RSA Private Keys and the Presence of Weak Keys: An Evaluation

Mahmoud M. Almazari[a], Eyad S. Taqieddin[a], Ahmed S. Shatnawi[b] and Zakarea AlShara[b]

[a]Department of Network Engineering and Security, Jordan University of Science and Technology, Irbid, 21110, Jordan.
[b]Department of Software Engineering, Jordan University of Science and Technology, Irbid, 21110, Jordan.

ARTICLE INFO

Keywords:
RSA Attacks
Two Private Keys
Universal RSA Key
RSA Factorization
Weak RSA Keys
RSA FIPS Conditions

ABSTRACT

Numerous applications that rely on assymmetric cryptography use the RSA algorithm. It can be applied to digital signatures and the encryption of sensitive data. The secure storage of the private key is essential for the algorithm's strength. Finding ways to use factorization or other heuristics to determine the value of the private key was the goal of several academic efforts. The Euler totient or the Carmichael functions are both used in this study to analyze the private key properties and demonstrate the existence of many private keys for the same public key. We further demonstrate that a universal key that complies with the FIPS standard exists. Moreover, by taking advantage of a condition imposed by FIPS recommendations, we present a new method for attacking the RSA modulus (N). The attack is based on the value of the private key being greater than $2^{n/2}$ with n representing the modulus size.

1. Introduction

The RSA encryption algorithm was invented by by Ron Rivest, Adi Shamir, and Len Adleman as an asymmetric cipher to deliver privacy and authenticity of messages (Rivest, Shamir, and Adleman, 1978). It is widely used for electronic payments, secure e-mail, and other web traffic requiring secure data transfer. The algorithm is based on number theory in its core with a straightforward procedure as listed below

1. Two large prime numbers, p and q, are chosen to compute the RSA modulus $N = p \cdot q$
2. Compute the Euler totient function, which represent the order of the multiplicative group Z_N^*, as $\phi(n) = (p-1) \cdot (q-1)$
3. Choose a value of e, the encryption exponent, that is relatively prime to $\phi(N)$ and use it to compute d, the decryption exponent, such that $e \cdot d \equiv 1 \mod \phi(N)$

Note that any integer d that is coprime with the Euler totient function and satisfies the condition $\frac{de-1}{\phi(n)} = k$ where k is an integer, is considered a private key. The pair (N, e) is used as the public key and the value of d must be secretly stored. To encrypt a message, M, we use the public key to compute the cipher message, C, as $C = M^e \mod N$. Decryption is done in the reverse by computing $M = C^d \mod N$. One possible attack against RSA is to factorize N to p and q and then run the steps above. However, factorization itself was shown to run in exponential or sub-exponential time. This paper covers multiple contributions. We first present an analysis of the private key and prove the existence of more than just two keys as has been presented in (Ibrishimova, 2017). Therefore demonstrating that this holds true for both implementations of the Charmichael function and the Euler totient function. We also show that RSA has a universal key as well as a set of weak keys. Finally, we present an attack to factor N when specific conditions are satisfied.

2. The First Set of Private Keys

Referring to (1), if we take d_1 as the private key for some $k_1 = \alpha$, we can find another private key, d_2 using a second integer $k_2 = \alpha + e$ for some integer $e \in \mathbb{N}$. In other words, the second private key in the first set of the private keys will be

$$d_2 = \frac{(\alpha + e).\phi(n) + 1}{e} \tag{1}$$

*Mahmoud M. Almazari

mmalmazari16@cit.just.edu.jo (M.M. Almazari); eyadtaq@just.edu.jo (E.S. Taqieddin); ahmedshatnawi@just.edu.jo (A.S. Shatnawi); zmalshara@just.edu.jo (Z. AlShara)

Corollary 2.0.1. *The first set of the private keys, denoted as d_x, for a given public key (n, e), is:*

$$d_x = \frac{(\alpha + X.e).\phi(n) + 1}{e} \tag{2}$$

Proof:

$$d_x = \frac{\alpha.\phi(n) + X.e.\phi(n) + 1}{e} = \frac{X.e.\phi(n)}{e} + \frac{\alpha.\phi(n) + 1}{e} = \frac{X.\phi(n)}{1} + \frac{\alpha.\phi(n) + 1}{e}$$

The second part of the sum is d_1, thus $d_x = X.\phi(n) + d_1, \forall X \in \mathbb{N}$. Accordingly, the distance between any two successive keys in the first set is $\phi(n)$. Next, we show that the key d_X is a valid key that can be used to decrypt the ciphertext C to yield the plaintext (M).

$$C^{d_X} \mod N$$
$$C^{(X.\phi(n)+d_1)} \mod N$$
$$((C^{X.\phi(n)} \mod N) * (C^{d_1} \mod N)) \mod N$$
$$((1) * (C^{d_1} \mod N)) \mod N = M$$

According to Euler's Theorem, the first term in the multiplication reduces to 1. Note that $(C^{d_1} \mod N)$ yields M, according to the RSA algorithm presented in 1.

3. The Existence of A Second Set of Private Keys

The Carmichael function, as opposed to the Euler totient function, is used in present-day implementations of the PKCS#1 standard. The Carmichael function allows for the generation of a private key that is both unique and of the shortest possible size. In this section, we demonstrate the impact of the Carmichael function and the conditions in which a second private key that is not part of the first set of private keys will exist. In addition, we'll talk about the conditions under which a second private key will exist.

Theorem 3.1. *Euler's totient theorem states that if gcd(n, a) = 1, n and a are positive integers then, $a^{\phi(n)} \equiv 1 \pmod{n}$ Also, using the reduced totient function (Carmichael function) $a^{\lambda(n)} \equiv 1 \pmod{n}$*

Theorem 3.2. *The unique factorization theorem states that every positive integer $(n \geq 2)$ can be represented in exactly and only one way as a product of prime powers:*

$$n = \prod_{i=1}^{k} p_i^{n_i}$$

where $p_1 < p_2 < \cdots < p_k$ are primes and the n_i are positive integers.

Referring to 3.2, $\lambda(n) = \alpha_1^{\beta_1} \times \alpha_2^{\beta_2} \times \alpha_3^{\beta_3} \times \cdots$. Let δ be an integer such that $\delta = \gamma_1^{v_1} \times \gamma_2^{v_2} \times \gamma_3^{v_3} \cdots$, where γ_x could be equal to α_x. Then

$$a^{\delta.\lambda(n)} \equiv 1 \pmod{n}$$
$$(a^{\lambda(n)} \mod n)^{\delta} = 1^{\delta} = 1$$

The Carmichael function is equal to the least common multiple of $(p-1)$ and $(q-1)$, due to the fact that p and q are odd numbers, then one of the common factors of $p-1$ and $q-1$ is 2 (i.e. GCD$(p-1, q-1) \geq 2$, and $\delta \geq 2$). As a consequence $\phi(n) \neq \lambda(n)$. However, for a private key computed as $d_1 = e^{-1} \mod \phi(n)$ and another private key $d_2 = e^{-1} \mod \lambda(n)$, where $\lambda(n) = \phi(n)/gcd(p-1, q-1)$ then, there is a possibility that $d_1 \neq d_2$ which yields in generating a new set of private keys, d_y, and the existence of a second private key. However, there are some conditions where some keys in the set d_x will be equal to a key in the set d_y, as we present next.

Theorem 3.3. *Based on Euler theorem and RSA:*

$$d_x \times e - \alpha \times \phi(n) = 1$$

and the second set will be

$$d_y \times e - \beta \times \frac{\phi(n)}{gcd(p-1, q-1)} = 1$$

Now, if $gcd(p-1, q-1)|\beta$ then $d_x \equiv d_y$. In other words, if β and $gcd(p-1, q-1)$ are relatively prime, then $d_x \neq d_y$.

Corollary 3.3.1. *The second set of the private keys will be*

$$d_y = \frac{(\beta + X.e).\lambda(n) + 1}{e}, \textbf{\textit{ and }} \beta = \frac{d_{y_0} \times e - 1}{\lambda(n)} \tag{3}$$

With a proof similar to that in section 1, it can be shown that the distance between any two successive keys in the second set is $\lambda(n)$. One interesting observation is that there is no strict relation between α in the first set of the private keys and β in the second. However, if $d_x \equiv d_y$ then

$$\beta = gcd(p-1, q-1) \times \alpha \tag{4}$$

where α is calculated based on totient function, and β is calculated based on the reduced totient function, as shown earlier. We illustrate this with a couple of examples.

Example 1:
$q = 100049$, $p = 465947$, $e = 1303$ Then, $\lambda(n) = 1792960208$ and $\phi(n) = 46616965408$.
The private key using $\phi(n)$, $d = 24471223591$ and the private key using $\lambda(n)$, $d = 1162740887$

Example 2:
$q = 100019$, $p = 465989$, $e = 1303$ Then, $\lambda(n) = 23303593892$ and $\phi(n) = 46607187784$
The private key using $\phi(n)$, $d = 3219222487$ and the private key using $\lambda(n)$, $d = 3219222487$

In the first example, it is clear that the two keys are not equal. This is further supported by the fact that the values of $\alpha = 684$ and $\beta = 845$ with the $gcd(p-1, q-1) = 26$ do not hold in Eqn. (4). Nevertheless, in the second example, the two keys are equal. Note that $\alpha = 90$ and $\beta = 180$ with the $gcd(p-1, q-1) = 2$ which satisfy Eqn. (4). The equality between the keys in the two sets is not necessarily dependent on their position in the set. A key in the set d_x at position i can equal a key in d_y at position j, where $i \neq j$, according to Eqn. (4). The question becomes, how do we determine the values of i and j to relate these two set together?

Considering the distance between the first keys in both sets, (d_x) and (d_y),

$$d_{x_0} - d_{y_0} = \frac{\alpha \times gcd(p-1, q-1) \times \lambda(n) + 1}{e} - \frac{\beta \times \lambda(n) + 1}{e} = \frac{\lambda(n)}{e} \times (\alpha.gcd(p-1, q-1) - \beta)$$

and because $\lambda(n)$ and e are relatively prime and $d_{x_0} - d_{y_0}$ is integer, then $e \mid (\alpha.gcd(p-1, q-1) - \beta)$. As a result,

$$dx_i - dy_i = \frac{\lambda(n) \times w \times e}{e} = \lambda(n) \times w$$

where $w = (\alpha.gcd(p-1, q-1) - \beta)/e$ is some positive integer value that represents the number of keys needed to be passed in the second set to find a key that is equal to the first key in the first set. In other words, $dy_w = dx_0$. Recall that the keys at position v in the two sets are:

$$dx_v = \frac{(\alpha + v.e).\phi(n) + 1}{e}$$

$$dy_v = \frac{(\beta + v.e).\lambda(n) + 1}{e}$$

Then,

$$\frac{d_{x_v} - d_{y_v}}{\lambda(n)} = (gcd(p-1, q-1) - 1) \times v + w$$

$$w = \frac{\alpha \times gcd(p-1, q-1) - \beta}{e}$$

To illustrate the point in the following example.

Example 3:
$q = 100213$, $p = 465781$, $e = 1303$. We compute $\lambda(n) = 555675540$, $\phi(n) = 46676745360$, $\alpha = 700$, $\beta = 165$, and $gcd(p-1, q-1) = 84$. Thus, $w = 45$. The calculations can be seen in the two following sets of keys.

$dx_0 = 25075764967$	$dy_0 = 70365667$	$dx_1 = 71752510327$	$dy_1 = 626041207$
$dx_2 = 118429255687$	$dy_2 = 1181716747$	$dx_3 = 165106001047$	$dy_3 = 1737392287$
$dx_4 = 211782746407$	$dy_4 = 2293067827$	$dx_5 = 258459491767$	$dy_5 = 2848743367$
$dx_6 = 305136237127$	$dy_6 = 3404418907$	$dx_7 = 351812982487$	$dy_7 = 3960094447$
$dx_8 = 398489727847$	$dy_8 = 4515769987$	$dx_9 = 445166473207$	$dy_9 = 5071445527$
$dx_{10} = 491843218567$	$dy_{10} = 5627121067$	$dx_{11} = 538519963927$	$dy_{11} = 6182796607$
$dx_{12} = 585196709287$	$dy_{12} = 6738472147$	$dx_{13} = 631873454647$	$dy_{13} = 7294147687$
$dx_{14} = 678550200007$	$dy_{14} = 7849823227$	$dx_{15} = 725226945367$	$dy_{15} = 8405498767$
$dx_{16} = 771903690727$	$dy_{16} = 8961174307$	$dx_{17} = 818580436087$	$dy_{17} = 9516849847$
$dx_{18} = 865257181447$	$dy_{18} = 10072525387$	$dx_{19} = 911933926807$	$dy_{19} = 10628200927$
$dx_{20} = 958610672167$	$dy_{20} = 11183876467$	$dx_{21} = 1005287417527$	$dy_{21} = 11739552007$
$dx_{22} = 1051964162887$	$dy_{22} = 12295227547$	$dx_{23} = 1098640908247$	$dy_{23} = 12850903087$
$dx_{24} = 1145317653607$	$dy_{24} = 13406578627$	$dx_{25} = 1191994398967$	$dy_{25} = 13962254167$
$dx_{26} = 1238671144327$	$dy_{26} = 14517929707$	$dx_{27} = 1285347889687$	$dy_{27} = 15073605247$
$dx_{28} = 1332024635047$	$dy_{28} = 15629280787$	$dx_{29} = 1378701380407$	$dy_{29} = 16184956327$
$dx_{30} = 1425378125767$	$dy_{30} = 16740631867$	$dx_{31} = 1472054871127$	$dy_{31} = 17296307407$
$dx_{32} = 1518731616487$	$dy_{32} = 17851982947$	$dx_{33} = 1565408361847$	$dy_{33} = 18407658487$
$dx_{34} = 1612085107207$	$dy_{34} = 18963334027$	$dx_{35} = 1658761852567$	$dy_{35} = 19519009567$
$dx_{36} = 1705438597927$	$dy_{36} = 20074685107$	$dx_{37} = 1752115343287$	$dy_{37} = 20630360647$
$dx_{38} = 1798792088647$	$dy_{38} = 21186036187$	$dx_{39} = 1845468834007$	$dy_{39} = 21741711727$
$dx_{40} = 1892145579367$	$dy_{40} = 22297387267$	$dx_{41} = 1938822324727$	$dy_{41} = 22853062807$
$dx_{42} = 1985499070087$	$dy_{42} = 23408738347$	$dx_{43} = 2032175815447$	$dy_{43} = 23964413887$
$dx_{44} = 2078852560807$	$dy_{44} = 24520089427$	$dx_{45} = 2125529306167$	$dy_{45} = 25075764967$

Note that $dx_0 = dy_{45}$. Also, the distance between two keys at any position v is directly proportional to the $(gcd(p-1, q-1) - 1)$, as explained earlier:

$$(d_{x_0} - d_{y_0})/555675540 = 0 * (84 - 1) + 45 = 045$$
$$(d_{x_1} - d_{y_1})/555675540 = 1 * (84 - 1) + 45 = 128$$
$$(d_{x_2} - d_{y_2})/555675540 = 2 * (84 - 1) + 45 = 211$$
$$(d_{x_3} - d_{y_3})/555675540 = 3 * (84 - 1) + 45 = 294$$
$$(d_{x_4} - d_{y_4})/555675540 = 4 * (84 - 1) + 45 = 377$$
$$(d_{x_5} - d_{y_5})/555675540 = 5 * (84 - 1) + 45 = 460$$

4. Multi Sets of Private Keys

In the previous section, we showed that any private key can be extended to set of private keys. Going one step further, we demonstrate in this section the existence of multi-private keys from which further sets can be found.

When generating the keys in the RSA cryptosystem, we seek to find the e modular inverse of $\lambda(n)$. In that process, we aim to find the public key's modular inverse of any integer that contains the λ factors within it. By examining the above equation where $\delta = \gamma_1^{v_1} \times \gamma_2^{v_2} \times \gamma_3^{v_3} \cdots$, it presents that there are multi sets of private keys. Consider $\phi(pq) = \lambda(pq) \times gcd(p-1, q-1)$, and from the previous sections we know that Euler's totient function is replaced by Carmichael function. As a result, we can express that as $\delta = gcd(p-1, q-1)$. To prove that such keys are valid, we consider the decryption of the ciphertext to find the plaintext:

$$
\begin{aligned}
c^d \mod N = c^{(\frac{k.\phi(n)+1}{e})} \mod N \\
&= M^{(k.\phi(n)+1)} \mod N \\
&= ((M^{k.\phi(n))} \mod N) \times (M^1 \mod N)) \mod N \\
&= (M^{k.\lambda(n).gcd(p-1,q-1)} \mod N) \times (M^1 \mod N) \\
&= (M^{\lambda(n)} \mod N)^{k.\delta} \times (M^1 \mod N) \\
&= (1)^{k.\delta} \times (M^1 \mod N) = M
\end{aligned}
$$

5. The Existence of A Universal Private Key And A New Set Of Weak Keys

In the previous section, we demonstrated that the private key d is any number that is $d = e^{-1} \mod s$, where $s = k.\lambda(n)$, k is any integer such that $gcd(s, e) = 1$. In other words, there exists a key that can decrypt any RSA modulus (a universal key) without knowing the factorization of N. Consider n to be the number of bits of N then,

$$
d_{uni} = e^{-1} \mod \frac{(2^{n/2})!}{gcd((2^{n/2})!, e^{\upsilon})} \tag{5}
$$

Where υ is a huge exponent to remove e values from the factorial. Such a key will be huge and is computationally infeasible to be generated. For example, with RSA-2048, $n = 2048$, the value of will be around 2.14×10^{301} GiB. In other words, the factorial will have a size of $(gp)^{g^2}$, where gp is the googolplex number and g is the googol number.

Therefore, to overcome this limitation, we exploit a flaw to define a new set of weak RSA keys that can satisfy the FIPS recommendation. The factorial is a massive increasing function, despite the length and size that is needed to calculate it, we have managed to compute the factorial of the prime numbers up to 2^{24}, which does not require a huge computation power. The private key size after computation was 0.274 MiB, such a key can decrypt any message encrypted with the same e if and only if the biggest factor of $(p-1, q-1)$ is lower than 2^{24}. We used $e = 2^{16} + 1$ but it can be easily changed to a different value, and code can be found in (Almazari, 2022).

Theorem 5.1. *If $p - 1 = \alpha_1^{\beta_1} \times \alpha_2^{\beta_2} \times \alpha_3^{\beta_3} \times \cdots$ and $q - 1 = \gamma_1^{\nu_1} \times \gamma_2^{\nu_2} \times \gamma_3^{\nu_3} \cdots$*
Then N is considered a broken key if and only if $max(\alpha_1, \alpha_2, \alpha_3, \gamma_1, \gamma_2, \gamma_3 \cdots) \leqslant 2^{(\tau)}$, where 2^{τ} depends on the computational power to compute the factorial of prime numbers from 1 up to 2^{τ}.

If we want a factorial of the prime numbers up to 2^{40} then such a key size will be $2^{\frac{2^{40}}{ln(2^{40})}*40/3}$ bits, where (40/3) bits is the average size of each prime from 1 to 2^{40}, roughly speaking, the maximum size of such a private key is 62 GiB.

6. A New Attack on RSA To Factor N

In the previous section, we discussed the existence of a universal key that can break a wide range of RSA pairs that satisfy the FIPS recommendations. In this section, we discuss a new attack and a new set of weak RSA keys by exploiting a vulnerability of the factors of $p-1, q-1$ that will lead to the factorization of N. Unfortunately, FIPS recommendations require the private key size to be bigger than $2^{n/2}$, where n is the modulus size, we show that if the private key is a little bigger than $2^{n/2}$, we can factorize N.

Theorem 6.1. *Suppose that $q - 1 = A \times C$, $p = B \times C$, where $C = \alpha_1^{\beta_1} \times \alpha_2^{\beta_2} \times \alpha_3^{\beta_3} \times \cdots$, then we can factorize N efficiently in polynomial time if and only if $A \times B$ can be brute forced.*

Note that the private key is bigger than $2^{n/2}$, when $\lambda(n)$ is small. Since, $\lambda(n)$ is small then $gcd(p-1, q-1)$ will be large. Moreover, based on Theorem 6.1, $C = gcd(p-1, q-1)$, because C is the common factor, then we exploit this GCD in order to factorize N as follows:

$$
\begin{gathered}
q - 1 = A.C, p - 1 = B.C \\
N = pq = (A.C + 1)(B.C + 1) = A.B.C^2 + (A + B).C + 1 \\
A.B.C^2 + (A + B).C + (1 - N) = 0
\end{gathered} \tag{6}
$$

If the size of A and B is small, we can brute force and solve the quadratic equation in polynomial time. We illustrate with a numerical example as shown below.

```
N = 18369583373607319524848230962864856788641872197252249438510296626216984019
    00767770231109723345229280047378054983385725531621576008806522718839768228
    95155752536323923971545099766616521104912801219459206580577418109585426788
    94186440036821454425304791711282798209813170929253634748758078024559105723
    17065705659759090744861931152060180797219017707220689811518504015189123409
    21973803084917534538315417471053185166367184094562280791943232148143653003
    55951159745383220310112790585573021538809712101420219793936813969140292008
    64660786683952675497641394732617079419376910978204951439718834170833126480
    0385010840190811956595297
A = 16135453 , B = 16372597
C = 83387371782197792172623397291771726569847672290744673235202388778220013318
    14997575307844024904832045978308876022952803468558728387340737937040841658
    68153727543780345009752984160464056256725252862795377473845049850261668367
    12775958307530475534348349797051782157566720607792197655530846287693897036
    99134
q = 13454930181851787123051327137017099807966283334067130099869660896186964485
    54382980714936777951827469507768418885511818815851663396337022719684394596
    64097986675574731992286538175309122379197462514807502618464855311415541876
    39376709748011175340521276837778885695696564147311624390375281603253093540
    2721302797703
p = 13652678330790962255321173166290698951223082898044293647766549249031186553
    92702338564924811586247784414883219686467690012109142307183898039257810730
    18404361151221154453656466792066613260766911048456450088421430416432446407
    22630855166579985411422451888421606173976304171229767119583513673373582355
    4615330230999
d(65537, lambda(N)) = 15584853613967811566689450274710991761254882518079720188
    45236463641204511391962721529706849410104785770789000522620797231652757928
    14689914740017562702078886693338838681236114468910880800809328412556411222
    30257775730425724104466358405034102915451430564640344986171358426560260491
    71055609777279681239248488057407524103
```

We brute force using different values of A and B to find the value of C. Thus, we can find the value of $q = A.C + 1$ and $p = B.C + 1$. Note that this attack succeeds due to the small values of A and B. One interesting observation is that the countermeasures of the Wiener Attack recommend increasing $gcd(p-1, q-1)$ (Wiener, 1990). However, as shown in this section, such a measure can be exploited in this attack, and code can be found in (Almazari, 2022).

7. Extending The Attack on RSA To Factor N

In the previous section, a new attack was introduced on RSA that targets a weakness in the FIPS recommendation. The attack, also, can be extended such that if there is a big common factor between $q - \alpha$ and $p - \beta$ where $\alpha, \beta \in \mathbb{Z}$ then:

$$q - \alpha = A.C$$
$$p - \beta = B.C$$
$$N = pq = (A.C + \alpha)(B.C + \beta) = A.B.C^2 + (\beta A + \alpha B).C + \alpha\beta$$
$$A.B.C^2 + (\beta A + \alpha B).C + (\alpha\beta - N) = 0 \tag{7}$$

Notice that $\alpha, \beta \in \mathbb{Z}$, which means that assuming $q + \alpha$ and $p + \beta$ is also possible. Nevertheless, by assuming the size of α, β, A and B to be n_α, n_β, n_A and n_B bits, respectively, the previous equation can be solved and factor N in $O(2^{(n_\alpha \times n_\beta \times n_A \times n_B)})$

8. Conclusion

We conducted a thorough analysis of the existence of multiple sets of private keys in this paper (rather than a single key). In addition, we demonstrated that the keys produced by the Charmichael function and the keys produced by the Euler totient function are connected, emphasising the relationship between the two sets of keys. Through our analysis, we proved that there is a universal key that satisfies the FIPS requirements. Last but not least, we demonstrated a new attack on RSA that would reveal the factors used to calculate N by taking advantage of a FIPS recommendation that the value of the private key must be bigger than $2^{(n/2)}$.

References

R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (1978) 120–126.

M. Ibrishimova, Proving the existence of a second private key that decrypts a message encrypted with the rsa encryption algorithm, https://marinaibrishimova.net/docs/otherkeys.pdf, 2017. (Accessed on 03/19/2022).

M. M. Almazari, Paper codes - universal key calculation and factorization attack, https://github.com/lcsig/RSAWeakKeys, 2022.

M. J. Wiener, Cryptanalysis of short rsa secret exponents, IEEE Transactions on Information theory 36 (1990) 553–558.