Crypto-World

Informační sešit GCUCMP

Vychází za podpory společnosti AEC-Data security company

Ročník 4, číslo 1/2002 **15. leden 2002**

1/2002

Připravil : Mgr.Pavel Vondruška

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/
+ http://cryptoworld.certifikuj.cz
(>340 e-mail výtisků)

Obsah : **Str.**

A. Soutěž 2001 (výsledky a řešení)

Pavel Vondruška, ÚOOÚ

Tak jako v loňském roce i letošní soutěž probíhala celkem ve čtyřech kolech. V každém ze sešitů 9/2001 až 12/2001 byla uveřejněna jedna nebo dvě soutěžní úlohy a současně byl uveden doprovodný text. Úlohy byly jednodušší než v roce 2000 a k úspěchu stačilo buď zopakovat postup předvedený v doprovodném textu (úlohy č.5, č.6) a nebo byla k dispozice výrazná nápověda. Osobně je mi líto, že se zúčastnil této soutěže jen malý počet čtenářů. Příprava úloh byla totiž v řadě případů náročnější než samotný proces řešení, a tak připravovat soutěž pro tak malý počet účastníků mi připadlo neadekvátní výsledku. Samotní úspěšní řešitelé hodnotili úlohy jako lehké. Řešitelé, kteří zaslali správné řešení ve stanoveném termínu, byli slosováni a výherce získal malou symbolickou cenu kola. Soutěž byla ukončena 30.12.2001 a z řešitelů, kteří získali nejvíce bodů, byl vylosován celkový vítěz. Hlavní cenu soutěže věnoval jeden z loňských úspěšných řešitelů (František P.), který i letos byl jedním z řešitelů, kteří dosáhli plného bodového zisku. Cena byla velice pěkná - na zakázku vyhotovená dřevěná krabice bulharského vína s šifrovým textem (viz. foto k úloze číslo 4).

Konečný stav

Řešitel	I.kolo 1.úloha	I.kolo 2.úloha	II.kolo 3.úloha	III.kolo 4.úloha	III.kolo 5.úloha	IV.kolo 6.úloha	IV.kolo 7.úloha
František P.	19.09/10	19.09/10	16.10/10	15.11/10	15.11/10	18.12/10	18.12/10
Jan J.	19.09/10	19.09/10	18.10/10	15.11/10	15.11/10	20.12/10	20.12/10
Mirek Š.	30.10/10	30.10/10	30.10/10	19.11/10	19.11/10	29.12/10	29.12/10
Miroslav P.	31.12/10	28.12/10	31.12/10	28.12/10	28.12/10	31.12/10	---
Tomáš V.	21.10/10	26.09/10	---	16.11/10	16.11/10	20.12/10	20.12/10
Vítězslav S.	---	6.11 /10	6.11 /10	19.11/10	19.11/10	1.1./10	1.1./10
Jan Kl.	20.11/10	20.11/10	30.10/10	20.11/10	16.11/10	---	---
Jozef K.	02.10/10	02.10/10	22.11/10	16.11/10	16.11/10	---	---
Karel Š.	10.10/10	10.10/10	31.10/10	20.12/ 8	20.12/ 5	---	---
Martin K.	---	19.11/10	20.11/ 10	19.11/10	19.11/10	---	---
Jan K.	---	30.09/10	21.10/10	---	17.11/10	---	27.12/10
Ivan S.	14.11/10	14.11/10	14.11/10	---	---	---	---
Richard K.	04.10/10	04.10/10	---	---	---	---	---

Způsob určení celkového vítěze:

Po kontrole oprávněnosti zařazení do losování o celkového vítěze soutěže bylo přiděleno pořadové číslo podle data zaslání poslední úlohy. Zaslané číslo od 1 do 100 se přičetlo k číslům, která zaslali ostatní řešitelé. Určení celkového vítěze pak proběhlo takto - označme S celkový součet všech čísel zaslaných úspěšnými řešiteli (jejich počet označme N). Vypočteme $V \equiv S \bmod N$. Hodnota V+1 pak určila celkového vítěze (nabývá hodnot od 1 do N ☺).

Losování o celkového vítěze

(dřevěná kazeta se značkovým vínem)

František P.	49	(18.12)	0	1
Jan J.	23	(20.12)	1	2
Mirek Š.	28	(29.12)	2	3
Součet	100			
(23+28+49)= 1	mod 3			

Vítězové jednotlivých kol

(CD s Crypto-Worldy 9/99-12/2001 a „placený“ certifikát u I.CA)

I.kolo	Tomáš V.
II.kolo	Karel Š.
III.kolo	Miroslav Š.
IV.kolo	František P.

V dalším textu si postupně připomeneme jednotlivé vyhlášené úlohy, uvedeme postup řešení a správný výsledek. Zadání a nápovědu uvádíme ve tvaru tak, jak byla uvedena v jednotlivých číslech Crypto-Worldu, respektive na domácí stránce našeho e-zinu.

I.kolo, úloha číslo jedna - JEDNODUCHÁ ZÁMĚNA

Zadání

Plný počet bodů (10) lze získat za zaslání převodové tabulky (samozřejmě těch znaků , které se v textu vyskytují). Současně prosím o zaslání informace, jak se Vám text podařilo „zlomit“. Pro klasický způsob luštění jednoduché záměny je tento materiál na první pohled trochu krátký… Dost nápovědy. Předpokládám, že pro naše stálé čtenáře bude tento rozehřívací úkol hračkou a že bylo těžší jej připravit, než vyluštit. A tak blahopřeji již předem k zisku prvních bodů.

ŠIFROVÝ TEXT

512	53	84	39	49	45	55	101	64	39	64	614	91	82	47	84
22	84	48	22	45	82	59	55	45	101	82	28	46	101	45	82
22	94	47	42	31	82	49	53	21	49	43	54	56	21	22	91
82	48	84	47	82	56	46	101	58	33	22	21	22	41	82	811
101	54	38	45	49	53	84	32	21	82	55	82	57	21	33	55
58	82	49	43	56	48	31	38	82	28	45	39	510	41	82	512
41	101	41	82	210	45	48	84	124	82	49	43	56	48	31	82
59	101	45	38	46	41	82	82	82	82	82	82	82	82	82	82

Doprovodný text viz Crypto-World 9/2001.

Nápověda 1: „Obecný návod na luštění zašifrovaných zpráv neexistuje. Je nutné pozorně číst, hodně vědět, dívat se, přemýšlet a být připraven … „

Nápověda 2: „Lze řešit jako jednoduchou záměnu (viz. Crypto -World 10/2001), ale úloha má být přece jednoduchá !? Zkuste najít lepší postup a prolistovat např. i další e-ziny 9/2000 až 9/2001.

ŘESENÍ

Tato první úloha měla být jen jakousi vstupní úlohou a nechtěl jsem, aby činila řešitelům potíže. Systém je zadán – jedná se o jednoduchou záměnu. Pokud řešitel uposlechl nápovědy a prolistoval starší e-ziny, jistě si povšiml i krátkého seriálu o záhadné pásce z Prahy.
V čísle 6/2001 je popsáno, jak se podařilo obsah této pásky dešifrovat. Uvedena je zde i příslušná převodová tabulka.

malá písmena				**velká písmena**				**speciální znaky**			
a	5	0	4	**A**	3	0	13	**Mezera**	8	11	2
á	6	0	4	**Á**				**Čárka**	9	0	1
b	2	0	8	**B**	8	0	11	**rozdělení**	9	0	2
c	12	0	4	**C**				**Tečka**	4	0	1
č	13	0	4	**Č**					4	0	4
d	3	0	9	**D**	8	0	14				
ď	3	0	10	**Ď**							
e	8	0	4	**E**	7	0	12				
ě	9	0	4	**Ě**							
é	10	0	4	**É**							
h	3	0	8	**H**							
i	2	0	1	**I**							
í	3	0	1	**Í**							
j	3	0	2	**J**	2	0	9				
k	5	0	5	**K**	2	0	10				
l	10	0	1	**L**							
m	6	0	14	**M**	3	A	0				
n	4	0	8	**N**	5	0	14				
o	4	0	5	**O**							
p	4	0	9	**P**	5	0	12				
q				**Q**							
r	4	0	3	**R**							
ř	5	0	3	**Ř**							
s	3	0	3	**S**							
š	4	0	2	**Š**	4	0	10				
t	2	0	2	**T**							
u	5	0	8	**U**	10	0	14				
v	5	0	6	**V**	10	0	1				
y	4	0	6	**W**	4	A	0				
ý	3	0	6	**Y**							
z	5	0	7	**Z**							
ž	4	0	7	**Ž**							

Právě tuto tabulku jsem využil i při přípravě první úlohy. Použil jsem jen malou modifikaci, která spočívá pouze ve vynechání „prostřední“ číslice (nula nebo A).

Text, který jsem si připravil k převodu do šifrového tvaru, zněl:
Předpokládám, že tento úkol bylo těžší připravit, než vyluštit. Blahopřeji k zisku prvních bodů. P.V. Konec první úlohy.

Převod podle upravené tabulky „záhadná páska z Prahy“:

5-12 5-3 8-4 3-9 4-9 4-5 5-5 10-1 6-4 3-9 6-4 6-14 9-1 8-2 4-7 8-4

```
P  ř  e  d  p  o  k     l  á  d  á  m  ,        ž  e

2-2  8-4  4-8  2-2 4-5   8-2     5-9  5-5  4-5  10-1 8--2     2-8  4-6  10-1 4-5 8-2
T    e    n    t   o           ú    k   o    l             b    y    l    o

2-2  9-4  4-7 4-2  3-1   8-2     4-9  5-3  2-1  4-9  4-3  5-4 5-6  2-1  2-2  9-1  8-2
T    ě    ž   š    í           p    ř    i    p    r    a   v    i    t    ,

4-8  8-4 4-7  8-2   5-6  4-6  10-1  5-8  3-3  2-2  2-1  2-2  4-1   8-2
N    e   ž         v    y    l     u    š    t    i    t    .

8-11 10-1 5-4 3-8    4-5  4-9  5-3  8-4  3-2 2-1  8-2  5-5  8-2  5-7  2-1  3-3  5-5  5-8  8-2
B    l    a   h      o    p    ř    e    j   i         k         z    i    s    k    u


4-9 4-3 5-6 4-8 3-1      3-8    8-2     2-8   4-5  3-9  5-10  4-1 5-12 4-1  10-1 4-1
P   r   v   n   í  (c)  h              b     o    d    ů     .   P    .    V    .

2-10  4-5  4-8  8-4 12-4  8-2  4-9  4-3   5-6   4-8  3-1   8-2  5-9 10-1  4-5  3-8  4-6  4-1
K     o    n    e   c          p    r     v     n    í          ú   l     o    h    y    .
```

Dostaneme:

```
5-12 5-3   8-4  3-9  4-9  4-5  5-5 10-1  6-4  3-9   6-4  6-14  9-1   8-2  4-7   8-4
2-2  8-4   4-8  2-2  4-5  8-2  5-9  5-5   4-5  10-1  8-2  2-8   4-6   10-1 4-5   8-2
2-2  9-4   4-7  4-2  3-1  8-2  4-9  5-3   2-1  4-9   4-3  5-4   5-6   2-1  2-2   9-1
8-2  4-8   8-4  4-7  8-2  5-6  4-6  10-1  5-8  3-3   2-2  2-1   2-2   4-1  8-2   8-11
10-1 5-4   3-8  4-5  4-9  5-3  8-4  3-2   2-1  8-2   5-5  8-2   5-7   2-1  3-3   5-5
5-8  8-2   4-9  4-3  5-6  4-8  3-1  3-8   8-2  2-8   4-5  3-9   5-10  4-1  8-2   5-12
4-1  10-1  4-1  8-2  2-10 4-5  4-8  8-4  12-4  8-2   4-9  4-3   5-6   4-8  3-1   8-2
5-9  10-1  4-5  3-8  4-6  4-1
```

Nyní dále vynecháme pomlčku, která odděluje jednotlivé cifry. Abychom rozlišili kódy např. 5-12 a 51-2, postupujeme takto: v prvém případě zarovnáme číslici 512 do sloupku tak, aby číslice dva přesahovala vpravo, v případě 51-2, bychom zarovnali číslo 512 tak, aby přesahovalo číslo 5 vlevo. Dostaneme tak šifrový text, který byl předložen jako prvá úloha.

Úloha č.1 (jednoduchá záměna)

```
 512  53   84   39   49   45  55  101   64   39   64   614  91   82   47   84
  22  84   48   22   45   82  59   55   45  101   82   28   46  101   45   82
  22  94   47   42   31   82  49   53   21   49   43   54   56   21   22   91
  82  48   84   47   82   56  46  101   58   33   22   21   22   41   82  811
 101  54   38   45   49   53  84   32   21   82   55   82   57   21   33   55
  58  82   49   43   56   48  31   38   82   28   45   39  510   41   82  512
  41 101   41   82  210   45  48   84  124   82   49   43   56   48   31   82
  59 101   45   38   46   41  82   82   82   82   82   82   82   82   82   82
```

Správné řešení:

Předpokládám, že tento úkol bylo těžší připravit, než vyluštit. Blahopřeji k zisku prvních bodů. P.V. Konec první úlohy.

I.kolo, úloha číslo dvě - KÓDOVÁ KNIHA

Zadání

Úlohou druhého kola je zaslat dešifrovaný text kódové zprávy (8 bodů) a zdroj (2 body), kde jste získali příslušnou "kořist" (kódovou knihu).

ŠIFROVÝ TEXT

NA-NIL-IN. HANE-AL-NEH BEH-BIH-KE-AS-CHINIGH A-KHA A-CHIN AH-NAH.
CHE-CHIL-BE-TAH-OLA YIL-DOI BE-LA-SANA TLA-GIN KLIZZIE-YAZZIE LIN
NO-DA-IH AH-JAD DIBEH-YAZZIE HUC-QUO A-WOH TLO-CHIN A-KHA
JAD-HO-LONI A-CHI TSAH WOL-LA-CHEE GLOE-IH BE-LA-SANA NE-AHS-JAH
A-CHIN CHA-GEE MA-E TKIN AH-LOSZ KLESH D-AH NIL-CHI-TSOSIE.
AL-TAH-JE-JAY YAH-DI-ZINI HA-HOL-ZIZ. ATSAH-BESH-LE-GAI A-KEH-DI-GLINI
TLO-CHIN A-CHIN BE AH-LOSZ SHI-DA DIBEH JAD-HO-LONI TSE-NILL.

Doprovodný text k tématu "Kódová kniha" viz. Crypto-World 9/2001.

ŘEŠENÍ

Z doprovodného textu i z nápovědy bylo jasné, že je potřeba získat kódovou knihu, podle které byl kódový text připraven. Přímo v e-zinu 9/2001, kde byla tato úloha uvedena, je v části „Letem šifrovým světem“ i upoutávka o nasazení Navajů za druhé světové války (Code Talkers) a o kódové řeči, kterou tito indiáni pro předávání tajných zpráv používali. Uvedená linka vedla na server root.cz, kde v té době právě vycházel můj třídílný seriál k tomuto tématu. V tomto seriálu byl uveden i odkaz na adresu, kde je možné originální kódovou knihu získat. Seriál „Code Talkers“ také vycházel v našem e-zinu v roce 2000 a to v číslech 4/2000-6/2000. V šestém čísle byla jako příloha přímo kódová kniha Navajů. Další indicie, které měly napovědět, že by mohla být použita kódová řeč Navajů, se daly nalézt v čísle 78/2001, případně v následujícím čísle 10/2001.

Text, který jsem připravil k převodu do kódové řeči, zněl :

CONFIDENTIAL. MESSAGE NUMBER ONE.
MAJOR JACK HULL COME TO OKINAWA ON T H E FIRST OCTOBER.
ATTACK CAN BEGIN. COLONEL VONDRUSKA.

Většina slov není v kódové knize přímo uvedena, a proto je nutné použít kódovací hláskovou abecedu. Převod do kódu pak vypadá takto:

CONFIDENTIAL. MESSAGE NUMBER
NA-NIL-IN. HANE-AL-NEH BEH-BIH-KE-AS-CHINIGH

O N E
A-KHA A-CHIN AH-NAH.

MAJOR J A C K
CHE-CHIL-BE-TAH-OLA YIL-DOI BE-LA-SANA TLA-GIN KLIZZIE-YAZZIE

H U L L COME T O
LIN NO-DA-IH AH-JAD DIBEH-YAZZIE HUC-QUO A-WOH TLO-CHIN

O K I N A W A
A-KHA JAD-HO-LONI A-CHI TSAH WOL-LA-CHEE GLOE-IH BE-LA-SANA

O N T H E
NE-AHS-JAH A-CHIN CHA-GEE

F I R S T OCTOBER .
MA-E TKIN AH-LOSZ KLESH D-AH NIL-CHI-TSOSIE

ATTACK CAN BEGIN .
AL-TAH-JE-JAY YAH-DI-ZINI HA-HOL-ZIZ

COLONEL V O N D
ATSAH-BESH-LE-GAI A-KEH-DI-GLINI TLO-CHIN A-CHIN BE

R U S K A
AH-LOSZ SHI-DA DIBEH JAD-HO-LONI TSE-NILL

Výsledný kódový text, který jsem předložil jako úlohu číslo dvě, je tento:

Úloha č.2

NA-NIL-IN. HANE-AL-NEH BEH-BIH-KE-AS-CHINIGH A-KHA A-CHIN AH-NAH.
CHE-CHIL-BE-TAH-OLA YIL-DOI BE-LA-SANA TLA-GIN KLIZZIE-YAZZIE
LIN NO-DA-IH AH-JAD DIBEH-YAZZIE HUC-QUO A-WOH TLO-CHIN
A-KHA JAD-HO-LONI A-CHI TSAH WOL-LA-CHEE GLOE-IH BE-LA-SANA
NE-AHS-JAH A-CHIN CHA-GEE MA-E TKIN AH-LOSZ KLESH D-AH NIL-CHI-TSOSIE.
AL-TAH-JE-JAY YAH-DI-ZINI HA-HOL-ZIZ. ATSAH-BESH-LE-GAI A-KEH-DI-GLINI
TLO-CHIN A-CHIN BE AH-LOSZ SHI-DA DIBEH JAD-HO-LONI TSE-NILL.

Správné řešení:
CONFIDENTIAL. MESSAGE NUMBER ONE.
MAJOR JACK HULL COME TO OKINAWA ON T H E FIRST OCTOBER.
ATTACK CAN BEGIN. COLONEL VONDRUSKA.

II.kolo, úloha číslo tři - ABSOLUTNĚ BEZPEČNÝ SYSTÉM

Zadání

Třetí úlohou je zaslat dešifrovaný text (Vernamova šifra), způsob skládání otevřeného textu a hesla, použité heslo (10 bodů).

ŠIFROVÝ TEXT

---

81 74 98 02 90 13 06 10 13 26 15 34 33 36 57 34 67 58 72 86 80 75 75

Doprovodný text k tématu "Absolutně bezpečný systém" viz. Crypto-World 10/2001.
Nápověda : Příloha Crypto-World 78/2000.

ŘEŠENÍ

Příloha e-zinu Crypto-World 78/2000, na kterou je v nápovědě odkazováno, obsahuje seznam prvních deseti tisíc prvočísel.

The First 10,000 Primes (the 10,000th is 104,729)
For more information on primes see http://www.utm.edu/research/primes

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229

……

Tento seznam jsem se rozhodl použít jako „zdroj“ hesla pro přípravu třetí úlohy. Text této úlohy jsem zvolil : JAK SE VAM LIBILA TATO ULOHA

Pro převod do číselné podoby jsem použil stejnou tabulku jako ve cvičném případě doprovodného textu Crypto-Worldu 10/2001, tedy:

Převodová (kódová tabulka)

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

O	**J**	**A**	**K**	**S**	**E**	**V**	**A**	**M**	**L**	**I**	**B**	**I**	**L**	**A**	**T**	**A**	**T**	**O**	**U**	**L**	**O**	**H**	**A**
O	74	65	75	83	69	86	65	77	76	73	66	73	76	65	84	65	84	79	85	76	79	72	65

V doprovodném textu jsou uvedeny tři možné metody skládání hesla s otevřeným textem :

I. metoda : Š = O + H (O = Š – H)
II. metoda : Š = O - H (O = Š + H)
III. metoda (tzv. symetrická) : Š = H - O (O = H – Š) .

Pro tuto soutěžní úlohu jsem zvolil metodu skládání I. Šifrový text se získá jako součet otevřeného textu s heslem (modulo 10). Jako heslo jsem použil řetězec získaný z prvočísel uvedených v již citované příloze ke Crypto-Worldu 78/2000. Počátek použitého hesla jsem zvolil prvočíslo 17.

2 3 5 7 11 13 **17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113**

H	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97	10	11	03	10
O	74	65	75	83	69	86	65	77	76	73	66	73	76	65	84	65	84	79	85	76	79	72	65
Š	81	74	98	02	90	13	06	10	13	26	15	34	33	36	57	34	67	58	72	86	80	75	75

Získaný výsledek jsem použil jako zadání pro třetí úlohu.

Úloha č.3

----

81 74 98 02 90 13 06 10 13 26 15 34 33 36 57 34 67 58 72 86 80 75 75

Správné řešení:

JAK SE VAM LIBILA TATO ULOHA

III.kolo, úloha číslo čtyři – neznámý šifrový systém

Zadání

Co je napsáno na obalu ceny pro celkového vítěze?
(10 bodů za úplný text , včetně správné interpretace číslic)
(pozor : 31 12 není datum, kdy se má víno vypít…)

Doprovodný text k obrázku Crypto-World 11/2001.

Nápověda : již staří Římané znali víno….

ŘEŠENÍ

Jedná se o klasickou šifru, někdy nazývanou Caesarovou šifrou. Šifrový text se získá z otevřeného tak, že se vezme následující písmeno – tj. písmeno stojící v abecedě o jedno místo dále vpravo. V případě, že je nutné zašifrovat písmeno Z, se vezme se jako šifra písmeno A.
(Obecný vzorec ST = OT + 1, cyklicky)
Podobný způsob šifrování uplatníme i na číslice. Tedy 2001 zašifrujeme jako 3112.

ST:	AB	WJUFATUWJ	W	LSZQUPMPHJDLF	TPVUFAJ	3112
OT:	ZA	VITEZSTVI	V	KRYPTOLOGICKE	SOUTEZI	2001

Úloha byla lehká a hlavním cílem bylo představit cenu pro celkového vítěze. Jediný problém byla interpretace číslic 31 12. Řada řešitelů se nejdříve domnívala, že se jedná o datum oznámení celkového vítěze apod. (konec soutěže byl vyhlášen na 30.12). Po malé nápovědě, že čísla 3112 vznikla také zašifrováním otevřeného textu, již nikomu z řešitelů úloha problémy nedělala.

Úloha č.4

AB WJUFATUWJ W LSZQUPMPHJDLF TPVUFAJ 3112

Správné řešení:
ZA VITEZSTVI V KRYPTOLOGICKE SOUTEZI 2001

III.kolo, úloha číslo pět – RSA

Zadání

Úloha číslo pět RSA- Klíč pro šifrování (modul, e) = (2479, 101)

VÁŠ ÚKOL

0385 1927 1713 1134 1519 0521 0142 0899 0544 2098 0920 1354 1502 1387 0927

Vaším úkolem je nalézt klíč pro dešifrování (tj. tajný exponent d) - (modul, d)=(2479,?) a dále zaslat dešifrovaný otevřený text (10 bodů za zaslání textu a hodnoty d).

Doprovodný text k tématu "RSA" viz. Crypto-World 11/2001.

Nápověda :

- převodová kódová tabulka je shodná s tabulkou v předchozím cvičném případě

Převodová (kódová tabulka)

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

Formátování je provedeno podle těchto pravidel:
- Má-li modul délku k, budeme zprávu v dekadickém tvaru dělit na skupiny délky k-1.
- Všechny skupiny musí mít délku k-1; nemá-li poslední skupina tuto délku, doplníme ji zprava příslušným počtem nul.
- Výsledek po šifrování má délku rovnou maximálně k; nemá-li ji, doplníme výsledek zleva nulami.

Pokud máte problémy s "velkými čísly" , pak mohu pro pohodlné výpočty nabídnout krátký program **RSAM** (9 kB), který využívá k modulárním výpočtům "Repeated Squaring Method"

ŘEŠENÍ

Postup je dostatečně předveden a procvičen v časopise Crypto-World 11/2001. Stačilo tedy postupovat přesně podle uvedeného návodu.

Zde si dovolím otisknout zaslané řešení jednoho z úspěšných řešitelů :

Kedze modul je maly, da sa pouzit metoda faktorizacie. Z faktorizacnych metod som si ako najjednoduchsiu a najrychlejsiu pre moje ucely zvolil klasicku Fermatovu metodu:

Najprv som si vypocital hornu celociselnu hranicu z hodnoty odmocniny z modulu n=2479, t.j. h=[2479^(1/2)]=50.

V prvom kroku som postupoval podla Fermatovej procedury, ktora je udana nasledovnou podmienkou (symbolika je ako obvykle, druha odmocnina je SQRT a mocnina je ozn. "strieskou" , t.j. '^'.): SQRT(h^2-n) by malo byt cele cislo.
Ak nie je, hodnota h sa inkrementuje, t.j. h=h+1 a vypocet vyrazu opakujeme dotial, pokial nedostaneme cele cislo.

Ak sme dospeli k celociselnemu vysledku a ked ozn. tuto hodnotu pism. a a cislo kroku v procedure ako k, dostavame rovnicu: sqrt((h+(k-1))^2-n)=a.

Z nej upravou ziskame nasledovnu rovnicu pre n: n=(h+(k-1)-a)*(h+(k-1)+a). Co je vlastne n rozlozene na faktory p a q, t.j. n=p*q.

Na nasom konkretnom module to vyzera nasaledovne:

I. sqrt(50^2-2479) = 4,582575694956, co nie je cele cislo,
II. sqrt(51^2-2479) = 11,04536101719, co tiez nevyhovuje,
III. sqrt(52^2-2479) = 15, dostali sme cele cislo, takze mozme upravovat:

n = 2479 = (52+15)*(52-15)=67*37, p=67 a q=37.

Teraz je uz mozne pristupit k vypoctu desifrovacieho exponentu. Eulerova funkcia pre modul je fi(n) = fi(p)*fi(q) (co, mimochodom vyplyva z multiplikativnej vlastnosti tejto funkcie) = (p-1)*(q-1). Pre nase ciselne hodnoty je to: fi(2479)=(67-1)*(37-1)
=2376.
Z podmienky RSA pre sifrovaci a desifrovaci exponent e*d = 1 mod fi(n) vyplyva kongruencia 101*d = 1 mod 2376, ktora sa riesi Euklidovym algoritmom nasledovne:

Rozpiseme si ju podla definicie: 101*d-1=2376*k, kde k je lubovolne cele cislo, z coho upravou 1=101*d+2376*k.
Je to vlastne diofanticka rovnica. Takze teraz uz postupujeme podla algoritmu.

2376 = 101*23+53, 101=53*1+48, 53=48*1+5, 48=5*9+3, 5=3*1+2, 3=2*1+1

Dostali sme zvysok 1, takze dalej postupujeme tak, ze si z posledne rovnosti vyjadrime tento zvysok a postupujeme naspat dosadzovanim jednotlivych medzivysledkov takto:

1=3+2*(-1)=3*2+5*(-1)=48*2+5*(-19)=53*(-19)+48*21=101*21+53*(-40)=2376*(-40)+101*941

Z tohto a z diofantickej rovnice vyplyva k=-40 a to co sme si zelali, nas desifrovaci exponent d=941.

Teraz uz konecne mozeme pristupit vlastnemu odhaleniu zasifrovanej spravy.
Kvoli lahkemu vyrieseniu a pretoze som nemal moznost pristupit k stiahnutiu vasho programu som si pomohol tak, ze som si podla algoritmu RSM (Repeat Squaring Method) zostavil svoj program v QBASIC-u(z dovodu jednoduchosti a rychlosti vyhotovenia implementacie). Nazval som ho podobne RSAM.BAS a je prilohou k tomuto e-mailu.

Jednoduchym desifrovanim podla vztahu M=C^d mod n som postupne dostal tieto cisla:

M: 838 465 767 483 846 983 697 582 989 084 797 679 716 977 920

Podla dohodnutych pravidiel kodovania ciselnych medzivysledkov Crypto #1.0 som previedol 84 na 084. Ziskal som trojmiestne cisla, ktore som nasledne rozdelil do dvojic, a tym som dosiahol moznost nahradit podla prevodovej tabulky tieto dvojmiestne cisla ich zodpovedajucim znakovym ekvivalentom.

M: 83 84 65 76 74 83 84 69 83 69 75 82 89 80 84 79 76 79 71 69 77 92
OT: S T A L J S T E S E K R Y P T O L O G E M !

Lucim sa s prianím pekného dňa
Jozef K. .

```
REM Metoda RSM na vypocet velkych mocnin modulo.
nav:
CLS
k = 1: j = 0: h = 0: ee = 0: n = 0: a$ = ""
DIM z(50)
DEF fnd (x, y) = INT(x / y)
PRINT "Metoda umocnovania velkych cisel"
PRINT "pomocou RSM (Repeat Squaring Method)."
PRINT "--------------------------------------"
PRINT "Autor: Jozef Krajcovic alias EIDO"
PRINT "E-mail: eido@post.sk"
PRINT "--------------------------------------"
INPUT "Zadaj cislo a exponent ?"; a, e
INPUT "Zadaj modul n="; n
LOCATE 12, 10: PRINT "Pocitam, cakaj!!!"
ee = e
DO
z(k) = ee MOD 2
ee = fnd(ee, 2)
k = k + 1
LOOP WHILE ee >= 1
h = 1
FOR j = k - 1 TO 1 STEP -1
t = h * h: b = n: GOSUB nav1: h = c
IF z(j) = 1 THEN t = h * a: b = n: GOSUB nav1: h = c
NEXT
PRINT : PRINT
PRINT "Vysledok "; a; " na "; e; " modulo "; n; " je: "; h
INPUT "Prajes si dalsi vypocet ?"; a$
IF a$ = "a" OR a$ = "A" THEN GOTO nav
END
REM Podprogram MOD
nav1:
c = 0
DO
IF t < b THEN c = t: GOTO nav2
t = t - b
LOOP WHILE t >= b
c = t
nav2:
RETURN
```

Děkuji za perfektně vypracované řešení. Dovolte mi jen malou poznámku k rozkladu čísla 2479 na prvočísla. Čtenář mohl také postupovat jednodušeji tak, že využil tabulku prvočísel, kterou získal již pro řešení úlohy č.3. Stačilo jednoduše dělit číslo 2479 jednotlivými prvočísly… pomocný program RSAM, je přiložen jako příloha ke Crypto-Worldu 11/2001 a lze jej získat downloadem z domovské stránky Crypto-Worldu.

Úloha č.5

Úloha číslo pět RSA- Klíč pro šifrování (modul, e) = (2479, 101)
0385 1927 1713 1134 1519 0521 0142 0899 0544 2098 0920 1354 1502 1387 0927

Vaším úkolem je nalézt klíč pro dešifrování (tj. tajný exponent d) - (modul, d)=(2479,?) a dešifrovat přiložený text.

Správné řešení:
(modul, d)=(2479,941)

dešifrovaný text:
S T A L J S T E S E K R Y P T O L O G E M !

IV.kolo, úloha číslo šest - Elektronický podpis

Zadání

VÁŠ ÚKOL

Vaším úkolem je získat Bobův podpis k tomuto textu M
M=SOUHLASIM S ROZVODEM
Bobův veřejný klíč je (modul, e) = (2479, 101)
(10 bodů za zaslání podpisu pod tento text)

Doprovodný text k tématu "Elektronický podpis" viz. Crypto-World 12/2001.

Nápověda :
- jedná se o schizofrenní úkol, kde chvíli jste útočník a chvíli Bob
- použijte stejnou metodu jako v e-zinu 12/2001, tj. připravte "jiný text", který se zdá náhodný a proto jej Bob podepíše
- z takto podepsaného textu odveďte Bobův podpis pod zprávu M
- převodová kódová tabulka je shodná s tabulkou v předchozím cvičném případě
- formátování použijte podle námi zavedeného standardu Crypto #1.12
- pro výpočet "velkými čísly" lze použít program **RSAM** (9 kB) ("Repeated Squaring Method")

ŘEŠENÍ

Vzhledem k tomu, že celý postup je důkladně probrán v Crypto-Worldu 12/2001, uvedu jen příslušný výpočet:

Text k podpisu = “SOUHLASIM S ROZVODEM“
Modul N = 2479
Veřejný exponent e = 101
Množitel C = 1171 (náhodně zvolené číslo)
C^e = 718

Text k podpisu po převodu (zformátovaný text)
0837 0985 0727 0665 0837 0377 0618 0361 0827 0990 0867 0968 0697 0700

Text po vynásobení (= M*C^e mod N) (zaslepený text)
1048 0715 1396 1502 1048 0475 2462 1382 1305 1826 0277 0904 2167 1842

Výsledek podepsaný Bobem (= $M^d * C \bmod N$) (zaslepený podepsaný text)
1191 0377 1121 0716 1191 2103 2312 0072 0951 0368 0533 0144 2113 0680

Získaný podpis původní zprávy ($M^d \bmod N$, získáno výpočtem se znalosti $M^d * C \bmod N$ a hodnoty C **) (odslepený text)**
2154 1044 0816 1220 2154 0675 0491 2297 1108 0447 1476 2115 0512 1311

Kontrolní výpočet (= $M^d \bmod N$) (přímý podpis Boba původní zprávy)
2154 1044 0816 1220 2154 0675 0491 2297 1108 0447 1476 2115 0512 1311

Závěrem poznamenejme, že zde uvedený postup byl prezentován jako možný útok – postup jak získat podpis pod námi připravený text. V praxi se této vlastnosti dá ovšem s výhodou využít jinak. Mluvíme o zaslepení textu před podepisující se osobou. Lze tak docílit podpisu pod text, se kterým se daná osoba neseznámí. Zaslepený podepsaný text lze potom námi popsanou metodou jednoduše ze znalosti zvolené konstanty C „odslepit“ a získat tak podpis pod text, se kterým se podepisující osoba neseznámila. Této zajímavé možnosti se využívá v některých protokolech především v bankovnictví a obchodu.

Úloha č.6

Vaším úkolem je získat Bobův podpis k tomuto textu M
M=SOUHLASIM S ROZVODEM
Bobův veřejný klíč je (modul, e) = (2479, 101)

Správné řešení:
2154 1044 0816 1220 2154 0675 0491 2297 1108 0447 1476 2115 0512 1311

IV.kolo, úloha číslo sedm – Záchyt (neznámý systém)

Zadání

ŠIFROVÝ TEXT

Poslední úlohou je zjistit obsah zprávy, kterou se vám podařilo zachytit (soubor uloha7.wav) !

(10 bodů za zaslání obsahu zprávy)
Záchyt (wav)

Nápověda:
- ti, kteří vyřešili všechny předchozí úlohy - nápovědu nepotřebují
- ostatní by měli začít řešením úkolů prvního kola ☺

ŘEŠENÍ

Záchyt obsahoval zprávu v kódové řeči Navajů. Bohužel žádnou originální nahrávku jsem nesehnal, a tak jsem ji musel připravit sám. Má „navašská“ výslovnost asi není nejlepší, a tak se tím úloha mohla trochu zkomplikovat. Úloha měla evokovat skutečný postup řešení

nějakého záchytu, kde luštitel nemá k dispozici přesně zachycenou písemnou podobu šifrového textu a musí si poradit s nekvalitní nahrávkou.

K vytvoření textu jsem použil hláskovou, kódovou tabulku podle kódové knihy Navajů. Tuto knihu již ti, co vyřešili druhou úlohu I.kola, měli k dispozici. Nápověda odkazovala na I.kolo, kde byl dostatek stop, které k Navajům jednoznačně vedly.

Text připravený ke kódování zněl:
A MERRY CHRISTMAS AND A HAPPY NEW YEAR

Přepis nahrávky	**Kódová hláska**
BE-LA-SANA	A
TSIN-TLITI	M
AH-JAH	E
GAH	R
DAH-NES-TSA	R
TSAH-AS-ZIH	Y
MOASI	C
CHA	H
GAH	R
TKIN	I
DIBEH	S
D-AH	T
NA-AS-TSO-SI	M
WOL-LA-CHEE	A
KLESH	S
TSE-NILL	A
A-CHIN	N
BE	D
BE-LA-SANA	A
LIN	H
TSE-NILL	A
BI-SO-DIH	P
NE-ZHONI	P
TSAH-AS-ZIH	Y
TSAH	N
AH-JAH	E
GLOE-IH	W
TSAH-AS-ZIH	Y
DZEH	E
WOL-LA-CHEE	A
DAH-NES-TSA	R

Správné řešení poslední úlohy soutěže:
A MERRY CHRISTMAS AND A HAPPY NEW YEAR

B. Santa's Crypto – Mikulášská kryptobesídka

Daniel Cvrček, Vašek Matyáš

Na Mikuláše (přesněji 10.-11. prosince) se v Praze uskutečnila velmi zajímavá akce v oblasti kryptologie. Přibližně osmdesát odborníků se setkalo na prvním ročníku netradičního českého workshopu o kryptologii – Mikulášské kryptobesídce.

Program kryptobesídky byl rozdělen do dvou dnů. První den byl méně formální a jeho náplní byla panelová diskuze na téma *Kryptografie – od standardů k aplikacím*. Diskuzi řídil Vašek Matyáš a dalšími účastníky byli Antonín Beneš, Vladimír Pračke, Fabien Petitcolas (Microsoft Research, UK) a Bart Preneel (KU Leuven, Belgie). Zhruba dvouhodinová diskuze se točila kolem několika témat – množství standardizačních institucí, které se stále zvyšuje, ačkoliv množství odborníků zůstává konstantní, tempo uvádění elektronického podpisu do praxe, jež je daleko za optimistickými předpověďmi a ochrana autorských práv, která nabývá stále zběsilejší podobu hlavně ve Spojených státech.

Druhý den začal vynikající přednáškou na téma NESSIE (nová evropská schémata pro podepisování, integritu a šifrování). Příspěvek přednesl Bart Preneel - osoba, která je jedním z hlavních postav tohoto projektu, který se dostává do poslední třetiny svého života a má před sebou závěrečné hodnocení kryptografických algoritmů. Nemá smysl vyjmenovávat všechny oblasti, na které se během dne dostalo. Co bychom ovšem rádi zmínili, tak je vystoupení Fabiena Petitcolase na téma *Steganografie, watermarking a kryptografie*. Autor je jednou z hlavních postav, které se oblastí steganografie a watermarkingu zabývají. Z českých příspěvků uveďme alespoň Tomáše Rosu a Vlastimila Klímu, kteří mluvili o kryptografických útocích využívajících postranní kanály (informace, které nutně vznikají při jakémkoliv výpočtu a na něž se často zapomíná) a jejichž příspěvek lze nalézt i v tomto Crypto-Worldu.

Den byl zakončen další panelovou diskuzí, jejímž hlavním tématem byl *elektronický podpis a praxe pohledem odborníků*. Během dvou hodin se diskutující dotkli témat, která sahala od právního významu el. podpisu, až po praktickou bezpečnost el. podpisu a možné oblasti jeho používání. Je zajímavé, že nikdo z diskutujících neuvedl *daňové přiznání* mezi prvotními aplikacemi, spíše naopak. Aktéry této diskuze byli Pavel Vondruška (moderátor panelu), ÚOOÚ, Ján Matejka, Ústav státu a práva ČAV, Petr Hanáček z VUT v Brně a Daniel Olejár, UK Bratislava, a Michal Sasínek, NBÚ MV SR, kteří mluvili z pozice předkladatelů a budoucích realizátorů zákona o el. podpisu na Slovensku. Z časových důvodů se ovšem nedostalo na mnoho zajímavých otázek, od důvěryhodnosti současných schémat používání el. podpisů až např. po způsoby vhodné pro vysvětlení funkce a významu el. podpisu normálním uživatelům.

Posledním bodem programu pak byla Mikulášská nadílka – rozdělená spravedlivým losem.

Co říci na závěr, snad jen, že se podařilo naplnit původní záměr – vytvořit komerčně nezávislou akci. Přestože akce se mohla v dané podobě konat především díky pomoci komerčních partnerů - SAP, RSA Security a Eracom Technologies, byl program kryptobesídky prost reklamních událostí a tlaků. Můžeme jen doufat, že se zorganizování podobné akce opět podaří hned na příštího Mikuláše. Nebo už na Velikonoce?

Další informace, program, příspěvky a fotografie z akce je možné nalézt na adrese http://ecom-monitor.cz/kryptobesidka

PS: Na poslední chvíli se nám podařilo ještě získat některé zajímavé statistiky (odevzdáno bylo 46 dotazníků a odpovídalo se 0/1, nebo ve škále 1 až 5 jako ve škole) z akce:

- Spokojenost respondentů s workshopem byla hodnocena 1,5.

- Pětina respondentů se o workshopu dozvěděla na stranách Crypto-Worldu.

- Workshop by se i do budoucna měl konat dva dny (82,61 %) a místa konání mohou být Brno (80,43 %), Praha (76,09 %) a Bratislava (47,83 %).

- Přednášky byly hodnoceny s celkovým průměrem 1,91 a jako tři nejlepší (a v Crypto-Worldu postupně nabídnuté) přednášky byly ohodnoceny:

    1. Vlastimil Klíma, Decros - ICZ; Tomáš Rosa, Decros - ICZ a ČVUT Praha - *O postranních kanálech, nové maskovací funkci a jejím konkrétním použití proti Mangerovu útoku na PKCS#1* (1,26).

    2. Bart Preneel, Katholieke Universiteit Leuven, Belgium - *New European Schemes for Signature, Integrity and Encryption (NESSIE): A Status Report* (1,28).

    3. Fabien Petitcolas, Microsoft Research Cambridge, UK - *Steganography, watermarking and cryptography* (1,42).

- Závěrečný panel moderovaný Pavlem Vondruškou byl dokonce hodnocen průměrem 1,2!

- Nejčastěji navrhovaní zvaní řečníci na příští workshopy jsou: Ross Anderson, Adi Shamir a Bruce Schneier.

- Termín konání dalšího workshopu o Velikonocích se zamlouvá 73,91 % respondentům.

C. O postranních kanálech, nové maskovací technice a jejím konkrétním využití proti Mangerovu útoku na PKCS#1

Vlastimil Klíma (ICZ a.s. , vlastimil.klima@i.cz)
Tomáš Rosa (ICZ a.s., Praha a ČVUT - FEL Praha tomas.rosa@i.cz)

Abstrakt

Tento příspěvek má tři hlavní cíle. Za prvé chceme upozornit na význam tvrzení o individuálních bitech RSA v souvislosti s postranními kanály. Za druhé navrhnout teoretickou konstrukci využívající zvláštní maskovací techniku ke snížení vyzařování informací z postranních kanálů a za třetí ukázat využití této maskovací techniky konkrétně při obraně proti Mangerově útoku na PKCS#1.

1 Úvod

Tři roky poté, co Daniel Bleichenbacher zveřejnil svůj útok ([BLEI98]) na formátovací metodu PKCS#1 verze 1.5, byl Jamesem Mangerem na konferenci Crypto´2001 popsán útok ([MANG01]) na opravenou verzi 2.1, konkrétně na formát, který se označuje jako EME-OAEP a je použit ve schématu RSAES-OAEP (některé zdroje používají označení RSA-OAEP). Dodejme, že tento útok nemá nic společného s kritikou odolnosti OAEP vůči útokům s voleným šifrovým textem, kterým tento formát čelí v obecné rovině, viz práce Victora Shoupa ([SHOU01]).

Tento stav ukazuje, že se v praxi začíná naplňovat důsledek často opomíjeného tvrzení o individuálních bitech RSA, které publikovali Johan Håstad a Mats Näslund na konferenci FOCS v roce 1998 ([HANA98]). Tvrzení o individuálních bitech RSA říká zhruba, že: *Pokud RSA není možné prolomit v náhodném polynomiálním čase, potom není možné předpovídat hodnotu libovolného zvoleného bitu otevřeného textu s pravděpodobností výrazněji odlišnou od hodnoty 1/2*. Prolomením RSA se zde rozumí získání hodnoty otevřeného textu, nikoliv získání hodnoty privátního klíče. V této formulaci se tvrzení o individuálních bitech využívá k ujištění, že jednotlivé bity otevřeného textu jsou chráněny stejně dobře jako celý otevřený text. Zároveň odtud ale plyne, že pokud umíme zvolený bit otevřeného textu predikovat s pravděpodobností výrazně odlišnou od hodnoty 1/2, potom existuje pravděpodobnostní polynomiální způsob vedoucí k luštění celého otevřeného textu!

V současné době se bouřlivě rozvíjí teorie postranních kanálů. Jedná se o studium metod založených na obecném modelu kryptografických modulů, které vedou k získání užitečných informací o výpočtech probíhajících v kryptografických modulech (ucelený přehled této problematiky viz [ROSA01], [MUIR01]). Například se může jednat právě o informaci o individuálních bitech otevřených textů vzniklých odšifrováním vstupních šifrových textů pomocí RSA. Jak se ukazuje, RSA je bez ohledu na použité kódovací schéma (například OAEP) při dostupnosti informace z postranních kanálů snadno náchylné k útokům s voleným šifrovým textem. Konkrétní metoda kódování použitá v napadeném šifrovacím schématu pochopitelně může tyto útoky více či méně ztížit. Jako příklad můžeme použít právě srovnání kódování EME-PKCS1-v1_5 dle PKCS#1 verze 1.5 a kódování EME-OAEP dle PKCS#1 verze 2.1. V prvním případě stačilo znát informaci o tom, zda byl otevřený text správně dekódován. Ve druhém případě již útočník potřebuje znát informaci, která se ze zařízení běžně neodesílá, ale i tak může být vyzářena některým z postranních kanálů.

Následující výklad má tři hlavní cíle. Za prvé chceme upozornit na význam tvrzení o individuálních bitech RSA v souvislosti s postranními kanály. Za druhé navrhnout teoretickou konstrukci využívající zvláštní maskovací techniku ke snížení vyzařování informací z postranních kanálů a za třetí ukázat využití této maskovací techniky konkrétně při obraně proti Mangerově útoku, který využívá postranní informaci o nejvyšším bajtu otevřeného textu.

Předpokládáme, že všechny implementace PKCS#1 by měly projít revizemi, které zjistí použitelnost Mangerova útoku. Při těchto revizích je možné současně také provést některé úpravy, které vyplývají z navrhované maskovací techniky a jsou navrženy konkrétně jako změny v jednotlivých procedurách PKCS#1. V souladu s důsledky tvrzení o individuálních bitech zde poukazujeme i na další možné

útoky na šifrovací schéma RSAES-OAEP, které jsou založeny na získaní postranních informací o jednotlivých bitech otevřeného textu RSA.

Navrhovaná maskovací technika je obecná a má relativně snadný teoretický popis. Obecnost zde znamená, že tato technika by při správném použití měla snižovat vyzařování na všech hrozících postranních kanálech bez ohledu na jejich konkrétní druh. Vlastní metoda vychází z toho, že do kritických operací je zaveden náhodně volený parametr, který neovlivní sémantický význam původní operace. Jeho přítomnost však vnáší do signálu šířeného po postranním kanálu náhodný šum, který snižuje efektivitu přenosu ostatních citlivých informací.

Pro odhad teoretických vlastností této konstrukce využijeme maticový model diskrétního kanálu, který se v teorii postranních kanálů zatím příliš nepoužívá, ačkoliv v teorii informace se jedná o naprosto základní konstrukci. Ukážeme, že navržená maskovací technika se dá chápat jako náhodná volba konkrétního druhu diskrétního kanálu.

Poslední část příspěvku se zabývá návrhem opatření proti Mangerově útoku na schéma RSAES-OAEP. Naším cílem bylo použít co možná nejuniverzálnější protiopatření, která jsou schopna účinně bránit využití několika různých postranních kanálů zároveň. Proto jsme navrhli využití maskovací techniky, jejíž vlastnosti jsme v tomto příspěvku teoreticky podložili. Naším cílem zde není předložit schéma, které prokazatelně odolá všem útokům založeným na postranních kanálech. S ohledem na rychlé tempo rozvoje této oblasti to patrně ani není možné. Naším záměrem je zde prezentovat základní aspekty, kterých by si taková protiopatření měla v obecné rovině všímat zejména. Je pravděpodobné, že při výskytu konkrétních druhů útoků cílených na konkrétní vlastnosti napadeného kryptografického modulu bude nutné doplnit také konkrétní a přesně cílená protiopatření. Námi prezentovaný příspěvek si klade za cíl jednak upozornit na to, že takové útoky mohou přijít (a uvést důvody pro tento předpoklad), jednak doporučit protiopatření obecného druhu, která mohou zpomalit dopad nově vzniklých útoků a tím poskytnout čas na doplnění zmíněných cílených protiopatření.

2 Poznámka o termínu „otevřený text“

V následujícím textu budeme často používat výraz otevřený text ve spojení s různými šifrovacími schématy na bázi RSA. Je důležité uvést, že pod tímto pojmem zde budeme rozumět přímo výsledek odšifrovací transformace RSA. Jedná se tedy o hodnotu m, pro kterou platí $m = c^d \bmod n$, kde c je příslušný šifrový text, d je privátní exponent a n je modul RSA. Většina současných šifrovacích schémat na bázi RSA tuto hodnotu m dále zpracovává operací dekódování (například EME-OAEP-Decode), čímž obdrží vlastní přenášenou zprávu M. I této zprávě se však někdy říká otevřený text, čímž by zde mohlo dojít k nedorozumění. Proto na tuto skutečnost raději ještě jednou upozorňujeme.

3 Vliv tvrzení o individuálních bitech

Tvrzení o individuálních bitech bylo poprvé publikováno v [HANA98]. Dodejme, že před tímto uveřejněním existovala řada tvrzení podobného druhu, která však byla poněkud slabší v tom smyslu, že se netýkala všech jednotlivých bitů (jejich přehled je v [HANA98] uveden). Tvrzení dokázané v [HANA98] již zahrnuje všechny bity otevřeného textu.

Z pohledu teorie postranních kanálů je důležité si uvědomit, že důkaz tvrzení o individuálních bitech obsahuje přímo popis luštícího algoritmu, který jako vstupní podmínku předpokládá přístup k orákulu, které pro vstupní šifrový text poskytuje informaci o jednotlivých bitech otevřeného textu. V případě Mangerova útoku [MANG01] toto orákulum poskytovalo informaci o nulovosti, respektive nenulovosti nejvyššího bajtu otevřeného textu. Bylo ukázáno, že přístup k takovému orákulu umožňuje sestavení velmi efektivního luštícího procesu. Další způsoby využití informace o individuálních bitech najdeme například v [BLEI98] a [STIN95, str. 144-145]. V posledně jmenovaném odkazu se využívá orákulum poskytující informaci o nejvyšším či nejnižším bitu (je ukázáno, že tato dvě orákula jsou polynomiálně převoditelná). Ve srovnání s důkazem tvrzení v práci [HANA98] lze učinit odhad, že mezi jednotlivými bity otevřeného textu existují určité rozdíly v tom,

k jak efektivnímu luštícímu algoritmu jejich znalost (přístup k orákulu, které tuto informaci poskytuje) vede. Toto pozorování je důležité zejména pro kryptoanalýzu, neboť dává návod k tomu, na jaké druhy orákul se má kryptoanalytik zaměřit v první řadě. Pro kryptografa je toto sice také podnětný závěr, neboť ví, na co si má dát určitě pozor, avšak v zásadě to velké ulehčení nepřináší. Z pohledu návrhu kryptoschémat totiž vzhledem k tvrzení [HANA98] musíme zabránit vyzáření jakékoliv informace vedoucí k možnosti úspěšného odhadu jednotlivých bitů otevřeného textu.

4 Odhad dalších možných útoků

V této části ukážeme další možný způsob napadení operace odšifrování ve schématu RSAES-OAEP. Vlastní popis útoku je založen na předpokladu, že existuje postranní kanál, vynášející jistou informaci o otevřeném textu. Konkrétně předpokládáme, že útočník má možnost zjistit Hammingovu váhu (budeme ji značit w(x)) určitého slova x. Náš předpoklad vychází z obecné vlastnosti napěťově-proudových postranních kanálů, které mají jasný sklon tuto informaci poměrně čitelným způsobem vyzařovat, viz [MDS99a]. Z citovaného zdroje jsme si sem dovolili pro ilustraci připojit obrázek 1, na kterém je vidět závislost průběhu signálu z napěťově-proudového postranního kanálu na Hammingově vzdálenosti jistých dvou datových položek (bližší komentář je uveden v odkazovaném článku). V uvedené práci je dále poznamenáno, že obdobně markantní závislost lze pozorovat i v případě Hammingovy váhy zpracovávaných dat. Na základě tohoto poznatku jsme navrhli dále popsaný postup útoku na schéma RSAES-OAEP. Poznamenáváme, že tento útok je možné s jistými obměnami provést i v případě, kdy máme přístup spíše k Hammingově vzdálenosti, než váze.

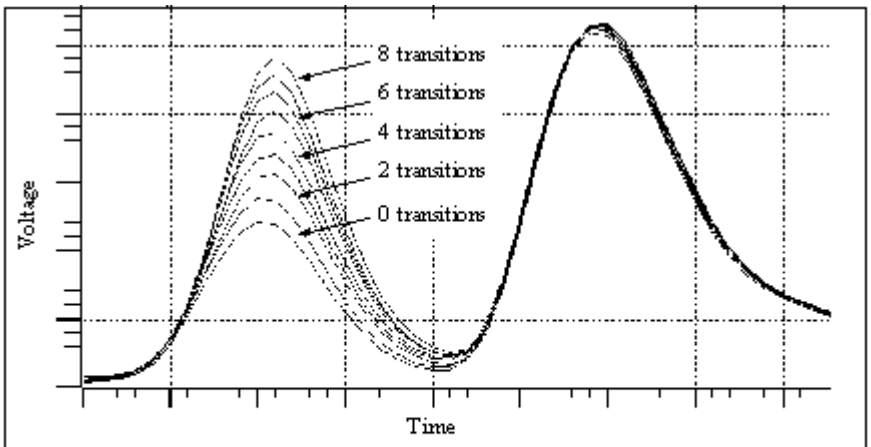


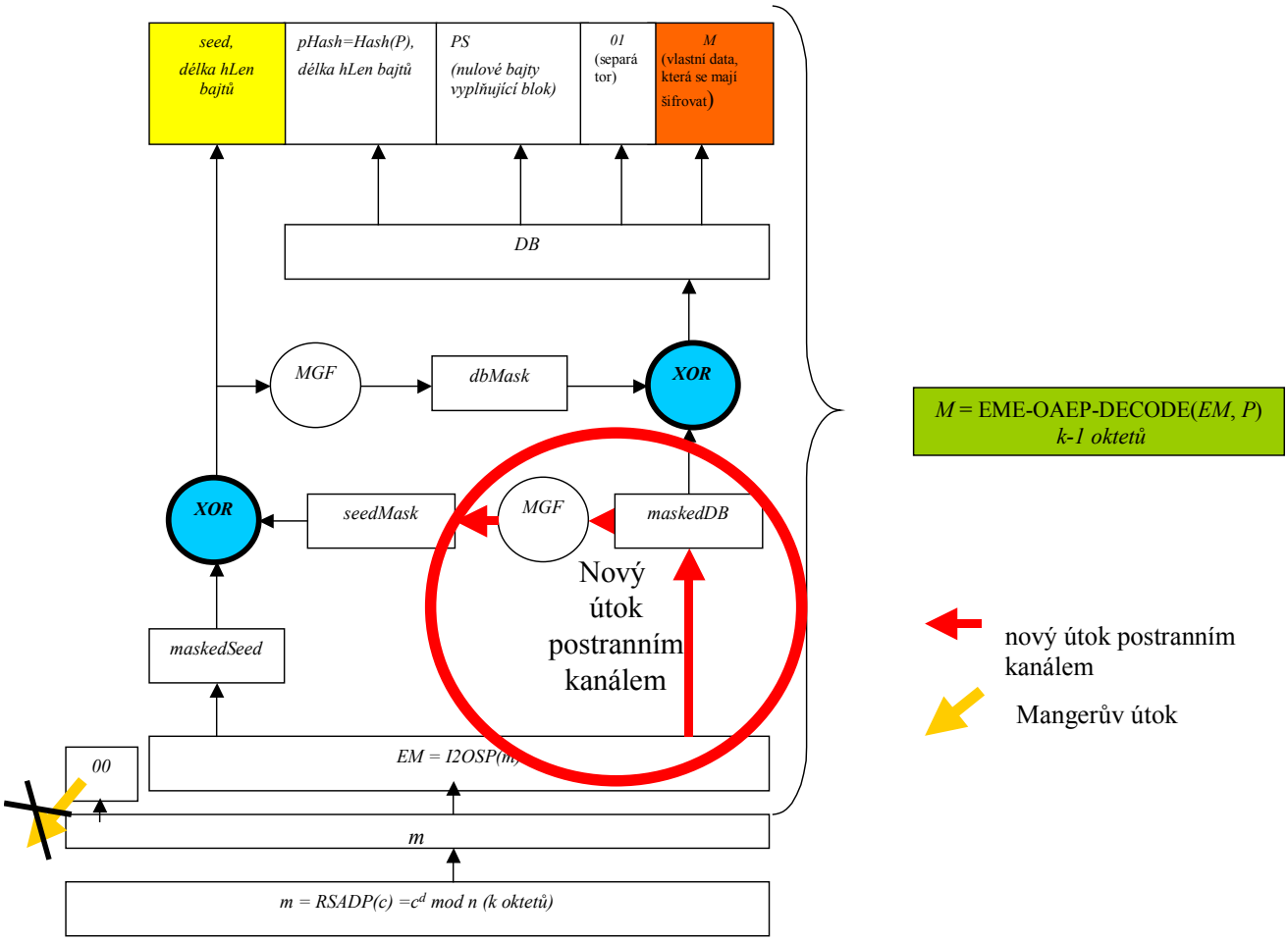
FIGURE 2. Number of Bit Transitions versus Power Consumption
These results show how the data effects the power levels. The nine overlayed waveforms correspond to the power traces of different data being accessed by an LDA instruction. These results were obtained by averaging the power signals across 500 samples in order to reduce the noise content. The difference in voltage between *i* transitions and *i*+1 transitions is about 6.5 mV.

Obrázek 1: Vyzařování informace o Hammingově vzdálenosti (převzato z [MDS99a])

Hledáním konkrétního zařízení s touto vlastností jsme se nezabývali, neboť to nebylo hlavním cílem tohoto příspěvku. Naším cílem je spojit obecně známý poznatek o chování napěťově-proudových postranních kanálů s důsledky tvrzení o individuálních bitech a ukázat tak způsob konstrukce dalšího možného útoku na schéma RSAES-OAEP. Touto konstrukcí chceme zejména podložit konstatování, že šifrovací schéma RSAES-OAEP je z pohledu postranních kanálů poměrně zranitelné. Přinejmenším více, než by se na první pohled zdálo.V tomto směru je třeba chápat Mangerův útok nikoliv jako ojedinělý exces, nýbrž jako první z řady dalších možných napadení tohoto druhu. Poznamenejme ještě jednou, že vliv postranních kanálů nevychází primárně z vlastností kódování EME-OAEP, ale ze základních vlastností RSA jako takového. Stejný dopad a stejné druhy útoků je tak možné očekávat ve všech šifrovacích schématech, která jsou na RSA založena.

4.1 Využití postranního kanálu k útoku na otevřený text, šifrovaný podle EME-OAEP PKCS#1 s využitím SHA-1

Uvažujme šifrování RSA s modulem n o délce N bitů. Protože nejčastěji používaná N jsou násobky 512 bitů, nechť N = 512*k, kde k je 1, 2, 3, ..., tj. vyšetřujeme mj. nejčastěji používané moduly o délkách 512, 1024, 2048 a 4096 bitů. Útok povedeme na schéma RSAES-OAEP ve fázi odšifrování přijatého šifrového textu. Předpokládáme, že jako funkce MGF1 je použita SHA-1 (bližší popis schématu viz [PKCS#1]). Bod, ve kterém útočíme, je znázorněn na obrázku 2.



Obrázek 2: Bod útoku novým způsobem

Při výpočtu seedMask je použita funkce MGF1 podle vzorce seedMask = MGF1(maskedDB, 20) = SHA-1(maskedDB || 00 00 00 00). Konkrétně tento tvar vyplývá z toho, že výsledek MGF1 má být 20 bajtů, tedy SHA-1 se použije jen jednou s nulovým counterem (counter = 00 00 00 00, viz definici MGF1 v [PKCS#1]). Protože používáme moduly n v délkách 512*k bitů (tj. k*64 bajtů), obsahuje maskedDB vždy 64*k - 1 - 20 bajtů a do zpracování SHA-1 jde tedy 64*k - 21 + 4 = 64*k -17 bajtů. Při výpočtu SHA-1(maskedDB || 00 00 00 00) tedy ve vlastní funkci SHA-1 dojde vždy k doplňování vstupní zprávy o 17 bajtů na násobek 64 bajtů tak, aby kompresní funkce SHA-1 mohla pracovat s bloky o délkách 64 bajtů (512 bitů). Posledních 21 bajtů posledního bloku známe, neboť se jedná o 4bajtový counter (00 00 00 00) a 17 bajtový doplněk. Abychom mohli konkrétně vyjádřit doplněk, uvažujme například 1024bitový modul. Potom do SHA-1 vstupuje (107 + 4 =) 111 bajtů, tj. 888 bitů. Máme 888 = 0x00 00 03 78. Doplněk je podle definice SHA-1 roven (bit jedna, nulové bity a posledních 64 bitů na vyjádření původní délky)

80 || 00 00 00 00 || 00 00 00 00 || 00 00 00 00 || 00 00 03 78. Posledních 21 bajtů je tedy rovno

00 || 00 00 00 80 || 00 00 00 00 || 00 00 00 00 || 00 00 00 00 || 00 00 03 78.

Pro potřeby zpracování funkcí SHA-1 je tento poslední blok naplněn do proměnných W_0,..., W_{15}, kde z W_{10} známe poslední bajt a W_{11} až W_{15} známe celé:

W_{10} = ?? ?? ?? 00

W_{11} = 00 00 00 80

W_{12} = 00 00 00 00

W_{13} = 00 00 00 00

W_{14} = 00 00 00 00

W_{15} = 00 00 03 78.

Při rozšiřování na slova W_{16} až W_{79} dále dostáváme

$W_{16} = S^1(W_{13}$ xor $\mathbf{W_8}$ xor W_2 xor $W_{12})$

$W_{17} = S^1(W_{14}$ xor $\mathbf{W_9}$ xor W_3 xor $W_{13})$

$W_{18} = S^1(W_{15}$ xor $\mathbf{W_{10}}$ xor W_4 xor $W_{14})$

atd.

Při výpočtu W_{16} se provádí jako první operace W_{13} xor W_8, přičemž hodnota W_{13} je nám známa. Tento okamžik je právě příkladem obecné situace, kdy do N-ární operace vstupuje N-1 známých parametrů a jeden neznámý. Zde jsou často aplikovatelné různé postranní kanály, zejména napěťově-proudový a pod. Nyní uvedeme předpoklad útoku. Předpokládáme, že v roli útočníka jsme schopni určit bod, kdy dochází k operaci W_{13} xor W_8 a z jejího průběhu jsme schopni odvodit Hammingovu váhu $\mathbf{w(W_8)}$ neznámého operandu W_8. Obdobnou schopnost předpokládáme i u dalších dvou operací, takže jsme schopni zjistit váhy $\mathbf{w(W_9)}$ a $\mathbf{w(W_{10})}$.

Nyní ukážeme, že z tohoto předpokladu jsme schopni předpovídat hodnotu nejnižšího bitu otevřeného textu (odpovídá bitu $W_{10,8}$, kde $\mathbf{W_{10}} = W_{10,31}\ W_{10,30}\ W_{10,29}...\ W_{10,0}$) s pravděpodobností odlišnou od hodnoty 1/2. Odtud podle tvrzení o individuálních bitech lze očekávat možnost nalezení útoku na celý otevřený text. Vzhledem k tomu, že se zabýváme určením poměrně „citlivého“ bitu, můžeme použít i upravený postup uvedený v [STIN95]. Konkrétní rozbor tohoto postupu již přesahuje ilustrační záměr této části celého příspěvku.

Vlastní postup získání netriviální informace o hodnotě $W_{10,8}$ vypadá následovně: Označme si jako c šifrový text, na který útočíme, jako n modul RSA a jako e veřejný exponent RSA. Nejprve necháme napadené zařízení odšifrovat původní šifrový text c. Během této operace vznikne v zařízení otevřený text m a my získáme hodnoty Hammingových vah $A_1 = w(W_{10})$, $B_1 = w(W_9)$ a $C_1 = w(W_8)$. V následujícím kroku požádáme zařízení o odšifrování hodnoty $c' = c*2^{-e} \bmod n$. Přitom vznikne otevřený text m' a my získáme Hammingovy váhy $A_2 = w(W_{10}')$, $B_2 = w(W_9')$ a $C_2 = w(W_8')$. Pokud byl bit $W_{10,8}$ nulový, potom po odšifrování vznikla hodnota $m' = m >> 1$. V opačném případě platí $m' = (m + n) >> 1$. Stanovíme-li si jako předpoklad, že $W_{10,8} = 0$, lze na základě uvedených vztahů pro otevřený text m' odvodit následující tabulku popisující vzájemný vztah hodnot (A_1, B_1, C_1) a (A_2, B_2, C_2). Pokud $W_{10,8} = 0$, potom některý (právě jeden) z těchto řádků popisuje platný vztah mezi uvedenými hodnotami. Toho využijeme tím způsobem, že postupně pro naměřené hodnoty vah zkoušíme, zda některému ze vztahů vyhoví. Pokud ne, potom hypotézu $W_{10,8} = 0$ zamítneme.

V opačném případě ji s určitou chybou (jejíž rozbor přesahuje rámec tohoto příspěvku) přijmeme.

$A_2 = A_1$	$B_2 = B_1$	$C_2 = C_1$
$A_2 = A_1$	$B_2 = B_1$	$C_2 = C_1 + 1$
$A_2 = A_1$	$B_2 = B_1 + 1$	$C_2 = C_1$
$A_2 = A_1$	$B_2 = B_1 + 1$	$C_2 = C_1 - 1$
$A_2 = A_1 + 1$	$B_2 = B_1$	$C_2 = C_1$
$A_2 = A_1 + 1$	$B_2 = B_1$	$C_2 = C_1 - 1$
$A_2 = A_1 + 1$	$B_2 = B_1 - 1$	$C_2 = C_1$
$A_2 = A_1 + 1$	$B_2 = B_1 - 1$	$C_2 = C_1 + 1$

Tabulka 1: Možné vztahy mezi získanými hodnotami vah

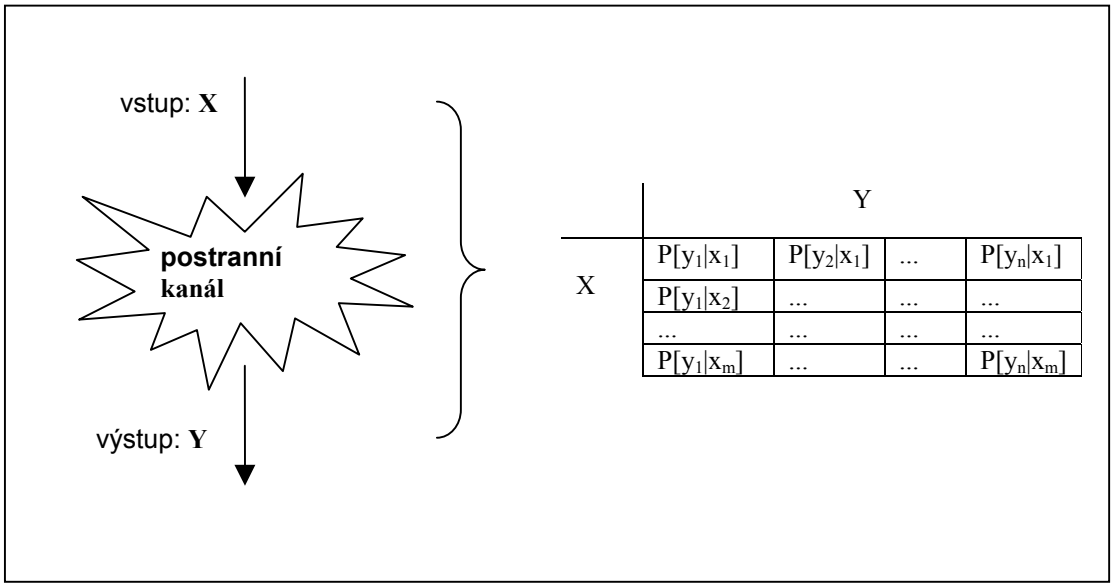
Určení chyby, s jakou s pomocí výše uvedeného postupu získáme hodnotu $W_{10,8}$ zde sice provádět nebudeme, nicméně ukážeme, že získaná informace je určitě netriviální a to v tom smyslu, že nám umožňuje odhadnout hodnotu $W_{10,8}$ s pravděpodobností lepší než 1/2. Označme si $H(W_{10,8} \mid \text{VÁŽENÍ})$ podmíněnou entropii bitu $W_{10,8}$ za předpokladu znalosti výsledku konfrontace získaných vah se vztahy v uvedené tabulce. Přitom VÁŽENÍ $\in$ {platí, neplatí}, kde VÁŽENÍ = platí iff některý z řádků tabulky popisuje platný vztah pro naměřené hodnoty vah. Z rozboru uvedeného postupu plyne, že $H(W_{10,8} \mid \text{VÁŽENÍ} = \text{neplatí}) = 0$, neboť za tohoto předpokladu máme výslednou hodnotu $W_{10,8}$ určenu jednoznačně. Protože $H(W_{10,8} \mid \text{VÁŽENÍ}) = H(W_{10,8} \mid \text{VÁŽENÍ} = \text{neplatí}) * P[\text{VÁŽENÍ} = \text{neplatí}] + H(W_{10,8} \mid \text{VÁŽENÍ} = \text{platí}) * P[\text{VÁŽENÍ} = \text{platí}]$ a $P[\text{VÁŽENÍ} = \text{platí}] < 1$, musí být $H(W_{10,8} \mid \text{VÁŽENÍ}) < 1$. Odtud přímo plyne, že jsme schopni odhadnout hodnotu bitu $W_{10,8}$ s pravděpodobností odlišnou od hodnoty 1/2. Lze tedy očekávat konstrukci úspěšného útoku na celé šifrovací schéma, který má s Mangerovým útokem společné právě jen to, že důsledně využívá zranitelnost RSA přes postranní kanály.

5 Obecná metoda obrany proti postranním kanálům (viz [KLRO01])

Nyní vysvětlíme námi navrhovanou obecnou metodu obrany proti obecným útokům, založeným na postranních kanálech. Poté ji zcela konkrétně aplikujeme na zodolnění formátování šifrovaných zpráv pomocí RSA-OAEP, použité v PKCS#1. Námi navrhovaná metoda je v řadě případů poměrně snadno prakticky implementovatelná, a přitom podle teoretického rozboru poskytuje užitečné obecné výsledky.

Definujme pojem postranního kanálu. *Postranním kanálem* nazýváme každý nežádoucí způsob výměny informací mezi kryptografickým modulem a jeho okolím (podrobněji viz [ROSA01] a série článků o postranních kanálech v [ARCH01]). Z této volné definice vidíme, o jak široké oblasti vlastně hovoříme. Její podání nám však už moc neříká o tom, co si máme pod tímto pojmem představit konkrétně. V kryptoanalýze nám to moc nevadí, neboť zde většinou pracujeme naráz jen s úzce specifickými druhy kanálů, kde se už s jejich přesným popisem nějak dokážeme vypořádat (mnohdy jej ani nepotřebujeme a těžiště leží v popisu metod *analýzy* a *útoku* – o pojmech podrobněji viz výše uvedené odkazy). Jiná situace je však v kryptografii. Zde s ohledem na to, že chceme vytvořit konstrukci odolnou vůči současným i budoucím druhům útoků, potřebujeme nějaký přesnější a zároveň dostatečně obecný model. Pro naše účely si zde představíme obecný model postranního kanálu, analogický k obecnému modelu diskrétního kanálu, který se již řadu let v teorii informace úspěšně používá (viz [HAMM80]).

V rámci našeho modelu si označíme jako X diskrétní náhodnou veličinu značící vstupující informaci a jako Y diskrétní náhodnou veličinu značící informaci vystupující z daného postranního kanálu. U obou veličin předpokládáme konečný obor hodnot, přičemž uvažujeme jen ty hodnoty, kterých tyto veličiny nabývají s nenulovou pravděpodobností. Tento předpoklad můžeme udělat s ohledem na to, že zdrojem veličiny X je v našem případě vždy nějaký počítač, který odpovídá konečnému automatu, a veličina Y je zase vyhodnocována nějakým konečným automatem útočníka. Předesíláme, že tímto modelem postranního kanálu nechceme v tuto chvíli pokrýt kanály založené na kvantové teorii informace.



Obrázek 3: Popis postranního kanálu kanálovou maticí

Vlastní kanál popíšeme maticí, kterou vidíme v pravé části obrázku 3.Tato matice má tvar **SC = (** $P_{i,j}$**)**, kde $P_{i,j} = P[Y = y_j \mid X = x_i]$. Vidíme, že jednotlivé řádky této matice odpovídají příslušným vstupním hodnotám a jednotlivé sloupce zase korespondují s hodnotami výstupu. Konkrétní prvek matice SC (označení od výrazu *Side Channel*) pak odpovídá podmíněné pravděpodobnosti, že na výstupu se objeví hodnota y_j za předpokladu, že na vstupu je hodnota x_i. Matici SC budeme také nazývat *kanálovou maticí*.

Vzhledem k tomu, že pracujeme s pravděpodobnostmi, lze pro prvky kanálové matice poměrně snadno odvodit následující základní vztahy:

$$\Sigma_{(j)} P_{i,j} = \Sigma_{(j)} P[Y = y_j \mid X = x_i] = 1 \qquad (1)$$

$$\Sigma_{(i)} \Sigma_{(j)} P[X = x_i] * P_{i,j} = \Sigma_{(i)} \Sigma_{(j)} P[X = x_i] * P[Y = y_j \mid X = x_i] = 1 \qquad (2)$$

Dále se budeme zabývat určením přenosových vlastností postranního kanálu. K tomuto účelu použijeme konstrukci založenou na vyjádření množství informace o veličině X, která je obsažena ve veličině Y. V anglické literatuře se pro tento pojem používá výraz *vzájemné informace* (*mutual information*), my zde budeme ještě používat termín *informační přenos* (také přenos informace). Tento přenos budeme značit I(X; Y) a definovat jako:

$$I(X; Y) = H(X) - H(X \mid Y) = H(Y) - H(Y \mid X) = I(Y; X) \qquad (3)$$

Výrazem H(X) zde rozumíme entropii veličiny X, H(X | Y) popisuje podmíněnou entropii veličiny X za předpokladu znalosti hodnoty veličiny Y. Stejně chápeme i výrazy H(Y) a H(Y | X).

5.1 O přenosu informace

Pro lepší přehled si výpočet přenosu I(X; Y) naznačíme v jeho významných krocích. Mějme dáno rozdělení vstupní veličiny X jako distribuční funkci P[X = x_i] a matici postranního kanálu **SC** = **(** $P_{i,j}$ **)** typu [m, n]. To znamená, že veličina X může nabývat (s nenulovou pravděpodobností) celkem m různých hodnot, kde každá z nich se může projevit jako n různých hodnot výstupní veličiny Y. Předpokládejme útočníka, který sleduje výstupní veličinu Y. Naším úkolem bude určit, jak velké množství informace o vstupní veličině X takový útočník může získat.

Nejprve si na základě matice SC určíme distribuční funkci veličiny Y jako P[Y = y_j]. Zde můžeme psát:

$$P[Y = y_j] = \sum_{(i)} P_{i,j} * P[X = x_i] \qquad (4)$$

Na základě získané distribuční funkce již snadno určíme entropii H(Y) jako:

$$H(Y) = \sum_{(j)} P[Y = y_j] * log_2(P[Y = y_j]^{-1}) \qquad (5)$$

Zde sčítáme přes všechny nenulové hodnoty distribuční funkce P[Y = y_j]. Dále pokračujeme ve výpočtu podmíněné entropie H(Y | X):

$$H(Y \mid X) = \sum_{(i)} P[X = x_i] * H(Y \mid X = x_i), \qquad (6)$$

$$kde\ H(Y \mid X = x_i) = \sum_{(j)} P_{i,j} * log_2(P_{i,j}^{-1}) \qquad (7)$$

Opět sčítáme přes všechny nenulové hodnoty $P_{i,j}$ a H(Y | X = x_i). Pro snazší pochopení těchto vztahů připomeňme, že $P_{i,j} = P[Y = y_j \mid X = x_i]$. Nyní již zbývá jen dosadit do rovnice (3), kterou použijeme ve tvaru $I(X; Y) = H(Y) - H(Y \mid X)$.

Z uvedeného výpočtu vidíme, že výsledný informační přenos je závislý nejen na vlastnostech kanálu jako takového (ty zachycuje matice SC), ale i na rozdělení vstupní veličiny X. Konkrétně sem tato závislost vstupuje prostřednictvím rovnic (4) a (6).

$SC_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ $SC_2 = \begin{bmatrix} 1/3 & 2/3 \\ 2/3 & 1/3 \end{bmatrix}$ $SC_3 = \begin{bmatrix} 1/3 & 2/3 \\ 1/3 & 2/3 \end{bmatrix}$

	SC_1	**SC_2**	**SC_3**
$P[x_1] = 1/2$ **$P[x_2] = 1/2$** **$H(X) = 1b$**	I(X;Y) = 1 I(X;Y) / H(X) = 1	I(X;Y) = 0.0817 I(X;Y) / H(X) = 0.0817	I(X;Y) = 0 I(X;Y) / H(X) = 0
$P[x_1] = 1/3$ **$P[x_2] = 2/3$** **$H(X) = 0.9183b$**	I(X;Y) = 0.9183 I(X;Y) / H(X) = 1	I(X;Y) = 0.0728 I(X;Y) / H(X) = 0.0793	I(X;Y) = 0 I(X;Y) / H(X) = 0
$P[x_1] = 1/10$ **$P[x_2] = 9/10$** **$H(X) = 0.469b$**	I(X;Y) = 0.469 I(X;Y) / H(X) = 1	I(X;Y) = 0.0298 I(X;Y) / H(X) = 0.0635	I(X;Y) = 0 I(X;Y) / H(X) = 0

Obrázek 4: Příklady výpočtu informačního přenosu

Pro lepší názornost jsou na obrázku 4 uvedeny kanálové matice pro tři konkrétní postranní kanály. Všechny jsou typu [2, 2], takže předpokládáme vstupní a výstupní veličiny nabývající nejvýše dvou různých hodnot. Připojená tabulka uvádí informační přenosy jednotlivých kanálů v závislosti na rozdělení vstupních hodnot.

5.2 Nulový informační přenos

Při pohledu na obrázek 4 vidíme, že nejhoršího přenosu dosahuje kanál, v jehož matici si jsou vektory všech řádků rovny. Lze dokázat, že takový kanál má bez ohledu na rozdělení vstupu vždy nulový informační přenos. Veličiny X a Y se za tohoto stavu chovají jako dvojice nezávislých náhodných veličin, takže $H(Y \mid X) = H(Y)$. Odtud pak přímo z rovnice (3) dostáváme, že $I(X; Y) = 0$.

5.3 Zajištění nulového přenosu

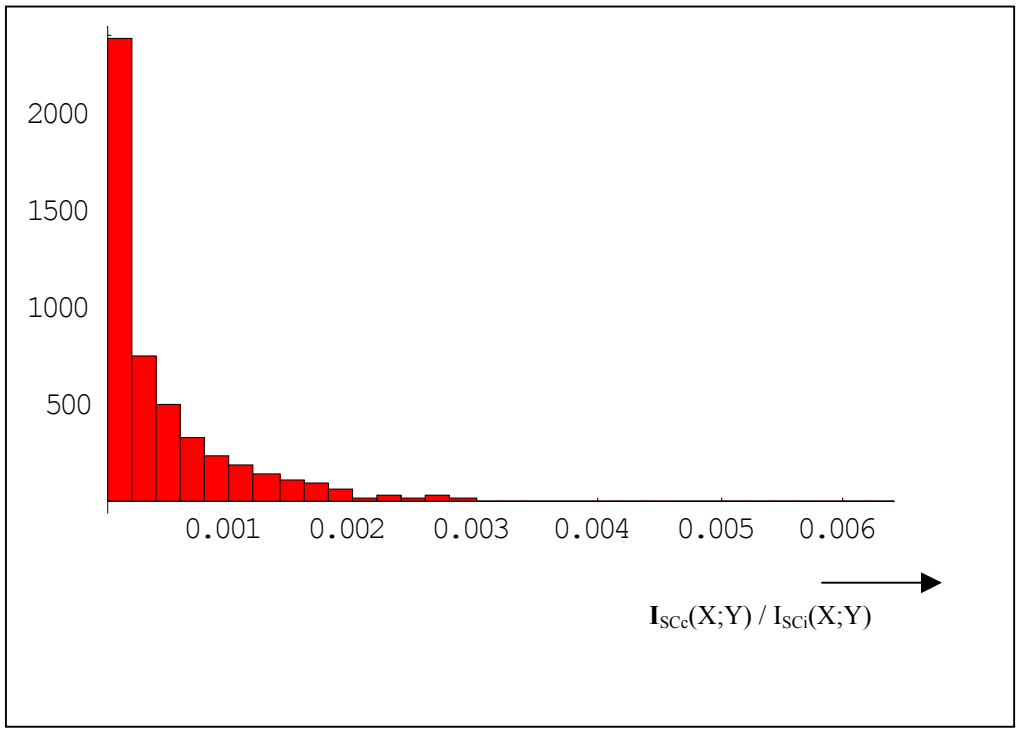
Z předchozího víme, jak by měla vypadat kanálová matice „neškodného" postranního kanálu. Otázkou však zůstává, jak takovou matici vytvořit. Cesta vedoucí přes přímé ovlivnění fyzikálních vlastností daného kanálu je s výjimkou použití dokonalého stínění technologicky téměř vyloučena. Alespoň tedy v obecném případě, a my se zde právě chceme na obecný případ zaměřit. Na první pohled by se mohlo zdát, že jsme zde v podobně svízelné situaci, v jaké jsou výzkumníci v oblasti teorie kódování – víme, jak by měla kanálová matice vypadat, ale nevíme, jak to schůdnou cestou zaručit. Zatímco v teorii kódování často nezbývá než tuto cestu zcela opustit a věnovat se toliko vhodnému přizpůsobení vysílače (vhodným kódem), my zde jistou šanci máme. Poznamenejme, že ji máme právě proto, že chceme dosáhnout minimálního a nikoliv maximálního přenosu.

Představme si, že sice nemáme možnost měnit fyzikální vlastnosti daného kanálu, ale že máme možnost nechat zařízení před každou vyzářenou informací náhodně zvolit jeden z r postranních kanálů. Předpokládejme, že tato volba probíhá s rovnoměrným rozdělením a že r je velké. Formálně tato situace znamená, že místo jedné matice SC máme množinu matic $\{ SC_1, SC_2, ..., SC_r \}$, z nichž se před každým odesláním informace do postranního kanálu náhodně vybere nějaká matice SC_i, podle které bude daný přenos probíhat. Před příštím přenosem se volba matice opět opakuje.

Položme si následující otázku: Jak bude vypadat výsledná kanálová matice takto řízeného kanálu z pohledu útočníka? Opět není příliš těžké dokázat, že situace se bude jevit, jako by byl použit postranní kanál popsaný maticí:

$$SCc = r^{-1} \sum_{i=1}^{r} SC_i \qquad (9)$$

V sumě je použit klasický maticový součet, násobení hodnotou r^{-1} představuje násobení matice skalárem. Zaměřme se nyní na chování hodnot v jednotlivých sloupcích výsledné matice SC_c (nazveme ji *maticí kanálové superpozice*). Zjednodušíme-li poněkud naše úvahy tím, že budeme odpovídající si hodnoty ve sloupcích matic SC_i považovat za hodnoty nezávislých náhodných veličin se stejným (po sloupcích) rozdělením, potom lze pro velká r podle zákona velkých čísel očekávat, že hodnoty ve sloupcích matice SC_c se budou blížit k určité střední hodnotě. Konkrétní číslo reprezentující tuto střední hodnotu zde pro nás není důležité. Důležité je, že vzdálenost mezi hodnotami ve sloupcových vektorech se bude s rostoucím r pravděpodobně zmenšovat, čímž se matice SC_c bude blížit tvaru, pro který dostáváme nulový informační přenos. Názorně tuto situaci ilustruje obrázek 5, na kterém je zachycena hustota distribuční funkce náhodné veličiny vyjadřující poměrnou změnu v informačním přenosu. Graf byl získán tak, že se 1000krát náhodně vygenerovala sada 256 (tj. r = 256) kanálových matic typu [2, 2]. Pro každou sadu se vypočítala výsledná matice SC_c a vyhodnotila se poměrná změna přenosu pro každou matici ze sady jako $I_{SCc}(X; Y)/I_{SCi}(X; Y)$. Každá sada tak poskytla 256 údajů o relativní změně, takže celkem se v grafu zpracovalo 256 000 takových změn. Vlastní graf byl vykreslen programem *Mathematica 4*. Pro tento ilustrační experiment bylo předpokládáno, že vstupní veličina X má rovnoměrné rozdělení. Nechceme zde tvrdit, že takto přesně bude vypadat chování všech možných superpozic. Chceme zde pouze prezentovat příklad popisující obecný trend relativní změny informačního přenosu, který plně podporuje námi odhadované chování celého systému. Tento trend říká, že ve většině případů dojde po superpozici k výraznému poklesu přenosu informace.



Obrázek 5: Rozdělení relativní změny informačního přenosu pro superponovaný kanál

5.4 Parazitní vyzařování operací

Zbývá ještě vyřešit otázku, jak do systému zanést náhodnou volbu kanálové matice. Pro tento účel se zaměříme na konkrétní operace, které probíhají v námi sledovaném a zabezpečovaném modulu. *Parazitním vyzařováním* zvolené operace nazveme postranní kanál, který přenáší informaci o vstupních hodnotách této operace. Mějme například operaci $f: A \rightarrow Im(f)$. Potom parazitní vyzařování této funkce bude popsáno kanálovou maticí, kde počet řádků bude odpovídat počtu prvků z množiny A, které s nenulovou pravděpodobností vstupují do funkce f. Počet sloupců pak bude korespondovat s počtem různých znaků, které je možné pozorovat na výstupu daného postranního kanálu. Pojem znak je v tomto kontextu třeba chápat velmi obecně.

Funkce, kterou jsme si představili, patří do kategorie unárních operací. Obecně si představme n-ární operaci vystupující jako zobrazení $f: A_1 \times A_2 \times ... \times A_n \rightarrow Im(f)$. Předpokládejme dále, že jeden z argumentů o dostatečně velkém rozsahu hodnot (m) není pro výsledek operace sémanticky důležitý, takže jej můžeme použít k libovolnému účelu (konkrétně nechť to je a_n, nabývající r hodnot). Navíc víme, že n-ární operaci $f(a_1, a_2, ..., a_n)$ můžeme pro vybraný argument a_n popsat jako r (n-1)-árních operací $\{ f_1(a_1, a_2, ..., a_{n-1}), f_2(a_1, a_2, ..., a_{n-1}), ..., f_m(a_1, a_2, ..., a_{n-1}) \}$, kde hodnotu a_n dosazujeme vždy implicitně. Přitom každá z těchto funkcí má vlastní charakter parazitního vyzařování, který je popsán maticemi $\{ SC_1, SC_2, ..., SC_r \}$. Volbou konkrétní hodnoty parametru a_n tak vlastně volíme konkrétní vyzařovací matici SC_i a to je právě ten „trik“, který jsme potřebovali.

5.5 Příklad použití

Ukázali jsme si, že ústřední myšlenkou popisované techniky je zanesení náhodné volby některého z parametrů zabezpečované operace. Tento parametr musí mít dostatečně velký rozsah hodnot, aby se začal projevovat zákon velkých čísel pro výslednou kanálovou matici parazitního vyzařování, a zároveň nesmí ovlivnit sémantiku této operace v daném kontextu. Představme si například, že potřebujeme ochránit součet dvou 16bitových (modulo 2^{16}) čísel a že máme k dispozici 32bitovou sčítačku. V takovém případě si můžeme za maskovací parametr zvolit obě horní (numericky významnější) poloviny vstupujících 32bitových slov, které naplníme náhodnými hodnotami. Do dolních polovin vstupních slov pak umístíme hodnoty, které chceme sečíst. Náhodné maskovací

hodnoty nám zde provádějí volbu jedné z 2^{32} kanálových matic, což by se mělo projevit výrazným poklesem nežádoucího informačního přenosu. Obdobně je možné maskovat operace násobení, logický součet, součin, nonekvivalenci a další.

5.6 Poznámka o účelu

Je třeba upozornit, že navrhovaná technika má sloužit zejména jako preventivní doplňková ochrana. Detailnímu rozboru jsme se zde věnovali proto, abychom ukázali, že její aplikace má svůj smysl, a že je tudíž vhodné věnovat jí během návrhu kryptografických modulů určitou pozornost. Nechceme však tvrdit, že tato technika je schopná nahradit ostatní protiopatření, která jsou konstruována přímo proti konkrétním druhům útoků (jejich popis je podán v připojených referencích). Na to je příliš obecná. V kombinaci s ostatními protiopatřeními však tato obecnost pomáhá čelit dosud neznámým druhům útoků, u kterých může výrazně zbrzdit jejich dopad. Protože útoky se většinou zdokonalují postupně, může toto zbrždění právě poskytnout konstruktérům čas na to, aby na nově vzniklé útoky reagovali vývojem cílených intenzivních protiopatření.

5.7 Shrnutí metody

Ukázali jsme si obecný model postranního kanálu a jeho souvislosti s parazitním vyzařováním operací, probíhajících v kryptografických modulech. Zavedli jsme si pojem informačního přenosu a odvodili jsme jeho závislost na matici postranního kanálu (SC). Na základě toho jsme prokázali kladný přínos techniky maskování citlivých operací náhodnou volbou sémanticky nedůležitých vstupních parametrů pro potlačení parazitního vyzařování těchto operací. Při odhadu síly konstruovaných mechanizmů jsme vyšli důsledně z teorie informace, což nám intuitivně říká, že výsledný návrh má dobré předpoklady pro to, aby v praxi obstál.

6 Některé návody pro obecná a praktická protiopatření proti postranním kanálům v implementacích PKCS#1

Klíčovou z hlediska Mangerova útoku na PKCS#1 byla procedura RSAES-OAEP-Decrypt, která je volána k odšifrování šifrového textu c. Tato procedura volá další dílčí procedury I2OSP a EME-OAEP-Decode. V následujícím mohou být všechny tyto procedury považovány za dílčí a mohou na ně být aplikována následující námi doporučovaná pravidla jako preventivní opatření proti útokům založeným na postranních kanálech. Uvažujme systém, který se skládá z posloupnosti několika částečných výpočtů (procedur) comp_1(...), comp_2(...), ..., comp_n(...).

6.1 Minimální obecná pravidla:

1. Nepoužívejme příkazy "stop" nebo "break". Zdá se to být zcela zřejmé, ale formálně jsou tyto příkazy v PKCS#1 použity a měly by být vyloučeny.
2. Pro různé datové vstupy udělejme výpočetní proces "spojitý" a "stejný", jak je to jen možné. Abychom se bránili časovému útoku, měla by být posloupnost výpočtů comp_1(...), comp_2(...), ... stejná a bez datově závislých větvení. Chování fyzikálního zařízení, které zajišťuje tyto výpočty, by mělo být co nejvíce nezávislé na datových vstupech. Pochopitelně, že je to teoreticky nemožné, ale v praxi bychom tento princip měli co nejvíce dodržovat, když píšeme program nebo používáme nějaké konkrétní zařízení.
3. Používejme standardní výstupy z dílčích výpočtů. Dílčí výsledky by měly vždy vracet nějaký chybový kód, nějaký pointer na výstupní data a délku těchto dat. Tyto proměnné by měly být počítány co možná nejvíce stejným procesem pro různé datové vstupy (i když někdy to není tak triviální, jak se na první pohled zdá). Dílčí procedury comp_X (X = 1, 2, ..., n) by měly vracet chybový kód error_X, pointer na výstupní data output_X a délku dat length_X. Poznamenejme, že ne všechny dílčí výpočty musí definovat všechny tři návratové hodnoty. Jakmile jsou ale definovány, musí být vždy počítány.

4. Dílčí návratové kódy by měly být nulové, jestliže vše proběhlo v pořádku, a náhodné nenulové, jestliže bylo něco špatně. Náhodné nenulové hodnoty (random nonzero, RNZ) by měly být k dispozici jako globální proměnné nebo by měly být vytvořeny na požádání jednou z dílčích procedur (například Get_RNZ(..)). Připomínáme zde, že se musí uplatnit pravidlo 2, což znamená, že volání a používání proměnné RNZ nesmí samo o sobě vytvářet větvení dílčí procedury. Poznámka: V některých případech může být těžké získat náhodnou hodnotu. Například v jednoduchých čipových kartách. V tomto případě ji můžeme odvodit přímo z nějakých částí dešifrované zprávy m. Musí to být uděláno velmi opatrně, jinak to může vytvářet nový postranní kanál.

5. V každém následujícím dílčím výpočtu comp_(X+1) kromě posledního můžeme využít datové výstupy z předchozích dílčích výpočtů (tj. output_X a length _X), ale nereagujeme na předchozí návratové chybové kódy error_X (pravděpodobně by to vytvořilo větvení v programu).

6. Po ukončení všech dílčích výpočtů vypočítáme závěrečný chybový kód jako OR všech dílčích chybových kódů: final_error = error_1 OR error_2 OR ... OR error_n. Podle této hodnoty se rozhoduje, zda výstupní data z celého výpočtu jsou platná nebo ne.

7. Nenulové náhodné návratové kódy by měly mít co největší rozsah, například to mohou být bajty nebo 32bitová slova. Čím delší, tím větší maskování se provádí. Tento princip je přímou aplikací techniky výběru náhodného kanálu, jak bylo popsáno výše. Konkrétně, pokud volíme bajtové hodnoty, používáme náhodný výběr jednoho z 255 náhodných kanálů.

8. Jako výsledek uvedených principů je možné z procedury I2OSP (klíčové pro Mangerův útok) vracet místo chybového hlášení "Integer too large" chybový kód rovný přímo nejvyššímu bajtu vstupního celého čísla, tj. error_ I2OSP = X, kde X je popsaný bajt, zatímco zbytek vstupního celého čísla se předává vždy k dalšímu zpracování (formou pointeru a délky). Návratový kód error_ EME-OAEP-Decode z procedury EME-OAEP-Decode je podle uvedených zásad buď nulový (dekódování a kontrola je v pořádku) nebo náhodný nenulový bajt. Výsledný chybový kód vznikne jako final_error = error_EME-OAEP-Decode OR error_ I2OSP , podle něhož se rozhoduje, zda výsledná data jsou platná, eventuelně se vydává závěrečné chybové hlášení z procedury RSAES-OAEP-Decrypt.

9. Předání chybových kódů z jednotlivých procedur musí být pokud možné prosté parazitního vyzařování. To se týká zejména bodu 8 a procedury I2OSP. Pro tyto hodnoty musí být použity paměťové oblasti s maximálně potlačeným parazitním vyzařováním (takové oblasti musí existovat, má-li dané zařízení vůbec obstát). Za určitých okolností mohou být stejně citlivé i návratové hodnoty lenght_X.

6.1.1 Příklad - Proč používat náhodné chybové kódy?

Ukážeme si to na příkladu PKCS#1, kdy použijeme jen hodnoty 0 a 1 pro chybové kódy error_I2OSP (zkráceně error_1) a error_EME-OAEP-Decode (error_2). Nechť X označuje nejvýznamnější bajt odšifrovaného celého čísla m ($m = c^d \bmod n$). Je-li X nenulové, šifrový text je špatný, takže nastavíme error_1 = 1. Je-li X nulové, nastavíme error_1 = 0. Výsledný chybový kód je defonován jako final_error = error_1 OR error_2. Útočník může volit šifrové texty a (například využitím napěťově-proudové analýzy) studovat chování systému v době, kdy je počítána final_error. Mohou nastat pouze tyto případy error_1 OR error_2:

(0 OR 0) - odpovídá správnému šifrovému textu

(1 OR 1) - odpovídá špatnému šifrovému textu, když nejlevější bajt není nula

(0 OR 1) - odpovídá špatnému šifrovému textu, když nejlevější bajt je náhodně nula

(1 OR 0) - skoro nemožná situace (při volbě šifrového textu za současné neznalosti textu otevřeného), když integritní kontrola na m je v pořádku, ale nejlevější bajt je špatně.

Jestliže útočník posílá správný šifrový text, učí se, jak se systém chová v prvním případě. Když posílá špatný šifrový text, učí se chování systému v druhém případě nebo ve třetím případě. Po fázi učení je útočník schopen rozlišit mezi případy, kdy error_final je počítána jako (0 OR 1) nebo jako (1 OR 1),

tedy zjistit error_1. Z error_1 však nyní dostává stejnou informaci jako z chybového hlášení "Integer too large" a máme zde zpět hrozbu v podobě Mangerova útoku.

Abychom předcházeli různým druhům postranních kanálů, musíme se obecně vyvarovat toho, aby (citlivá) proměnná X vstupovala do N-árních operací, kde zbývajících N-1 operandů je známých útočníkovi. Zejména to platí pro případ analýzy spotřeby energie. Například musíme vyloučit operace typu "X + const", "if (X != 0) then" atd. Z tohoto obecného principu a z výše uvedeného plyne, že pokud nastane chyba v proceduře EME-OAEP-Decode, jí vracená hodnota error_OAEP by měla být náhodná nenulová (pokud by byla konstantní, mohla by prozrazovat s ní zpracovávanou hodnotu error_1).

Abychom vyloučili jakýkoliv útok (zejména jeho učící fázi) využívající konstantní chybové kódy, je lepší používat náhodné nenulové hodnoty pro všechny chybové kódy v daném programu nebo aplikaci (teď už nehovoříme jen o PKCS#1). Tyto náhodné nenulové hodnoty by ale měly být připraveny před voláním odpovídajících procedur (comp_X) nebo voláním procedury "Get_RNZ" uvnitř nich na jejich počátku.

7 Závěr

V tomto příspěvku jsme připomněli některé zásadní důsledky, které má pro kryptosystém RSA tvrzení o individuálních bitech, které bylo formulováno a dokázáno v [HANA98]. Ačkoliv platnost tohoto tvrzení je obecně považována za dobrou vlastnost RSA, my jsme zde upozornili na možné negativní důsledky, které umožňují konstrukci útoků založených na postranních kanálech. Jak dokazují práce [BLEI98] a [MANG01], je schéma RSA náchylné k útokům založeným na postranních kanálech nejen teoreticky, ale i prakticky. V příspěvku [MANG01] byl původ této náchylnosti připisován vlastnostem použité kódovací metody označované jako OAEP. My však považujeme za důležité uvést, že skutečný původ této sensitivity jde daleko za rámec použitého kódování. Skutečný původ podle nás spočívá právě v tvrzení o individuálních bitech. Vlastní důkaz tohoto tvrzení je totiž zároveň sám o sobě návodem k tomu, jak z částečné znalosti otevřeného textu získat jeho znalost úplnou!

Použitý typ kódování může diskutovanou náchylnost snížit (což je vidět prakticky při srovnání formátů PKCS1-v1_5 a EME-OAEP, viz [PKCS#1], a příslušných útoků [BLEI98], [MANG01]), ale pro její úplné zamezení je patrně třeba provést specifické úpravy přímo konkrétních implementacích. Pro podložení tohoto názoru jsme v sekci 4 nastínili další z možných útoků na šifrovací schéma RSAES-OAEP, kde narozdíl od Mangerova přístupu útočíme na tu část otevřeného textu, která je pod „správou“ metody OAEP. Ukazujeme, že při dostupnosti určitého druhu postranního kanálu jsme schopni získat informaci o nejnižším bitu otevřeného textu. Na jejím základě je pak možné konstruovat další postupy vedoucí až k získání celého otevřeného textu. Pro zabránění tomuto útoku je třeba zamezit parazitnímu vyzařování jednotlivých operací v dílčích procedurách celého schématu, což už jde daleko za rámec obecného popisu kódovací metody OAEP.

Ve snaze přispět k obecným druhům opatření proti postranním kanálům jsme dále teoreticky prokázali přínos maskovací techniky založené na náhodné volbě sémanticky nevýznamných argumentů zabezpečovaných operací. Ve své podstatě se jedná o celkem jednoduchou myšlenku, avšak její teoretický rozbor ukazuje, že přes svoji jednoduchost může být tato metoda v praxi velmi přínosná. Její účel spatřujeme zejména v roli doplňkové ochrany, která má za úkol zpomalit dopad budoucích útoků a poskytnout tak čas na implementaci cílených protiopatření.

V šesté kapitole jsou pak uvedena obecná doporučení, která mají za úkol pomoci vytvořit implementaci schématu RSAES-OAEP, která je jednak odolná vůči aktuálnímu Mangerovu útoku [MANG01], jednak bere v úvahu další možné útoky založené na postranních kanálech. V tomto směru zejména doporučujeme sestavovat celé schéma ze základních funkčních bloků, u kterých byla provedena dostatečná ochrana proti parazitnímu vyzařování. To se zde v konkrétním případě týká nejen funkce SHA-1, ale i dalších operací, které pracují s citlivými informacemi. Ještě jednou připomínáme, že mezi citlivé informace patří všechny bity otevřeného textu. V roli doplňkové ochrany pak doporučujeme zvážit využití popsané maskovací techniky.

8 Reference

[ABDM00] Akkar, M.-L., Bevan, R., Dischamp, P. and Moyart, D.: *Power Analysis, What Is Now Possible...*, in Proc. of ASIACRYPT 2000, pp. 489-502, 2000.

[ANDE01] Anderson, R.: *Security Engineering*, John Wiley & Sons, Inc., 2001.

[ANKU96] Anderson, R. and Kuhn, M.: *Tamper Resistance – a Cautionary Note*, in Proc. of 2nd USENIX Workshop On Electronic Commerce, pp. 1-11, 1996.

[ANKU97] Anderson, R. and Kuhn, M.: *Low Cost Attacks on Tamper Resistant Devices*, in Proc. of *Security Protocols '97*, pp. 125-136, 1997.

[ANKU98] Anderson, R. and Kuhn, M.: *Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations*, in Proc. of Information Hiding '98, pp. 124-142, 1998.

[ARCH01] Archiv článků http://www.decros.cz/bezpecnost/_kryptografie.html.

[BDH+97] Bao, F., Deng, R.-H., Han, Y., Jeng, A., Narasimhalu, A.-D. and Ngair, T.: *Breaking Public Key Cryptosystems on Tamper Resistant Devices in the Presence of Transient Faults*, in Proc. of Security Protocols '97, pp. 115-124, 1997.

[BISH97] Biham, E. and Shamir, A.: *Differential Fault Analysis of Secret Key Cryptosystems*, in Proc. of CRYPTO '97, pp. 513-525, 1997.

[BDL97] Boneh, D., DeMillo, R. A. and Lipton, R. J.: *On the Importance of Checking Cryptographic Protocols for Faults*, in Proc. of EUROCRYPT '97, pp. 37-51, 1997.

[BLEI98] Bleichenbacher, D.: *Chosen Ciphertexts Attacks Against Protocols Based on the RSA Encryption Standard PKCS#1*, in Proc. of CRYPTO '98, pp. 1-12, 1998.

[BONE99] Boneh, D.: *Twenty Years of Attacks on the RSA Cryptosystems*, Notices of the American Mathematical Society, vol. 46, no. 2, pp. 203-213, 1999, available at http://crypto.stanford.edu/~dabo/pubs.html.

[CJRR99] Chari, S., Jutla, C.-S., Rao, J. and Rohatgi, P.: *Towards Sound Approaches to Counteract Power-Analysis Attacks*, in Proc. of CRYPTO '99, pp. 398-411, 1999.

[COGO00] Coron, J.-S. and Goubin, L.: *On Boolean and Arithmetic Masking against Differential Power Analysis*, in Proc. of CHES 2000, pp. 231-237, 2000.

[CSD00] Clavier, C., Coron, J.-S. and Dabbous, N.: *Differential Power Analysis in the Presence of Hardware Countermeasures*, in Proc. of CHES 2000, pp. 253-263, 2000.

[DKL+98] Dhem, J.-F., Koeune, F., Leroux, P.-A., Mestré, P. and Quisquater, J.-J. and Willems, J. - L.: *A Practical Implementation of the Timing Attack*, Technical Report CG-1998/1, 1998.

[FIPS-140] *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*, National Institute of Standards and Technology, Issued May 25 2001, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

[GOOG01] the thread "*OAEP attack paper?*", 21st August 2001, sci.crypt, available at http://groups.google.com/groups?hl=cs&rnum=2&selm=3B822AED.2CCA0DD3%40zetnet.co.uk

[GOPA99] Goubin, L. and Patarin, J.: *DES and differential power analysis*, in Proc. of CHES '99, pp. 158-172, 1999.

[HAMM80] Hamming, R.-W.: *Coding and Information Theory*, Prentice Hall, 1980.

[HANA98] Håstad, J. and Näslund M.: *The Security of Individual RSA Bits*, in Proc. of FOCS '98, pp. 510-521, 1998.

[KSWH98] Kelsey, J., Schneier, B., Wagner, D. and Hall, C.: *Side Channel Cryptanalysis of Product Ciphers*, in Proc. of ESORICS '98, pp. 97-110, 1998.

[KJB99] Kocher, P., Jaffe, J. and Jun, B.: *Differential Power Analysis*, in Proc. of Crypto '99, pp. 388-397, 1999.

[KJJ98] Kocher, P., Jaffe, J. and Jun, B.: *Introduction to Differential Power Analysis and Related Attacks*, Technical Report, 1998, http://www.cryptography.com/dpa/technical.

[KJJ99] Kocher, P., Jaffe, J. and Jun, B.: *Differential Power Analysis: Leaking Secrets*, in Proc. of CRYPTO '99, pp. 388-397, 1999.

[KLRO01] Klíma V. a Rosa T.: *RSA v novém světle (3)*, Chip 01/2002, dostupné na [ARCH01].

[KOCH96] Kocher, P.: *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*, in Proc. of CRYPTO '96, pp. 104-113, 1996.

[KÖKU99] Kömmerling, O. and Kuhn, M.: *Design Principles for Tamper-Resistant Smartcard Processors*, in Proc. of USENIX Workshop on Smartcard Technology, pp. 9-20, 1999.

[MANG01] Manger, J.: *A Chosen Ciphertext Attack On RSA Optimal Asymmetric Encryption Padding (OAEP) as Standardized In PKCS #1*, in Proc. of CRYPTO 2001, August 2001.

[MASO00] Mayer-Sommer, R.: *Smartly Analyzing the Simplicity and the Power of Simple Power Analysis on Smartcards*, in Proc. of CHES 2000, pp. 78-92, 2000.

[MDS99a] Messegers, T.-S., Dabbish, E. A. and Sloan, R. H.: *Investigations of Power Analysis Attacks on Smartcards*, in Proc. of USENIX Workshop on Smartcard Technology, pp. 151-161, 1999.

[MDS99b] Messerges, T.-S., Dabbish, E. A. and Sloan, R. H.: *Power Analysis Attacks of Modular Exponentiation in Smartcards*, in Proc. of CHES '99, pp. 144-157, 1999.

[MESE00] Messerges, T.-S.: *Using Second-Order Power Analysis to Attack DPA Resistant Software*, in Proc. of CHES '00, pp. 238-251, 2000.

[MESE00b] Messerges, T.-S.: *Securing the AES Finalists Against Power Analysis Attacks*, in Proc. of FSE 2000, pp. 150-164, 2000.

[MOV96] Menezes, A. J., van Oorschot, P. C. and Vanstone, S. A.: *Handbook of Applied Cryptography*, CRC Press, 1996, online at http://www.cacr.math.uwaterloo.ca/hac/.

[MUIR01] Muir, J.-A.: *Techniques of Side Channel Cryptanalysis*, A thesis presented to the University of Waterloo, Canada, 2001, http://www.math.uwaterloo.ca/~jamuir/sidechannel.htm.

[PKCS#1] *PKCS#1 v2.1: RSA Cryptography Standard*, RSA Laboratories, DRAFT2 – January 5 2001, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/.

[RARO01] Rao, J.-R and Rohatgi, P.: *EMpowering Side-Channel Attacks*, preliminary technical report, May 11 2001.

[SCHI00] Schindler, W.: *A Timing Attack against RSA with the Chinese Remainder Theorem*, in Proc. of CHES 2000, pp. 109-124, 2000.

[SHOU01] Shoup, V.: *OAEP Reconsidered (Extended Abstract)*, in Proc. of CRYPTO 2001, August 2001.

[ROSA01] Rosa, T.: *Kryptoanalýza s využitím postranních kanálů*, Vojenská kryptografie IV, Sborník příspěvků, str. 113 – 156, 2001, dostupné v [ARCH01].

[STIN95] Stinson, D.-R.: *Cryptography – Theory and Practice*, CRC Press, 1995.

D. Velikonoční kryptologie

ECOM-MONITOR.COM

3.-4. duben 2002, Brno

Základní informace (www.ecom-monitor.cz/velikonoce)

Velikonoční kryptologie se koná na jaře jako český a slovenský workshop zaměřený na podporu úzké spolupráce odborníků pracujících na poli aplikované kryptografie a v příbuzných oblastech. Volně navazuje na ukončený úspěšný cyklus seminářů **Vojenská kryptografie** a také na workshop **Mikulášská kryptobesídka**. Další navazující workshopy se budou konat každý rok a to v období Velikonoc a Mikuláše. Workshopy jsou pořádány za účelem podpory výměny informací a nápadů z minulých, současných i budoucích projektů.

Nosné téma tohoto workshopu bude ***Stanovení míry kryptografické bezpečnosti a přijatelná rizika kryptografické bezpečnosti.***

Pokyny pro autory

Zájemci mohou poslat rozšířené abstrakty navrhovaných příspěvků s následujícími tématy:

- Stanovení míry kryptografické bezpečnosti.
- Přijatelná rizika kryptografické bezpečnosti.
- Modularita a opakované použití (ověřených kritických) komponent.
+ Ostatní zajímavá témata související s aplikovanou kryptografií.

Rozšířené abstrakty (500-1000 slov), společně s autorovou emailovou adresou, telefonním číslem a poštovní adresou, musí programový výbor (PV) obdržet nejpozději *20. února 2002*. Elektronická podání jsou preferována; papírová podání musí obsahovat 8 vytištěných kopií. Rozšířený abstrakt musí respektovat výše uvedené omezení rozsahu, prezentovat stručně a výstižně základní myšlenky příspěvku a obsahovat informace (nejlépe ve vyhrazených kapitolách) o:

- diskutovaném problému a dopadech;
- používaných a/nebo navržených metodách řešení;
- vlastním přínosu, příp. pohledu na řešení problému.

Abstrakt bude posouzen PV a autoři budou informováni o přijetí/odmítnutí do *4. března*. Finální verze kompletního příspěvku (5-15 stran A4), společně s krátkým životopisem (50-100 slov) musí být dodány do *4. května*. Příspěvky mohou být napsány v češtině, slovenštině nebo angličtině.

Je také vyhlášena soutěž o nejlepší příspěvek, jehož autorem nebo spoluautorem s majoritním podílem je *student*. Několik nejlepších studentských příspěvků bude odměněno úhradou části nákladů spojených s účastí na workshopu.

Rozšířené abstrakty i kompletní příspěvky by měly být odeslány v RTF nebo LaTeX, vzory pro kompletní příspěvky budou poskytnuty.

Zasílání příspěvků

Preferujeme elektronické podání příspěvků.
E-mail: *Vaclav.Matyas@ecom-monitor.cz*
Předmět: "VKB 2002"
Poštovní adresa: *V. Matyáš*
ecom-monitor.com, a.s.
PO Box 7
664 01 Bílovice nad Svitavou

Důležitá data

Podání rozšířených abstraktů: 20. února 2002
Oznámení o přijetí/odmítnutí: 4. března 2002
Pracovní verze příspěvků: 18. března 2002
Workshop: 3.– 4. dubna 2002
Podání finálních příspěvků: 4. května 2002

Programový výbor

Daniel Olejár, UK Bratislava
Vašek Matyáš, ecom-monitor.com a MU Brno
Oldřich Pekárek, NBÚ ČR - předseda
Jiří Sobotík, VA Brno
Jaroslav Šmíd, NBÚ ČR
Pavel Vondruška, ÚOOÚ
Jozef Vyskoč, VaF Bratislava

Organizační výbor

Jaroslav Dočkal, Vojenská akademie Brno
Vít Kratina, ecom-monitor.com - tajemník
Roman Pavlík, ecom-monitor.com
Zdeněk Říha, ecom-monitor.com a MU Brno
Michal Sasínek, NBÚ MV SR
Jan Staudek, MU Brno

E. Letem šifrovým světem

O čem jsme psali v lednu roku 2000 a 2001

Crypto-World 1/2000

Crypto-World 1/2001

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (Internet, noviny) nebo se jedná o původní 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 (nejdříve 15 dní po jeho rozeslání) a předchozí sešity GCUCMP (zkonvertovány do PDF formátu), informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :

http://www.mujweb.cz/veda/gcucmp

Pokud se zajímáte pouze o sešit Crypto-World, můžete jej najít na lépe dostupné adrese:

http://cryptoworld.certifikuj.cz

2. Registrace / zrušení registrace

Zájemci **o zasílání** tohoto sešitu se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@uoou.cz (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://www.mujweb.cz/veda/gcucmp/ . Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání sešitu.

Ke **zrušení registrace** stačí zaslat krátkou zprávu na e-mail pavel.vondruska@uoou.cz (předmět: ruším odběr Crypto-Worldu !). Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byl sešit zasílán.

3. Spojení

běžná komunikace**, zasílání příspěvků k otištění** , informace

pavel.vondruska@uoou.cz (**vondruskap@uoou.cz**)
pavel.vondruska@post.cz
vondruska.p@seznam.cz