Development of the Attack against RSA with Low Public Exponent and Related Messages

P. Antonov, V. Antonova

Abstract: *Problems of security of the asymmetric cryptographic algorithm RSA are considered, which might occur when choosing small values of public keys and related plaintexts and a development of the well known in these cases cryptoattack of Franklin-Reiter-Coppersmith is offered.*

Key words: *RSA, low public exponent attack, related messages.*

INTRODUCTION

It is known that during the recent nearly 30 years RSA (Rivest, Shamir, Adleman) is the most popular cipher among the asymmetric cryptographic algorithms (ciphers with public keys), and is widely used for digital signatures and for ciphering of the session secret keys in hybrid cryptographic schemes [1, 2, 3, 4 etc.]. In fact, at present RSA is actually World Standard for cryptography with public keys.

At the generation of the couple *"public/secret"* keys for RSA initially two large enough prime numbers a and b are chosen and after that the product $N = ab$ and Euler's function $\Phi(N) = (a-1)(b-1)$ are calculated. The public key K_P and the secret key K_S are determined by the interrelations:

$\gcd[K_P, \Phi(N)] = 1$ ($\gcd$ – the greatest common divisor) and

$$(K_S K_P) \bmod \Phi(N) = 1. \qquad (1)$$

Further on, in the procedures for ciphering and deciphering, the couples of numbers (K_P, N) and (K_S, N) are used, the first couple being made public attribute, K_S is kept in secret, and the initial prime numbers a and b are destroyed.

When ciphering an plaintext $M = (M_1 M_2 ... M_J ...)$ each block E_J of the ciphertext E is determined by the relation $E_J = (M_J^{K_P}) \bmod N$, where $(1 < M_J < N)$, and when deciphering - the corresponding block M_J of the plaintext is restored by the formula $M_J = (E_J^{K_S}) \bmod N$.

Since the moment of its creation in 1977 year and up to now RSA is continuously subjected to crypto-analysis aiming at detecting defects [2, 3, 4, 5, 6 etc.]. Many crypto-attacks have been developed in this direction but no serious defects of the cipher have been found, as these cryptoattacks are successful only in certain specific conditions. Regardless of all that, however, such developments are of great significance, as on their basis recommendations are formulated to avoid the conditions for successful crypto-attacks, which leads to higher security in RSA realizations.

In connection with this, in the present paper we offer development of one of the known cryptoattacks of RSA – the attack of *Franklin-Reiter-Coppersmith* [3, 4, 5, 6, 10 etc.], taking place at low public exponent and related plaintexts. It should be noted that in [10] there is given development and generalization of the attack of Franklin-Reiter with the usage of two methods for restoration of the open text [5]: *direct one*, and *one with greatest common divisors*. That is why in the present paper this generalization is referred to as attack of *Franklin-Reiter-Coppersmith* with two different methods for restoration, and the development offered concerns the variant of this attack with direct restoration of the plaintext.

DESCRIPTION OF THE PROBLEM

It is known that the difficulties in practical realization of RSA are related to finding the initial large primes a and b, to the necessity of integer arithmetic for multifigured numbers, and to determination of the couples *"public/secret"* keys.

In fact, the practical finding of keys K_P and K_S in correspondence with the necessary conditions (1) is a slow process, which involves the realization of a great number of checks. As there is no special requirements about the magnitude of K_P and K_S, in order to speed up the procedures for choosing keys and for ciphering/deciphering, it is advisable that they are small numbers. For example, the standard PEM (Privacy Enhanced Mail) for protected e-mail in Internet recommends for public keys K_P to be chosen the number 3, and recommendation X.509 of ITU-T – the number 65537=(2^{16} + 1).

It should be noted, however, that choosing the number 3 and other small numbers for public keys K_P might be dangerous, as for these cases cryptoattacks [2, 3, 4, 5, 6, 7, 8, 9, 10 etc.] are well known, which under certain circumstances allows easy restoration of M_J. One of these cryptoattacks is the mentioned above attack with related plaintexts of *Franklin-Reiter-Coppersmith*.

In the attack of *Franklin-Reiter* there are used two $(k = 2)$ related plaintexts M_J and $M_{J+1} = (M_J + 1)$ and a public key $K_P = 3$ [3,10 etc.]. If M_J is ciphered and after that M_{J+1} is ciphered, then $E_J = M_J^3 \bmod N$ and $E_{J+1} = M_{J+1}^3 \bmod N = (M_J + 1)^3 \bmod N$.

At that condition, if the offender knows E_J and E_{J+1}, then M_J can be easily found from the interrelation

$$\frac{E_{J+1} + 2E_J - 1}{E_{J+1} - E_J + 2} = \frac{(3M_J^2 + 3M_J + 3)M_J}{3M_J^2 + 3M_J + 3} = M_J \bmod N. \qquad (2)$$

This attack is generalized for M_J and $M_{Jc+d} = (cM_J + d)$, supposing that c and d are known. In this case $E_J = M_J^3 \bmod N$, $E_{Jc+d} = (cM_J + d)^3 \bmod N$ and it can be shown [10], that

$$\frac{(E_{Jc+d} + 2c^3E_J - d^3)d}{(E_{Jc+d} - c^3E_J + 2d^3)c} = \frac{(3c^2M_J^2d + 3cM_Jd^2 + 3d^3)cM_J}{(3c^2M_J^2d + 3cM_Jd^2 + 3d^3)c} = M_J \bmod N. \qquad (3)$$

In [10] a development is also made for $K_P = 5$, but only with related plaintexts M_J and $M_{J+1} = (M_J + 1)$. In this case $E_J = M_J^5 \bmod N$ and $E_{J+1} = (M_J + 1)^5 \bmod N$, and for the restoration of the plaintext M_J the following interrelations [10] can be used:

$$\begin{aligned} P &= E_{J+1}^3 - 3E_JE_{J+1}^2 + 3E_J^2E_{J+1} - E_J^3 + 37E_{J+1}^2 + 176E_JE_{J+1} + 37E_J^2 + \\ &+ 73E_{J+1} - 73E_J + 14 \\ M_JP &= 2E_{J+1}^3 - E_JE_{J+1}^2 - 4E_J^2E_{J+1} + 3E_J^3 + 14E_{J+1}^2 - 88E_JE_{J+1} - 51E_J^2 - \\ &- 9E_{J+1} + 64E_J - 7, \end{aligned} \qquad (4)$$

from where $\frac{M_JP}{P} = M_J \bmod N$.

It is evident that the interrelations (4) are considerably more complex than (2), which

means that the direct restoration of the plaintext M_J when increasing the values of public keys becomes considerably more difficult.

The generalization mentioned above (for M_J and M_{Jc+d}) and development (for $K_P = 5$) of the attack of *Franklin-Reiter*, is referred to in the present paper as *attack of Franklin-Reiter-Coppersmith with direct method for restoration of the open text*.

In [10] also is offered generalization for arbitrary small values of public keys, where for the restoration of the open texts biggest common divisors are used. That is why this variant can be specified as *attack of Franklin-Reiter-Coppersmith for restoration of the plaintext with greatest common divisors*.

Further on in this paper we present several variants of development of the first formulated variant of the *attack of Franklin-Reiter-Coppersmith – with direct method for restoration of the plaintext.*

VARIANTS OF DEVELOPMENT OF THE ATTACK FRANKLIN-REITER-COPPERSMITH

- ***The first variant*** is a development of the attack for $K_P = 5$, but using 3 $(k = 3)$ related plaintexts: M_J, $M_{J-1} = (M_J - 1)$ and $M_{J+1} = (M_J + 1)$. In this case, if initially an block M_J is ciphered, and after that $(M_J - 1)$ and $(M_J + 1)$ with public key $K_P = 5$, then

$$\begin{aligned} E_J &= M_J^5 \bmod N \\ E_{J-1} &= (M_J - 1)^5 \bmod N = (M_J^5 - 5M_J^4 + 10M_J^3 - 10M_J^2 + 5M_J - 1) \bmod N \text{ and} \\ E_{J+1} &= (M_J + 1)^5 \bmod N = (M_J^5 + 5M_J^4 + 10M_J^3 + 10M_J^2 + 5M_J + 1) \bmod N . \end{aligned} \quad (5)$$

It can be shown that if the offender knows the ciphered blocks E_J, E_{J-1} and E_{J+1}, then M_J can be easily calculated from the following interrelation

$$\frac{E_{J+1} + E_{J-1} + 8E_J}{E_{J+1} - E_{J-1} + 8} = \frac{(10M_J^4 + 20M_J^2 + 10)M_J}{10M_J^4 + 20M_J^2 + 10} = M_J \bmod N. \quad (6)$$

It can be seen that the interrelation (6) found out for that case is considerably more simple than the given in [10] interrelation (4). Besides it is possible to make generalization, which is considered as following second variant of the development of the cryptoattack.

- ***The second variant*** is generalization of the case above for $K_P = 5$, but with related plaintexts M_J, $M_{Jc-d} = (cM_J - d)$ and $M_{Jc+d} = (cM_J + d)$. Then

$$\begin{aligned} &E_J = M_J^5 \bmod N, \\ &E_{Jc-d} = (cM_J - d)^5 \bmod N = \\ &= (c^5M_J^5 - 5c^4M_J^4d + 10c^3M_J^3d^2 - 10c^2M_J^2d^3 + 5cM_Jd^4 - d^5) \bmod N, \\ &E_{Jc+d} = (cM_J + d)^5 \bmod N = \\ &= (c^5M_J^5 + 5c^4M_J^4d + 10c^3M_J^3d^2 + 10c^2M_J^2d^3 + 5cM_Jd^4 + d^5) \bmod N, \end{aligned} \quad (7)$$

and for known ciphertexts E_J, E_{Jc-d} and E_{Jc+d}, the plaintext M_J is restored simply from the following derived formula

$$\frac{(E_{Jc+d} + E_{Jc-d} + 8c^5 E_J)d}{(E_{Jc+d} - E_{Jc-d} + 8d^5)c} = \frac{(10c^4 M_J^4 d + 20c^2 M_J^2 d^3 + 10d^5)cM_J}{(10c^4 M_J^4 d + 20c^2 M_J^2 d^3 + 10d^5)c} = M_J \bmod N. \qquad (8)$$

- ***The third variant*** is an attempt for development of the first variant, but for $K_P = 7$. If the given above first variant of the cryptoattack for $K_P = 5$ is developed for $K_P = 7$, then

$$E_J = M_J^7 \bmod N,\ E_{J-1} = (M_J - 1)^7 \bmod N \text{ and } E_{J+1} = (M_J + 1)^7 \bmod N. \qquad (9)$$

For that case, however, was derived only the following interrelation (10), analogical to (6):

$$\frac{E_{J+1} + E_{J-1} + 12E_J}{E_{J+1} - E_{J-1} + 12} = \frac{(14M_J^6 + 42M_J^4 + 70M_J^2 + 14)M_J}{14M_J^6 + 70M_J^4 + 42M_J^2 + 14} \neq M_J \bmod N, \qquad (10)$$

from which it can be seen that, due to the different coefficients in front of M_J^4 and M_J^2, the block M_J of the plaintext cannot be directly restored. From here we can only draw the supposition that the public key $K_P = 7$ might be resistible against such attack with 3 related plaintexts M_J, $M_{J-1} = (M_J - 1)$ and $M_{J+1} = (M_J + 1)$. It is logical to spread this supposition upon the generalized case M_J, $M_{Jc-d} = (cM_J - d)$ and $M_{Jc+d} = (cM_J + d)$.

- ***The fourth variant*** is development of the initial cryptoattack of *Franklin-Reiter*, where it is supposed that the raised to power $K_P = 3$ values of the related blocks for ciphering are smaller than N, i.e.

$$E_J = M_J^3 \bmod N = M_J^3 \text{ and } E_{J+1} = (M_J + 1)^3 \bmod N = (M_J + 1)^3, \qquad (11)$$

which is not true in the general case. That is why in the present variant we consider a possible situation, at which the interrelation (11) is fulfilled only for the plaintext M_J.

Let M_J and $M_{J+1} = (M_J + 1)$ are ciphered with public key $K_P = 3$ and let also $M_J^3 < N$, and $M_{J+1}^3 = (M_J + 1)^3 > N$. Then

$$E_J = M_J^3 \bmod N = M_J^3 \quad \text{and} \quad E_{J+1} = (M_J + 1)^3 \bmod N = (M_J + 1)^3 - GN, \qquad (12)$$

where G is the quotient of the division of $(M_J + 1)^3$ by N.

As $M_J^3 < N$, $(M_J + 1)^3 = (M_J^3 + 3M_J^2 + 3M_J + 1)$ and for $M_J \geq 4$ the inequality $M_J^3 > (3M_J^2 + 3M_J + 1)$ is true, then

$$N < M_{J+1}^3 = (M_J + 1)^3 < 2N, \quad G = 1 \quad \text{and} \quad E_{J+1} = (M_J + 1)^3 - N. \qquad (13)$$

At that, if E_J and E_{J+1}, are known, the plaintext M_J can be easily found from the interrelation

$$\frac{E_{J+1}+2E_J-1+N}{E_{J+1}-E_J+2+N}=\frac{(3M_J^2+3M_J+3)M_J}{3M_J^2+3M_J+3}=M_J. \quad (14)$$

- ***The fifth variant*** is generalization of the fourth variant, considered above for the related plaintexts M_J and $M_{J+d}=(M_J+d)$. It is supposed that the difference d, is known, $M_J^3<N$ and $M_{J+d}^3=(M_J+d)^3>N$. It can be shown that if at this $(d\le 0.25M_J)$, then

$$N<M_{J+d}^3=(M_J+d)^3<2N,\ G=1 \text{ and } E_{J+d}=(M_J+d)^3-N. \quad (15)$$

By analogy to the variant before, if the offender knows E_J and E_{J+d}, the plaintext M_J can be easily restored from the interrelation (16), which is derived as generalization of (14)

$$\frac{(E_{J+d}+2E_J-d^3+N)d}{E_{J+d}-E_J+2d^3+N}=\frac{(3M_J^2d+3M_Jd^2+3d^3)M_J}{3M_J^2d+3M_Jd^2+3d^3}=M_J. \quad (16)$$

- ***The sixth variant*** represented is development of the first variant of the attack for $K_P=5$, but for the case $M_{J-1}^5=(M_J-1)^5<N$, $M_J^5<N$ and $M_{J+1}^5=(M_J+1)^5>N$. Then

$$E_{J-1}=(M_J-1)^5 \bmod N=(M_J-1)^5,\ E_J=M_J^5 \bmod N=M_J^5 \text{ and}$$
$$E_{J+1}=(M_J+1)^5 \bmod N=(M_J+1)^5-GN, \quad (17)$$

where G is the quotient of the division of $(M_J+1)^5$ by N.

As $M_J^5<N$, and $(M_J+1)^5>N$, and for $M_J\ge 7$ the inequality $M_J^5>(5M_J^4+10M_J^3+10M_J^2+5M_J+1)$ is true, then

$$N<M_{J+1}^5=(M_J+1)^5<2N,\ G=1 \text{ and } E_{J+1}=(M_J+1)^5-N. \quad (18)$$

It can be shown that if the ciphered blocks E_J, E_{J-1} and E_{J+1} are known, then M_J can be easily found from the interrelation

$$\frac{E_{J+1}+E_{J-1}+8E_J+N}{E_{J+1}-E_{J-1}+8+N}=\frac{(10M_J^4+20M_J^2+10)M_J}{10M_J^4+20M_J^2+10}=M_J. \quad (19)$$

- ***The seventh variant*** is generalization of the foregoing sixth variant for $K_P=5$, but for an arbitrary difference d between the related plaintexts. Besides $M_{J-d}^5=(M_J-d)^5<N$, $M_J^5<N$ and $M_{J+d}^5=(M_J+d)^5>N$. Then if the ciphered blocks E_J, E_{J-d} and E_{J+d} are known, M_J can be determined by the interrelation

$$\frac{(E_{J+d}-E_{J-d}+8E_J+N)d}{E_{J+d}-E_{J-d}+8d^5+N}=M_J. \quad (20)$$

- ***The eighth variant*** considers the general case when the raised to power K_P values of the related blocks for ciphering are greater than N.

Let us look at the variant of the attack with two related plaintexts M_J and $M_{J+1} = (M_J + 1)$ and a public key $K_P = 3$. Let, in addition to that, the inequalities $M_J^3 > N$ and $M_{J+1}^3 = (M_J + 1)^3 > N$ be true. Then we can write the following interrelations about the corresponding ciphertexts E_J and E_{J+1}:

$$E_J = M_J^3 \bmod N = M_J^3 - QN \text{ and } E_{J+1} = (M_J + 1)^3 \bmod N = (M_J + 1)^3 - GN, \quad (21)$$

from where $E_J + QN = M_J^3 = E_J^*$ and $E_{J+1} + GN = (M_J + 1)^3 = E_{J+1}^*$. (22)

Further on, if instead of the actual ciphertexts E_J and E_{J+1} we use the introduced in (22) modified ciphertexts E_J^* and E_{J+1}^*, then the formula (2) can be written in the following way:

$$\frac{E_{J+1}^* + 2E_J^* - 1}{E_{J+1}^* - E_J^* + 2} = M_J = \frac{E_{J+1} + 2E_J - 1 + N(G + 2Q)}{E_{J+1} - E_J + 2 + N(G - Q)}. \quad (23)$$

It can be seen that for the restoration of the plaintext M_J it is necessary to determine the modified ciphertexts E_J^* and E_{J+1}^* first, or the unknown values of Q and G to be found. The only possibility here is to use supposition, beginning with $Q = 1$.

Let us consider the following simple example of RSA: $N = 33$, $K_P = 3$ and $K_S = 7$. Let also $M_J = 4$ and $M_{J+1} = (M_J + 1) = 5$. At that,

$$E_J = 4^3 \bmod 33 = 31 = 64 - 1.33 \text{ and } E_{J+1} = 5^3 \bmod 33 = 26 = 125 - 3.33, \quad (24)$$

where $Q = 1$ and $G = 3$. In this case the offender knows only: $N = 33$, $K_P = 3$, $E_J = 31$ and $E_{J+1} = 26$. Then, using interrelation (23) (after several suppositions for Q and G), we come to the solution we were after, and at that the division leaves no remainder:

$$\frac{E_{J+1} + 2E_J - 1 + N(G + 2Q)}{E_{J+1} - E_J + 2 + N(G - Q)} = M_J = \frac{26 + 2.31 - 1 + 33(3 + 2.1)}{26 - 31 + 2 + 33(3 - 1)} = \frac{252}{63} = 4. \quad (25)$$

It is evident that the possible number of suppositions for Q and G will define the mean time necessary to find the solution for M_J. On its behalf, this number of suppositions will depend on the difference $(G - Q)$. To determine this difference, from the interrelation (21) we get:

$$E_{J+1} - E_J = \Delta = 3M_J^2 + 3M_J + 1 - N(G - Q) \quad \text{and} \quad (26)$$

$$(G - Q) = (3M_J^2 + 3M_J + 1 - \Delta)/N = D_{K_P=3}. \quad (27)$$

If we apply interrelation (27) to the discussed above example of RSA, then for the difference we get $(G - Q) = 2$ and the first possible supposition $Q = 1$ and $G = 3$ will lead us to the solution we seek. The problem is, however, in the fact that the difference $(G - Q)$ is not known in advance as it depends on the unknown plaintext M_J.

It can be seen that for greater security against the present eighth variant of the cryptoattack with related plaintexts, the difference $(G-Q)$ must be as large as possible, which requires blocks M_J to be close to N. In the limiting case $M_J \to N$ and $(G-Q) \to (3N+4) \cong 3N$, at which the number of the suppositions for Q and G will tend to maximum.

In conclusion we shall also consider the first presented in this paper variant of development of the attack of *Franklin-Reiter-Coppersmith* for $K_P = 5$ and 3 related plaintexts, but provided that $M_{J-1}^5 = (M_J - 1)^5 > N$, $M_J^5 > N$ and $M_{J+1}^5 = (M_J + 1)^5 > N$. In this case interrelation (6) can be written in the following way:

$$\frac{(M_J+1)^5 - GN + (M_J-1)^5 - FN + 8(M_J^5 - QN)}{(M_J+1)^5 - GN - (M_J-1)^5 + FN + 8} = M_J = \\ = \frac{10M_J^5 + 20M_J^3 + 10M_J - N(G+F+8Q)}{10M_J^4 + 20M_J^2 + 10 - N(G-F)}. \quad (28)$$

In this situation, for the receipt of maximum security the difference $(G-F)$ must be as large as possible. It can be shown that

$$(G-F) = (5M_J^4 + 20M_J^2 + 2 - \Delta)/N = D_{K_P=5}, \quad \text{where } \Delta = (E_{J+1} - E_{J-1}). \quad (29)$$

It can be seen that in this case the blocks M_J must be close to N too. For that purpose it is necessary to mix up the small blocks for ciphering M_J beforehand with official blocks of random choice (random padding), which have values close to N. In the limiting case $M_J \to N$ and $(G-F) \to (5N^3 + 20N + 1) \cong 5N^3$, due to which the number of suppositions for F, Q and G will tend to maximum. The dominating conclusion is that the security against such an attack for $K_P = 5$ is many times higher in comparison with $K_P = 3$. If $M_J \to N$ then $\max\Delta \cong M_J$ and

$$\frac{D_{K_P=5}}{D_{K_P=3}} = D \cong \frac{(5M_J^4 + 20M_J^2 - M_J)}{3M_J^2 + 2M_J} \cong \frac{5}{3}M_J^2. \quad (30)$$

CONCLUSIONS

The variants of development of the attack of *Franklin-Reiter-Coppersmith* represented in this paper confirm the conclusions about possible problems with the security of RSA with low public exponent. To neutralize these problems, the small blocks M_J of the plaintext can be mixed up in advance with arbitrary blocks (random padding) [2,4,5,9,10 etc.]. At that, the dimensions of the resulting blocks must be close to N, as otherwise the presented in this paper fourth, fifth, sixth, and seventh variants of the attack may occur to be successful. Regardless of this possibility, however, for greater security of RSA, it is advisable to avoid the usage of numbers 3 and 5 for public keys, as larger values of K_P guarantee higher security against the eighth variant of development of the attack.

REFERENCES

[1] П. Ц. Антонов, С. В. Малчев. Криптография в компютърните комуникации. - Варна, 2000. - 315 с.

[2] B. Schneier. Applied Cryptography: Protocols, Algorithms and Source Code in C. - John Wiley & Sons, 1996. - 758 p.

[3] S. Goldwasser, M. Bellare. Lecture Notes on Cryptography. - Cambridge, Massachusetts Institute of Technology, 1997. - 194 p.

[4] C. Frederico Cid. Cryptanalysis of RSA: A Servey. – SANS Institute 2003. http://www. sans.org/reading_rom/whitepapers/vpns/1006php]

[5] I. K. Salah, A. Darwish, S. Oqeili. Mathematical Attacks on RSA Cryptosystem. – Journal of Computer Science 2(8), 2006. – pp. 665 – 671.

[6] D. R. L. Brown. Breaking RSA may be as Difficult as Factoring. – Certicom Research, April 12, 2006. [http://eprint.iacr.org/2005/380pdf]

[7] P. Fonque, S. Kunz-Jacques, G. Martinet, F. Muller, F. Valette. Power Attack on Small RSA Public Exponent from Partial Information. – October 13, 2006. [http://security.ece. orst.edu/ches2006/Presentations%20Fonque.pdf]

[8] O. Regev. Attack on RSA with Low Public Exponent. – Lattices in Computer Science, Tel Aviv University, 2004.
[http://www.cs.tau.ac.il/~odedr/teching/lattices_fdl_2004/ ln/rsa.pdf]

[9] J. Dyer. Lattice Reduction on Low-Exponent RSA. – August 2002. [http://math.arisona. edu/~ura/022/McCallum_group/DyerFind.pdf]

[10] D. Coppersmith, M. Franklin, J. Patarin, M. Reiter. Low-Exponent RSA with Related Messages. - Advances in Cryptology - EUROCRYPT'96 (Lecture Notes in Computer Science 1070, U. Maurer, Ed. 1996, Springer-Verlag.

ABOUT THE AUTHORS

Assoc. Prof. Dr. Peter T. Antonov, Department of Computer Science and Engineering, Technical University of Varna, 1 Studentska Str., 9010 Varna, Bulgaria, E-mail: peter.antonov@ieee.org

Ass. Prof. Valentina R. Antonova, Department of Computer Science and Engineering, Technical University of Varna, 1 Studentska Str., 9010 Varna, Bulgaria, E-mail:valyvarna@yahoo.com