Annales Mathematicae Silesianae 12 (1998), 65–74

Prace Naukowe Uniwersytetu Śląskiego nr 1751, Katowice

REMARKS TO SHORT RSA PUBLIC EXPONENTS

OTOKAR GROŠEK*, KAROL NEMOGA†, AND LADISLAV SATKO‡

Abstract. In this paper we discuss pertinent questions closely related to well known RSA cryptosystem [5]. From practical point of view it is reasonable to use as a public exponent an integer $s = 2^k + 1$, i.e., so called *short exponent*, with the lowest possible binary weight. The most common are for $k = 1$ and $k = 2^4$, the two Fermat primes. In this paper we prove two theorems which give a percentage of acceptable public exponents $s = 2^k + 1, \quad 1 \leqslant k \leqslant 1023$ to two randomly selected primes of 512 bits each. In fact, our results are valid for arbitrary set of exponents s. We also present results of our experiments. In our simulation, for all such acceptable public exponents, the corresponding secret exponent t had a weight within the range of 451–567. Thus, although it is recommended in [8] not to use short public exponents, by our observation to use the attack based on continuos fractions is infeasible.

1. Introduction

There exists a paper [6] which deals with short keys for RSA algorithm, i.e. such primes p, q having only a limited ones in their binary expansion. Here we deal with a different problem.

To reduce the exponentiation time, there is besides Quisquater and Couvreur technique [4] another way, to use short public or secret exponents in RSA algorithm. An example of this is when RSA is used in communication between a smart card and a larger computer. In this case it is an advantage for the smart card to have a short public exponent in order to reduce the processing required in the smart card. However, one must be wary of short

Received on August 18, 1998.

1991 *Mathematics Subject Classification* 68P25, 94A60, 11K99.

Key words and phrases: RSA modulus, RSA exponents, short exponents.

* This work was supported by VEGA grant 1/4289/97.

† This work was supported by VEGA grant 1/1227/97.

‡ This work was supported by VEGA grant 1/4289/97.

exponent attacks on RSA [3]. We say that an exponent s is *acceptable for a prime* p if there exists an RSA modulus $m = pq$ to which s can be an RSA public/secret exponent. The problem, we are dealing with, is as follows:

Let p, q be two randomly selected primes of the magnitude 512 bits each.

1. For a given public exponent $s = 2^k + 1,\ \ 1 \leqslant k \leqslant 1023$ what is the probability that s will be coprime to $\phi(pq)$[1]?
2. What is the probability that all short exponents s, $s = 2^k + 1$, $1 \leqslant k \leqslant 1023$ are acceptable for the randomly selected p, q?
3. To all such acceptable public exponents what is the corresponding weight of the secret exponent t?

As a numerical experiment we generated 100 pairs of 512 bits primes and verify which of short exponents s, $s = 2^k + 1,\ \ 1 \leqslant k \leqslant 1023$ is coprime to the randomly selected p, q.

2. Solution of problems

Here we prove our main result which allows to calculate probability mentioned in the first two problems above.

It is clear that the answer to the first problem strongly depends on the prime factorization of s. In fact, any RSA exponent must be coprime to $\phi(pq) = (p-1)(q-1)$. Under the supposition for choosing RSA modulus we may assume $p-1$ and $q-1$ to be stochasticaly independent and $\gcd(s, p-1) = \gcd(s, q-1) = 1$. Moreover $\gcd(s, p) > 1$ leads to a possible factorization of the modulus $m = pq$. Further, any prime p is of the form $p = sl+c,\ 1 \leqslant c < s$ providing

$$\gcd(s,p) = \gcd(s, sl + c) = \gcd(s, c) = 1 \tag{1}$$

$$\gcd(s, p-1) = \gcd(s, sl + c - 1) = \gcd(s, c-1) = 1. \tag{2}$$

Conversely for any c such that $\gcd(s, c) = 1$ there exist primes of the form $p = sl + c$, and they are (due to well known Dirichlet's theorem) equally distributed. Thus, there is a pertinent question to find cardinality of the set

$$N_s = \{c \mid 1 \leqslant c \leqslant s,\ \ \gcd(c, s) = \gcd(c-1, s) = 1\}. \tag{3}$$

To simplify next proofs we start with an example.

EXAMPLE 1. Let $s = 5^2 * 7 = 175$. We would like to know cardinality of the set N_s in this case.

[1] ϕ is the Euler ϕ-function.

We solve this problem in two steps: Firstly, we find the answer for $s' = 5 * 7 = 35$, and then we prove that $|N_s| = 5 * |N_{s'}|$.

Let

$$
(4) \qquad \begin{aligned}
A_5^0 &= \{c|\ 1 \leqslant c \leqslant 35, \quad c \equiv 0 \pmod 5\} \\
A_5^1 &= \{c|\ 1 \leqslant c \leqslant 35, \quad c \equiv 1 \pmod 5\} \\
A_7^0 &= \{c|\ 1 \leqslant c \leqslant 35, \quad c \equiv 0 \pmod 7\} \\
A_7^1 &= \{c|\ 1 \leqslant c \leqslant 35, \quad c \equiv 1 \pmod 7\} \\
B_5 &= A_5^0 \cup A_5^1 \\
B_7 &= A_7^0 \cup A_7^1.
\end{aligned}
$$

Then the following relations are valid:

1. $A_5^0 \cap A_5^1 = A_7^0 \cap A_7^1 = \emptyset$;
2. $|A_5^0| = |A_5^1| = s'/5 = 7, |A_7^0| = |A_7^1| = s'/7 = 5$;
3. By Chinese remainder theorem
$$|A_5^0 \cap A_7^1| = |A_5^0 \cap A_7^0| = |A_5^1 \cap A_7^0| = |A_5^1 \cap A_7^1| = 1;$$
4. $c \in N_{35}$ if and only if $c \notin B_5 \cup B_7$;
5. $|N_{35}| = 35 - |B_5 \cup B_7|$;
6. $|B_5 \cup B_7| = |B_5| + |B_7| - |B_5 \cap B_7|$;
7. Using item 1 and 3 we have
$$\begin{aligned}|B_5 \cap B_7| &= |(A_5^0 \cup A_5^1) \cap (A_7^0 \cup A_7^1)| \\ &= |A_5^0 \cap A_7^0| + |A_5^0 \cap A_7^1| + |A_5^1 \cap A_7^0| + |A_5^1 \cap A_7^1| = 4.\end{aligned}$$

Hence
$$\begin{aligned}|N_{35}| &= 35 - |B_5 \cup B_7| = 35 - |B_5| - |B_7| + |B_5 \cap B_7| \\ &= 35 - 2 * 7 - 2 * 5 + 4 = 15.\end{aligned}$$

Now assume, that the same consideration can be done for integers $36 \leqslant c \leqslant 70, \ldots, 141 \leqslant c \leqslant 175$ providing the same cardinalities of similar sets N. Thus $|N_{175}| = 5 * |N_{35}| = 75$. Moreover, after some arithmetics $|N_{35}| = 35 * \frac{5-2}{7} * \frac{7-2}{5} = (\phi(5) - 1)(\phi(7) - 1)$. $\square$

Now we focus on the general case.

THEOREM 1. *Let $s = p_1 p_2 \ldots p_r$ be the product of different primes. Then cardinality of the set N_s, given by (3) is*

$$(5) \qquad |N_s| = \prod_{i=1}^{r} (\phi(p_i) - 1).$$

PROOF. We prove the Theorem analogously like in the Example 1. Let for $1 \leqslant i \leqslant r$

$$\begin{aligned} A^0_{p_i} &= \{c \mid 1 \leqslant c \leqslant s, \quad c \equiv 0 \pmod{p_i}\}, \\ A^1_{p_i} &= \{c \mid 1 \leqslant c \leqslant s, \quad c \equiv 1 \pmod{p_i}\}, \\ B_{p_i} &= A^0_{p_i} \cup A^1_{p_i}. \end{aligned} \tag{6}$$

Then the following relations are valid:

1. $A^0_{p_i} \cap A^1_{p_i} = \emptyset$;
2. $|A^0_{p_i}| = |A^1_{p_i}| = s/p_i$;
3. $c \in N_s$ if and only if $c \notin \bigcup_{i=1}^r B_{p_i}$;
4. $|N_s| = s - |\bigcup_{i=1}^r B_{p_i}|$;
5.

$$|\bigcup_{i=1}^r B_{p_i}| = \sum_{i=1}^r |B_{p_i}| - \sum_{i \neq j} |B_{p_i} \cap B_{p_j}| + \cdots + (-1)^{r+1} |\bigcap_{i=1}^r B_{p_i}|. \tag{7}$$

6. Let $z_j, \quad j = 1, \ldots, l$ be 0 or 1. Then for $i = 1, \ldots, r$, by Chinese reminder theorem, any of the sets

$$\bigcap_{j=1}^l A^{z_j}_{p_{i_j}}$$

has cardinality

$$\frac{s}{\prod_{j=1}^l p_{i_j}}$$

and thus (assuming item 1)

$$|\bigcap_{j=1}^l B_{p_{i_j}}| = |\bigcap_{j=1}^l (A^0_{p_{i_j}} \cup A^1_{p_{i_j}})| = 2^l \frac{s}{\prod_{j=1}^l p_{i_j}}. \tag{8}$$

Hence

$$|\bigcup_{i=1}^r B_{p_i}| = \sum_{i=1}^r 2 \frac{s}{p_i} - \sum_{i \neq j} 2^2 \frac{s}{p_i p_j} + \cdots + (-1)^{r+1} 2^r. \tag{9}$$

Finally, considering $s = p_1 p_2 \dots p_r$ we have

$$
\begin{aligned}
|N_s| &= s - |\bigcup_{i=1}^{r} B_{p_i}| = s - \sum_{i=1}^{r} 2\frac{s}{p_i} + \sum_{i\neq j} 2^2 \frac{s}{p_i p_j} - \dots + (-1)^r 2^r \\
&= \prod_{i=1}^{r}(p_i - 2) = \prod_{i=1}^{r}(\phi(p_i) - 1).
\end{aligned} \tag{10}
$$

□

THEOREM 2. *Let $s = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ be the prime factorization of s. Then cardinality of the set N_s, given by (3) is*

$$
|N_s| = \frac{s}{p_1 p_2 \dots p_r} \prod_{i=1}^{r}(\phi(p_i) - 1). \tag{11}
$$

PROOF. To prove this Theorem we only repeat the same considerations as in Example 1:
For $s' = p_1 p_2 \dots p_r$ the set $N_{s'}$ has the cardinality given by Theorem 1.
Let $K = \frac{s}{p_1 \dots p_r} - 1$. For $k = 0, \dots, K$ we define sets

$$
N_{ks'} = \{c |\ 1 + ks' \leqslant c \leqslant s' + ks', \ \ \gcd(c, s') = \gcd(c - 1, s') = 1\}.
$$

Then

$$
N_s = \bigcup_{k=0}^{K} N_{ks'},
$$

which immediately yields that

$$
|N_s| = \frac{s}{p_1 \dots p_r} |N_{s'}| = \frac{s}{p_1 \dots p_r} \prod_{i=1}^{r}(\phi(p_i) - 1).
$$

This concludes the proof. □

3. Probability of short exponent primes

Here we use our Theorem 2 and calculate probabilities mentioned in Introduction. We assume that choice of two randomly selected primes p, q is independent.

Let $P(x)$ be the set of all first x primes. Then for a given RSA exponent s we can write $p = sl + c,\ 1 \leqslant c < s$

$$P(x) = \bigcup_{c:\ \gcd(s,c)=1} H_c,$$

where H_c consists of all primes $p \in P(x),\ \ p \equiv c \pmod{s}$. Due to Dirichlet's theorem for a large x all sets H_c consists (approximately) of the same number of primes, $x/\phi(s)$. If such a prime $p \in H_c$ is acceptable for the given public exponent s then it necessarily must satisfy also condition (2). Number of such classes H_c which satisfy (2) is given by Theorem 2. Thus for a given RSA exponent $s = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ probability that a randomly selected prime $p \in P(x)$ can be a part of RSA modulus is

$$\text{Prob} \approx \frac{|N_s| * x/\phi(s)}{x} = \frac{|N_s|}{\phi(s)},$$

and for randomly selected RSA modulus pq we have

$$\text{(12)}\qquad \text{Prob}\{pq|\ p,q \in H_c,\ c \in N_s\} \approx \frac{|N_s|^2}{\phi^2(s)} = \prod_{i=1}^{r} \Big(1 - \frac{1}{\phi(p_i)}\Big)^2.$$

Clearly, the larger is x the better is approximation in (12).

Now we answer the second problem. Here, contrary to the first problem a running argument is exponent s. Using Theorem 2 we can find probability that all short exponents $s,\ s = 2^k + 1,\ \ 1 \leqslant k \leqslant 1023$ are acceptable for the randomly selected but fixed primes p, q.

Let

$$\text{(13)}\qquad D = \{p_i : p_i|\ 2^k + 1 \ \text{ for some } \ k,\ \ 1 \leqslant k \leqslant 1023\},$$

and random variable X counts number of acceptable exponents of the form $2^k + 1$ with $1 \leqslant k \leqslant 1023$. Let

$$d = \prod_{p_i \in D} p_i$$

be a fictive RSA exponent. Then we are searching for probability that for a randomly selected prime p, $p - 1$ is coprime to all $s = 2^k + 1$. But this is the same as $\gcd(d, p-1) = 1$. Moreover, as in (1) $p = dl + c,\ \gcd(d, c) = 1$. Thus, for searched probability we have

$$\text{(14)}\qquad \text{Prob}(X = 1023) = \frac{|N_d|^2}{\phi^2(d)} = \prod_{p_i \in D} \Big(1 - \frac{1}{\phi(p_i)}\Big)^2.$$

Using well known tables [1] and [2] it is not difficult (but time consuming!) to calculate this probability. If we assume only all prime divisors $\leqslant 101$, then

$$D^* = \{3, 5, 11, 13, 17, 19, 29, 37, 41, 43, 53, 59, 61, 67, 83, 97, 101\}.$$

Hence

$$\text{Prob}(X = 1023) \leqslant \prod_{p_i \in D^*} \left(1 - \frac{1}{\phi(p_i)}\right)^2 = 0.04875. \tag{15}$$

If we assume that there are another 100 prime divisors, all fairly greater than 101, then

$$\text{Prob}(X = 1023) \geqslant 0.04875 \times 0.99^{100} \approx 0.0178.$$

Thus for practical purposes we can conclude that $Prob(X = 1023)$ is within the range $[0.02, 0.04]$.

An answer to the third problem is probably not trivial. As a result of our experiment we can only say that all secret exponents are within the range of $451 - 567$ ones. The continued fraction algorithm [8] can be used to find RSA secret exponents with up to approximately one-quarter as many bits as the modulus, i.e. up to 256 bits in our case. Thus we may conclude that such an attack is infeasible.

4. Experimental results

Below we list the coincidence of probability (12) in our sample of 100 pairs of primes for $1 \leqslant k \leqslant 10$.

k	Experiment	*Prob*
1	0.25	0.2500
2	0.49	0.5625
3	0.25	0.2500
4	0.90	0.8789
5	0.19	0.2025
6	0.45	0.4727
7	0.25	0.2382
8	0.98	0.9922
9	0.23	0.2244
10	0.49	0.5347

Table 1. Coincidence of probability (12)

In our experiment we had 3 out of 100 pairs of 512 bits primes such that all short exponents s, $s = 2^k + 1$, $1 \leqslant k \leqslant 1023$ were acceptable for them[2]. This is a good fit with our estimation (15). We list them in hexadecimal form together with Means and Standard Errors of number of 1's of t, $st \equiv 1 \pmod{\phi(pq)}$.

```
VAR45
>>>p:  D1206253 2B464083 36A2F8E5 78CF8F31
       F79CA3F9 97B6DB7E 27AC67B3 BB0D798F
       12DF5C99 A8B4A4B0 1D85961A A62034CF
       B4DFA706 73E85FFE 549F2A10 522D170F

>>>q:  D3A86351 9F49618A 48B7E9C6 7F5ADE40
       39C4E6CF 930EC0B7 5FC5E6B1 474AE836
       35B52F12 269E8828 9C6DB381 4C04D89B
       4A5B8DEE D17CE2C0 CDEF102C 64E84F2B
                  Mean =  511.4
       Standard Error =   16.27
.............................................
VAR50
>>>p:  D6CDDC8F 9AD53A59 58CE3D8E 2D9D1937
       73E9F0FC 6F0D80F2 36118D9F 179D9351
       606BD49F 71A3363E 8B322207 C68D4548
       93DA6B4A CEFED921 1F93CCB9 482F1FD3

>>>q:  EA11250F 821ABCBE 2E2441E8 120D411B
       D12C2244 85EE3378 A5CC4107 B2E9A1BD
       FDFBEF79 895F46F3 CD6048C8 01AC41C8
       98762A83 15B65D10 7890C51F 4B5562EB
                  Mean =  511.6
       Standard Error =   15.78
.............................................
```

[2]It is clear that any pair out of 6 found primes can be an RSA modulus.

```
VAR74
>>>p:  D89B3F4B A91F84D3 585D188B BEA062C2
       17950566 87E10F32 861DF519 890112F4
       A8A14169 229FCF1D 68AAE81D A79A3788
       F194D080 7E99A851 9D3AAAE1 5A76C80B

>>>q:  F2035614 00E4EEC8 AF37D8F1 9CF63E84
       6CABEED3 A5E39DBD 46339D18 D3366262
       1B6BE0A6 A5AE83AB 5AD1E262 FA895B8F
       60AC46B8 AF8A744D E3C08318 DBDFF4DF
                  Mean = 510.6
       Standard Error =  15.95
```

To generate and test these 100 pairs of primes we used two computers with Intel Pentium Pro processors, 12 hours each. More details about computers are as follows:

1. Genuine Intel; Type: Single; Family: 6; Model: 1; Stepping: 7; 180MHz Level 1 Cache 16 KB which includes Level 1 Data Cache 8 KB which includes Level 1 Instruction Cache 8 KB Level 2 Unified Cache 256 KB.
2. Genuine Intel; Type: Single; Family: 6; Model: 1; Stepping: 9; 200MHz Level 1 Cache 16 KB which includes Level 1 Data Cache 8 KB which includes Level 1 Instruction Cache 8 KB Level 2 Unified Cache 256 KB.

Acknowledgment. The authors would like to express their gratitude to TimotejJeško from SWH-Siemens Laboratories for his excellent programming job and time spent with one of the authors.

References

[1] J. Brillhart, D. H. Lehmer, J. L. Selfdridge, B. Tuckerman, and S. S. Wagstaff, *Factorizations of* $b^n \pm 1, b = 2, 3, 5, 6, 7, 10, 11, 12$, *up to high powers*, Sec. ed. AMS Publisher, (1995).

[2] ——— ,, *Update 2.9 by S. S. Wagstaff*, Jr., Sept. (1995).

[3] J. Hastad, *On using RSA with low exponent in a public key network*, Lecture Notes in Computer Science, Vol. 218, Springer-Verlag, Berlin, (1986), 403–408.

[4] J. J. Quisquater and C. Couvreur, *Fast decipherment algorithm for RSA public-key cryptosystem*, Electron. Lett., 18 (1982), 905–907.

[5] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public key cryptosystems*, Commun. ACM., **21** (1978), 158–164.

[6] S. A. Vanstone and R. J. Zuccherato, *Short RSA keys and their Generation*, J. of Cryptology, **8** (1995), 101–114.

[7] G. J. Simmons and M. J. Norris, *Preliminary comments on the M.I.T. Public-Key Cryptosystem*, Cryptologia **1** (1977), 406–414.

[8] M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Trans. Information Theory. Vol. IT 36, (1990), 553–558.

Department of Mathematics
Slovak University of Technology
812–19 Bratislava
Slovakia

Institute of Mathematics
Slovak Academy of Sciences
814–73 Bratislava
Slovakia

Department of Mathematics
Slovak University of Technology
812–19 Bratislava
Slovakia

e-mail:
grosek@elf.stuba.sk
nemoga@savba.sk
satko@kmat.elf.stuba.sk