Podklady pre opis algoritmu na identifikáciu málo bezpečných privátnych kľúčov v slovenských eID

(prednáška z predmetu Aplikovaná kryptografia dňa 6.11.2017)

Detailný opis útoku bol uvedený v článku [1]:

The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli*

Matus Nemec
Masaryk University,
Ca' Foscari University of Venice
mnemec@mail.muni.cz

Marek Sys†
Masaryk University
syso@fi.muni.cz

Petr Svenda
Masaryk University
svenda@fi.muni.cz

Dusan Klinec
EnigmaBridge, Masaryk University
dusan@enigmabridge.com

Vashek Matyas
Masaryk University
matyas@fi.muni.cz

na konferencii
https://www.sigsac.org/ccs/CCS2017/

preprint článku
https://crocs.fi.muni.cz/_media/public/papers/nemec_roca_ccs17_preprint.pdf

Bibbtex:

```
@inproceedings{2017-ccs-nemec,
  Author        = {Matus Nemec and Marek Sys and Petr Svenda and Dusan
Klinec and Vashek Matyas},
  Title         = {The Return of Coppersmith's Attack: Practical
Factorization of Widely Used RSA Moduli},
  BookTitle     = {24th ACM Conference on Computer and Communications
Security (CCS'2017)},
  Year          = {2017},
  ISBN          = {978-1-4503-4946-8/17/10},
  Publisher     = {ACM},
  Pages         = {1631-1648}
}
```

Základné informácie o útoku a relevantné linky sú uvedené na stránke
https://crocs.fi.muni.cz/public/papers/rsa_ccs17

Je mu venovaná aj stránka na Wikipedii
https://en.wikipedia.org/wiki/ROCA_vulnerability

Online test verejného kľúča je možné realizovať na tejto stránke
https://keytester.cryptosense.com/

Offline test je možné realizovať pomocou zdrojových kódov v GIT archíve (phyton, java, C#)
https://github.com/crocs-muni/roca

Optimalizovaný kód (neobsahuje časť redundantných testov v povodnom "ROCA GIT archíve") v jazyku C (zdrojový kód **roca.c**, ktorý využíva funkcie openSSL knižnice) [2]
https://gist.github.com/robstradling/f525d423c79690b72e650e2ad38a161d

Podstata algoritmu na detekciu problematických privátnych kľúčov založená na zisteniach v článku
https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/svenda
a podrobnejšej správe [3]:

FI MU

Faculty of Informatics
Masaryk University, Brno

The Million-Key Question - Investigating the Origins of RSA Public Keys

by

Petr Švenda
Matúš Nemec
Peter Sekan
Rudolf Kvašňovský
David Formánek
David Komárek
Václav Matyáš

FI MU Report Series FIMU-RS-2016-03

 July 2016

Autori ukázali (str. 33 v správe [3]), že karty Infineon JTOP 80K generujú prvočísla so štatistickými anomáliami

	Remainder																							
Divisor	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	…	22	…	26	…	36
3	1/2	1/2																						
5	1/4	1/4	1/4	1/4																				
7	1/6	1/6	1/6	1/6	1/6	1/6																		
11	1/2	0	0	0	0	0	0	0	0	1/2														
13	1/6	0	1/6	1/6	0	0	0	0	1/6	1/6	0	1/6												
17	1/8	1/8	0	1/8	0	0	0	1/8	1/8	0	0	0	1/8	0	1/8	1/8								
19	1/9	0	0	1/9	1/9	1/9	1/9	0	1/9	0	1/9	0	0	0	0	1/9	1/9	0						
23	1/22	1/22	1/22	1/22	1/22	1/22	1/22	1/22	1/22	1/22	1/22	1/22	1/22	1/22	1/22	1/22	1/22	1/22	…	1/22				
29	1/28	1/28	1/28	1/28	1/28	1/28	1/28	1/28	1/28	1/28	1/28	1/28	1/28	1/28	1/28	1/28	1/28	1/28	…	1/28	…	1/28	…	
31	1/30	1/30	1/30	1/30	1/30	1/30	1/30	1/30	1/30	1/30	1/30	1/30	1/30	1/30	1/30	1/30	1/30	1/30	…	1/30	…	1/30	…	
37	1/3	0	0	0	0	0	0	0	0	1/3	0	0	0	0	0	0	0	0	…	0	…	1/3	…	0

Table 6: *Probability of remainders modulo small primes for primes and moduli generated by Infineon JTOP 80K smartcard. Additionally, we detected that the remainders modulo 53, 61, 71, 73, 79, 97, 103, 107, 109, 127, 151 and 157 are also from certain subgroups of residue classes and do not represent all residue classes. The values are almost uniformly distributed modulo all other primes (tested up to 547), as expected from the Dirichlet's theorem. We use the remainder modulo 3 for our classification. The card generates uniformly distributed moduli modulo 3, therefore the criterion is not applicable to this card. However, if we would focus more on this source in our analysis, by using the remainders modulo other primes, the card could be identified much more easily. Hence for specialized cases other criteria can be more useful than for our general analysis.*

Ich analýzou (čínska veta o zvyškoch) sa dopracovali k štruktúre prvočísel, ktoré sú generované v tavre [1]

$$p = k * M + (65537^{a} \bmod M). \qquad (1)$$

pričom hodnota M je tzv. (angl) primodial

Definition for primorial numbers [edit]

For the nth prime number p_n, the primorial $p_n\#$ is defined as the product of the first n primes:[1][2]

$$p_n\# \equiv \prod_{k=1}^{n} p_k,$$

where p_k is the kth prime number. For instance, $p_5\#$ signifies the product of the first 5 primes:

$$p_5\# = 2 \times 3 \times 5 \times 7 \times 11 = 2310.$$

The first six primorials $p_n\#$ are:

1, 2, 6, 30, 210, 2310 (sequence A002110 in the OEIS).

The sequence also includes $p_0\# = 1$ as empty product. Asymptotically, primorials $p_n\#$ grow according to:

$$p_n\# = e^{(1+o(1))n \log n},$$

where $o(\,)$ is little-o notation.[2]

https://en.wikipedia.org/wiki/Primorial

Modul pre RSA je tvorený súčinom dvoch prvočísel s touto vlastnosťou, čo vedie ku kongruencii, ktorá je základom rýchleho detekčného algoritmu (Fingerprinting):

2.2 Fingerprinting

The public RSA modulus N is a product of two primes p, q. The *RSALib* generates primes of the described form (1). The moduli have the corresponding form:

$$N = \overbrace{(k * M + 65537^a \bmod M)}^{p} * \overbrace{(l * M + 65537^b \bmod M)}^{q}, \quad (2)$$

for $a, b, k, l \in \mathbb{Z}$. The previous identity implies

$$N \equiv 65537^{a+b} \equiv 65537^c \bmod M, \quad (3)$$

for some integer c. The public modulus N is generated by 65537 in the multiplicative group $\mathbb{Z}_M^*$. The existence of the discrete logarithm $c = \log_{65537} N \bmod M$ is used as the fingerprint of the public modulus N generated by the *RSALib*.

Na prednáške bude ukázané ako je zo vzťahu (3) možné odvodiť optimalizovaný kód algoritmu v zdrojovom kóde **roca.c** [2]. Využité budú základné fakty z oblasti Galoisových polí preberané v rámci prednášok a cvičení z predmetu Aplikovaná kryptografia. Bude využitá aj nasledujúca vlastnosť platná (aj) pre prvky z GF:

Theorem 8.2.3
Let G be a finite group. Then for every $a \in G$ it holds that:

1. $a^{|G|} = 1$
2. *ord*(a) *divides* $|G|$

The first property is a generalization of Fermat's Little Theorem for all cyclic groups. The second property is very useful in practice. It says that in a cyclic group only element orders which divide the group cardinality exist.

Example 8.7. We consider again the group $\mathbb{Z}_{11}^*$ which has a cardinality of $|\mathbb{Z}_{11}^*| = 10$. The only element orders in this group are 1, 2, 5, and 10, since these are the only integers that divide 10. We verify this property by looking at the order of all elements in the group:

$$\begin{aligned} \text{ord}(1) &= 1 & \text{ord}(6) &= 10 \\ \text{ord}(2) &= 10 & \text{ord}(7) &= 10 \\ \text{ord}(3) &= 5 & \text{ord}(8) &= 10 \\ \text{ord}(4) &= 5 & \text{ord}(9) &= 5 \\ \text{ord}(5) &= 5 & \text{ord}(10) &= 2 \end{aligned}$$

Indeed, only orders that divide 10 occur.

◇