Math. Slovaca, **44** (1994), No. 2, 279–285

Mathematica
Slovaca
©1994
Mathematical Institute
Slovak Academy of Sciences

Dedicated to Academician Štefan Schwarz
on the occasion of his 80th birthday

REMARKS CONCERNING RSA-CRYPTOSYSTEM EXPONENTS

OTOKAR GROŠEK

(Communicated by Štefan Porubský)

ABSTRACT. Two problems associated with RSA-encryption exponents are discussed. Firstly, how many plaintexts are to be read by the Simmons and Norris attack for given exponent and modulus. Secondly, what is the number of exponents belonging to a possible k-attack for given k and modulus. The goal is to find an explicit formula for the cardinality of all encryption exponents with the greatest period in a case when strong pseudoprimes are used.

The *RSA cryptosystem* is a mapping (permutation) $\pi_s \colon S_m \to S_m$, where $S_m = \{0, 1, 2, \dots, m-1\}$ is the multiplicative semigroup of integers modulo m. For any $x \in S_m$, $\pi_s(x) \equiv x^s \mod m$, where $\mathrm{GCD}(s, \phi(m)) = 1$, and ϕ is the Euler ϕ-function. In fact, for $x = 0$ and 1 the cryptosystem is useless. But if 0 and 1 are messages as well, we can use the structure of the semigroup S_m. This semigroup has been described in many papers. We recall only two simple facts:

1. If $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$, then the semigroup S_m contains exactly 2^r idempotents including 0 and 1.

2. To every idempotent $e \in S_m$ there is a unique largest group $G(e)$ (subgroup of S) containing e as its identity element.

Simmons and Norris [9] observed that there exists a very simple attack in some cases, but in those nothing was learned about the factorization of the modulus $m = p \cdot q$. Their attack was based on the fact that in some cases

$$\pi_s^{k+1}(x) = \pi_s\big(\pi_s(\ldots \pi_s(x)) \ldots\big) = x^{s^{k+1}} = x^s = \pi_s(x)\,,$$

AMS Subject Classification (1991): Primary 94A60, 68P25.
Key words: RSA, Encryption exponent.

hence $\pi_s^k(x)$ must have been a plaintext message. This is referred to as a k-attack.

Rivest in [8] formulated the practical requirements to make such situations to be very unlikely: A necessary but not sufficient condition which must be imposed to protect against the kind of weakness illustrated above is to require that $\mathrm{GCD}\big(\phi(p),\phi(q)\big)$ be small and that very large primes divide $\phi(p)$ and $\phi(q)$, respectively. Such primes are called strong primes. More precisely:

A prime p is called *strong* [6] if the following congruences are true:

$$p \equiv 1 \mod r\,, \qquad p \equiv t-1 \mod t\,, \qquad r \equiv 1 \mod j\,.$$

where r, t, j are large random primes, respectively.

How many plaintexts $x \in S$ will be decrypted by a k-iteration process π_s^k for given encryption exponent s? The answer is well known. It is the number of solutions of

$$x^{s^k} = x \quad \text{or} \quad x^{s^{k+1}} = x^s\,, \qquad \text{i.e.} \quad \pi_s^{k+1}(x) = \pi_s(x)\,.$$

All these solutions form a semigroup $Z_k = Z(s^k, 1, p\cdot q)$, and their cardinality is ([1]–[6], [10])

$$|Z_k| = \big[1+\mathrm{GCD}(s^k-1, p-1)\big]\big[1+\mathrm{GCD}(s^k-1, q-1)\big]\,.$$

Clearly, for different k, Z_k might possess the same elements. Now the question is: Using step-by-step $k = 1,2,3,\dots$, how many new cryptograms can we decrypt by k? The answer is given by the two following lemmas.

LEMMA 1.

a) *$Z_l \cap Z_k = Z_d$, where $d = \mathrm{GCD}(l,k)$;*

b) *if $l\,|\,k$, then $Z_l \subset Z_k$.*

Proof.

a) Let x belong to the group $G(f)$, where $f \neq 0$ is one of the three non-zero idempotents of S_m. The equations

$$x^{s^l-1} = f \quad \text{and} \quad x^{s^k-1} = f$$

have common solutions if and only if $\mathrm{GCD}(s^l-1, s^k-1) = s^d-1$ for $d = \mathrm{GCD}(l,k)$.

For b) we have $\mathrm{GCD}(l,k) = l$. Hence $Z_l \cap Z_k = Z_l$, $Z_l \subset Z_k$.

Lemma 2. *Let* $Z_k^* = \{x \mid x = x^{s^k}, \ x^{s^l} \neq x$ *for all* $l < k\}$. *Then*

a) $Z_k^* = Z_k \setminus \bigcup\limits_{d|k,\, d\neq k} Z_d$;

b) $|Z_k^*| = |Z_k| - \left[\sum |Z_d| - \sum |Z_{d_i} \cap Z_{d_j}| + \cdots + (-1)^{\tau(k)-1} |\bigcap Z_d|\right]$, *where the sums run over all* $d \,|\, k$, $d \neq k$ *and* $\tau(k)$ *denotes the number of positive divisors of* k ;

c) *if* $k = p^\alpha$, p *prime, then* $|Z_k^*| = |Z_k| - |Z_{\frac{k}{p}}|$.

Proof. If $x \in Z_k^*$, then $x \notin Z_l$ for any $l < k$, $\mathrm{GCD}(l,k) \neq 1$. Hence $Z_k^* \subset Z_k \setminus \bigcup\limits_{\substack{(l,k)\neq 1\\ l\neq k}} Z_l$. The opposite inclusion is obvious. Hence $Z_k = Z_k^* \setminus \bigcup Z_l \cap Z_k = Z_k \setminus \bigcup\limits_{d|k,\, d\neq k} Z_d$. Now $\bigcup Z_d \subset Z_k$ and $|Z_k^*| = |Z_k| - |\bigcup Z_d|$.

Formula b) is a consequence of elementary set theory.

Formula c) follows from

$$Z_1 \subset Z_p \subset Z_{p^2} \subset \cdots \subset Z_{p^{\alpha-1}},$$

and $\bigcup\limits_{d|k,\, d\neq k} Z_d = Z_{\frac{k}{p}}$.

Remark 1. Let λ denote the Carmichael function defined for $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ by

$$\lambda(m) = \begin{cases} 1 & \text{if } m = 1, \\ 2^{\alpha-2} & \text{if } m = 2^\alpha,\ \alpha > 2, \\ \phi(m) & \text{if } m = 2, 4, p^\alpha \\ & \text{with } p \text{ an odd prime}, \\ \mathrm{LCM}\{\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \ldots, \lambda(p_r^{\alpha_r})\} & \text{in other cases}. \end{cases}$$

Then, using [10; Proposition 6.4], the group of all permutations π_s of S_m is isomorphic with the group of units of $S_{\lambda(m)}$. Hence $\pi_s = \pi_{s+\lambda(m)}$, and the period $\lambda(m)$ cannot be replaced by a smaller number. Moreover, in our special case $m = p \cdot q$, $\pi_s^{\lambda(\lambda(m))} = \mathrm{id}$ for all s, and the exponent $\lambda(\lambda(m))$ cannot be replaced by a smaller one. Hence all k for which $|Z_k^*| \neq 0$ should be divisors of $\lambda(\lambda(m))$.

Example 1. Let $p = 3$, $q = 59$, $s = 17$. Then $\lambda\bigl(\lambda(3 \cdot 59)\bigr) = 28$. and for $k = 1, 2, 4, 7$ and 14, according to Lemmas 1 and 2, we obtain:

$$\begin{aligned}
|Z_1^*| &= |Z_1| = 9\,,\\
|Z_2^*| &= |Z_2| - |Z_1| = 0\,,\\
|Z_4^*| &= |Z_4| - |Z_2| = 168\,,\\
|Z_7^*| &= |Z_7| - |Z_1| = 0\,,\\
|Z_{14}^*| &= |Z_{14}| - \bigl[\,|Z_1| + |Z_2| + |Z_7| - 3 \cdot |Z_1| + |Z_1|\,\bigr] = 0\,.
\end{aligned}$$

As we can see in our simple example, although we have four "candidates" for a possible k-attack, only two are actual possibilities, and clearly $|Z_1^*| + |Z_1^*| = |S_m|$. It is known that the universal deciphering exponent t is the solution of $17 \cdot t \equiv 1 \mod \phi(3 \cdot 59)$, $t = 6$.

Our additional observation is as follows: Given a modulus $m = p \cdot q$ and k, enumerate the number of permutations π_s of order k, i.e. the number of solutions $\pi_s^{k+1} = \pi_s$ or $\pi_s^k = \mathrm{id}$.

As we pointed out in Remark 1, all admissible permutations π_s form a group of units of $S_{\lambda(m)}$. The identity mapping $\mathrm{id}(x) = x$ now plays the role of the unit element 1. Let us denote it by $G_\lambda(1)$. It should be emphasized that $S_{\lambda(m)}$ has a structure more complicated than that of S_m. Following [10] we denote the semigroup of solutions of $\pi_s^{k+1} = \pi_s$ by $\tilde{Z}_k = Z(k+1, 1, p \cdot q, e = 1)$.

Let $\lambda(p \cdot q) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$. Then, from the same article, one can derive the formula for the cardinality of $\tilde{Z}_k$ (another approach is in [1]–[4]):

$$|\tilde{Z}_k| = \delta_1 \cdot \delta_2 \cdot \ldots \cdot \delta_r\,,$$

where

$$\delta_i = \begin{cases} \mathrm{GCD}\bigl(k, \phi(p_i^{\alpha_i})\bigr) & \text{if } p_i \text{ is odd, or } p_i^{\alpha_i} = 2 \text{ or } 4\,,\\ \mathrm{GCD}(k, 2) \cdot \mathrm{GCD}(k, 2^{\alpha-2}) & \text{if } p_i^{\alpha_i} = 2^\alpha\,,\ \ \alpha \ge 3\,. \end{cases}$$

The following illustrates the remarks made above. Now the set $\tilde{Z}_k^*$ plays the same role in $S_{\lambda(m)}$ as Z_k^* in S_m.

Example 2. Using the same modulus $p \cdot q$ as in Example 1, we can compute the number of different permutations, i.e. different π_s "having weakness k". Firstly, $\lambda(p \cdot q) = 58$, $\delta_1 = \mathrm{GCD}(k, 1) = 1$, $\delta_2 = \mathrm{GCD}(k, 28) = 1, 2, 7$ or 28, $|\tilde{Z}_k| = \delta_1 \cdot \delta_2 = \delta_2 = \mathrm{GCD}(k, 28)$.

Now, by Lemma 2, we obtain:

If $k = 1$, then there exists only one – trivial – encryption exponent $s = 1$, $\pi_s^1 = \pi_s$ for all $x \in S_m$. The same result gives our formulae $|\tilde{Z}_1^*| = |\tilde{Z}_1| = 1$.

If $k = 2$, then $|\tilde{Z}_2| = \mathrm{GCD}(2, 28) = 2$ and $|\tilde{Z}_2^*| = |\tilde{Z}_2| - |\tilde{Z}_1| = 1$, which conforms with $s = 57$.

If $k = 4$, then $|\tilde{Z}_4^*| = |\tilde{Z}_4| \setminus |\tilde{Z}_2| = 4 - 2 = 2$, or concretely $s = 17$ and 41.

If $k = 7$, then $|\tilde{Z}_7^*| = |\tilde{Z}_7| - |\tilde{Z}_1| = 7 - 1 = 6$, or $s \in \{7, 23, 25, 45, 49, 53\}$.

Finally, for $k = 14$ we have $|\tilde{Z}_{14}^*| = |\tilde{Z}_{14} \setminus (\tilde{Z}_1 \cup \tilde{Z}_2 \cup \tilde{Z}_7)| = |\tilde{Z}_{14}| - \big(|\tilde{Z}_2| + |\tilde{Z}_7| - |\tilde{Z}_1|\big) = 6$, and, similarly, for $k = 28$ we obtain $|\tilde{Z}_{28}^*| = 12$. In the last two cases, encryption exponents belong to $\{5, 9, 13, 33, 35, 51\}$ or $\{3, 11, 15, 19, 21, 27, 31, 37, 39, 43, 47, 55\}$, respectively. Altogether we have for $m = 3 \cdot 59$

$$\sum_{k|\lambda(\lambda(m))} |\tilde{Z}_k^*| = \phi\big(\lambda(m)\big) = 28\,. \tag{1}$$

Remark 2. It is well known that $\phi(a) = \lambda(a)$ if and only if $a = 2, 4, p_1^\alpha$ or $2p_1^\alpha$ with p_1 an odd prime. Hence, for $a = \lambda(p \cdot q) = \mathrm{LCM}(p-1, q-1)$ we have the following solutions except for commutativity:

If $a = \lambda(p \cdot q) = 2$, then $p = 2$ or 3, $q = 3$;
if $a = \lambda(p \cdot q) = 4$, then $p = 2, 3$ or 5, $q = 5$;
if $a = \lambda(p \cdot q) = 2p_1^\alpha$, then $p = 2, 3$ or $2p_1^\alpha + 1$, $q = 2p_1^\beta + 1$.

The case $a = \lambda(p \cdot q) = p_1^\alpha$ is obviously impossible.

The formula (1) and Remark 2 naturally suggest the use of the Möbius inversion formula ([7]):

THEOREM. *Let the relation* $\phi\big(\lambda(p \cdot q)\big) = \lambda\big(\lambda(p \cdot q)\big)$ *be valid. Then the set of all encryption exponents* s, *i.e.* $\mathrm{GCD}\big(s, \phi(p \cdot q)\big) = 1$ *with the greatest period* $k = \lambda\big(\lambda(p \cdot q)\big)$ *has the cardinality* $|\tilde{Z}_k^*| = \phi\big(\lambda\big(\lambda(p \cdot q)\big)\big)$.

Proof. Recall that the sets $\tilde{Z}_k^*$ are mutually disjoint and the number of all possible s is $\phi\big(\lambda(p \cdot q)\big)$. Hence summands in

$$\sum_{k|\lambda(\lambda(p \cdot q))} |\tilde{Z}_k^*| = \phi\big(\lambda(p \cdot q)\big)$$

represent "functions" of k. On behalf of the assumption $\phi\big(\lambda(p \cdot q)\big) = \lambda\big(\lambda(p \cdot q)\big)$ and by the Möbius formula

$$F(n) = \sum_{k|n} f(k) \iff f(n) = \sum_{k|n} \mu(k) F\Big(\frac{n}{k}\Big)$$

for

$$F = \mathrm{id}\,, \qquad f(k) = |\tilde{Z}_k^*| \qquad \text{and} \qquad n = \lambda\big(\lambda(p \cdot q)\big)\,,$$

we obtain the desired result

$$f(n) = \sum_{k|n} \mu(k) \cdot \frac{n}{k} = \phi(n)\,.$$

Example 3. In case $p = 3$, $q = 2 \cdot 29 + 1 = 59$ discussed above. we have $\phi\big(\lambda(p \cdot q)\big) = \lambda\big(\lambda(p \cdot q)\big) = 28$ and

$$\big|\tilde{Z}^*_{\lambda(\lambda(p \cdot q))}\big| = \phi\big(\lambda\big(\lambda(p \cdot q)\big)\big) = \phi(28) = 12\,.$$

For all such $s \in \tilde{Z}^*_{28} = \{3, 11, \dots, 55\}$, $\pi_s^{28}(x) = x$, and if $x \notin Z_1$, the exponent $k = 28$ cannot be replaced by a smaller one.

COROLLARY 1. *For the pair of primes* $p = 2p_1^\alpha + 1$, $q = 2p_1^\beta + 1$ *with* $\alpha < \beta$ *we have exactly*

$$\big|\tilde{Z}^*_{\lambda(\lambda(p \cdot q))}\big| = \phi\big(\lambda\big(\lambda(p \cdot q)\big)\big) = p_1^{\beta-2} \cdot (p_1 - 1)\phi(p_1 - 1)$$

possible encryption exponents with the greatest "weakness". Hence the ratio of the "best" encryption exponents to all possible ones is $\dfrac{\phi(p_1 - 1)}{p_1}$ *in this case, and if* p *is a strong prime, this ratio is close to* 1.

COROLLARY 2. *Let* $p = 2p_1^\alpha + 1$, $q = 2q_1^\beta + 1$, *and* $\mathrm{GCD}(p_1, q_1) = \mathrm{GCD}(p_1, q_1 - 1) = \mathrm{GCD}(p_1 - 1, q_1) = 1$. *Then*

$$\big|\tilde{Z}^*_{\lambda(\lambda(p \cdot q))}\big| = \phi\big(\lambda\big(\lambda(p \cdot q)\big)\big) \cdot \mathrm{GCD}(p_1 - 1, q_1 - 1)\,.$$

Proof. In this case the relation $\phi\big(\lambda(p \cdot q)\big) = \lambda\big(\lambda(p \cdot q)\big)$ is not valid. but it is not difficult to derive the relation

$$\phi\big(\lambda(p \cdot q)\big) = \lambda\big(\lambda(p \cdot q)\big) \cdot \mathrm{GCD}(p_1 - 1, q_1 - 1)\,.$$

Again the ratio of the best encryption exponents to all possible ones in this case is

$$\frac{\phi\big(\lambda\big(\lambda(p \cdot q)\big)\big)}{\phi\big(\lambda(p \cdot q)\big)} = \frac{\phi\big(\mathrm{LCM}(p_1 - 1, q_1 - 1)\big)}{p_1 \cdot q_1}\,.$$

REFERENCES

[1] BLAKELY, B.—BLAKELY, G. R.: *Security of number theoretic public key cryptosystems against random attack I*, Cryptologia **2** (1978), 305–321.

[2] BLAKELY, B.—BLAKELY, G. R.: *Security of number theoretic public key cryptosystems against random attack II*, Cryptologia **3** (1979), 29–42.

[3] BLAKELY, B.—BLAKELY, G. R.: *Security of number theoretic public key cryptosystems against random attack*, Cryptologia **3** (1979), 105–118.

[4] BLAKELY, G. R.—BOROSH, I.: *Rivest-Shamir-Adelman public key cryptosystem do not always conceal messages*, Comput. Math. Appl. **5** (1979), 105–118.

[5] ECKER, A.: *Finite semigroups and the RSA-cryptosystem.* In: Lecture Notes in Comput. Sci. 149, Springer, New York-Berlin, 1983, pp. 353–369.

[6] GORDON, J.: *Strong primes are easy to find.* In: Advances in CRYPTOLOGY, EUROCRYPT'84, Spinger Verlag, Berlin, 1985, pp. 216–223.

[7] NIVEN, I.—ZUCKERMAN, H. S.: *An Introduction to the Theory of Numbers*, John Wiley & Sons Inc., New York, 1972.

[8] RIVEST, R. L.: *Remarks on a proposed cryptanalytic attack on the M.I.T. public-key cryptosystem*, Cryptologia **2** (1978), 62–65.

[9] SIMMONS, G. J.—NORRIS, M. J.: *Preliminary comments on the M.I.T. public-key cryptosystem*, Cryptologia **1** (1977), 406–414.

[10] SCHWARZ, Š.: *The role of semigroups in the elementary theory of numbers*, Math. Slovaca **31** (1981), 369–395.

Received July 31, 1992

Revised December 18, 1992

Department of Mathematics
Slovak Technical University
Ilkovičova 3
SK-812 19 Bratislava
Slovakia
E-mail: grosek@elf.stuba.cs