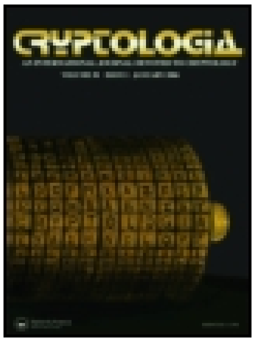

CRYPTOLOGIA

ISSN: 0161-1194 (Print) 1558-1586 (Online) Journal homepage: https://www.tandfonline.com/loi/ucry20

SECURITY OF NUMBER THEORETIC PUBLIC KEY CRYPTOSYSTEMS AGAINST RANDOM ATTACK, I

Bob Blakley & G. R Blakley

SECURITY OF NUMBER THEORETIC PUBLIC KEY CRYPTOSYSTEMS AGAINST RANDOM ATTACK, I

Bob Blakley and G. R Blakley

Recently W. Diffie and M. Hellman [2] introduced public key cryptosystems. More recently R. L Rivest, A. Shamir and L. Adleman [5] used elementary number theory to construct the most elegant known public key cryptosystem. The gist of the major results below is as follows. There are integers c $d \geq 2$ which make the congruence

$$x^{cd} \equiv x \bmod (m)$$

into an identity in x if and only if the modulus m is square free. When m is the product of k distinct primes there are at least 3^k positive integers $x \leq m$ such that

$$x^e \equiv x \bmod (m)$$

for any odd e It follows that an RSA public key cryptosystem must always leave at least nine messages unchanged by its coding process. Six of these nine messages constitute a definite weakness, but their discovery by a cryptanalyst or transmission by a sender is unlikely. Some RSA public key cryptosystems, unfortunately, fail to change any messages [1] by their coding process. However, it is possible to choose a coding exponent c in an RSA public key cryptosystem in such a fashion that only these nine messages satisfy the congruence

$$x^c \equiv x \bmod (m).$$

Thus most messages are scrambled by the coding process in a well chosen RSA public key cryptosystem. If safe primes (defined below in the paper) are multiplied together to yield m the cryptosystem is more resistant to sophisticated factoring algorithms applied to m, as Rivest, Shamir and Adleman have noted. But it also has other interesting properties, as shown below. The second paper in this series, which will appear in the next issue of CRYPTOLOGIA, carries these ideas further.

1. Introduction. Public key cryptosystems have become a household word since the appearance of *New Directions in Cryptography* by W. Diffie and M. Hellman [2]. More recently R. L. Rivest, A. Shamir and L. Adleman have enunciated [5] an elegant number theoretic method for obtaining digital signatures and public key cryptosystems. Since these brief readable papers are already classics, many readers of this paper will be familiar with them. Nevertheless the treatment below is self contained. Section 2 defines the needed cryptographic terminology and outlines the RSA public key cryptosystem. A central point of the paper [5] concerns a person who wants to receive coded messages and decode them. This would-be message receiver wants to be able to produce lists (c,d,m) of three positive integers with the property that the congruence $x^{cd} \equiv x \bmod (m)$ holds for every integer x (*i.e.* is an identity in x). Section 3 shows that it is possible to find c and d larger than 1 to do this if and only if m is square free. A precise statement of this is contained in Theorems 1.1 and 1.2. But first we introduce the $*$ and $\uparrow$ notations common in computer science. The symbol $x\uparrow f$ will stand for the fth power of x, and the symbol $a*b$ for the product of a and b. Thus $3*5 = 5*3 = 15$. Also $3\uparrow 5 = 243$, and $5\uparrow 3 = 125$.

Theorem 1.1: Let m be a positive integer. Suppose that there is a prime p such that $p\uparrow 2$ is a factor of m. Then there is no integer $f \geq 2$ such that the congruence $x\uparrow f \equiv x \bmod (m)$ holds identically in x.

To avoid a crazy quilt of notation all up and down the page we define six useful symbols. Let A be a finite set of integers and let f be a function whose domain includes A. Then the symbols

$\Pi\{f(a) \mid a \in A\}$, $\Sigma\{f(a) \mid a \in A\}$, $\mathrm{LCM}\ \{f(a) \mid a \in A\}$,

$\mathrm{GCD}\ \{f(a) \mid a \in A\}$, $\mathrm{MAX}\ \{f(a) \mid a \in A\}$, and $\mathrm{MIN}\ \{f(a) \mid a \in A\}$

stand for, respectively, the

product, sum, least common multiple [4, p. 22],

greatest common divisor [4, p. 14], maximum, and minimum

of the numbers $f(a)$ over every member a of the set A. For example suppose that $A = \{-15, -10, 10, 20\}$ and that $f(x) = x{\uparrow}2$ for every x. Then

$$\Pi\{f(a) \mid a \in A\} = \Pi\{a{\uparrow}2 \mid a \in A\} = 225*100*100*400 = 900{,}000{,}000$$

$$\Sigma\{f(a) \mid a \in A\} = \Sigma\{a{\uparrow}2 \mid a \in A\} = 225+100+100+400 = 825$$

$$\mathrm{LCM}\ \{f(a) \mid a \in A\} = \mathrm{LCM}\ \{a{\uparrow}2 \mid a \in A\} = \mathrm{LCM}\ \{225,100,100,400\} = 3{,}600$$

$$\mathrm{GCD}\ \{f(a) \mid a \in A\} = \mathrm{GCD}\ \{a{\uparrow}2 \mid a \in A\} = \mathrm{GCD}\ \{225,100,100,400\} = 25$$

$$\mathrm{MAX}\ \{f(a) \mid a \in A\} = \mathrm{MAX}\ \{a{\uparrow}2 \mid a \in A\} = \mathrm{MAX}\ \{225,100,100,400\} = 400$$

$$\mathrm{MIN}\ \{f(a) \mid a \in A\} = \mathrm{MIN}\ \{a{\uparrow}2 \mid a \in A\} = \mathrm{MIN}\ \{225,100,100,400\} = 100$$

It is well known [4, p. 22] that if A contains exactly two elements then $\Pi\{f(a) \mid a \in A\} = (\mathrm{LCM}\ \{f(a) \mid a \in A\})*(\mathrm{GCD}\ \{f(a) \mid a \in A\})$.

A positive integer m is *square free* if and only if it is the product of distinct primes belonging to some finite set T of primes. In other words $m = \Pi\{p \mid p \in T\}$. In this case let $\lambda(m) = \mathrm{LCM}\ \{p-1 \mid p \in T\}$. The converse of Theorem 1.1 now has the following form.

Theorem 1.2: Let m be a positive integer which is not divisible by the square of any prime p. If a positive integer s is relatively prime to $\lambda(m)$ then there are positive integer solutions t to the congruence $st \equiv 1 \bmod(\lambda(m))$. For such s, t and m the congruence $x{\uparrow}st \equiv x \bmod(m)$ holds identically in x. In fact, let f be an integer and suppose that $2 \le f$. Then the congruence $x{\uparrow}f \equiv x \bmod(m)$ holds identically in x if and only if $f \equiv 1 \bmod(\lambda(m))$.

Definition 1.1: A *number theoretic public key cryptosystem* is a list (c,d,m) of three integers, where m is square free and

$2 \le c \le m-1$, $2 \le d \le m-1$, and $cd \equiv 1 \bmod(\lambda(m))$.

The integer m is called the *public coding modulus*. The integer c is called the *public coding exponent*. The integer d is called the *secret decoding exponent*.

The Diffie-Hellman public key distribution system sketched in [2, p. 649] is, in a sense, a number theoretic public key cryptosystem based on a modulus $m = p$ which is a product of $n = 1$ primes. The RSA public key cryptosystem [5] is a number theoretic public key cryptosystem based on a modulus $m = pq$ which is a product of $n = 2$ primes. Diffie and Hellman [2, private communication] have pointed out a weakness in their key distribution system aforementioned which can be remedied by requiring that $p = 2a + 1$, where a is also prime. Rivest, Shamir and Adleman have also pointed out a weakness [5, p. 124] in the RSA public key cryptosystem unless $p-1$ and $q-1$ have very large factors. We shall second these two separate motions and argue below for the strongest possible assumption along these lines, to wit that every prime divisor p of the square free coding modulus m in a number theoretic public key cryptosystem be of the form $p = 2a + 1$, where a is also prime. Such primes p will, for this reason, be called *safe primes*.

With the general definition of number theoretic public key cryptosystems at our disposal we can say that the Diffie-Hellman public key distribution system and the RSA number theoretic method are, respectively, the cases $n = 1$ and $n = 2$ of the general definition of a number theoretic public key cryptosystem, in which the coding modulus m is the product of n distinct primes. It is also possible to buy even greater resistance to cryptanalysis, at the cost of increasing the size of m, by making it the product of three or more 100 digit primes.

Definition 1.2: Let m and c be positive integers. Suppose that $c \le m-1$. Then c is called a *permuting exponent* for m if any x, y which satisfy the congruence $x\uparrow c \equiv y\uparrow c \bmod(m)$ also satisfy the congruence $x \equiv y \bmod(m)$.

Definition 1.3: A permuting exponent $c \ge 2$ for a positive integer modulus m is called a *deranging exponent* for m when x satisfies the congruence $x\uparrow c \equiv x \bmod(m)$ if and only if it satisfies the congruence $x\uparrow 3 \equiv x \bmod(m)$.

As in [1] the idea is that to some m (namely square free positive integer m, as we shall see below) there corresponds at least one integer exponent $e > 1$ such that the function $f(x) = x\uparrow e$ determines a permutation of the residue classes modulo m. Any such exponent e can be used as a public coding exponent in a number theoretic public key cryptosystem based on the coding modulus m. A message receiver would like the f corresponding to the public coding exponent to be more than a permutation. He would like it to be a derangement, *viz.* a permutation with no fixed points. This would mean that no message is unchanged by the coding process. The hope is, of course, a vain one since $0\uparrow e \equiv 0 \bmod(m)$ and $1\uparrow e \equiv 1 \bmod(m)$. More generally it will become clear below that a coding exponent e must be odd, and that $x\uparrow e \equiv x \bmod(m)$ whenever $x\uparrow 3 \equiv x \bmod(m)$. But this is as far as it has to go. A careful message receiver can choose n distinct primes (whose product is m) and a positive integer $c < m$ in such a way that the function $f(x) = x\uparrow c$ effects a permutation of the residue classes modulo m and also has the property that there are only the inevitable $3\uparrow n$ solution classes to the congruence $x\uparrow c \equiv x \bmod(m)$, namely those residue classes x modulo m which obey the congruence $x\uparrow 3 \equiv x \bmod(m)$. Thus careful selection of the prime factors of m guarantees the existence not merely of a permuting exponent for m but of a deranging exponent for m. This point, which has never been addressed before, is crucial. It implies that the coding process in an appropriately constructed RSA public key cryptosystem (namely a number theoretic public key cryptosystem based on a modulus m which is the product of two prime factors) really codes. It changes the appearance of all but nine messages. The exact result is as follows.

Theorem 1.3: Let m be a positive integer which is not divisible by the square of any prime p. Let c be a positive integer. To avoid trivial cases assume that $2 \le c \le m-1$. Then c is a deranging exponent for m if and only if both the following conditions hold:

$$\mathrm{GCD}\{\lambda(m),\ c\} = 1; \text{ and } \qquad \mathrm{GCD}\{\lambda(m),\ c-1\} = 2.$$

These three theorems constitute a fundamental property of number theoretic public key cryptosystems. They follow from the results stated in Section 3. In the interests of brevity the results in Sections 3 and 4 are not themselves proved here since the proofs are all easy for anybody acquainted with number theory to provide, once the results are stated. For more on proofs, consult the sequel.

2. The RSA number theoretic method. This section is an outline of the parts of the theory of RSA public key cryptosystems which are needed below. The reader interested in digital signatures, key distribution, forgery and certain other topics omitted below should consult [2,5]. All logarithms in this paper are to base 2. Thus, for example, $\log(8) = 3$.

A *directorate* publishes, and periodically updates, a *directory*, available to anybody in the world willing to pay for a copy or borrow it from a library. This directory begins by specifying two positive real numbers, the *gauge* g, and the *width* w. It then describes a universally agreed upon scheme for going back and forth between short pieces of messages typed in Hollerith characters and integers x such that $0 < \log(x) < 2g$. One such standard scheme, described in [5], is to represent Hollerith characters as two digit numbers so that, for example,

BLANK $\leftrightarrow$ 00, A $\leftrightarrow$ 01, B $\leftrightarrow$ 02, C $\leftrightarrow$ 03, ...

In this translation scheme the number 201 04000 30120 = 0201 04000 30120 is rendered as the phrase BAD CAT and *vice versa*. Everybody who can afford a copy of the directory will use this scheme to go back and forth between (possibly very long) Hollerith character typescripts and (possibly very long) lists of (possibly very small) positive integers. The remaining pages of the directory are devoted to numerous listings. A *listing* consists of the name N of a *receiver* (*i.e.* person or organization hoping to receive coded communications) together with two positive integers $m(N)$ and $c(N)$, which receiver N has communicated to the directorate. The *coding modulus* $m(N)$ of the receiver N is an integer such that $2g < \log(m(N)) < 2g + 2w$. The *coding exponent* $c(N)$ of the receiver N is a positive integer less than $m(N)$. The directorate is trustworthy to the following extent. If the directory contains a listing involving the receiver N then that listing originated with N and is exactly as N submitted it. This is a realistic assumption since each receiver N whose name occurs in a listing in the directory can check the listing and issue a public denial if necessary. See [5] for more on this.

Suppose that you want to send a private communication in the form of a Hollerith character typescript to receiver N over a public channel. You obtain a copy of the directory. You use the

The last congruence holds because $c(N)$ is an odd positive integer in consequence of the way it was chosen.

The general idea of number theoretic public key cryptosystems, suggesting a development based on Theorems 1.1, 1.2 and 1.3, has several advantages. First, the Diffie-Hellman key distribution scheme and the RSA number theoretic method are both subsumed under it, as are a host of other cryptosystems. Second, it replaces $\phi(m)$ with the more fundamental $\lambda(m)$ in accordance with a suggestion made by Rivest, Shamir and Adleman [5, p. 126], and thus clarifies the situation. Third, it is possible to understand the solution set of the congruence $x\uparrow cd \equiv x \bmod(m)$ whether or not the message receiver is correct in his assumption that p and q are both prime.

A few remarks about computational difficulty are in order. It is easy to tell whether a large positive integer is a square, a cube, a fifth power,... . It is easy to verify that a large positive integer is not prime, or that it is prime to all intents and purposes. It is easy to add, subtract, multiply and raise large positive integers to large positive integer powers modulo a large positive integer modulus. It is easy to calculate logarithms to base two, greatest common divisors and least common multiples. It is hard to factor a large positive integer, to tell whether a large positive integer is prime, or even to tell whether a large positive integer is square free. As of this writing every positive integer p known to be prime satisfies the inequality $0 < \log(p) < 19937$. So it is hard to find large primes.

3. <u>The background in modular arithmetic</u>.

Definition 3.1: The *Euler totient* [4, pp. 27-29] function ϕ and the *universal exponent* [4, p. 53] function λ are defined as follows. Let b be any positive integer. Let q be any odd prime. Let T be any finite set of primes. Then

$$\phi(1) = \phi(2) = \lambda(1) = \lambda(2) = 1$$

$$\phi(4) = \lambda(4) = \lambda(8) = 2$$

$$\phi(2\uparrow(1+b)) = \lambda(2\uparrow(2+b)) = 2\uparrow b$$

$$\phi(q\uparrow b) = \lambda(q\uparrow b) = (q-1)q\uparrow(b-1)$$

$$\phi(\Pi\{p\uparrow e(p) \mid p \in T\}) = \Pi\{\phi(p\uparrow e(p)) \mid p \in T\}$$

$$\lambda(\Pi\{p\uparrow e(p) \mid p \in T\}) = \mathrm{LCM}\{\lambda(p\uparrow e(p)) \mid p \in T\}.$$

Now suppose that a and m are positive integers, and that a is a divisor of m. It is obvious from Definition 3.1 that $\lambda(a)$ is a divisor of $\lambda(m)$, as well as that $\phi(a)$ is a divisor of $\phi(m)$. It is also clear that $\lambda(m)$ is a divisor of $\phi(m)$ for every positive integer m. The only m at which these two functions coincide are 1, 2, 4, the powers of any single odd prime q, and twice the powers of any single odd prime. For example,

$$\lambda(628\ 67805) = \lambda(3*5*7*11*13*53*79) = \mathrm{LCM}\ \{2,4,6,10,12,52,78\} = 780$$

$$\phi(628\ 67805) = \phi(3*5*7*11*13*53*79) = 2*4*6*10*12*52*78 = 233\ 62560$$

universally agreed upon translation scheme described at the front of the directory to turn this typescript into a list of cleartext messages. A *cleartext message* is an integer x such that $0 < \log(x) < 2g$. Anybody with a copy of the directory can easily turn your list of cleartext messages back into a copy of your original typescript, of course. But now you code each cleartext message x in the list. This is done as follows. Form the smallest positive integer y such that $y \equiv x\uparrow c(N) \bmod (m(N))$. The number y is the *coded message* corresponding to the cleartext message x. You now transmit your list of coded messages to receiver N, perhaps by printing them as an ad in *Newsweek*. Receiver N has three closely held secrets. They are two positive integers $p(N)$ and $q(N)$, which he believes to be primes, and a third positive integer $d(N)$, his *decoding exponent*. Before submitting his listing to the directory he looked at a copy and ascertained g and w. He then chose an integer r at random subject to the constraint that $g < \log(r) < g + w$. He then applied one of the fairly cheap probabilistic tests mentioned in [5] to r in order to see whether r is *prime to all intents and purposes, i.e.* to see whether the probability that r is a prime is as close to 1 as he can afford to verify, given the time and money at his disposal, and the value to him of secure incoming communications. If r failed the test he discarded it, picked another integer, subject to the same constraints, and tested again. The first two of these numbers which passed the tests, *i.e.* turned out to be prime to all intents and purposes, became $p(N)$ and $q(N)$. Rivest, Shamir and Adleman [5] suggest the use of two 100 digit primes $p(N)$ and $q(N)$. This amounts to a choice of $g = 328.870\ldots$, and $w = 3.321\ldots$. The coding modulus $m(N)$ in the directory listing corresponding to the message receiver N is their product. Thus $m(N) = p(N)q(N)$. The receiver then found a positive integer $c(N)$ which is relatively prime to both $p(N) - 1$ and $q(N) - 1$. It follows that $c(N)$ was odd. After that, he found the smallest positive integer solution d to the congruence $c(N)d \equiv 1 \bmod ([p(N)-1][q(N)-1])$. This smallest positive solution is his third secret number $d(N)$. To turn your coded message y into his *decoded message* z, the message receiver N finds the smallest positive integer z such that $z \equiv y\uparrow d(N) \bmod (m(N))$. If he is correct in his assumption that $p(N)$ and $q(N)$ are both prime then $z = x$. In other words the progression from cleartext message x to coded message y to decoded message z is a loop which ends where it started. He decodes the entire list of cleartext messages from you in the same way. Then he turns each of them back into a piece of Hollerith typescript according to the universally agreed upon procedure for doing this which is printed at the front of every copy of the directory. And the typescript he reads is the same as the one you wrote--if he was correct in assuming that $p(N)$ and $q(N)$ are both primes. Recall that a cleartext message x satisfies the inequalities $0 < \log(x) < 2g < \log(m(N))$. It follows that $2 \le x \le m(N) - 1$. In particular the numbers 0 and 1 are not cleartext messages. This is quite reasonable, since three trivial numbers are unchanged by the coding process. In other words,

$$0\uparrow c(N) \equiv 0 \bmod (m(N))$$

$$1\uparrow c(N) \equiv 1 \bmod (m(N))$$

$$(m(N)-1)\uparrow c(N) \equiv (-1)\uparrow c(N) \equiv -1 \equiv (m(N)-1) \bmod (m(N)).$$

$$\lambda(1200) = \lambda(16*3*25) = \text{LCM } \{4,2,20\} = 20$$

$$\phi(1200) = \phi(16*3*25) = 8*2*20 = 320.$$

Lemma 3.1: If m is a positive integer and x is an integer then $x\uparrow(m+\lambda(m)) \equiv x\uparrow m \bmod(m)$.

Lemma 3.2: If a positive integer m is square free then $x\uparrow(1+\lambda(m)) \equiv x \bmod(m)$ for every integer x.

Definition 3.2: Let m be a positive integer. Let x be an integer. The *multiplicative cycle* of x modulo m (written cyc[x,m]) is the smallest positive integer s to which there corresponds an integer $t(s)$ such that $x\uparrow(t(s)+s) \equiv x\uparrow t(s) \bmod(m)$. The *multiplicative period* of x modulo m (written per[x,m]) is the smallest positive integer r such that $x\uparrow(1+r) \equiv x \bmod(m)$. The *multiplicative order* of x modulo m (written ord[x,m]) is the smallest positive integer n such that $x\uparrow n \equiv 1 \bmod(m)$.

Obviously the phrase *integer* $t(s)$ *such that* in the definition of multiplicative cycle can be replaced by the phrase *positive integer* $t(s)$ *such that* to yield an equivalent definition. To see this merely note that if $x\uparrow(t(s)+s) \equiv x\uparrow t(s) \bmod(m)$ and if $w > |t(s)|$ then $w + t(s)$ is positive and $x\uparrow(w+t(s)+s) \equiv x\uparrow(w+t(s)) \bmod(m)$.

For example the successive positive integer powers of 39, 40, and 41 modulo 45 are as follows:

$$\{39\uparrow n \bmod(45) \mid 1 \le n\} = \{39,36,9,36,9,36,9,36,9,36,\ldots\}$$

$$\{40\uparrow n \bmod(45) \mid 1 \le n\} = \{40,25,10,40,25,10,40,25,10,40,\ldots\}$$

$$\{41\uparrow n \bmod(45) \mid 1 \le n\} = \{41,16,26,31,11,1,41,16,26,31,\ldots\}$$

Therefore ord[39,45], per[39,45] and ord[40,45] do not exist. Also

$$\text{cyc}[39,45] = 2$$

$$\text{per}[40,45] = \text{cyc}[40,45] = 3$$

$$\text{ord}[41,45] = \text{per}[41,45] = \text{cyc}[41,45] = 6.$$

Lemma 3.3: Let m be a positive integer and let x be an integer. Then ord[x,m] exists if and only if x is relatively prime to m. Moreover per[x,m] exists if and only if every prime common factor p of x and m occurs to at least as high a power in x as it does in m.

Lemma 3.4: Let m be a positive integer. If v is a factor of $\lambda(m)$ then there is a positive integer b such that ord[b,m] = v. Conversely, if cyc[x,m] = s then s is a factor of $\lambda(m)$.

Let Z be the set of integers. It is an obvious corollary of Lemma 3.4 that

$$\{\text{ord}[x,m] \mid x \in Z\} = \{\text{per}[x,m] \mid x \in Z\} = \{\text{cyc}[x,m] \mid x \in Z\}$$
$$= \{f \mid f \text{ is a positive integer factor of } \lambda(m)\}.$$

Theorem 3.1: Let Y be a finite set of pairwise relatively prime positive integers. Let m be the product of the members of Y. Then cyc[x,m] = LCM {cyc[x,y] | y ∈ Y}.

For example 5 and 9 are relatively prime and

cyc[2,5] = 4, cyc[2,9] = 6,

cyc[33,5] = 4, cyc[33,9] = 1.

Taking the least common multiple, we see that cyc[2,45] = LCM {4,6} = 12 and that cyc[33,45] = LCM {1,4} = 4. It then also follows that ord[2,45] = per[2,45] = 12. On the other hand cyc[2,15] = 4 and cyc[2,3] = 2. So the relative primeness assumption in Theorem 3.1 is necessary.

Lemma 3.5: Let p be a prime and let m be a positive integer. If p↑2 is a divisor of m then the congruence p↑v ≡ p mod(m) cannot be satisfied by any integer $v \geq 2$.

A partial converse of Lemma 3.5, adequate to the purposes at hand, is the following.

Lemma 3.6: If an odd positive integer m is square free then the congruence x↑(1+v) ≡ x mod(m) is an identity in x if and only if v is a multiple of $\lambda(m)$.

As a corollary we have

Theorem 3.2: Suppose an odd positive integer m is square free. Let c and d be integers. They satisfy the congruence cd ≡ 1 mod(λ(m)) if and only if the congruence x↑cd ≡ x mod(m) is an identity in x.

We now note an obvious consequence of Lemma 3.6 and Theorem 3.2. Let m be a positive integer Then there is a positive integer v such that the congruence x↑(1+v) ≡ x mod(m) is an identity in x if and only if m is square free. When m is square free the only such exponents v are those for which v is a multiple of the universal exponent $\lambda(m)$.

At this point we have proved Theorems 1.1 and 1.2.

Theorem 3.3: Let m be a positive integer. Suppose that the integers c and $\lambda(m)$ are relatively prime. Suppose that $1 < c < \lambda(m)$. Every integer d such that the congruence x↑cd ≡ x mod(m) holds identically in x satisfies the inequality $|d| > \lambda(m)/c - 1$. One of these integers d satisfies the inequality $1 < d < \lambda(m)$.

Corollary 3.1. Let a, b, p and q be primes. Suppose that $a < b$, that $2a + 1 = p$, that $2b + 1 = q$, and that $pq = m$. Suppose that c is relatively prime to 2ab. Suppose that $1 < c < 2ab$. Then every integer d such that the congruence x↑cd ≡ x mod(m) holds identically in x satisfies the inequality $|d| > 2ab/c - 1$. One of these integers satisfies the inequality $1 < d < 2ab$.

Theorem 3.4: Let m be a positive integer. Then cyc[x,m] exists for every integer x. If v, w and x are integers for which x↑(v+w) ≡ x↑v mod(m) then w is a multiple of cyc[x,m]. If an integer x has a multiplicative order modulo m then it has a multiplicative period modulo m and ord[x,m] = per[x,m]. If an integer x has a multiplicative period modulo m then per[x,m] = cyc[x,m]. Finally, it is true that x↑(v+cyc[x,m]) ≡ x↑v mod(m) for every integer $v \geq m$.

Corollary 3.2: $cyc[x\uparrow u\ m]$ divides $cyc[x,m]$ if x, u, and m are positive integers.

You do not change the multiplicative period modulo m of a message in a number theoretic public key cryptosystem when you code it or decode it. To see this merely note that $y \equiv x\uparrow c \bmod(m)$ if and only if $x \equiv y\uparrow d \bmod(m)$. An application of Corollary 3.2 to each of these congruences shows that $cyc[y,m]$ is a factor of $cyc[x,m]$ and conversely. Therefore $per[x,m] = per[y,m]$.

Lemma 3.7: A positive integer m is prime if and only if every integer which is not a multiple of m has a multiplicative order modulo m. A positive integer m is square free if and only if every integer has a multiplicative period modulo m.

Lemma 3.8: Let m be a square free positive integer. Let c be a positive integer. Let x be an integer. Then $x\uparrow c \equiv x \bmod(m)$ if and only if $per[x,m]$ is a common divisor of $c-1$ and $\lambda(m)$.

Theorem 3.5: Let m be a square free odd positive integer. Let c be an odd positive integer. Suppose that $GCD\ \{c-1,\ \lambda(m)\} = 2$. Then $x\uparrow c \equiv x \bmod(m)$ if and only if $per[x,m] \le 2$.

Lemma 3.9: A positive integer c is a permuting exponent for a square free odd positive integer modulus m if and only if $GCD\ \{\lambda(m),\ c\} = 1$.

Theorem 3.6: Suppose that a positive integer c is a permuting exponent for a square free odd positive integer modulus m. Then c is a deranging exponent for m if and only if $GCD\ \{\lambda(m),\ c-1\} = 2$.

Corollary 3.3: Let m be a square free odd positive integer modulus. Let $c \ge 2$ be an integer. Then c is a deranging exponent for m if and only if both $GCD\{\lambda(m),\ c\} = 1$ and $GCD\{\lambda(m),\ c-1\} = 2$.

At this point we have proved Theorem 1.3.

4. Coding moduli which are products of distinct safe primes. Rivest, Shamir and Adleman point out in [5, p. 124] that the prime factors p and q of a coding modulus m should be chosen so that $p-1$ and $q-1$ themselves have large prime factors. This provides some protection against sophisticated factoring algorithms. They did not explicitly pursue this precaution to its logical conclusion, the notion of a safe prime. But they confined their treatment of examples largely to safe primes. So did Simmons and Norris [7].

Definition 4.1: A prime p is *safe* if there is an odd prime a such that $2a + 1 = p$. An *unsafe* prime is a prime which is not safe. If p is a safe prime let $a(p)$ be the odd prime such that $2a(p) + 1 = p$. If no confusion is likely to result we shall write a instead of $a(p)$.

Thus 7, 11, 23, 47, 59, 83, 107, 167, 179, 227, 263, 347, 359, 383, 467, 479, 503, 563, 587, 719, 839, 863, 887, 983, 1019, 1187 and 1283 are the smallest safe primes. Every safe prime is congruent to 3 modulo 4. The primes p and q in Corollary 3.1 are safe.

Lemma 4.1: Suppose that p and q are safe primes whose product is m. Then the inequality $4 < (m-1)/a(p)a(q) < 5.5$ always holds.

Lemma 4.2: Suppose that p and q are distinct safe primes whose product is m. Then there are exactly three positive integers $f \le m$ such that the congruence $x{\uparrow}f \equiv x \bmod(m)$ holds identically in x.

Theorem 4.1: If p is a safe prime then the equalities

$$\mathrm{per}[0,p] = \mathrm{per}[1,p] = 1, \qquad \mathrm{per}[p-1,p] = 2,$$
$$\mathrm{per}[x{\uparrow}2,p] = a, \quad \text{and} \quad \mathrm{per}[p-x{\uparrow}2,p] = 2a$$

hold for every integer x such that $2 \le x \le a$.

Comment: The assumption that p is a safe prime makes all the difference from a cryptographic viewpoint since, for example, $3{\uparrow}3 \equiv 9{\uparrow}3 \equiv 5{\uparrow}4 \equiv 1 \bmod(13)$. To see one application to cryptography, merely let T be a set containing n safe primes. Then Theorems 3.1 and 4.1 give the exact structure of the multiplicative period of every residue x modulo m, where $m = \Pi\{p \mid p \in T\}$. It suffices to know the multiplicative period of x modulo p for every $p \in T$. This will turn out to be important below. Theorems 3.1 and 4.1 have the following immediate corollary.

Theorem 4.2: Let T be a finite set of safe primes. Let $m = \Pi\{p \mid p \in T\}$. Then $\lambda(m) = 2\,\Pi\{a(p) \mid p \in T\}$. Moreover, $\mathrm{per}[x,m]$ is a divisor of $\lambda(m)$ for every integer x.

Theorem 4.2, in turn, has the following special case when T has exactly two members.

Corollary 4.1: Suppose that p and q are distinct safe primes. Suppose that $a = a(p)$, that $b = a(q)$, and that $pq = m$. Then $\mathrm{per}[x,m]$ is one of the eight members of the set $\{1,2,a,b,2a,2b,ab,2ab\}$

Theorem 4.3 below is the explicit statement of the joint import of Theorem 3.1 and Theorem 4.1. We need some notation before stating it. Let p be a safe prime. Then there are four pairwise disjoint sets which, between them, exhaust the set Z of integers:

$$A(p) = \{x \mid x \equiv 0 \bmod(p) \quad \text{or} \quad x \equiv 1 \bmod(p)\};$$
$$B(p) = \{x \mid x \equiv -1 \bmod(p)\};$$
$$C(p) = \{b \mid b \equiv x{\uparrow}2, \text{ where } x \notin A(p) \cup B(p)\};$$
$$D(p) = \{b \mid b \equiv -x{\uparrow}2, \text{ where } x \notin A(p) \cup B(p)\}.$$

Thus $C(p)$ is the set of nontrivial quadratic residues modulo p (*i.e.* squares which are not congruent to either 0 or 1 modulo p). The set $D(p)$ consists of all numbers of the form $p-c$, where c belongs to $C(p)$. It is thus the set of nontrivial quadratic nonresidues modulo p. Each of these two sets is the union of $a-1$ residue classes modulo p. The set $B(p)$ is a single residue class modulo p, namely the residue class containing $p-1$. The set $A(p)$ is the union of the zero residue class modulo p and the class to which 1 belongs modulo p.

Theorem 4.3: If p and q are distinct safe primes let $a = a(p)$, let $b = a(q)$, and let $m = pq$. Then the set $A(p) \cap A(q)$ consists of integers with multiplicative period 1 modulo m. It is the union of 4 residue classes modulo m. The set

$$[A(p) \cap B(q)] \cup [A(q) \cap B(p)] \cup [B(p) \cap B(q)]$$

consists of integers with multiplicative period 2 modulo m. It is the union of 5 residue classes modulo m. The set $A(p) \cap C(q)$ consists of integers with multiplicative period b modulo m. It is the union of $2(b-1)$ residue classes modulo m. The set $A(q) \cap C(p)$ consists of integers with multiplicative period a modulo m. It is the union of $2(a-1)$ residue classes modulo m. The set

$$[B(p) \cap C(q)] \cup [B(p) \cap D(q)] \cup [A(p) \cap D(q)]$$

consists of integers with multiplicative period $2b$ modulo m. It is the union of $4(b-1)$ residue classes modulo m. The set

$$[B(q) \cap C(p)] \cup [B(q) \cap D(p)] \cup [A(q) \cap D(p)]$$

consists of integers with multiplicative period $2a$ modulo m. It is the union of $4(a-1)$ residue classes modulo m. The set $C(p) \cap C(q)$ consists of integers with multiplicative period ab modulo m. It is the union of $(a-1)(b-1)$ residue classes modulo m. The set

$$[C(p) \cap D(q)] \cup [C(q) \cap D(p)] \cup [D(p) \cap D(q)]$$

consists of integers with multiplicative period $2ab$ modulo m. It is the union of $3(a-1)(b-1)$ residue classes modulo m.

The integer m in the statement of Theorem 4.3 is square free. Therefore $\mathrm{per}[x,m]$ exists for every integer x. If y belongs to one of the $m + 1 - p - q$ residue classes which are relatively prime to m then y has multiplicative order modulo m, and $\mathrm{ord}[y,m] = \mathrm{per}[y,m]$. Therefore we have

Corollary 4.2: If p and q are distinct safe primes let $a = a(p)$, let $b = a(q)$, and let $m = pq$. Then every integer with multiplicative order 1 modulo m is congruent to 1 modulo m. The integers x with multiplicative order 2 modulo m are those which satisfy one of the following three pairs of simultaneous congruences:

$$x \equiv 1 \bmod (p), \qquad x \equiv -1 \bmod (q);$$

or

$$x \equiv -1 \bmod (p), \qquad x \equiv 1 \bmod (q);$$

or

$$x \equiv -1 \bmod (p), \qquad x \equiv -1 \bmod (q).$$

The integers with multiplicative order b modulo m make up $b-1$ residue classes modulo m. They are the integers which have multiplicative period b modulo m and are not congruent to zero modulo p. A similar statement holds regarding integers with multiplicative order a modulo m. The integers with multiplicative order $2b$ modulo m make up $3(b-1)$ residue classes modulo m. They are the integers which have multiplicative period b modulo m and are not congruent to zero modulo p. A similar statement holds regarding integers with multiplicative order 2a modulo m. Finally

$$\mathrm{ord}[x,m] = ab \quad \text{if and only if} \quad \mathrm{per}[x,m] = ab$$
$$\mathrm{ord}[x,m] = 2ab \quad \text{if and only if} \quad \mathrm{per}[x,m] = 2ab.$$

Example 4.1: The primes 7 and 23 are safe. Evidently

0	=	0*7	=	0*23
1	=	1+0*7	=	1+0*23
70	=	10*7	=	1+3*23
92	=	1+13*7	=	4*23
22	=	1+3*7	=	-1+1*23
69	=	-1+10*7	=	3*23
91	=	13*7	=	-1+4*23
139	=	-1+20*7	=	1+6*23
160	=	-1+23*7	=	-1+7*23

Hence we have all the numbers whose multiplicative period modulo 161 is either 1 or 2. More generally, the situation which Theorem 4.3 classifies is exemplified in Table 1 below.

Theorem 4.4: Suppose that p and q are distinct primes whose product is m. Suppose that x is not congruent modulo m to one of the trivial values -1, 0 or 1. If per[x,m] = 1 then GDC {x,m} is either p or q. If per[x,m] = 2 then GCD {x+1,m} is either p or q.

Example 4.2: Rivest, Shamir and Adleman considered an instructive example [5] of a number theoretic public key cryptosystem. G. J. Simmons and J. N. Norris [7] also considered it. Let p = 47 and q = 59. Then

$$a(p) = a = 23, \qquad a(q) = b = 29, \qquad pq = m = 2773, \text{ and}$$
$$(1/2)\phi(2773) = \lambda(2773) = 2*23*29 = 1334.$$

Thus we know from Lemma 4.2 that the congruences

$$x\uparrow 1 \equiv x\uparrow 1335 \equiv x\uparrow 2669 \equiv x \bmod(2773)$$

hold identically in x. Other positive integer exponents r for which the congruence $x\uparrow(1+r) \equiv x \bmod(2773)$ holds identically in x are of the form r = 1334t where 3 ≤ t. It is easy to verify that

0	=	0*47	=	0*59
1	=	1 + 0*47	=	1 + 0*59
236	=	1 + 5*47	=	4*59
2538	=	54*47	=	1 + 43*59.
235	=	5*47	=	-1 + 4*59
471	=	1 + 10*47	=	-1 + 8*59
2302	=	-1 + 49*47	=	1 + 39*59

$$2537 = -1 + 54*47 = 43*59$$
$$2772 = -1 + 59*47 = -1 + 47*59.$$

Therefore $per[0,2773] = per[1,2773] = per[236,2773] = per[2538,2773] = 1$ and $per[235,2773] = per[471,2773] = per[2302,2773] = per[2537,2773] = per[2772,2773] = 2$. In accordance with Theorem 4.4 one sees that

$$GCD\ \{236,2773\} = GCD\ \{1+235,2773\} = GCD\ \{1+471,2773\} = 59 = q$$
$$GCD\ \{2538,2773\} = GCD\ \{1+2302,2773\} = GCD\ \{1+2537,2773\} = 47 = p.$$

Thus neither $ord[0,2773]$ nor $ord[236,2773]$ nor $ord[2538,2773]$ exist. It is also easy to see that neither $ord[235,2773]$ nor $ord[2537,2773]$ exist. On the other hand 1 has multiplicative order 1 modulo 2773. Moreover 471, 2302 and 2772 are relatively prime to 2773, and therefore have multiplicative order 2 modulo 2773. These nine integers represent the only residue classes with multiplicative period less than 23 modulo 2773. Since 7 and 953 and 2287 are all relatively prime to $1334 = \lambda(2773)$ it is clear from the foregoing that

$$\begin{aligned}
0\uparrow 2287 &\equiv 0\uparrow 953 \equiv 0\uparrow 7 \equiv 0\uparrow 3 \equiv 0 \bmod(2773),\\
1\uparrow 2287 &\equiv 1\uparrow 953 \equiv 1\uparrow 7 \equiv 1\uparrow 3 \equiv 1 \bmod(2773),\\
235\uparrow 2287 &\equiv 235\uparrow 953 \equiv 235\uparrow 7 \equiv 235\uparrow 3 \equiv 235 \bmod(2773),\\
236\uparrow 2287 &\equiv 236\uparrow 953 \equiv 236\uparrow 7 \equiv 236\uparrow 3 \equiv 236 \bmod(2773),\\
471\uparrow 2287 &\equiv 471\uparrow 953 \equiv 471\uparrow 7 \equiv 471\uparrow 3 \equiv 471 \bmod(2773),\\
2302\uparrow 2287 &\equiv 2302\uparrow 953 \equiv 2302\uparrow 7 \equiv 2302\uparrow 3 \equiv 2302 \bmod(2773),\\
2537\uparrow 2287 &\equiv 2537\uparrow 953 \equiv 2537\uparrow 7 \equiv 2537\uparrow 3 \equiv 2537 \bmod(2773),\\
2538\uparrow 2287 &\equiv 2538\uparrow 953 \equiv 2538\uparrow 7 \equiv 2538\uparrow 3 \equiv 2538 \bmod(2773),\\
2772\uparrow 2287 &\equiv 2772\uparrow 953 \equiv 2772\uparrow 7 \equiv 2772\uparrow 3 \equiv 2772 \bmod(2773).
\end{aligned}$$

Thus if one chooses 7 or 953 or 2287 as public coding exponent, or as secret decoding exponent, these nine message are unchanged by the coding process. The public key cryptosystems in question are (7, 953, 2773), (7, 2287, 2773), (953, 7, 2773), (953, 1341, 2773), (953, 2675, 2773), (2287, 7, 2773), (2287, 1341, 2773), and (2287, 2675, 2773). For each of these nine messages, 0, 1, 235, ... , 2772, the ciphertext is equal to the cleartext, in accordance with Theorem 3.5, no matter what coding exponent is chosen. It follows from Theorem 4.3 and Corollary 4.2 that Table 2 below describes numbers of residue classes with the various possible multiplicative periods and orders modulo $m = 2773$.

Let $c = 7$, let $d = 953$, and let $e = 2287$. Then $cd = 6671 = 1 + 5*1334$, and $ce = 16009 = 1 + 12*1334$. Therefore $x\uparrow cd \equiv x\uparrow ce \equiv x \bmod (2773)$ for every integer x. Note that $e > d > 191 > 1334/7 - 1 = \lambda(m)/c - 1$ in accordance with Theorem 3.3. We close this consideration of 47 and 59 with a few remarks which will be useful when we return to these safe primes in the sequel. Note that the sets $A(47)$ and $A(59)$ contain 0 and 1, that $46 \in B(47)$, that $58 \in B(59)$, and that it is easy to verify that the typical members of $C(47)$, $D(47)$, $C(59)$ and $D(59)$ are shown in Table 3 below. By a *typical member* of the set $C(p)$ (resp. $D(p)$) we mean a member j of $C(p)$ (resp. $D(p)$) such that $1 < j < p$. It follows from Table 3 and Theorem 4.3 that

	A(7) contains		B(7) contains	C(7) contains		D(7) contains	
	0	1	6	2	4	3	5
A(23) contains	in this box period is 1			in this box period is 3			
0	0	92	69	23	46	115	138
1	70	1	139	93	116	24	47
B(23) contains	in this box period is 2			in this box period is 6			
22	91	22	160	114	137	45	68
C(23) contains	in this box period is 11			in this box period is 33			
2	140	71	48	2	25	94	117
3	49	141	118	72	95	3	26
4	119	50	27	142	4	73	96
6	98	29	6	121	144	52	75
8	77	8	146	100	123	31	54
9	147	78	55	9	32	101	124
12	35	127	104	58	81	150	12
13	105	36	13	128	151	59	82
16	154	85	62	16	39	108	131
18	133	64	41	156	18	87	110
D(23) contains	in this box period is 22			in this box period is 66			
5	28	120	97	51	74	143	5
7	7	99	76	30	53	122	145
10	56	148	125	79	102	10	33
11	126	57	34	149	11	80	103
14	14	106	83	37	60	129	152
15	84	15	153	107	130	38	61
17	63	155	132	86	109	17	40
19	42	134	111	65	88	157	19
20	112	43	20	135	158	66	89
21	21	113	90	44	67	136	159

Table 1
The eight boxes above contain a complete set of residues modulo 161.
The row a residue occurs in identifies it modulo 23 and the column identifies it modulo 7.
Each box contains nothing but residues with the multiplicative period modulo 161 peculiar to that box.
The scheme above exemplifies Theorem 4.3.

d	number of residue classes modulo m with multiplicative period d modulo m	number of residue classes modulo m with multiplicative order d modulo m
1	4	1
2	5	3
23	44	22
29	56	28
46	88	66
58	112	84
667	616	616
1334	1848	1848
Total	2773	2668

Table 2

Typical members of C(47)	Typical members of D(47)	Typical members of C(59)	Typical members of D(59)
2	5	3	2
3	10	4	6
4	11	5	8
6	13	7	10
7	15	9	11
8	19	12	13
9	20	15	14
12	22	16	18
14	23	17	23
16	26	19	24
17	29	20	30
18	30	21	31
21	31	22	32
24	33	25	33
25	35	26	34
27	38	27	37
28	39	28	38
32	40	29	39
34	41	35	40
36	43	36	42
37	44	41	43
42	45	45	44
		46	47
		48	50
		49	52
		51	54
		53	55
		57	56

Table 3

$$per[2,2773] = per[5,2773] = per[6,2773] = per[8,2773] = per[10,2773] = per[11,2773] = 1334$$
$$per[3,2773] = per[4,2773] = per[7,2773] = per[9,2773] = 667$$

Note the following equalities, which have obvious interpretations as congruences modulo 47 and modulo 59:

$$49*47 = 2 + 39*59 = 2303;$$
$$44*47 = 3 + 35*59 = 2068;$$
$$1 + 54*47 = 2 + 43*59 = 2539;$$
$$1 + 49*47 = 3 + 39*59 = 2304;$$
$$-1 + 44*47 = 2 + 35*59 = 2067;$$
$$-1 + 39*47 = 3 + 31*59 = 1832;$$
$$12*59 = 3 + 15*47 = 708;$$
$$20*59 = 5 + 25*47 = 1180;$$
$$1 + 8*59 = 3 + 10*47 = 473;$$
$$1 + 16*59 = 5 + 20*47 = 945;$$
$$-1 + 16*59 = 3 + 20*47 = 943;$$
$$-1 + 24*59 = 5 + 30*47 = 1415.$$

It therefore follows from Table 3 and Theorem 4.3 that

$$per[2303,2773] = per[2539,2773] = per[2067,2773] = per[1832,2773] = 58$$
$$per[2068,2773] = per[2304,2773] = 29$$
$$per[1180,2773] = per[945,2773] = per[1415,2773] = per[943,2773] = 46$$
$$per[473,2773] = per[708,2773] = 23$$

The sequel, II, will appear in the next issue of CRYPTOLOGIA. It deals with the resistance of number theoretic public key cryptosystems based on safe primes to random searches for solutions of congruences of the form $x\uparrow f \equiv x \bmod(m)$ and with practical measures which a message receiver can take, when setting up such a cryptosystem, to avoid certain weaknesses.

REFERENCES

1. Blakley, G. R. and Borosh, I., Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages, to appear.

2. Diffie, W. and Hellman, M. E., New directions in cryptography, IEEE Trans. on Infor. Th., IT-22, 6 (1976), 644-654. Also private communication regarding safe primes in public key distribution systems, April 1978.

3. Hardy, G. H. and Wright, E. M., An Introduction to the Theory of Numbers, Fourth Edition. (London: Oxford University Press, 1965).

4. LeVeque, W. J., Topics in Number Theory, Volume 1, First Edition. (Reading, Massachusetts: Addison-Wesley Publishing Company, 1958).

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

6. Rivest, R. L., Remarks on a proposed cryptanalytic attack of the "M.I.T. public key cryptosystem". CRYPTOLOGIA, 2 (1978), 62-65.

7. Simmons, G. J. and Norris, J. N., Preliminary comments on the M.I.T. public key cryptosystem, CRYPTOLOGIA, 1 (1977), 406-414.