J. Cryptology (1992) 5: 139–150

Journal of Cryptology

A Cubic RSA Code Equivalent to Factorization

J. H. Loxton*
School of Mathematics, Physics, Computing, and Electronics,
Macquarie University, NSW, Australia 2109

David S. P. Khoo
Department of Computer Science, University of Sydney,
NSW, Australia 2006

Gregory J. Bird
Department of Pure Mathematics, University of Sydney,
NSW, Australia 2006

Jennifer Seberry**
Department of Computer Science, University College,
University of New South Wales, Canberra, ACT, Australia 2600

Communicated by Ernest F. Brickell

Received 21 September 1987 and revised 10 September 1991

Abstract. The RSA public-key encryption system of Rivest, Shamir, and Adelman can be broken if the modulus, R say, can be factorized. However, it is still not known if this system can be broken without factorizing R. A version of the RSA scheme is presented with encryption exponent $e \equiv 3 \pmod 6$. For this modified version, the equivalence of decryption and factorization of R can be demonstrated.

Key words. Encryption, Public-key, RSA, Factorization, Eisenstein integers, Cubic residues.

1. Introduction

The RSA scheme can be developed in any domain with unique factorization. Here we use the ring $\mathbf{Z}[\omega]$ of Eisenstein integers, where $\omega = \frac{1}{2}(-1 + \sqrt{-3})$ is a primitive cube root of unity. The public-key encryption system is made up of a community of users, each with individual encryption and decryption keys. The encryption key consists of a modulus R in $\mathbf{Z}[\omega]$ and a positive integer e, called the encryption

* Research supported in part by a grant from the ATERB.
** Research supported in part by a grant from the ACRB.

exponent. The decryption key is another integer exponent d. For each user, the encryption key is made publicly accessible, but the decryption key is kept secret. The modulus R is the product of two carefully selected large primes p and q in $\mathbf{Z}[\omega]$. In addition, e must be relatively prime to $\varphi(R) = (p\bar{p} - 1)(q\bar{q} - 1)$. With this proviso, d can be obtained by solving the congruence $de \equiv 1 \pmod{\varphi(R)}$.

The protocol for sending messages follows the usual lines. First, assign numerical equivalents to the symbols of the message (for example, $A = 01, B = 02, \ldots$). If the resulting numerical string is very long, break it into blocks representing numbers no larger than $|R|$. Take the blocks in pairs and interpret the pair a, b as the Eisenstein integer $a + b\omega$. To send a message M, coded in this way as an element of $\mathbf{Z}[\omega]$, the sender computes $C \equiv M^e \pmod{R}$ using the encryption key (R, e). (As in $\mathbf{Z}$, the congruence notation $\alpha \equiv \beta \pmod{m}$ in $\mathbf{Z}[\omega]$ means that m divides $\alpha - \beta$. We are working with the complete set of residues described in Section 3 below). To determine the plaintext M from the ciphertext C, the recipient uses the secret key d and calculates $M \equiv C^d \pmod{R}$. If R can be factorized, then d is easy to determine given R and e. So breaking the cipher is at most as difficult as factorization.

The purpose of this paper is to present a modified version of the RSA cryptosystem in $\mathbf{Z}[\omega]$. It will be shown that breaking the system is equivalent to factorizing the modulus R. In what follows, R will be the product of two primes in specified congruence classes modulo 9 in $\mathbf{Z}[\omega]$, so factorizing R is not quite the same as factorizing an arbitrary integer in $\mathbf{Z}[\omega]$. On the other hand, there is no reason to believe that factorizing R is any easier than factorizing an arbitrary integer in $\mathbf{Z}[\omega]$.

Williams [Wi1], [Wi2] and Rabin [R] have also proposed public-key schemes which are provably as intractable as factorization. The papers [Wi1] and [R] take the encryption exponent $e = 2$ and [Wi2] takes $e = 3$. This paper provides an alternative approach to the case $e = 3$. The main difference in the description of the system lies in the choice of the complete set of residues used in defining the message space in Section 3. The choice used here has a geometrical flavour which we have found helpful.

2. Arithmetic in $\mathbf{Z}[\omega]$

In this section we summarize the essential facts about cubic residues in $\mathbf{Z}[\omega]$. A basic reference is Chapter 9 of [IR].

As above, set $\omega = \frac{1}{2}(-1 + \sqrt{-3})$. The ring $\mathbf{Z}[\omega]$ comprises all numbers of the form $a + b\omega$ with a and b in $\mathbf{Z}$, the ring of rational integers. Multiplication is easily performed using $\omega^2 = -1 - \omega$. For $\alpha = a + b\omega$ in $\mathbf{Z}[\omega]$, we define the *norm* $N\alpha = \alpha\bar{\alpha} = a^2 - ab + b^2$. There are six units in $\mathbf{Z}[\omega]$, namely ± 1, $\pm\omega$, $\pm\omega^2$. The numbers α, β in $\mathbf{Z}[\omega]$ are called *associates* if $\alpha = \beta u$ for some unit u in $\mathbf{Z}[\omega]$. A number $\alpha = a + b\omega$ is called *primary* if $a \equiv 2 \pmod{3}$ and $b \equiv 0 \pmod{3}$. Each α in $\mathbf{Z}[\omega]$ with $N\alpha \equiv 1 \pmod{3}$ has a unique associate which is primary. In particular, this applies to any prime p in $\mathbf{Z}[\omega]$ with $Np \neq 3$ because it can be shown that $Np \equiv 1 \pmod{3}$.

Let p be a prime in $\mathbf{Z}[\omega]$ with $Np \neq 3$. A number α in $\mathbf{Z}[\omega]$ is called a *cubic residue* modulo p if $\alpha \equiv \beta^3 \pmod{p}$ for some β in $\mathbf{Z}[\omega]$. Exactly one-third of the residue classes relatively prime to p are cubic residues modulo p and each nonzero cubic residue has exactly three cube roots modulo p. Indeed, if $\alpha \equiv \beta^3 \pmod{p}$, then the three cube roots of α are β, $\omega\beta$, and $\omega^2\beta$.

Let p and q be distinct primes in $\mathbf{Z}[\omega]$ with $Np, Nq \neq 3$. By the Chinese remainder theorem, the residue classes in $\mathbf{Z}[\omega]$ modulo pq correspond to the pairs $[\alpha, \beta]$, where α, β run through the residue classes in $\mathbf{Z}[\omega]$ modulo p and q, respectively. The residue class $\delta \pmod{pq}$ corresponds to the pair $[\alpha, \beta]$ if and only if $\delta \equiv \alpha \pmod{p}$ and $\delta \equiv \beta \pmod{q}$. Consequently, if δ is a cube relatively prime to pq, say $\delta \equiv \delta_1^3 \pmod{pq}$, then δ has nine cube roots modulo pq obtained by running through the three cube roots modulo p and the three cube roots modulo q independently. That is, if $\delta_1 = [\alpha, \beta]$, say, the nine cube roots of δ are

$$\begin{array}{lll}
\delta_1 = [\alpha, \beta], & \delta_2 = [\omega\alpha, \omega\beta], & \delta_3 = [\omega^2\alpha, \omega^2\beta], \\
\delta_4 = [\alpha, \omega\beta], & \delta_5 = [\omega^2\alpha, \beta], & \delta_6 = [\omega\alpha, \omega^2\beta], \\
\delta_7 = [\omega\alpha, \beta], & \delta_8 = [\alpha, \omega^2\beta], & \delta_9 = [\omega^2\alpha, \omega\beta].
\end{array}$$

Let p be a prime in $\mathbf{Z}[\omega]$ with $Np \neq 3$. For α in $\mathbf{Z}[\omega]$, the *cubic residue symbol* is the cubic character given by

$$(\alpha|p)_3 = \begin{cases} 0 & \text{if } \alpha \equiv 0 \pmod{p}, \\ 1 & \text{if } \alpha^{(Np-1)/3} \equiv 1 \pmod{p}, \\ \omega & \text{if } \alpha^{(Np-1)/3} \equiv \omega \pmod{p}, \\ \omega^2 & \text{if } \alpha^{(Np-1)/3} \equiv \omega^2 \pmod{p}. \end{cases}$$

This is well defined because $\alpha^{Np-1} \equiv 1 \pmod{p}$. Moreover, α is a cubic residue if and only if $(\alpha|p)_3 = 1$. The definition is extended multiplicatively to any modulus R for which NR is not divisible by 3 as follows: if

$$R = \prod_{i=1}^{k} p_i^{e_i},$$

where the p_i are distinct primes in $\mathbf{Z}[\omega]$ and $Np_i \neq 3$, then

$$(\alpha|R)_3 = \prod_{i=1}^{k} (\alpha|p_i)_3^{e_i}.$$

The cubic residue symbol has the properties:

1. If $\alpha_1 \equiv \alpha_2 \pmod{R}$, then $(\alpha_1|R)_3 = (\alpha_2|R)_3$,
2. $(\alpha_1\alpha_2|R)_3 = (\alpha_1|R)_3(\alpha_2|R)_3$, and
3. $(\alpha|R_1R_2)_3 = (\alpha|R_1)_3(\alpha|R_2)_3$,

whenever the symbols are defined. Further, we have the following much deeper

4. *Law of cubic reciprocity*:
   a. If $R = 3m - 1 + 3n\omega$ is primary, then $(1 - \omega|R)_3 = \omega^{2m}$, $(\omega|R)_3 = \omega^{m+n}$.
   b. If R, S are primary and $NR \neq NS$, then $(R|S)_3 = (S|R)_3$.

The reciprocity law makes it easy to calculate the cubic residue symbol. Consider $(Q_1|Q_2)_3$, where $3 \nmid NQ_2$. We write $Q_i = (1 - \omega)^{l_i}u_iR_i$, where $(1 - \omega)^{l_i}$ is the exact power of the prime $1-\omega$ dividing Q_i, u_i is a unit, and R_i is primary. If $(Q_1, Q_2) \neq 1$, then $(Q_1|Q_2)_3 = 0$. Otherwise, since $3 \nmid NQ_2$,

$$(Q_1|Q_2)_3 = (1-\omega|R_2)_3^{l_1}(u_1|R_2)_3(R_1|R_2)_3$$

and the first two symbols on the right are given by 4a above. Using the Euclidean algorithm, we can write

$$R_1 = k_1R_2 + Q_3, \qquad 0 < NQ_3 \leq \tfrac{3}{4}NR_2, \qquad Q_3 = (1-\omega)^{l_3}u_3R_3$$

$$R_2 = k_2R_3 + Q_4, \qquad 0 < NQ_4 \leq \tfrac{3}{4}NR_3, \qquad Q_4 = (1-\omega)^{l_4}u_4R_4, \qquad \text{and so on.}$$

Since the norms of the remainders decrease geometrically, the algorithm must terminate and finally we reach the statement that Q_{m+1}, say, is a unit and $R_{m+1} = -1$. By the reciprocity law,

$$(R_1|R_2)_3 = (Q_3|R_2)_3 = (1-\omega|R_2)_3^{l_3}(u_3|R_2)_3(R_3|R_2)_3,$$

$$(R_3|R_2)_3 = (R_2|R_3)_3 = (Q_4|R_3)_3 = (1-\omega|R_3)_3^{l_4}(u_4|R_3)_3(R_4|R_3)_3, \qquad \text{and so on.}$$

This algorithm runs in time polynomial in the length of the numbers involved.

The following calculation is used later.

Lemma 1. *Suppose $R = pq$, where p, q are distinct primes in $\mathbf{Z}[\omega]$, $3 \nmid NR$ and $Nq \equiv 2Np - 1 \pmod 9$. If $(M|R)_3 = 1$, then*

$$M^{(1/3)(Np-1)\cdot(1/3)(Nq-1)} \equiv (M|p)_3^{(2/3)(Np-1)} \pmod R.$$

Proof. Since $(M|R)_3 = 1$, we have $(M|p)_3 \cdot (M|q)_3 = 1$, giving three cases according as $(M|p)_3 = 1$, ω, or ω^2. If, say, $(M|p)_3 = \omega$, then

$$M^{(1/3)(Np-1)} \equiv \omega \pmod p,$$

$$M^{(1/3)(Np-1)\cdot(1/3)(Nq-1)} \equiv \omega^{(1/3)(Nq-1)} = \omega^{(2/3)(Np-1)} \pmod p.$$

Also

$$M^{(1/3)(Nq-1)} \equiv \omega^2 \pmod q, \qquad M^{(1/3)(Np-1)\cdot(1/3)(Nq-1)} \equiv \omega^{(2/3)(Np-1)} \pmod q.$$

Combining these two assertions gives the required congruence modulo pq. The other two cases are done similarly. □

We use the cubic residue symbol to separate the cube roots modulo R in $\mathbf{Z}[\omega]$. For this purpose, it is necessary to make some assumptions on R. If p is a primary prime in $\mathbf{Z}[\omega]$ and $Np \not\equiv 1 \pmod 9$, then $(\omega|p)_3 \neq 1$ and so the three cube roots of α^3 modulo p, namely α, $\omega\alpha$, and $\omega^2\alpha$, give different values of the cubic residue symbol $(\cdot|p)_3$. We can therefore define the *principal cube root* α of α^3 modulo p to be the choice with $(\alpha|p)_3 = 1$.

Now suppose $R = pq$, where p and q are primary primes in $\mathbf{Z}[\omega]$ and $Np, Nq \not\equiv 1 \pmod 9$. As explained above a cube, δ^3 say, has nine cube roots modulo pq. We choose the principal cube root $[\alpha, \beta]$ as follows: α is the principal cube root of δ^3 modulo p and β is the principal cube root of δ^3 modulo q. The nine cube roots of δ^3 modulo R are given by $\delta = [u\alpha, v\beta]$, where u and v run through the cube roots of unity. Note that

$$(\delta|R)_3 = (u|p)_3(v|q)_3 = u^{(1/3)(Np-1)}v^{(1/3)(Nq-1)},$$

so we can split the nine roots into three types each containing three of the roots as follows: we say δ has *type* 1, 2, or 3 according as $(\delta|R)_3 = 1, \omega$, or ω^2. Note that the type can be determined without factorizing R since it only depends on the value of the cubic residue symbol.

Suppose, in addition, that $Np \not\equiv Nq \pmod 9$. After interchanging p and q if necessary, we may suppose that $Np \equiv 7 \pmod 9$ and $Nq \equiv 4 \pmod 9$. Now it is easy to check that the nine cube roots of δ^3 modulo pq are grouped as follows:

type 1: $\delta_1 = [\alpha, \beta]$, $\delta_2 = [\omega\alpha, \omega\beta] = \omega\delta_1$, $\delta_3 = [\omega^2\alpha, \omega^2\beta] = \omega^2\delta_1$,
type 2: $\delta_4 = [\alpha, \omega\beta]$, $\delta_5 = [\omega^2\alpha, \beta] = \omega^2\delta_4$, $\delta_3 = [\omega\alpha, \omega^2\beta] = \omega\delta_4$,
type 3: $\delta_7 = [\omega\alpha, \beta]$, $\delta_8 = [\alpha, \omega^2\beta] = \omega^2\delta_7$, $\delta_9 = [\omega^2\alpha, \omega\beta] = \omega\delta_7$.

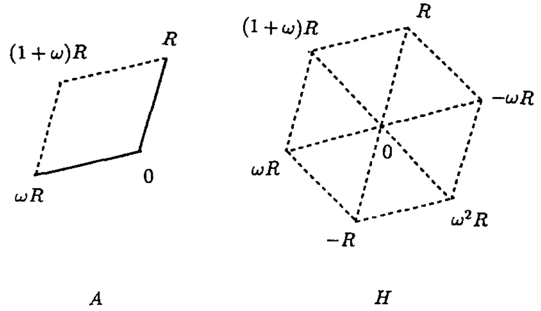
(Here, δ_1 is the principal cube root.)

There is a number w in $\mathbf{Z}[\omega]$ such that $(w|R)_3 \neq 1$. Multiplying by w changes the type. For definiteness, we investigate the case $p \equiv 8 + 6\omega \pmod 9$ and $q \equiv 5 + 6\omega \pmod 9$ for which $(1 - \omega|R)_3 = \omega$. (The last assertion follows from the first part of the cubic reciprocity law.) In this case, if X has type t, then $(1 - \omega)X$ has type $(t + 1) \pmod 3))$ and $(1 - \omega)^2X$ has type $(t + 2) \pmod 3$. Other choices for p and q modulo 9 can be handled with minor modifications.

3. The Message Space

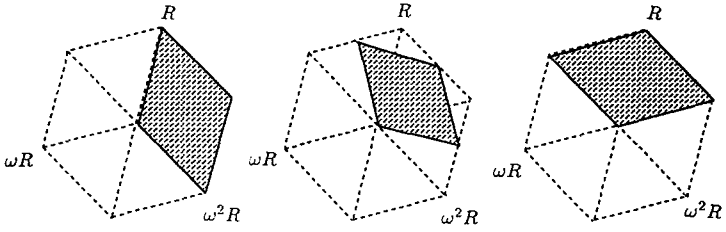
In what follows, we suppose $R = pq$, where p, q are primary primes in $\mathbf{Z}[\omega]$, $p \equiv 8 + 6\omega \pmod 9$, and $q \equiv 5 + 6\omega \pmod 9$.

A *complete set of residues* modulo R, or a fundamental region, is a set A such that each element of the lattice $\mathbf{Z}[\omega]$ is congruent modulo R to exactly one element of A. We take A to be the parallelogram with vertices $0, R, (1 + \omega)R$, and ωR, including the lattice points on the sides joining 0 to R and 0 to ωR, but not the endpoints R and ωR, nor the lattice points on the other two sides. (See Fig. 1.) In the figure, ωA and $\omega^2 A$ are respectively obtained by rotating A through $2\pi/3$ and $4\pi/3$ anticlock-



A H

Fig. 1



$t = 1$ $t = 2$ $t = 3$

Fig. 2

wise and H is the hexagon $H = A \cup \omega A \cup \omega^2 A$ obtained by taking the union of A, ωA, and $\omega^2 A$ and deleting all the lattice points for which $\arg z/R$ is an integral multiple of $\pi/3$.

Given a message M in $\mathbf{Z}[\omega]$, we first form $M_1 = (1 - \omega)M + 1$ to ensure that M_1 is not divisible by $1 - \omega$. Suppose M_1 has type t, that is $(M_1|R)_3 = \omega^{t-1}$ with $t = 1, 2$, or 3. The first stage in the encryption is given by

$$E_1(M) = (1 - \omega)^{4-t} M_1$$

which yields an element of type 1.

Definition. The *message space* Λ is the set of all messages M in the fundamental region A such that $E_1(M)$ is in H.

Note that multiplying X by $1 - \omega$ corresponds to rotating X through $\pi/6$ clockwise and multiplying the magnitude of X by $\sqrt{3}$. If M is in the message space, then $E_1(M)$ must be in the appropriate parallelogram shaded in Fig. 2. The three cases are distinguished by the value of t, the type of M_1 as above. Thus, ignoring points close to the boundary of A, M must lie in $\frac{1}{9}A$ in the case $t = 1$ (since $|E_1(M)| \approx 9|M|$ in this case), in $\frac{1}{6}A$ in the case $t = 2$ (since $|E_1(M)| \approx 3\sqrt{3}|M|$ and $E_1(M)$ lies in a rhombus of side $\frac{1}{2}\sqrt{3}|R|$ and similar to A), and in $\frac{1}{3}A$ in the case $t = 3$ (since $|E_1(M)| \approx 3|M|$). The type is uniformly distributed between its three possible values in each of these three regions. So the size of the message space is asymptotically

$$\frac{1}{3}\left(\frac{1}{9} + \frac{1}{36} + \frac{1}{81}\right)|A| = \frac{49}{972}|R|^2.$$

Note that the number of lattice points close to the boundary of A is proportional to the length of the boundary, so is $O(|R|)$, while the total number of lattice points in A is $|A| = NR = |R|^2$.

4. Encryption and Decryption

As before, let $R = pq$, where p, q are primary primes in $\mathbf{Z}[\omega]$, $p \equiv 8 + 6\omega \pmod 9$ and $q \equiv 5 + 6\omega \pmod 9$. Note that $\varphi(R) = (Np - 1)(Nq - 1)$ is an even integer and congruent to 18 modulo 27. Let h be a rational integer such that $(h, \varphi(R)) = 1$. The encryption exponent is $e = 3h$; note that $e \equiv 3 \pmod 6$.

Encryption. Let M be a message in Λ and set $M_1 = (1 - \omega)M + 1$. We assume that M_1 is relatively prime to R. To effect encryption, first calculate

$$N = E_1(M) = (1 - \omega)^{4-t} M_1, \qquad \text{where} \quad (M_1 | R)_3 = \omega^{t-1} \quad (t = 1, 2, \text{or } 3).$$

Then determine $E_2(N)$ to be the point in the fundamental region A satisfying

$$E_2(N) \equiv N^e \pmod R.$$

To summarize, for a plaintext M in Λ, the ciphertext C is given by

$$C = E(M) = E_2(E_1(M)).$$

Decryption. Decryption is also the result of two steps. The decryption exponent d is obtained by solving the congruence

$$hd \equiv \tfrac{1}{3}(1 + \tfrac{1}{9}\varphi(R)) \pmod{\varphi(R)}.$$

The first decryption stage is to determine $D_2(C)$ to be the point in the fundamental region A satisfying

$$D_2(C) \equiv C^d \pmod R.$$

Lemma 2 below shows that D_2 is almost the inverse of E_2.

We proceed to the second stage of the decryption process. Given X in A with $X \neq 0$ and $\arg X/R \neq \pi/3$, there is a unique point $Y = F(X)$, say, in H^c, the closure of H, such that $Y \equiv X \pmod R$ and $1 - \omega | Y$. In fact, if $0 \leq \arg X/R < \pi/3$, there are three points in H^c which are congruent to X modulo R, namely X, $X - R$, and $X - \omega^2 R$, and these three points form a complete set of residues modulo $1 - \omega$. Exactly one of them is divisible by $1 - \omega$. If $\pi/3 < \arg X/R \leq 2\pi/3$, the same argument applies to the points X, $X - \omega R$, and $X - \omega^2 R$. Now let $(1 - \omega)^s$ be the exact power of $1 - \omega$ dividing Y and choose $Z = G(Y)$, say, to be that one of Y, ωY, or $\omega^2 Y$ such that

$$-\frac{(s+1)\pi}{6} \leq \arg \frac{Z}{R} < -\frac{(s-3)\pi}{6}.$$

Set

$$D_1(X) = \frac{1}{1 - \omega}\left(\frac{Z}{(1 - \omega)^s} - 1\right).$$

The decrypted text obtained from the ciphertext C is

$$D(C) = D_1(D_2(C)),$$

provided this is defined (that is, $C \neq 0$ and $\arg D_2(C) \neq \pi/3$).

It remains to verify the assertions made above and to confirm that D_2 is essentially the inverse of E_2 (Lemma 2) and that D is the inverse of E (Theorem 1).

Lemma 2. *Suppose $R = pq$ where p and q are distinct primes in* $\mathbf{Z}[\omega]$, $Np \equiv 7 \pmod 9$ *and* $Nq \equiv 4 \pmod 9$. *If* $(N|R)_3 = 1$, *then*

$$D_2E_2(N) = E_2D_2(N) \equiv N(N|p)_3^2 \pmod R.$$

Moreover, if $(K, R) = 1$, *then*

$$E_2D_2E_2(K) = E_2(K).$$

Proof. Suppose $(N|R)_3 = 1$. By Lemma 1,

$$X \text{ (say)} = D_2E_2(N) = E_2D_2(N) \equiv N^{ed} \equiv N^{1+\varphi(R)/9} \equiv N(N|p)_3^2 \pmod R.$$

Next, suppose K is relatively prime to R. Let N be a cube root of K^3 of type 1, that is $N^3 \equiv K^3 \pmod R$ and $(N|R)_3 = 1$. Then

$$E_2(N) \equiv N^{3h} \equiv K^{3h} \equiv E_2(K) \pmod R$$

and so, by the first part,

$$E_2D_2E_2(K) \equiv E_2D_2E_2(N) \equiv E_2(N(N|p)_3^2) \equiv N^{3h} \equiv E_2(K) \pmod R.$$

However, $E_2(K)$ and $E_2D_2E_2(K)$ both lie in the fundamental region A, so they are in fact equal. □

The next theorem confirms that decryption is the inverse of encryption.

Theorem 1. *If M is in Λ and $M_1 = (1 - \omega)M + 1$ is relatively prime to R, then*

$$D(E(M)) = D_1D_2E_2E_1(M) = D_1E_2D_2E_1(M) = M.$$

Proof. Suppose M is in Λ. Then $N = E_1(M)$ is in H, $1 - \omega | N$, and $(N|R)_3 = 1$. By Lemma 2,

$$X \text{ (say)} = D_2E_2(N) = E_2D_2(N) \equiv N(N|p)_3^2 \pmod R.$$

Since X is in A, N is in H, and $1 - \omega | N$, it follows that $F(X) = N(N|p)_3^2$. Suppose $M_1 = (1 - \omega)M + 1$ has type t, so that N lies in the corresponding shaded parallelogram of Fig. 2. The preceding definitions yield $G(F(X)) = N$ and so $D_1(X) = M$. This proves the theorem. □

Example. It may be helpful to give an example with "small" numbers to illustrate the construction of this section. Take the modulus $R = 41 + 12\omega$ and encryption exponent $e = 3$. Then $R = -pq$, where $p = -1 + 6\omega$ and $q = 5 + 6\omega$ are primary primes in the prescribed residue classes modulo 9. Take the message $M = 1 + 2\omega$, so that $M_1 = 4 + 3\omega$ and M is in the message space and we have $(M_1, R) = 1$. We follow through the coding and decoding algorithms, using the notation of this section. By the definition of the cubic residue symbol and the law of cubic reciprocity, we can compute

$$(4 + 3\omega|p)_3 = \omega^2, \qquad (4 + 3\omega|q)_3 = \omega, \quad \text{and} \quad (4 + 3\omega|R)_3 = 1,$$

so we have $N = (1 - \omega)^3M_1 = 6 - 15\omega$ and the ciphertext is $C\ (\equiv N^3 \pmod R) =$

$11 - 13\omega$. The decryption exponent is $d = 47$ and, by Lemma 2, the first stage of the decoding gives

$$X = D_2(C)\,(\equiv N(N|p)_3^2 \pmod{R}) = 15 + 21\omega = -(1-\omega)^3(-3+\omega).$$

Since $(1-\omega)^3 \| X$, we set $Y = X = 15 + 21\omega$ and $Z = \omega^2 Y = 6 - 15\omega = (1-\omega)^3(4+3\omega)$. Finally, $D_1(X) = 1 + 2\omega$ which returns the original message M.

5. Factorization and Decryption

The security of an RSA scheme depends on the difficulty of factorizing the modulus of the system. Certainly, if R is factorized, then $\varphi(R)$ is easy to compute and the decryption procedure of Section 4 runs in polynomial time, that is $O(\log NR)$ multiprecision operations. For general RSA schemes, it is not known whether there is a method for breaking the code which is easier than factorizing the modulus. However, we shall establish the equivalence of factorizing the modulus R and decrypting the modified RSA scheme of Section 4. This statement is made precise in Theorem 2 below.

The factorization algorithm is based on the observation that if we can find two cube roots, X and Y say, of the same number modulo R, but of different types, then we have

$$(X-Y)(X-\omega Y)(X-\omega^2 Y) = X^3 - Y^3 \equiv 0,\ X \not\equiv Y, X \not\equiv \omega Y, X \not\equiv \omega^2 Y \pmod{R}$$

and so one of the greatest common divisors $(X - \omega^i Y, R)$ gives a nontrivial factor of R.

Let $\Psi = \{C\colon C = E(M) \text{ for some } M \text{ in } \Lambda\}$ be the space of ciphertexts. A decryption procedure D^* is a function defined on Ψ such that $D^*E(M) = M$ for each M in Λ.

Theorem 2. *Suppose D^* is a decryption procedure for the encryption scheme of Section 4. Then there is a probabilistic polynomial-time algorithm for factorizing R requiring on average a bounded number of applications of D^*.*

Proof. First, we describe the inverses of the functions E_1 and D_1 defined in Section 4. Suppose $N = E_1(M)$ with M in Λ. If $(1-\omega)^s$ is the exact power of $1-\omega$ dividing N, then

$$M = E_1^{-1}(N) = \frac{1}{1-\omega}\left(\frac{N}{(1-\omega)^s} - 1\right).$$

Next, suppose $M = D_1(X)$ is in Λ and set $N = E_1(M)$ so that N is in H. By Theorem 1 and the calculation of Lemma 2,

$$X = D_2E_2(N) \equiv N, \omega N, \text{ or } \omega^2 N \pmod{R}.$$

The exact power of $1-\omega$ dividing N is $4-t$ where t is the type of $(1-\omega)M + 1$. Set $Z = (1-\omega)^{4-t}((1-\omega)M + 1)$. Then determine $Y = Z$, ωZ, or $\omega^2 Z$ by the condition that $1 - \omega | Y$ and determine X in A so that $X \equiv Y \pmod{R}$. With this construction, $X = D_1^{-1}(M)$ for M in Λ. Note that Y is uniquely defined because $Y = N, \omega N$, or $\omega^2 N$ is in H.

Let $\Phi = \{N\colon N = E_1(M) \text{ for some } M \text{ in } \Lambda\}$. We now have the functions $E_2\colon \Phi \to \Psi$ and $D_2 = D_1^{-1}D^*\colon \Psi \to \Phi$ and from the proof of Theorem 1,

$$D_2E_2(N) \equiv N, \omega N, \text{ or } \omega^2 N$$

for N in Φ.

Suppose that we can find K such that $(K, R) = 1$ and $(K|R)_3 \neq 1$ and $X = E_2(K) \equiv K^e \pmod R$ is in Ψ. Set $N = D_2(X)$, so that N is in Φ and, in particular, $(N|R)_3 = 1$. Moreover, by Lemma 2, $E_2(N) = E_2(K)$. Since $(h, \varphi(R)) = 1$, there is a unique W in A such that $W^h \equiv X \pmod R$. Now, N^{3h}, K^{3h}, and W^h are all congruent to X modulo R. Thus N and K are cube roots of W of different types and the remark at the beginning of this section can be used to obtain the factorization of R.

We find K with the properties listed above by trial and error. The sets Λ, Φ, and Ψ have the same number of elements and this number is asymptotic to $(49/972)NR$. Consider X in Ψ. There is a unique W such that $W^h \equiv X \pmod R$ and there are nine choices of K satisfying $K^3 \equiv W \pmod R$. Of these, six have $(K|R)_3 \neq 1$. So the number of K with the properties required above is asymptotically $(294/972)NR$. On the average, the number of trials needed to find a suitable K is $972/294 \approx 3\cdot 3$. □

Theorem 2 relies on an oracle D^* which decrypts all ciphertexts. This is actually more than we need. Suppose that the oracle D^* only decrypts a certain fraction ψ^{-1} of the ciphertexts in Ψ. Then we need to choose K above so that $E_2(K)$ is an element of Ψ which can be decrypted by D^*. The number of K with this additional property is asymptotically $(294/972)\psi^{-1}NR$. The expected number of applications of D^* in the algorithm is now $(972/294)\psi$.

6. Concluding Remarks

The main result of this paper is comparable to that of Williams in [Wi2]. The approach used is a natural extension of the method of Williams [Wi1] concerned with the encryption function $M \to M^2 \pmod R$. Both here and in [Wi2], the basic problem to be solved is to distinguish the cube roots of a number modulo R so that a ciphertext can be correctly decoded. In the present paper this is done by restricting the message space and giving an algorithm to find the distinguished cube root corresponding to a valid message. In [Wi2] the idea is to transmit additional information with the ciphertext, namely the values of certain cubic residue symbols, in order that the ciphertext can be correctly decoded. There is another technical difference in that [Wi2] uses the rational integers $\{0, 1, 2, \ldots, NR - 1\}$ as the complete set of residues modulo R. It seems to us that the geometrical flavour of the specification used in this paper shows more promise for an extension to higher exponents such as $e = 5$. (However, we have not carried this through.)

With a minor modification of the usual method, the encryption scheme of Section 4 allows users to sign their messages. Suppose A has the encryption map $E^A = E_2^A E_1^A$ and decryption map $D_A = D_1^A D_2^A$ and B has similarly encryption map E^B and decryption map D^B. If A wishes to sign and encrypt a message M, A computes the signed message $S = D_2^A E_1^A(M)$ and sends the ciphertext $C = E^B(S)$ to B. On receiving

C, B decrypts it by calculating $D^B(C) = S$ and then confirms that A is the sender of the message by computing $D_1^A E_2^A(S) = D_1^A E_2^A D_2^A E_1^A(M) = M$. (The algebra relies on the second part of Theorem 1.)

We have proved that decrypting the RSA scheme of this paper and factorizing the modulus are computationally equivalent. However, there may still be certain messages which can be decoded easily. This is certainly the case if, for example, $E(M) = M$. This leads to the important notion of concealability.

A cryptosystem is called *totally concealable* if there is no message M such that $E(M) = M$. The concealment of the RSA cryptosystem is studied in [BB] and the cryptosystem of [Wil] is analysed in [KL]. Consider the case $e = 3$ of the present paper where $E(M) \equiv \{(1-\omega)^{4-t}((1-\omega)M + 1)\}^3 \pmod{R}$ and $t = 1, 2,$ or 3. Set $M_1 = (1-\omega)M + 1$. The equation $E(M) = M$ is equivalent to

$$M_1^3 \equiv \frac{M_1 - 1}{(1-\omega)^{3s+1}} \pmod{R},$$

where $s = 1, 2,$ or 3. By the Chinese remainder theorem, M_1 satisfies this congruence modulo R if and only if it satisfies the congruence simultaneously with the moduli p and q. In these latter cases, where we are working over a field, the solutions are given by Cardan's formula, as follows. The equation has the shape $x^3 + px + q = 0$ with $p = -(1-\omega)^{-3s-1}$ and $q = (1-\omega)^{-3s-1}$. Define the discriminant $\Delta = -4p^3 - 27q^2$ and the resolvents $\xi = \{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3\Delta}\}^{1/3}$ and $\eta = \{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3\Delta}\}^{1/3}$, where the two cube roots are chosen so that $\xi\eta = -3p$. There are three choices for the pair (ξ, η) and, correspondingly, three roots $x = \frac{1}{3}(\xi + \eta)$ of the equation (See pp. 187–189 of [Wa].) If -3Δ is a square modulo p and q and the quantities $-\frac{27}{2}q \pm \frac{3}{2}\sqrt{-3\Delta}$ are cubes modulo p and q, then there are nine unconcealed messages M with $E(M) = M$. By the laws of quadratic and cubic reciprocity, all these conditions are satisfied for primes lying in certain complete arithmetical progressions. If -3Δ is a square modulo p and q and at least one of the quantities $-\frac{27}{2}q \pm \frac{3}{2}\sqrt{-3\Delta}$ is not a cube modulo p or q, then there are no unconcealed messages. This implies that the cryptosystem is totally concealable for all the primes lying in certain complete arithmetical progressions. (The situation is more complicated if -3Δ is not a square.)

Rivest has pointed out that any cryptosystem in which there is a constructive proof of the equivalence of factorization and the breaking of the cipher will be vulnerable to a chosen ciphertext attack. (See [Wil].) Suppose B wishes to compromise the security of A's system. As in the proof of Theorem 2, B chooses K such that $(K|R)_3 \neq 1$ and sends $X = E_2^A(K)$ to A. To decrypt the message, A computes $N = D_2^A(X)$ and $M = D_1^A(N)$. If B can obtain M from A, then B can break A's system because B knows both K and $N = E_1^A(M)$. As noted in the proof of Theorem 2, these are cube roots of the same number and of different types and $(N - \omega^i K, R)$ is a nontrivial factor of R for $i = 0, 1,$ or 2. In general, B may have difficulty in persuading A to reveal M. However, if this scheme is used as a key exchange protocol, then A would return $E^B(M)$ to B, so enabling B to compute the key $M = D^B E^B(M)$.

The scheme of this paper works, in particular, with exponent $e = 3$. However, there is a weakness in using an RSA cryptosystem with a fixed small encryption exponent e. Suppose the same message M is sent to at least $3e$ receivers, the ith receiver having public encryption modulus R_i, and M lies in each of the corresponding message spaces. The type of $M_1 = (1 - \omega)M + 1$ will depend on i, in general, but it has only three possible values. We can therefore pick out e of the receivers for which M_1 has the same type. Consider only these e receivers and renumber them 1 to e. The ciphertext sent to the ith of these receivers is then $C_i \equiv N^e \pmod{R_i}$ where $N = E_1(M)$ is independent of i. If, as is likely, the R_i are relatively prime, then we can use the Chinese remainder theorem to find N^* such that

$$N^* \equiv N^e \pmod{R_1 R_2 \cdots R_e}$$

and $|N^*| < |R_1 R_2 \cdots R_e|$. Since N lies in the fundamental hexagon modulo R_i, we have $|N| < |R_i|$ for each i and so $N^e < R_1 R_2 \cdots R_e$. Therefore, $N^* = N^e$ and $N = (N^*)^{1/e}$ is revealed without the factorization of the moduli. To counter this attack, it is necessary to take a relatively large value of e as envisaged in the discussion of this paper.

While our discussion is mainly of theoretical interest, there is no serious difficulty in implementing the encryption and decryption procedures. Arithmetic in $\mathbf{Z}[\omega]$ is easy because this ring is a Euclidean domain and the various algorithms required are implicit in the descriptions we have given.

References

[BB] G. R. Blakley and I. Borosh, Rivest–Shamir–Adelman public key cryptosystem do not always conceal massages, *Comput. Math. Appl.* **5** (1979), 169–178.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1982.

[KL] S. Kothari and S. Lakshmivarahan, On the concealability of messages by the Williams public-key encryption scheme, *Comput. Math. Appl.* **10** (1984), 15–24.

[R] M. O. Rabin, Digitized signatures and public-key functions as intractable as factorization, Technical Report LCS/TR-212, M.I.T. Laboratory for Computer Science, 1979.

[Wa] B. L. van der Waerden, *Algebra*, vol. 1, Ungar, New York, 1970.

[Wi1] H. C. Williams, A modification of the RSA public-key procedure, *IEEE Trans. Inform. Theory* **26** (1980), 726–729.

[Wi2] H. C. Williams, An M^3 public-key encryption scheme, *Advances in Cryptology, CRYPTO '85*, Lecture Notes in Computer Science, vol. 218, Springer-Verlag, Berlin, pp. 358–368.