečné části seriálu se budeme zabývat komplexnějšími prostředky pro lokální hardening OS Linuxu.

PAM

Myšlenka modulů PAM (Pluggable Authentication Modules) spočívá v tom, že místo toho, aby určitá aplikace četla soubor s hesly, požádá PAM, aby autorizaci provedl. PAM umožňují komplexnější autorizaci než jednoduché ověření hesla a hlavně celou operaci ověřování uživatele dělají univerzální a aplikace si tyto moduly mohou pouze volat a nemusejí si vytvářet své vlastní ověřovací metody, které by mohly být nekvalitní. Pokud aplikace potřebuje autorizovat uživatele, tak se nejprve snaží najít příslušnou funkci v konfiguračních souborech dané aplikace. Pokud tam žádné nejsou, použije se implicitní konfigurační soubor modulů PAM, kde aplikace dostane instrukce, jak má autorizaci provést. Aplikace se pak dozví, jestli byl uživatel úspěšně autorizován, či nikoliv.

Konfigurační soubory modulů PAM jsou umístěny implicitně v adresáři */etc/pam.d*. Vyhodnocování v těchto souborech probíhá po řádcích - tzn. že na každém řádku probíhá určité kritérium ověřování uživatele. Každý soubor má následující tvar:

module_type control_flag module_path arguments

Module_type může být jedna ze čtyř hodnot. První je hodnota *Auth*, která přikazuje aplikaci, aby vyzvala uživatele k zadání hesla, a uděluje práva uživatelů a skupin. Druhou hodnotou je *Account*, která provádí ověřování na základě jiných vlastností než je heslo a to například čas nebo místo (konsole, apod.). Další hodnotou je *Session*, která určuje, jaká akce se má provést před a po přihlášení uživatele. A poslední modul *Password* umožňuje uživateli změnu hesla.

Control_flag nám umožňuje určit, jak bude naloženo s úspěchem, či neúspěchem autorizace daného modulu. Může nabývat hodnoty *Required*, což znamená, že autorizace musí být provedena úspěšně. Druhou hodnotou je *Requisite*, která je podobná hodnotě *Required* s tím rozdílem, že při neúspěchu se další moduly nevolají a aplikace dostane zprávu o neúspěchu autorizace. Hodí se, pokud chceme ověřit určité faktory ještě před přihlášením uživatele. Další hodnotou je *Sufficient*, která v případě úspěchu a toho, že se v souboru nenacházejí další příznaky *Required* nebo *Sufficient*, vrátí úspěch. Posledním příznakem je *Optional*, který dovoluje i v případě neúspěchu kontrolovat další moduly.

Module_path určuje platnou cestu do adresáře modulu. Kompletní seznam modulů naleznete na URL http://www.kernel.org/pub/linux/libs/pam.

Arguments může u každého modulu nabývat jiných voleb, proto zde uvedu jen ty, které jsou pro všechny společné. Příznak *Debug* zasílá informace o ladění programu do logovacího systému. Volba *no_warn* zajistí, aby se aplikaci nepředala žádná varovná zpráva. *Use_first_pass* zabrání tomu, aby bylo heslo po uživateli požadováno dvakrát. Při volbě *try_first_pass* bude požadováno opětovné zadání hesla pouze v případě, že první heslo vrátí

neúspěch. *Use_mapped_pass* zapříčiní, že se heslo předá z předchozího modulu do aktuálního modulu a použije se k vygenerování například šifrovacího klíče.

Již zmíněným implicitním souborem, který se načte, pokud aplikace neobsahuje svůj konfigurační soubor pro PAM, je */etc/pam.d/other*.

Pokud budeme chtít donutit uživatele, aby zadali bezpečné heslo o minimální délce 8 znaků, provedeme to úpravou souboru */etc/pam.d/passwd*, který by mohl vypadat nějak takto:

```
auth        required    /lib/security/pam_stack.so  service=system-auth
account     required    /lib/security/pam_stack.so  service=system-auth
password    required    /lib/security/pam_cracklib.so  retry=3D3  minlen=8
password    sufficient  /lib/security/pam_unix.so  nullok use_authtok md5 shadow
password    required    /lib/security/pam_deny.so
```

Kromě běžné rutiny je důležitý především třetí řádek, kde je použita PAM knihovna *cracklib* k ověření prolomitelnosti hesla a také minimální délky hesla. Ovšem funguje tu tzv. kreditní systém. To znamená, že délka určená příznakem *minlen* je do jisté míry dynamická. Pokud například použijete v hesle jako jeden ze znaků číslici nebo nealfanumerický znak, zkrátí se vám povinná minimální délka hesla o jeden znak, takže budete moci změnit heslo, i když jeho skutečná délka nebude dosahovat hodnoty určené příznakem *minlen*. Pokud uživatel nezadá správné heslo, nebude mu dovoleno toto heslo změnit. Pro úplnost bych měl ještě dodat, jak bude vypadat soubor */etc/pam.d/system-auth*:

```
auth        required    /lib/security/pam_env.so
auth        sufficient  /lib/security/pam_unix.so  likeauh  nullok
auth        required    /lib/security/pam_deny.so
account     required    /lib/security/pam_unix.so
session     required    /lib/security/pam_limits.so
session     required    /lib/security/pam_unix.so
```

Je nutno upozornit, že superuživatel *root* může být vůči těmto omezením imunní. To, že superuživatel může ledacos přepsat nebo obejít je vlastnost všech operačních systémů unixového typu.

Jsou k dispozici moduly pro autentizační metody jako například LDAP (http://ldap-abook.sourceforge.net/), SecurID (http://www.unc.edu/ais/systems/security/securid.html), Kerberos (http://web.mit.edu/kerberos/www/), atd. PAM nám umožní použít různé autentizační metody pro různé služby, proto se stává velmi účinným autorizačním nástrojem, který lze použít při omezování uživatelů.

chroot

Chroot je zkratka pro "change root" a je tím myšleno to, že kořenový adresář je změněný nebo spíše posunutý. Pomocí této systémové funkce (resp. stejnojmenného příkazu) můžeme vytvořit uzavřené prostředí, ve kterém můžeme nechat běžet nebezpečné aplikace. Výsledek bude takový, že daná aplikace a nebo vetřelec, který se zmocní dané aplikace, uvidí pouze soubory v tomto uzavřeném prostředí (což jsou většinou pouze soubory nutné k chodu dané aplikace) a neohrozí tím celý systém, protože k tomu, aby se dostal do skutečného kořenového adresáře, by musel překonat samotný chroot - je známo několik způsobů, jak toto

udělat. Tímto způsobem nemusíme omezovat jen aplikace, ale i samotné domovské adresáře uživatelů.

K vytvoření chroot prostředí je nutné si nejprve vytvořit adresář, kam zkopírujeme všechny potřebné knihovny a soubory k běhu dané aplikace, přičemž musíme zachovat strukturu adresářů - tzn. že v našem vytvořeném adresáři vytvoříme například adresář */etc*, kam zkopírujeme potřebné soubory, které byly původně v adresáři */etc* skutečného kořenového adresáře. A pak je samozřejmě nutné upravit konfigurační soubory a spouštěcí soubory tak, aby pracovaly s novým prostředím.

Do tohoto prostředí by měly být umisťovány především problematické síťové služby jako například BIND nebo Apache. Uzavření domovského adresáře do prostředí chroot může být značně problematické, protože je potřeba zabránit připojení segmentu sdílené paměti vytvořený mimo chroot, připojení unixového soketu mimo chroot, ovládání a manipulace procesů mimo chroot, zvedání priority procesů v chrootu vzhledem k procesům vně chrootu, atd. Některé z uvedených problémů můžeme řešit pomocí IDS (Intrusion Detection System) jako například grsecurity (http://www.grsecurity.net/) nebo LIDS (http://www.lids.org/).

Omezování pomocí syscallu chroot() není zas až tak běžné, protože konfigurace programů, které se běžně v chroot prostředí nepouštějí, nemusí být vůbec bezproblémová. Druhým problémem je to, že udělat chroot prostředí opravdu bezpečné není zase až tak lehké a v minulosti se našlo pár způsobů, jak se z prostředí chroot vymanit a na těchto chybách bylo založeno například exploitování FTP serveru wu-ftpd v2.4.2-beta18 (exploit využívající tuto chybu - http://www.securityfocus.com/archive/1/12962).

K vytváření chroot prostředí lze také využít nadstavbu a tou je Jail (http://www.jmcresearch.com/projects/jail/).

K zajištění vyšší bezpečnosti se jistě vyplatí nechat některé služby (jako například web server či name server) běžet v chroot prostředí, ale pro akademické sítě bych viděl největší výhodu v tom, že můžeme jednotlivé uživatele uzamknout do tohoto prostředí a tím jim vlastně zabránit v pohybu mimo jejich domovský adresář. Tito uživatelé jsou pak úplně izolováni od samotného systému a to jim brání v získávání informací o tomto systému - takže i v případné nekalé činnosti.

Openwall patch

Zkráceně řečeno, Openwall patche (http://www.openwall.com/linux/) by měly řešit jisté bezpečnostní problémy na úrovni jádra za účelem zvýšení bezpečnosti. Při aplikování záplaty a následné konfiguraci kompilace jádra se volby záplaty Openwall objeví v sekci "Security Options". V nynější době lze tento patch aplikovat na linuxová jádra řady 2.0, 2.2 a 2.4, přičemž aktuální stabilní jádro je již řady 2.6.

Záplata Openwall přidá vlastnosti jako například nespustitelné zásobníky (angl. *non-executable user stack area*), což zabrání spouštění kódu umístěného v zásobníku. Takový kód je většinou vytvářen crackery, kteří zneužívají chybu v přetečení vyrovnávací paměti. Další vlastností je omezení odkazů v adresáři */tmp* - zabraňuje například uživatelům ve vytváření odkazů na soubory, jejichž nejsou vlastníkem a některá další omezení. Dalším omezením v adresáři */tmp/* je zákaz vytváření pojmenovaných rour (angl. *pipes*), které mohou být využity k přesměrování dat mezi uživateli. Dále jsou upravena přístupová práva v */proc* tak, že

uživatelé nevidí procesy jiných uživatelů, pokud nejsou ve speciální skupině (tohoto lze také dosáhnout například pomocí již zmiňovaného grsecurity). Obsahuje i některá další bezpečnostní vylepšení spojená především se správou paměti - například odalokování paměti, která nesměřuje na žádný proces, aj.

Samozřejmě toto vás neochrání na sto procent. Existují exploity, které v jistých situacích dokáží obejít ochrany vytvořené patchem Openwall. Co se týče přetečení haldy (angl. *heap overflow*), není schopen zabránit vůbec - vyhnu se přesnému vysvětlování těchto pojmů, což je součástí nízkoúrovňové bezpečnosti, kterou se tady nezabývám.

Součástí této záplaty je i program *stacktest*, kterým si lze vyzkoušet, zdali je náš systém náchylný k přetečení zásobníku. Po úspěšném aplikování patche Openwall byste měli po spuštění programu dostat hlášku "Segmentation fault" místo "Succeeded.", což značí, že k tomuto útoku náchylní jste.

Do této kapitoly můžeme zařadit i příbuzné projekty jako například Medusa DS9 Security Systems (http://medusa.fornax.sk/), LoMaC (http://opensource.nailabs.com/lomac/), SELinux (http://www.nsa.gov/selinux/), RSBAC (http://www.rsbac.de/) a také mnohem komplexnější programy jako LIDS (http://www.lids.org/), grsecurity (http://www.grsecurity.org/) a další.

Bastille

Původně měla z projektu Bastille (http://www.bastille-linux.org/) vzniknout celá linuxová distribuce, která by měla jako hlavní prioritu vlastní bezpečnost. Ovšem to bylo časově náročnější, než autoři původně zamýšleli a tak radši vytvořili sadu modulů, které tenkrát měly upevnit bezpečnost nově nainstalované distribuce Red Hat. Tato utilita se však nyní dá použít nejen bezprostředně po instalaci, ale kdykoliv. A jsou již podporovány i jiné distribuce než je Red Hat, pro který byl tento program navržen původně. Bastille lze aplikovat na Mandrake, Debian, SuSE nebo operační systémy unixového typu jako HP-UX či Mac OS X.

Tento program se ovládá sérií textových menu. Každé z těchto menu popisuje určitou situaci, kde hrozí potencionální bezpečnostní riziko a program se vás ptá, zdali si přejete tuto situaci zabezpečit. Tato menu se spouští skriptem *InteractiveBastille.pl*. Po projití této konfigurace se nastavení uloží do souboru *BackEnd.pl*. Tento soubor lze pak použít na jiném systému, kde chceme aplikovat stejné bezpečnostní úpravy. Stačí překopírovat starý *BackEnd.pl* a spustit skript *AutomatedBastille.pl*.

Bastille nabízí ochrany jako omezení root-setuid binárních souborů, které bude moci spouštět pouze superuživatel. Dále umožňuje nastavit platnost hesla na 180 dní. Nabídne vám několik možností přísnějších nastavení *umask*. Dále je umožněno omezit přihlašování superuživatele *root* - například ho donutit, aby se nemohl přihlašovat přímo z konzole a musel použít program *su* po přihlášení pod běžným uživatelem. Pomocí omezení práv zamezí používání R* služeb, pokud se na systému nacházejí. Zvláště užitečnou věcí je návrh omezení uživatelů v používání nástroje *cron* pomocí souborů */etc/cron.allow* a */etc/cron.deny*.

Také umožňuje použít heslo v zavaděči systému (pokud máte fyzický přístup k počítači) - toto je záležitost především fyzické bezpečnosti. Pokud by totiž měl útočník přístup k vašemu počítači, mohl by nabootovat jiný operační systém například z CD nebo diskety a tím se dostat k vašim datům. Dalším bezpečnostním prvkem týkajícím se fyzické bezpečnosti je ten, že Bastille umožňuje nadefinovat akci, která se provede po stisknutí kombinace kláves

Ctrl+Alt+Del. Nadefinovat lze také heslo pro jednouživatelský režim. Dále umožňuje konfiguraci TCP wrappers. Bastille vám také pomůže editovat bannery, o kterých sem zde již psal. Dále můžete vypnout *telnet*, zamezit uživatelům používat kompilátor, nastavit zabezpečení subsystémů jako web server, mail server či DNS server a mnohé další.

libsafe

Knihovna libsafe (http://www.research.avayalabs.com/project/libsafe/) ochrání náš systém proti přetečení zásobníku (angl. *buffer overflow*), ale ne na úrovni jádra, jako tomu je v případě záplaty Openwall. Libsafe funguje jako sdílená knihovna. Ještě před spuštěním daného programu se zkontrolují možná přetečení zásobníku ve funkcích jako *strcat(), getwd(), gets(), scanf(), sprintf(), vsprintf(),* atd. Výhoda je jistě v tom, že není potřeba znovu kompilovat kernel.

Podobně funguje i program StackGuard (http://immunix.org/stackguard.html), kterým můžete zkontrolovat kompilovaný kód. Funguje to tak, že StackGuard vloží speciální identifikátor do zásobníku před spuštěním funkce. Po spuštění se zkontroluje integrita tohoto identifikátoru, a pokud byl identifikátor přepsán, proces se ukončí. Nevýhodou však je, že aplikace, které chcete kontrolovat, musíte kompilovat právě pomocí programu StackGuard, k čemuž potřebujete zdrojový kód, který nemusíte mít vždy dostupný.

Seriál nás provedl možnostmi zabezpečení Linuxu na úrovni operačního systému. Vidíme, že i administrátor má prostředky, které může účinně využít v boji proti hrozbám, kterým jsou jím spravované systémy dennodenně vystavovány. Narozdíl od síťové bezpečnosti je u bezpečnosti na úrovni OS potřeba daleko více brát v potaz neúmyslné hrozby, které vycházejí z vlastností operačního systému Linux - omezení uživatelů v používání výpočetních prostředků apod.

V dnešní době si každý pod bezpečností IT představí firewally, VPN a jiné prvky síťové bezpečnosti a bezpečnost samotného operačního systému zaostává v pozadí. Každopádně provázanost obou sfér je tak významná, že bychom ani jednu z nich neměli opomíjet. A co vy, na jaké úrovni je vaše lokální bezpečnost?

Použitá literatura

Josef Kadlec: GNU/Linux a bezpečnost v akademických sítích, bakalářská práce FJFI ČVUT, Praha 2004
Bob Toxen: Bezpečnost v Linuxu, Computer Press, Brno 2003, ISBN 80-7226-716-7
Vicki Stanfield, Roderick W. Smith: Správa operačního systému Linux, SoftPress, Praha 2002, ISBN 80-86497-25-9

C. Může biometrie sloužit ke kryptografii?

Martin Drahanský, drahan@fit.vutbr.cz , http://www.fit.vutbr.cz/~drahan
Filip Orság, orsag@fit.vutbr.cz , http://www.fit.vutbr.cz/~orsag

V tomto článku bychom se rádi pokusili zamyslet nad využitím biometrie ke generování kryptografických klíčů. Vzhledem k tomu, že se tento e-zin věnuje z velké části právě kryptografii, nebudeme opakovat základní pojmy, které každý ze čtenářů jistě zná. V úvodu tohoto článku se zaměříme na biometrii.

Biometrie je dle definice automatizované rozpoznávání osob na základě jejich charakteristických *anatomických rysů* (např. obličej, otisk prstu, duhovka, sítnice) a nebo charakteristického *chování* (např. podpis, chůze, pohyby rtů). Z této definice je patrné, že existují dvě základní biometrické kategorie. Obě kategorie mají jednu věc společnou a to tu, že jejich rozlišovací schopnost musí být natolik vysoká, aby na základě dané vlastnosti mohli být jednoznačně rozlišeni dva jedinci. První kategorie obsahuje takové biometrické vlastnosti, které lze získat z lidského těla a nehraje u nich roli časová složka, tedy jsou stacionární. Naopak ve druhé kategorii se časová složka vyskytuje, jedná se tedy o dynamické biometrické vlastnosti.

Rozhodnutí, kterou biometrickou vlastnost použít v dané konkrétní situaci, není jednoduché. Na prvním místě je třeba promyslet cílovou skupinu, tj. kolik uživatelů by měl být schopen daný biometrický systém rozlišovat. Dále musíme myslet na finanční náklady na daný systém, jeho portabilitu, umístění, míru akceptování uživateli a v neposlední řadě na charakteristiky daného systému (kvalitu), vyjádřené např. pomocí FMR (*False Match Rate*), FNMR (*False Non-Match Rate*), ROC (*Receiver Operating Curve*), případně jinými.

Vraťme se ale k první vlastnosti, kterou jsme uvedli v předchozím odstavci – k cílové skupině, tj. kolik uživatelů má daný systém umět rozlišovat. Ostatní parametry biometrického systému jsou zajímavé pro samotnou praktickou realizaci, ale vzhledem k tématu našeho článku je důležitá rozlišovací schopnost daného biometrického systému. Oč se vlastně jedná? Nechť máme biometrický systém, který má za úkol rozlišit N uživatelů. Minimem pro N jsou jistě 2 uživatelé, což je sice extrémní případ, ovšem k rozlišení těchto uživatelů může posloužit kupř. obvod přes boky. Uvažujeme-li ale opačnou variantu, maximum pro N leží někde kolem 6 miliard, což zhruba odpovídá celé naší populaci. Je zcela zřejmé, že informace o obvodu pasu asi již neposlouží k rozlišení mezi takovým množstvím jedinců, nehledě na to, že je tato vlastnost nestacionární. Musíme se proto orientovat na klasické a již prověřené biometrické vlastnosti. Zde je nutno zdůraznit, že žádná biometrická vlastnost lidí nebyla testována na celé populaci Země a to ze zcela zřejmých důvodů. Tvrzení o jednoznačně silné rozlišovací schopnosti je založeno především na empirických zkušenostech a znalostech, jako je tomu např. u otisků prstů.

S rozlišovací schopností biometrického systému úzce souvisí množství informace, kterou jsme schopni z dané biometrické vlastnosti člověka extrahovat. Uveďme si velmi jednoduchý příklad. Vezmeme-li jako biometrickou vlastnost již zmíněný obvod pasu a definujeme-li, že pas je měřen v centimetrech s přesností na jedno desetinné místo, můžeme se pohybovat v intervalu <0.0;250.0> (klidně přehánějme). Jelikož máme desetinná místa, která mohou nabývat hodnoty od .0 do .9, existuje celkem 250×10=2500 možností. Určitě můžeme ale vyloučit osoby s pasem do 30 *cm* a od 200 *cm*. Máme tedy 170×10=1700 možností. A co to znamená? Pomineme-li chybu měření, může tento systém rozlišit maximálně 1700 osob a to

za podmínky, že každý bude mít jiný obvod pasu, jinak systém selže. Je jasné, že obvod pasu bude nejpravděpodobněji ležet v oblasti <50;100>, což redukuje rozlišovací schopnost na ještě menší počet lidí. Na tomto prostém příkladu vidíme, že je třeba použít takovou biometrickou vlastnost, která má mnohem vyšší rozlišovací schopnost a vylučuje chybné přijetí nesprávné osoby, či zamítnutí správného uživatele.

Podívejme se nyní podrobněji na známé a prakticky prověřené biometrické vlastnosti. Které z nich mají silnou rozlišovací schopnost a které jsou naopak slabé? Mezi biometrické vlastnosti lidí s nejvyšší rozlišovací schopností patří bezesporu tyto (seřazeny sestupně): *DNA*, *otisk prstu*, *duhovka oka*, *sítnice oka*, *termogram obličeje*, *žíly ruky*, *obličej*, *podpis* (statické vlastnosti), *geometrie ruky* a *hlas*. Záměrně pomíjíme naprosto zvláštní typy, jako např. rozpoznávání chůze, pohyby rtů, kód nehtu apod. Takovéto atypické vlastnosti nejsou dobře prozkoumány a o jejich dobré rozlišovací schopnosti jsou stále silné pochybnosti. Jak si jistě pozorný čtenář povšiml, mezi výše uvedenými „vhodnými" vlastnostmi se nachází téměř výhradně charakteristiky statické (anatomické) a až na hlas chybí vlastnosti dynamické. U dynamických vlastností hraje významnou roli ještě jeden faktor – časová složka. Zde je obvyklým problémem velká proměnlivost v čase a tedy neschopnost spolehlivé rozlišitelnosti osob. Výjimkou může být snad právě hlas a snad i dynamika pohybu při psaní, přičemž u druhé nebyl podán žádný důkaz svědčící pro.

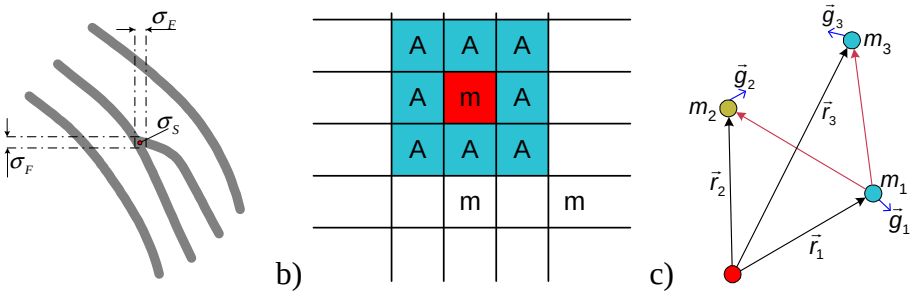
Jelikož se oba autoři tohoto článku zabývají konkrétním typem biometrických vlastností lidí (otisky prstů a hlas), bude tento článek orientován těmito směry. V dalším textu bude popsán rozbor vhodnosti otisku prstu a hlasu ke kryptografickým účelům. Stále jsme si ale ještě nedefinovali, co to vlastně ta „vhodnost" je. V podstatě se jedná o rozlišovací schopnost, tj. kolik informace jsme schopni z dané biometrické vlastnosti extrahovat, abychom jednoznačně rozlišili co největší populaci. U N=2 nám stačí 2^1 kombinací, tedy jeden bit informace. Naopak u N=6.000.000.000 potřebujeme minimálně 2^{33} kombinací, tj. přibližně 5 bytů informace. Vzhledem k mezi- (např. dvojčata) a vnitro-třídním (např. změna mezi dvěma snímky obličeje stejného uživatele – změna výrazu) variacím biometrických vlastností jednotlivých osob je potřeba větší množství informace. Před samotným podrobnějším rozborem dvou již zmíněných biometrických vlastností si uveďme jeden konkrétní příklad. K rozpoznávání duhovky oka je patentován *Daugmanův algoritmus*, který z duhovky extrahuje vždy množinu dat o stejné velikosti. Tato množina obsahuje 2048 bitů, což znamená, že by tato množina měla umět rozlišit až $3{,}23 \cdot 10^{616}$ osob. Představíme-li si takovýto vektor (pořadí prvků hraje roli) jako klíč, můžeme jistě tento klíč použít ke kryptografickým účelům. K symetrické kryptografii sloužit jistě může, neboť v současné době postačují klíče s délkou přes 80 bitů. I pro asymetrickou kryptografii by bylo možné tento klíč použít, vzhledem k tomu, že délky klíčů se pohybují od 1024 bitů. U asymetrické kryptografie je celý problém ale maličko složitější, protože bychom potřebovali vytvořit pár klíčů (soukromý a veřejný), což by asi nebyla nejjednodušší úloha. Vhodnost pro kryptografii založenou na eliptických křivkách nebyla testována.

Ještě před samotným rozborem zmíněných biometrických vlastností je dobré si uvědomit, že se jedná o teoretické odhady využitelné entropie (množství náhodné informace) z biometrických vlastností. Ony mezi- a vnitro-třídní variace redukují ve výsledku skutečné množství entropické informace. Musíme být totiž maličko tolerantnější ke všem údajům z daného biometrického nosiče, abychom zajistili opakovatelnost původního biometrického vektoru (šablony). Pro korekci drobných odchylek v šabloně mohou sloužit *samoopravné kódy* (kupř. Reed-Solomonovy či Fireovy kódy). Jejich vhodnost a především vliv na entropii musí být ještě prozkoumány. Tyto výpočty však přesahují rámec tohoto článku. Navíc

realizace těchto výpočtů by měla být provedena v rámci studie *BioKeys*, kterou v současné době vypisuje BSI (*Bundesamt für Sicherheit in der Informationstechnik*).

Entropie v otisku prstu

U otisku prstu se musíme nejprve zeptat, co činí otisk prstu natolik jednoznačným. Jsou to zvláštnosti papilárních linií. Na povrchu prstů (dlaní a nohou) se u lidí nacházejí zvláštní průběhy kůže, které se vytvářejí již v embryonálním stadiu, a jsou po celý život neměnné. Tyto reliéfy kůže nazýváme papilárními liniemi. Jejich tloušťka se pohybuje v průměru kolem 0,33 *mm* [1]. Papilární linie neprochází ovšem pouze spojitě z jedné strany prstu na druhou, ale jejich průběh je někdy ukončen, či se rozdvojují. Takovéto zvláštnosti v průběhu papilárních linií nazýváme *ukončení linie* a *vidlička* (*rozdvojení*). Obecně tyto zvláštnosti nazýváme *markanty*. Existuje velké množství markantů. V IT (přístupové systémy) se používají pouze dva z nich (ukončení a vidlička). Ostatní nachází uplatnění v kriminalistice, tzv. daktyloskopii, přičemž jsou kombinací těchto dvou základních markantů. Prvním důležitým údajem je *rozlišení papilární linie*, označíme ho $\sigma_F = 0{,}33$ *mm* [1], viz. obrázek 1a). Druhým údajem je rozlišení senzoru, který se používá ke snímání otisku prstu. Na trhu se nachází celkem velké množství senzorů, které mají různá rozlišení. Dle definice daktyloskopů by měl mít senzor rozlišení přibližně 600 *dpi*. Přepočteme-li tuto informaci na reálnou velikost jednoho pixelu, získáme $\sigma_S = 0{,}043$ *mm* [1], což je tedy *rozlišení senzoru* – viz. obrázek 1a).



a) b) c)

Obrázek 1: a) Vidlička v biologickém rozlišení σ_F a redukce rozlišení na σ_S; b) Definice markantu (m) a antimarkantu (A); c) Informace charakterizující markanty

Třetí důležitou informací je *velikost otisku prstu*, resp. jak velkou oblast v obrázku skutečně zabírá samotný otisk prstu. Z měření uvedených v [1] vyplývá, že plocha prstu, která se v průměru nachází v obrázcích otisků prstů, odpovídá rozměrům 10×15 *mm* (šířka × výška).
Postoupíme-li dále, je nutné definovat opak markantu, tzv. *antimarkant*. Podíváme-li se na obrázek 1b), vidíme uprostřed markant *m*. Chceme-li od sebe odlišit dva markanty, musí mezi nimi existovat nějaký předěl, aby nesplynuly dohromady, čímž by došlo k nedetekování ani jednoho z nich. Tento předěl definujeme jako *antimarkant A*, tedy jakýsi minimální předěl mezi dvěma markanty. Rozlišení antimarkantu je stejné jako markantu, tj. $\sigma_F = 0{,}33$ *mm* [1].
Z předešlých údajů můžeme vyjádřit počet mřížek (markantů a antimarkantů) v otisku prstu o rozměrech 10×15 *mm*. Koncentrujme se na rozlišení papilární linie σ_F, protože rozlišení senzoru σ_S je příliš jemné a ve výsledku dojde stejně ke kvantizaci pozic. Počet pozic pro umístění markantů v rozlišení σ_F je $31\sigma_F \times 46\sigma_F$ (odpovídá 10×15 *mm*). Nyní nás zajímá, kolik markantů můžeme maximálně uložit do takovéto mřížky o rozměrech 31×46, přičemž nesmí dojít ke kolizi, tj. uvažujeme jak markanty, tak i antimarkanty. K výpočtu můžeme použít následující vzorec:

$$P_M = \left\lfloor \frac{31+1}{2} \right\rfloor \cdot \left\lfloor \frac{46+1}{2} \right\rfloor = 368 \quad (1)$$

Do otisku prstu o rozměrech 10 × 15 *mm* lze uložit v rozlišení σ_F maximálně 368 markantů (bez kolizí).

Co charakterizuje každý markant? Jsou to následující údaje: *poloha* (*x* a *y* souřadnice), *typ* (ukončení / vidlička) a *gradient* (směr papilární linie). Jednotlivé markanty můžeme popsat pomocí vektorů – takovouto situaci můžeme vidět na obrázku 1c). V tomto obrázku je vidět, že poloha je vyjádřena pomocí pozice v mřížce (rozměr 10 × 15 mm a rozlišení senzoru 600 *dpi* ⇒ 230 × 350 pixelů) a při 230 × 350 pixelech (80.500 pozic) je třeba zakódovat polohu vektoru z počátku pomocí 17 bitů, tedy 2^{17}. Pro *M* markantů můžeme psát:

$$\left(2^{17}\right)^{M-1} \quad (2)$$

Na zakódování typů nám postačí pouze jeden bit, tedy pro *M* markantů to je celkem 2^M. Pro vyjádření gradientů se využívá pouze omezená množina směrů, přičemž krokem je 22,5°. Celkem tedy existuje 16 variant a pro *M* markantů můžeme psát:

$$16^{M-1} = \left(2^4\right)^{M-1} \quad (3)$$

Důvodem, proč je v rovnicích (2) a (3) hodnota $^{M-1}$ je fakt, že markant nejbližší středu otisku prstu je označen jako *referenční markant* [1,2] a z něj vychází celá síť vektorů. U referenčního markantu je uchována pouze informace o jeho typu, ostatní údaje jsou u něj ignorovány.

Na tomto místě můžeme přejít k minimální a maximální entropii, kterou lze získat z otisku prstu, na základě uvedených rovnic. Minimálně musí být v otisku prstu nalezeno 12 markantů (pravidlo 12 markantů pro jednoznačné rozlišení dvou otisků prstů – viz. FBI / BKA nebo [1,2]). Pro *minimální entropii* potom platí:

$$(2^{17})^{12-1} \cdot (2^{12}) \cdot (2^4)^{12-1} = 2^{243} = 1,4135 \cdot 10^{73} \quad (4)$$

Pro výpočet maximální entropie můžeme použít oněch 368 markantů, které jsem spočítali dříve. Pro *maximální entropii* potom platí:

$$(2^{17})^{368-1} \cdot (2^{368}) \cdot (2^4)^{368-1} = 2^{8075} = 6,5647 \cdot 10^{2430} \quad (5)$$

Aplikujeme-li výše zmíněný krok *kvantizace*, tj. redukce pozic v otisku prstu (k zajištění opakovatelnosti), výsledkem je pochopitelně nižší entropie. Pro redukci entropie můžeme použít následující vztah:

$$\sigma_Q = n \cdot \sigma_F, \quad n = 1, 2, ... \quad (6)$$

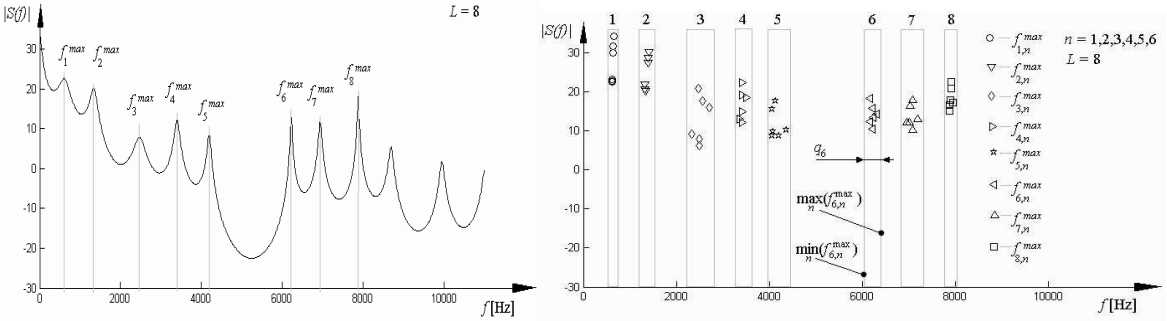
Příklady aplikace kvantizace na množinu markantů je možné nalézt v tabulce 1.

Tabulka 1: Kombinace a entropické faktory pro různé koeficienty kvantizace

Rozlišení $\sigma_Q = n \cdot \sigma_F$	Počet míst ⇒ Počet bitů na zakódování odpovídajících pozic	Počet umístitelných markantů P_M	Maximální entropický faktor pro P_M	Entropický faktor pro P_M = 12
n = 1 (σ_Q = 0,33 *mm*)	30 × 45 = 1350 ⇒ 2^{11}	345	~ 2^{5505}	~ 2^{177}
n = 2 (σ_Q = 0,66 *mm*)	15 × 22 = 330 ⇒ 2^9	88	~ 2^{1219}	~ 2^{155}
n = 3 (σ_Q = 1,00 *mm*)	10 × 15 = 150 ⇒ 2^8	40	~ 2^{508}	~ 2^{144}
n = 5 (σ_Q = 1,66 *mm*)	6 × 9 = 54 ⇒ 2^6	15	~ 2^{155}	~ 2^{122}

Entropie v hlasu

Nalézt hodnotu entropie v hlasu není v žádném případě tak jednoznačné, jak tomu je u otisků prstů. Důvodem pro toto tvrzení je především fakt, že hlas není stacionární, tj. mění se v průběhu času, a proto extrakce informací, které by byly dostatečně robustní a odolné změnám času, není jednoduchou záležitostí. Dalším negativním faktorem je ta skutečnost, že z hlasu lze extrahovat mnoho informací a je těžké stanovit, která z nich je ta pravá. Konkrétní hodnoty entropie lze jen velmi těžko vyjádřit a vždy je potřeba zvolit množinu příznaků, na níž je vyjádření hodnoty entropie závislé.
Zkusme vyjít z nejzákladnějších charakteristik hlasu – takových, kterými poznává i člověk člověka. Jsou to *hlasové frekvence řeči*, které jsou přímo závislé na konfiguraci hlasového traktu. První je *základní tón řeči*, což je hodnota, kterou lze velmi dobře ovlivnit a v praxi je její použití stejně vhodné, jako použití obvodu pasu k rozpoznání jedinců. Její poloha se nalézá v intervalu od 50 Hz do 500 Hz. Kromě základní frekvence lze v řeči nalézt několik dalších významných frekvencí, které se projevují především při vyslovení samohlásek, ale i znělých hlásek. Tyto frekvence se nazývají *formanty* a v češtině jsou významné první dva z nich. Jejich frekvenční rozsah velmi závisí na konfiguraci hlasového traktu odpovídající tomu, co právě říkáme. Podstatně se liší konfigurace hlasového traktu při vyslovení jednotlivých hlásek. První formant leží na frekvencích od 300 Hz do 800 Hz, druhý ca. od 800 Hz do 2300 Hz [5] (hodnoty jsou pouze orientační a mohou se celkem významně lišit u různých jedinců).
Nejvíce zajímavé z hlediska rozpoznávání mluvčích jsou vyšší formanty, protože se téměř nedají ovlivnit a charakterizují *barvu hlasu*, což je informace, která by byla vhodná jako rozpoznávací znak. Nezavrhujme však ani první formanty, protože každý z nás mluví odlišným způsobem a jinak konfiguruje svůj hlasový trakt, což má za následek rozdílné pozice formantů na frekvenční ose. Je zřejmé, že je-li pozice formantů do jisté míry ovlivnitelná, je nutné vycházet z hodnot, které jsou naměřené v delším časovém intervalu, protože okamžité hodnoty mohou být změněny. Dostatečně kvalitní informací se zdá být průběh *dlouhodobého LPC spektra* [4]. V průběhu tohoto spektra lze pozorovat několik maxim (typicky až jedenáct), která se liší u jednotlivých mluvčích a u jednoho mluvčího zůstávají relativně stacionární. Na obrázku 2 lze vidět příklad takového spektra a příklad pozice maxim u několika hlasových vzorků téhož jedince.



Obrázek 2: Vlevo je dlouhodobé LPC spektrum s vyznačením osmi maxim a vpravo jsou pozice jednotlivých maxim extrahovaných z LPC spektra z několika vzorků téhož jedince.

Je zřejmé, že pozice maxim se nachází v určitém intervalu. Musíme brát v úvahu, že je dána *vzorkovací frekvence signálu* a tím i maximální frekvence, kterou z něj můžeme určit. Dále musíme brát v úvahu rozptyl polohy maxim u jediného mluvčího. Pokud bereme toto jako fakt, docházíme k závěru, že musíme polohu maxima určitým způsobem kvantizovat. Ve [3] je ukázán postup kvantizace a postup, kterým bylo stanoveno, že kvantizační krok je určen na základě několika dlouhodobých spekter, čímž je zajištěna jedinečnost. Kromě kvantizačního kroku je také potřeba specifikovat počáteční posun a toleranci. Výsledkem je, že každý

jedinec bude mít jiný kvantizační krok a počáteční posun. Celkový rozsah výsledných hodnot byl omezen na 256 a výsledná hodnota je vypočítávána jako zbytek po dělení touto hodnotou. Použijeme-li osm maxim (což je počet, který má dlouhodobé spektrum většiny mluvčích), můžeme tvrdit, že entropie jednoho vzorku je 2^{64}, neboť k zakódování maxim je potřeba osm hodnot z intervalu 0-255, tedy osm bytů, což odpovídá 64 bitům. Chceme-li využít i absolutní hodnotu daného maxima, musíme brát v potaz několik základních faktů. Absolutní hodnota je silně závislá nejen na síle hlasu, kterou můžeme libovolně měnit, ale i na nastavení mikrofonu a jeho citlivosti! Toto silně omezuje možnosti využití absolutní hodnoty daného maxima. Zobecníme-li uvedený postup a označíme-li počet maxim L, počet bitů/maximum B_L, pak lze entropii vyjádřit jako

$$E = 2^{L \cdot B_L} \qquad (7)$$

Je však nutné si uvědomit, že toto je jen jedna z mnoha možností! Z hlasu lze extrahovat mnohem více informací a je jen otázka času, kdy se podaří nalézt vhodnou kombinaci.

Slovo závěrem

Z předchozích dvou částí můžeme utvořit následující závěry. U otisků prstů (za výše definovaných podmínek) lze použít k výpočtu entropické síly následujícího vzorce:

$$E = \left(2^{N_B}\right)^{P_M - 1} \cdot 2^{P_M} \cdot \left(2^{N_G}\right)^{P_M - 1} \qquad (8)$$

kde P_M je počet nalezených (umístitelných) markantů, N_B je počet pozic v nějakém konkrétním případě (závislý na mřížce pixelů) a N_G je počet gradientů, tj. směrů. Jako interval, ve kterém může ležet teoretická entropie, definujeme: $<2^{243};2^{8075}>$, přičemž se jedná jen o teoretickou hodnotu. V praxi je nutné použít kvantizační krok, příp. samoopravné kódy, které významně redukují celkové množství entropie (viz. tabulka 1). I když redukujeme množství informace i na relativně nízkou úroveň, je bitová délka kolem 150 bitů jistě postačující k použití pro symetrickou kryptografii. Samotný proces generování biometrického klíče z otisku prstu [1] je ovšem mnohem složitější, zejména z důvodu opakovatelnosti a zároveň ponechání dostatečné rozmanitosti, aby od jiného uživatele nemohl být po korekci a toleranci generován stejný klíč.

V případě hlasu je situace mnohem horší. Chceme-li generovat klíč, musí platit, že tento klíč musí být znovu kdykoliv vypočitatelný z nového zvukového záznamu téhož jedince. Pokud tomu tak nebude, nemá smysl hovořit o klíči a jeho extrakci z hlasu. Konkrétní příklad hodnoty entropie udává vzorec (7). Je to jen jedna z mnoha možností jak z hlasu vygenerovat klíč. Otázkou zůstává, do jaké míry je to hodnota vhodná z hlediska opakovatelnosti získání stejných hodnot i v jiném čase. Po mnoha úvahách si troufám říci, že hlas je pro účely generování klíče dosud nevhodný, protože nebyly nalezeny takové informace, které by byly dostatečně stacionární a vědomě neměnné, s časem, psychickým nebo zdravotním stavem jedince.

Použitá literatura

[1] Drahanský, M.: *Biometric Security Systems – Fingerprint Recognition Technology*, disertační práce, FIT VUT, 2005, s. 140

[2] Drahanský, M., Smolík, L.: *Entropic Numbers from the Fingerprint*, BMWA 2004, Londýn, s. 20

[3] Orság, F.: *Biometric Security Systems – Speaker Recognition Technology*, disertační práce, FIT VUT v Brně, s. 109, 2004

[4] Sigmund, M.: *Speaker Recognition - Identifying People by their Voices*, habilitační práce FEE VUT, Brno, 2000, ISBN 80-214-1590-8

[5] Krčmová, M.: *Fonetika a fonologie*, skripta, Filosofická fakulta, MU Brno

D. Mikulášská kryptobesídka 2005

http://www.buslab.org/mkb/

Workshop o kryptologii a informační bezpečnosti se letos uskuteční 1.- 2.12.2005. Místem konání je hotel Olympik v Praze. **Registrace se uzavírá 24.11.2005.** Tentokrát budou součástí programu čtyři zvané příspěvky od skvělých odborníků ve své oblasti:

Luboš Brim – *Automated Formal Verification*
Pracuje na Masarykově univerzitě v Brně, kde se zabývá formální verifikací, logikou, časově kritickými systémy, verifikačními nástroji a distribuovanou verifikací. Na workshopu bude mluvit o automatizované formální verifikaci.

Georgie Danezis – *An Introduction to Traffic Analysis*
Od léta pracuje na univerzitě v Leuvenu. Do té doby se mu ale podařilo ve spolupráci s dalšími skvělými odborníky (Adrei Serjantov, Ross Anderson) dostat oblast analýzy bezpečnosti anonymizačních systémů a útoku na ně na pevné základy založené na teorii informace. Provede nás úvodem do analýzy síťového provozu.

Dieter Gollmann – *Protocol Design: Coming Down from the Cloud*
Asi nemusím představovat. Mnoho z vás jistě zná skvělou knihu "Computer Security", která se velmi brzy dočká druhého rozšířeného vydání. Dieter strávil svůj čas na Royal Holloway, Universities of London, Karlsruhe, Graz, QUT Brisbane a Microsoft Research in Cambridge.

Christian Rechberger, Vincent Rijmen – *Recent results on SHA-1 and SHA-256*
Christian je doktorským studentem u Vincenta Rijmena, se kterým již publikoval několik článků na téma bezpečnosti hašovacích funkcí. Bude mluvit o bezpečnosti funkcí SHA-1 a SHA-256. Jistě zajímavé téma v posledních dvou letech...

Kromě zvaných přednášek vybral programový výbor k prezentaci pět příspěvků, které shledal dostatečně kvalitními pro prezentaci na MKB 2005. Jsou to:

Bypassing personal firewalls under Windows NT or: feel free to fix them on your own (Petr Matoušek)
In this paper the autor will present two widely known generic methods that allow distributed processes to access restricted resources that affect not just Kerio, but other firewall applications as well…

One-Time HNP or Attacks on a Flawed El Gamal Revisited (Tomáš Rosa)
We present a modification of the well-known hidden number problem (HNP)… We Show that carefully designed instances of OT-HNP can be used to break certain flawed implementations of public schemes efficiently…

Využitie zložitosti súborových formátov na vytváranie zmysluplných MD5 kolizií (Ondrej Mikle)
Využívame jednu známu kolíziu poblukovanú Dr. Wangovou na demonštráciu páru samorozbalovacích archívov s rovnakými MD5 hašmi, ktoré ale po rozpakování vygenerujú úplne rozdielne súbory…

Slabiny šifrovacieho algoritmu Puzzle (Martin Stanek, L. Staneková)
V článku analyzujeme nedávno navrhnutý šifrovací algoritmus Puzzle, určený na efektívne šifrovanie videodát v reálnom čase...

Srovnání protokolů pro "Remotely Keyed Encryption" (Petr Švenda)
Protokoly RKE umožňují přenést většinu operací na stranu hostitele a zároveň ponechat šifrovací klíč pouze na čipové kartě. Příspěvek popisuje známé RKE protokoly a provádí jejich funkční a výkonnostní srovnání…

Jestli se vám to ještě pořád nezdá dost, tak dalšími "položkami" v programu budou panelová diskuse, jejíž téma se teď právě dohaduje, aby pro vás bylo co nejzajímavější a vyhlášení výsledků studentské soutěže KEYMAKER.

Předběžný program

1. prosince 2005 (čtvrtek)

U každého příspěvku je min. 5 minut pro dotazy a diskusi k tématu

9:00 – 10:00	*Registrace*
10:00 – 10:10	*zahájení workshopu*
10:10 – 11:10	George Danezis – An Introduction to Traffic Analysis
11:10 – 11:40	Petr Matoušek – Bypassing personal firewalls under Windows NT or: feel free to fix them on your own
11:40 – 12:10	Petr Švenda – Srovnání protokolů pro "Remotely Keyed Encryption"
12:10 – 13:00	KEYMAKER, vyhlášení výsledků – sponzor Grisoft
13:00 – 14:10	*oběd*
14:10 – 14:40	Martin Stanek, L. Staneková – Slabiny šifrovacieho algoritmu Puzzle
14:40 – 15:10	Ondrej Mikle – Využitie zložitosti súborových formátov na vytváranie zmysluplných MD5 kolizií
15:10 – 15:40	*přestávka na kávu*
15:40 – 16:40	Christian Rechberber, Vincent Rijmen – Recent results on SHA-1 and SHA-256
16:40 – 18:10	*panelová diskuse*
18:10 – 18:30	*konec prvního dne*
18:30 –	*večeře*

2. prosince 2005 (pátek)

8:55 – 9:00	*zahájení druhého dne workshopu*
9:00 – 10:00	Dieter Gollmann – Protocol Design: Coming Down from the Cloud
10:00 – 10:30	*přestávka na kávu*
10:30 – 11:00	Tomáš Rosa – One-Time HNP or Attacks on a Flawed El Gamal Revisited
11:00 – 12:00	Luboš Brim – Automated Formal Verification
12:00 – 13:00	*tombola (sponzor Microsoft)*
13:00 –	*závěr workshopu*

Mikulášská kryptobesídka se koná letos popáté. I tentokrát se nám podařilo získat velmi kvalitní přednášející – a to jak pro zvané přednášky, tak i pro přednášky vybrané programovým výborem.
Naším hlavním cílem je vytvořit prostředí pro neformální výměnu informací a nápadů z minulých, současných i budoucích projektů. Doufáme, že nám v tom i letos pomůžete svou účastí!

Srdečně vás zvou všichni členové programového a organizačního výboru.

Mikulášskou kryptobesídku pořádá TNS, a.s. a BUSLab, za podpory

LOOK
LISTEN &
COMMUNICATE

Sponzor tomboly

Microsoft

Sponzor soutěže KEYMAKER

GRISOFT

Mediální partneři

Důležité linky:

web konference	http://www.buslab.org/mkb
upoutávkový leták	http://www.buslab.org/mkb/poster.pdf
web KEYMAKER	http://www.buslab.org/mkb/cfp_keymaker.htm
upoutávkový leták	http://www.buslab.org/mkb/docs/KEYMAKER-poster.pdf
registrace	https://www.buslab.cz/conftool/
předběžný program	http://www.buslab.cz/mkb/program.html

E. Konference IT SECURITY GigaCon

http://www.bin.org.pl/cz/

Srdečně zveme všechny čtenáře Crypto-Worldu na konferenci **IT SECURITY GigaCon Bezpečnost a spolehlivost informačních systémů**, která se bude konat dne 23.listopadu 2005 v hotelu Step v Praze.

Na konferenci je vstup ***zdarma***, podmínkou účasti je pouze ***registrace***.

Konference se zabývá různými aspekty informační bezpečnosti - od kryptologie, přes e-komunikaci až po řešení a technologie, které zajišťují spolehlivost a bezpečnost informačních systémů.

Na účastníky konference čekají (mimo zajímavých přednášek a materiálů konference) i další překvapení. Můžete se např. zúčastnit soutěže o tři libovolná linuxová školení z nabídky společnosti EIITE. Dále deset z vylosovaných účastníků získá knižní odměnu od vydavatelství Zoner Press (bestseller spisovatele Iona Ericksona - Hacking – umění exploitace)...

Pořadatelem soutěže je tým Software-Konferencje
http://www.konferencje.software.com.pl/main/
Oficiální stránka konference: http://www.bin.org.pl/cz/

Mediální partneři konference:
Crypto-World, Computer Press, Zoner Press, Linux+, ePrfofil.cz, Databázový svět

---

F. O čem jsme psali v listopadu 1999 – 2004

Crypto-World 11/1999

A.	Jak je to s bezpečností eliptických kryptosystémů ? (J.Pinkava)	2-4
B.	Známý problém přístupu k zabezpečeným serverům pomocí protokolu https s aplikací Internet Explorer 5 v systému Windows NT 4.0 s aktualizací SP4	4-5
C.	Y2Kcount.exe - Trojský kůň v počítačích	5
D.	Matematické principy informační bezpečnosti (J.Souček)	6
E.	Letem šifrovým světem	6-8
F.	E-mail spojení	8
G.	Trocha zábavy na závěr (malované křížovky)	9

Crypto-World 11/2000

A.	Soutěž ! Část III. - Jednoduchá transpozice	2 - 6
B.	Působnost zákona o elektronickém podpisu a výklad hlavních pojmů - Informace o přednášce	7 - 9
C.	Rozjímání nad ZoEP, zvláště pak nad § 11 (P.Vondruška)	10 - 13
D.	Kryptografie a normy III. (PKCS #5) (J.Pinkava)	14 - 17
E.	Letem šifrovým světem	18 - 19
F.	Závěrečné informace	19

Crypto-World 11/2001

A.	Soutěž 2001, III.část (Asymetrická kryptografie - RSA)	2 - 7
B.	NESSIE, A Status Report (Bart Preneel)	8 -11
C.	Dostupnost informací o ukončení platnosti, zneplatnění a zrušení kvalifikovaného certifikátu (P.Vondruška)	12-16
D.	Odpovědnost a přechod odpovědnosti ve smyslu zákona o elektronickém podpisu (J.Hobza)	17-19
E.	Eliptické křivky a kryptografie (J.Pinkava)	20-22
F.	Mikulášská kryptobesídka (V.Matyáš,Z.Říha)	23
G.	Letem šifrovým světem	24 -25
H.	Závěrečné informace	26

Crypto-World 11/200

A.	Topologie certifikačních autorit (P.Vondruška)	2 - 9
B.	Srovnání výkonnosti hašovacích algoritmů SHA-1, SHA-256, SHA-384 a SHA-512 (M.Kumpošt)	10-16
C.	Informace z aktuálních kryptografických konferencí (J.Pinkava)	
-	Konference ECC2002	17-18
-	Konference CHES 2002	18-20
-	CRYPTO 2002	20-21
D.	The RSA Challenge Numbers	22-23
E.	Letem šifrovým světem	24-25
F.	Závěrečné informace	26

Crypto-World 11/2003

A.	Soutěž 2003 – průběžná zpráva (P.Vondruška)	2
B.	Mikulášská kryptobesídka – Program	3
C.	Cesta kryptologie do nového tisíciletí IV. (Od NESSIE ke kvantovému počítači) (P.Vondruška)	4– 7
D.	Kryptografie a normy. Politika pro vydávání atributových certifikátů, část 2. (J.Pinkava)	8 –11
E.	Archivace elektronických dokumentů (J.Pinkava)	12-16
F.	Unifikace procesů a normy v EU (J.Hrubý)	17-27
G.	Letem šifrovým světem	27-29
H.	Závěrečné informace	30

Crypto-World 11/2004

A.	Soutěž 2004 – úlohy závěrečného kola! (P.Vondruška)	2-4
B.	Jedno-dvoumístná záměna (P.Vondruška)	5-6
C.	Fleissnerova otočná mřížka (P.Vondruška)	7-8
D.	Formáty elektronických podpisů (J.Pinkava)	9-13
E.	Elektronická faktúra a elektronické daňové priznanie aj bez zaručeného elektronického podpisu. (R.Rexa)	14
F.	Nedůvěřujte kryptologům (V.Klíma)	15
G.	O čem jsme psali v listopadu 1999-2003	16
H.	Závěrečné informace	17

Příloha : Cypto-World 11/2004 – speciál (24 stran)

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 P.Vondrušky a 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 sešity GCUCMP, 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
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf

NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška

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/
Jaroslav Pinkava	jaroslav.pinkava@pvt.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/