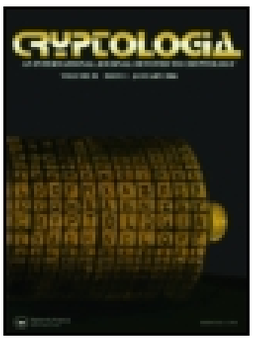

CRYPTOLOGIA

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, III

Bob Blakley & G. R. Blakley

To cite this article: Bob Blakley & G. R. Blakley (1979) SECURITY OF NUMBER THEORETIC PUBLIC KEY CRYPTOSYSTEMS AGAINST RANDOM ATTACK, III, CRYPTOLOGIA, 3:2, 105-118, DOI: 10.1080/0161-117991853909

To link to this article: https://doi.org/10.1080/0161-117991853909

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

Bob Blakley and G. R. Blakley

This paper concludes the discussion we began in the last two issues of CRYPTOLOGIA. A typical message receiver using an RSA public key cryptosystem *believes* that the secret nontrivial factors p and q of his public coding modulus m are primes. But he need not *know* that p or q are prime, or even square free. We give a few examples below. In some of them the "RSA public key cryptosystem" based on integers P and Q erroneously thought both to be prime works perfectly, but is more vulnerable to a cryptanalytic attack of the type G. J. Simmons and J. N. Norris [7] have suggested. In other cases these cryptosystems malfunction in an obvious fashion likely to be apprehended quickly by the message receiver. After the examples we prove all the results in I and II except a few which, like Theorems 1.1, 1.2 and 1.3, are obvious corollaries of other results in those papers.

8. Examples. We continue the numbering scheme of the previous paper in this series, II, which appeared in the last issue of CRYPTOLOGIA. This is Section 8. Consider the square free positive integer m = 105. Evidently $\lambda(105) = 12$. It follows that (c,d,105) is a number theoretic public key cryptosystem based on 105 whenever c and d are integers larger than 2 such that $cd \equiv 1 \bmod(12)$. Therefore, in particular, (5,5,105), (7,7,105), (11,11,105), (11,23,105) and (47,59,105) are number theoretic public key cryptosystems. It follows from Table 8 below that there are 45 solution classes modulo 105 of $x\uparrow 5 \equiv x \bmod(105)$, that there are 63 solution classes modulo 105 of $x\uparrow 7 \equiv x \bmod(105)$, and that there are 27 solution classes modulo 105 of each of the four congruences:

$x\uparrow 11 \equiv x \bmod(105)$; $x\uparrow 23 \equiv x \bmod(105)$; $x\uparrow 47 \equiv x \bmod(105)$; and $x\uparrow 59 \equiv x \bmod(105)$.

Example 8.1: Suppose a message receiver acts as if P = 15 and q = 7 were both primes because they pass a few tests based on a presumed "converse to Fermat's theorem," to wit:

$4\uparrow 14 \equiv 4 \bmod(15)$; $11\uparrow 14 \equiv 11 \bmod(15)$;
$2\uparrow 6 \equiv 2 \bmod(7)$; and $5\uparrow 6 \equiv 5 \bmod(7)$.

He thinks that the modulus m = Pq = 105 is the coding modulus of an RSA public key cryptosystem. He acts as if $\lambda(105) = \mathrm{LCM}\{14,6\} = 42$ and $\phi(105) = 14*6 = 84$. As coding exponent he may choose the prime c = 47. He observes that 47*59 = 1 + 33*84, whence he believes, erroneously, that (47,59,105) is an RSA public key cryptosystem. It is, as we have just seen, a number theoretic public key cryptosystem, but not an RSA public key cryptosystem. He notes that $\mathrm{GCD}\{47,42\} = 1$ and $\mathrm{GCD}\{46,42\} = 2$, so he believes, erroneously, that there are only 9 solution classes modulo 105 of the congruence $x\uparrow 47 \equiv x \bmod(105)$. He also believes, erroneously, that Table 9 describes the numbers of multiplicative periods of various residue classes modulo 105. The real state of affairs has been given in Table 8. In summary, his cryptosystem works, though not for the reasons he believes. But it is more vulnerable than he thinks to an attack of the type G. J. Simmons and J. N. Norris describe in [7] because both the maximum and the average multiplicative orders of residue classes modulo 105 are smaller than he thinks.

The average is less than 6, whereas he believes it to exceed 21. The masimum is 12, whereas he believes it to be 42.

Example 8.2: A message receiver who acts as if P = 15 and q = 7 were both primes might choose c = 13. Since 13*55 = 1 + 17*42 he might believe, erroneously, that (13,55,105) is a number theoretic public key cryptosystem. In fact the congruence $(x\uparrow 13)\uparrow 55 \equiv x \bmod(105)$ is equivalent to the congruence $x\uparrow 7 \equiv x \bmod(105)$. There are exactly 63 residue classes modulo 105 whose members satisfy it. But the other 42 residue classes modulo 105 contain no x which satisfy it. If the message receiver sends himself enough test messages he will become aware of the discrepancey.

Example 8.3: Suppose a message receiver acts as if Q = 21 and p = 5 were primes. In setting up what he thinks is an RSA public key cryptosystem with 105 = m = pQ as coding modulus he forms [p - 1][Q - 1] = 4*20 = 80 which he thinks is $\phi(105)$. Similarly he thinks that $\lambda(105) = 20$. Evidently 37*80 + 1 = 63*47. So he incorrectly concludes that (47,63,105) is an RSA public key cryptosystem. It is not, in fact, a number theoretic public key cryptosystem of any sort. He notes that GCD{47,20} = 1 and GCD{46,20} = 2 and is misled into believing that there are only 9 solution classes modulo 105 of the congruence $x\uparrow 47 \equiv x \bmod(105)$. Finally, he is in error in his belief that $(x\uparrow 47)\uparrow 63 \equiv x \bmod(105)$ for all x. This congruence is equivalent to $x\uparrow 9 \equiv x \bmod(105)$, which holds for x belonging to 45 residue classes modulo 105. But the other 60 residue classes modulo 105 consist of numbers with multiplicative periods modulo 105 which are divisible by 3, and do not satisfy the congruence. If he sends himself check messages the message receiver is likely to discover the discrepancy and abandon the idea that 105 is the product of two primes.

Example 8.4: A message receiver who acts as if P' = 3 and Q' = 35 were primes believes that $\phi(105) = 2*34 = 68$ and that $\lambda(105) = 34$. Evidently 38*68 + 1 = 55*47. So he incorrectly concludes that (47,55,105) is an RSA public key cryptosystem. It is not, in fact, a number theoretic public key cryptosystem of any kind since $\lambda(105) = 12$ and 47*55 = 12*215 + 5. He notes that GCD{47,34} = 1 and that GCD{46,34} = 2 and concludes, erroneously, that there are only 9 solution classes modulo 105 of the congruence $x\uparrow 47 \equiv x \bmod(105)$. He believes that the congruence $(x\uparrow 47)\uparrow 55 \equiv x \bmod(105)$ holds for all x. But it is equivalent to the congruence $x\uparrow 5 \equiv x \bmod(105)$, which holds only for the 45 residue classes mentioned in Example 8.3.

Example 8.5: Since 651 = 31*21 = 31*7*3 it is obvious that $\lambda(651) = 30$. Somebody who acted as if 21 were prime would be misled into believing that $\lambda(651) = \text{LCM}\{20,30\} = 60$. Such a person would look for positive integers c and d such that the congruence $cd \equiv 1$ held modulo 60 and would believe that (c,d,651) was an RSA cryptosystem based on the primes 21 and 31. Although this would be false, the fact that the foregoing congruence holds modulo 30 when it holds modulo 60 would guarantee that any such (c,d,651) was a number theoretic public key cryptosystem.

Example 8.6: Consider P = 27, and q = 11, and m = 297. Since 297 is not square free it cannot be the coding modulus of any number theoretic public key cryptosystem. See Table 10. It shows that 88 of the 297 residue classes modulo 297 consist of integers which have a multiplicative cycle modulo 297 but lack a multiplicative period modulo 297. Note that
$\lambda(297) = \text{LCM}\{18,10\} = 90$.

d	The number of residue classes modulo 105 with multiplicative period d modulo 105 is
1	8
2	19
3	8
4	18
6	28
12	24
	105

Table 8

7 is a safe prime. Somebody who thinks 15 is a prime thinks the number of residue classes modulo 105 with multiplicative period d modulo 105 would be

d	
1	4
2	5
3	4
6	8
7	12
14	24
21	12
42	36
	105

Table 9

d	Number of residue classes modulo 297 whose members have multiplicative period d modulo 297	number of residue classes modulo 297 whose members lack multiplicative period modulo 297 but have multiplicative cycle d modulo 297	TOTAL
1	4	16	20
2	5	8	13
3	4		4
5	8	32	40
6	8		8
9	12		12
10	16	32	48
15	8		8
18	24		24
30	24		24
45	24		24
90	72		72
	209	88	297

Table 10

d	Somebody who thinks 27 is a prime thinks the number of residue classes modulo 297 with multiplicative period d would be
1	4
2	5
5	8
10	16
13	24
26	48
65	48
130	144
	297

Table 11

Example 8.7: Somebody who acts as if P = 27 and q = 11 are both primes will erroneously believe that they are both safe primes and that $\phi(297) = 260$ and $\lambda(297) = 130$. He will look for solutions c,d of the congruence $cd \equiv 1 \bmod(260)$. Now 83*47 = 15*260 + 1. So he will think that (47,83,297) is an RSA public key cryptosystem, even though the function $f(x) = x\uparrow 47$ does not even permute the residue classes modulo 297. He will think that the numbers of multiplicative periods modulo 297 are as shown in Table 11. He notes that GCD{47,130} = 1 and GCD{46,130} = 2 so he believes that there are exactly 9 solutions to the congruence $x\uparrow 47 \equiv x \bmod(297)$. He is correct, even though there are 33 residue classes modulo 297 whose members have a multiplicative cycle no larger than 2. The message receiver will probably code and decode some test messages. Since the congruence $(x\uparrow 47)\uparrow 83 \equiv x \bmod(297)$ holds if and only if $x\uparrow 31 \equiv x \bmod(297)$ we know that it holds only for x belonging to those 77 residue classes whose members have multiplicative periods modulo 297 which are factors of 30. Therefore the message receiver can discover that (47,83,297) is not a number theoretic public key cryptosystem, and abandon the notion that 297 is the product of two primes.

Example 8.8: Somebody who acts as if P = 9 and Q = 33 were both primes would nevertheless form GCD{9,33} = 3 as a precaution, and would not try to use 297 as a coding modulus under these circumstances. This points up the fact that a coding modulus m will be square free if and only if every one of the factors the message receiver multiplied together to obtain m is square free, given that the message receiver acts rationally and forms GCD{p,q} for every pair p,q of distinct factors of m which are known to him.

Example 8.9: The Carmichael [11] numbers P = 11 93221 and Q = 2 94409 are interesting as the basis of a purported RSA cryptosystem with coding modulus M = 35 12950 01389. Evidently $\lambda(11\ 93221) = 1260$, $\lambda(2\ 94409) = 216$, and $\lambda(35\ 12950\ 01389) = 7560$. Somebody who believes that P and Q are prime thinks, erroneously, that

$$\lambda(M) = LCM\{11\ 93220,\ 2\ 94408\} = 97581\ 53160 = 129076*7560.$$

Since M is square free it follows that every (C,D,M) such that $CD \equiv 1 \bmod(97581\ 53160)$ is a number theoretic public key cryptosystem. But it is much different from, and much more vulnerable to a Simmons-Norris [7] attack than, an RSA number theoretic public key cryptosystem with a public coding modulus m of approximately the same size. The need for Rabin's [12] refinements (see also [10] and [11]) of a "converse to Fermat's theorem" search for primes is apparent here. The congruence $x\uparrow 11\ 93320 \equiv 1 \bmod(11\ 93221)$ holds more than 95% of the time, and the congruence $x\uparrow 2\ 94408 \equiv 1 \bmod(2\ 94409)$ holds more than 95% of the time since 2 79936/2 94409 > 11 34000/11 93221 > 95/100. Careless testing of these candidates might lead one to believe they were prime.

Corollary 2 in [1] can be expressed as follows.

Lemma 8.1: Let m be an odd square free integer larger than 2. Let e be an odd integer larger than 2. If there is an integer x such that $x\uparrow e \not\equiv x \bmod(m)$ then at most 60% of all residue classes y modulo m satisfy the congruence $y\uparrow e \equiv y \bmod(m)$.

Comment: The non square free m case remains. In this case it is possible to construct examples in which a large majority of residue classes modulo m satisfy the congruence $x\uparrow e \equiv x \bmod(m)$. For example, it follows from Table 10 that just over 70% of all residue classes x modulo 297 satisfy the congruence $x\uparrow 91 \equiv x \bmod(297)$. But, in any case, one of the factors P of m which

the message receiver knows has a square factor. If $P = R\uparrow 2$ for some R the simple extraction of a square root will show this. Otherwise $P = S*R\uparrow 2$. But then some factor of P is smaller than the cube root of P. If P is not much greater than the square root of m the message receiver need only search among numbers no larger than the sixth root of m. If $m \leq 10\uparrow 204$ then m would have a nontrivial factor $W \leq 10\uparrow 34$. This might still be hard to find.

9. Proofs. This section gives proofs of the results in I and II which are not obvious corollaries of immediately preceding results. For the sake of completeness a proof is given here if it is not readily accessible elsewhere. But most are so natural that no claim to substantial originality, other than that the result was unlikely to be sought outside a cryptographic context, should be inferred.

Proof of Lemma 3.1: A. E. Livingston and M. L. Livingston proved a stronger result [9, Theorem 3.2], of which this is a special case.

Proof of Lemma 3.2: E. Hewitt proved a stronger result [8] from which this follows.

Proof of Lemma 3.3: We know [4, p. 54] that $x\uparrow\lambda(m) \equiv 1 \bmod(m)$ if x is relatively prime to m. Conversely if p is a prime common factor of x and m, and if b is a positive integer, then it is impossible that

$$x\uparrow b - 1 = (p\uparrow b)c - 1$$

be a multiple of p. So it cannot be a multiple of m. This proves the first statement. To prove the second statement we merely appeal to [9, Theorem 3.1]. It suffices to note that, in the notation of that paper, $\xi_m(a) = 1$ 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.

Proof of Lemma 3.4: We know [4, p. 55] that there is a number a such that $\mathrm{ord}[a,m] = \lambda(m)$. So if a positive integer v is a factor of $\lambda(m)$ it is obvious [4, p. 48] that

$$\mathrm{ord}[a\uparrow(\lambda(m)/v),m] = v.$$

Now we prove the second statement. Choose any integer x. It satisfies the congruence $x\uparrow(m+\lambda(m)) \equiv x\uparrow m \bmod(m)$. If s is a positive integer then, clearly,

$$x\uparrow(m+s+\lambda(m)) \equiv x\uparrow(m+s) \bmod(m).$$

Now suppose that the multiplicative cycle of x modulo m is the positive integer b. Evidently $b \leq \lambda(m)$, and there is some positive integer s such that $x\uparrow(m+s+b) \equiv x\uparrow(m+s) \bmod(m)$. It follows from the division algorithm that there are nonnegative integers Q and R such that $R < b$ and $\lambda(m) = Qb + R$. Consequently

$$m + s + Qb \leq m + s + \lambda(m) = m + s + Qb + R,$$

and therefore

$$x\uparrow(m+s) \equiv x\uparrow(m+s+b) \equiv x\uparrow(m+s+2b) \equiv \ldots \equiv$$

$$\equiv x\uparrow(m+s+Qb) \equiv x\uparrow(m+s+\lambda(m)) \equiv x\uparrow(m+s+Qb+R) \bmod(m).$$

But b is the smallest positive integer for which the congruence $x\uparrow(T+b) \equiv x\uparrow T \bmod(m)$ holds for any integer T. Moreover $0 \leq R < b$ and

$$x\uparrow(m+s+Qb) \equiv x\uparrow(m+s+Qb+R) \bmod(m).$$

Consequently $R = 0$. Thus $\lambda(m) = Qb$. This completes the proof.

Proof of Theorem 3.1: It is more natural to prove a stronger result, *viz.* that for all integers x, all finite sets Y of positive integers, we have the equality

$$\text{cyc}[x,\text{LCM}\{y \mid y \in Y\}] = \text{LCM}\{\text{cyc}[x,y] \mid y \in Y\}.$$

To each $y \in Y$ there corresponds a positive integer $A(y)$ such that for every pair s, t, of integers larger than $A(y)$ the congruence $x\uparrow s \equiv x\uparrow t \bmod(y)$ holds if and only if $t-s$ is a multiple of $\text{cyc}[x,y]$. Let

$$A = \text{MAX}\{A(y) \mid y \in Y\}$$

and consider a pair s, t of integers larger than A. If

$$t-s = \text{LCM}\{\text{cyc}[x,y] \mid y \in Y\}$$

then $t-s$ is a multiple of $\text{cyc}[x,y]$ for each $y \in Y$. So $x\uparrow t - x\uparrow s$ is a multiple of y for each $y \in Y$. Therefore $x\uparrow t - x\uparrow s$ is a multiple of $\text{LCM}\{y \mid y \in Y\}$. Hence $t - s$ is a multiple of $\text{cyc}[x,\text{LCM}\{y \mid y \in Y\}]$. Consequantly

$$\text{cyc}[x,\text{LCM}\{y \mid y \in Y\}] \leq \text{LCM}\{\text{cyc}[x,y] \mid y \in Y\}.$$

On the other hand consider two integers s, t such that $A \leq s < t$, and that

$$t-s < \text{LCM}\{\text{cyc}[x,y] \mid y \in Y\}.$$

Since $t-s$ is strictly positive it follows that there exists $y \in Y$ such that $\text{cyc}[x,y]$ is not a factor of $t-s$. But s and t both exceed A and, therefore, $A(y)$ also. It follows that $x\uparrow s \not\equiv x\uparrow t \bmod(y)$ whence

$$x\uparrow s \not\equiv x\uparrow t \bmod(\text{LCM}\{y \mid y \in Y\})$$

This ends the proof.

Proof of Lemma 3.5: Obviously $p\uparrow 2 - p$ is not a multiple of $p\uparrow 2$. If $3 \leq v$ then

$$p\uparrow v - p = p[p-1][(p\uparrow(v-2)+p\uparrow(v-3)+\ldots+p)+1] = p(p-1)(pq+1).$$

Thus, in any case, $p\uparrow v - p$ cannot by a multiple of $p\uparrow 2$. So it cannot be a multiple of m.

Proof of Lemma 3.6: E. Hewitt [8] showed that $\lambda(m)$ is the smallest positive integer b such that the congruence $x\uparrow(1+b) \equiv x \bmod(m)$ is an identity in x. Evidently

$$x\uparrow(1+2\lambda(m)) \equiv [x\uparrow(1+\lambda(m))][x\uparrow\lambda(m)] \equiv (x)(x\uparrow\lambda(m)) \equiv x\uparrow(1+\lambda(m)) \equiv x \bmod(m).$$

$$x\uparrow(1-\lambda(m)) \equiv [x\uparrow 2][x\uparrow(-1-\lambda(m))] \equiv [x\uparrow 2][x\uparrow(1+\lambda(m))]\uparrow(-1) \equiv$$

$$\equiv (x\uparrow 2)(x\uparrow(-1)) \equiv x \bmod(m).$$

It follows in a similar fashion that $x\uparrow(1+Q\lambda(m)) \equiv x \bmod(m)$ for every integer Q. If v is an integer for which the congruence $x\uparrow(1+v) \equiv x \bmod(m)$ holds identically in x then the division algorithm yields integers Q and R such that $0 \leq R < \lambda(m)$ and $v = Q\lambda(m) + R$. But then

$$x\uparrow(1+v) \equiv x\uparrow(1+Q\lambda(m)+R) \equiv [x\uparrow(1+Q\lambda(m))][x\uparrow R] \equiv x(x\uparrow R) \equiv x\uparrow(1+R) \bmod(m).$$

Since $0 \leq R < \lambda(m)$ and since $\lambda(m)$ was the smallest positive integer of this sort, it follows that $R = 0$. So v was a multiple of $\lambda(m)$. This completes the proof.

Proof of Theorem 3.2: It is an obvious corollary of Lemma 3.6.

Proof of Theorem 3.3: We prove the second statement first. We know that the congruence $x\uparrow cd \equiv x \bmod(m)$ holds identically in x if and only if $cd \equiv 1 \bmod(\lambda(m))$. Since c and $\lambda(m)$ are relatively prime there is one equivalence class modulo $\lambda(m)$ of solutions d to the latter congruence. This solution class cannot contain 0 or 1. Therefore its smallest positive member d satisfies the inequality $1 < d < \lambda(m)$. Now consider the proof of the first statement. The congruence $cd \equiv 1 \bmod(\lambda(m))$ means that there is an integer a such that $cd = a\lambda(m) + 1$. We know that $cd \neq 1$ by the way c was chosen. Hence $a \neq 0$. The equality immediately above implies the inequalities.

$$c|d| \geq |a|\lambda(m) - 1 \geq \lambda(m) - 1.$$

Therefore

$$|d| \geq \lambda(m)/c - 1/c > \lambda(m)/c - 1.$$

This proves the first statement and, therewith, the theorem. Corollary 3.1 now follows as a special case.

Proof of Theorem 3.4: There are only finitely many residue classes modulo m. So $cyc[x,m]$ exists for every x. To prove the second statement let s be the multiplicative cycle of x modulo m. Then $s \leq w$ and there are nonnegative integers Q and R such that $R < s$ and $w = Qs + R$. Also there is a nonnegative integer y such that $x\uparrow(y+s) \equiv x\uparrow y \bmod(m)$. Evidently $x\uparrow(y+v+w) \equiv x\uparrow(y+v) \bmod(m)$. Thus $[x\uparrow v][x\uparrow(y+Qs+R) - x\uparrow y] \equiv 0 \bmod(m)$. But

$$x\uparrow y \equiv x\uparrow(y+s) \equiv x\uparrow(y+2s) \equiv \ldots \equiv x\uparrow(y+Qs) \bmod(m).$$

Therefore

$$[x\uparrow v][x\uparrow(y+Qs+R) - x\uparrow y] \equiv [x\uparrow v][x\uparrow(y+R) - x\uparrow y] \equiv 0 \bmod(m).$$

Since $R < s$ and $x\uparrow(v+y+R) \equiv x\uparrow(v+y) \bmod(m)$ it follows from the minimality of s that $R = 0$. This proves the second statement. Obviously $per[x,m]$ exists and $per[x,m] \leq ord[x,m]$ when the multiplicative order of x modulo m exists. If r and n are positive integers such that $x(x\uparrow r - 1) \equiv 0 \bmod(m)$ and $x\uparrow n - 1 \equiv 0 \bmod(m)$ then x is relatively prime to m. It follows that $x\uparrow r - 1 \equiv 0 \bmod(m)$. If n is the multiplicative order of x modulo m it follows that $n \leq r$. Consequently $ord[x,m] \leq per[x,m]$. This proves the third statement. Obviously $cyc[x,m] \leq per[x,m]$ when the multiplicative period of x modulo m exists. Conversely let r be the multiplicative period of x modulo m. Let $m = \Pi\{p\uparrow e(p) \mid p \in D\}$, where $D = A \cup B$, and A consists of all prime common divisors of m and x, and B consists of all prime divisors of m which are relative prime to x. Then:

$$m = ab; \qquad a = \Pi\{p\uparrow e(p) \mid p \in A\}; \text{ and } \qquad b = \Pi\{p\uparrow e(p) \mid p \in B\}.$$

If s and t are any positive integers for which $(x\uparrow t)(x\uparrow s - 1) \equiv 0 \bmod m$ then $x\uparrow s - 1$ is a multiple of b and $x\uparrow t$ is a multiple of a. But the existence of $per[x,m]$ implies, in view of Lemma 3.3, that x is a multiple of a and, hence, that $x(x\uparrow s - 1) \equiv 0 \bmod(m)$. Therefore $per[x,m] \leq s$. The trivial case $t = 0$ causes no difficulty. So it follows that $per[x,m] \leq cyc[x,m]$. This proves the fourth statement. Finally, let s be the multiplicative cycle of x modulo m, and suppose that $v \geq m$. We know

$$\{x\uparrow j \bmod(m) \mid 1 \leq j \leq m\} = \{x\uparrow k \bmod(m) \mid k \text{ is a positive integer}\}$$

because the set of powers of x modulo (m) has at most m members. So if there is a nonnegative integer t such that $x\uparrow(t+cyc[x,m]) \equiv x\uparrow t \bmod(m)$ then there is already a nonnegative integer $u \leq m$ for which $x\uparrow(u+cyc[x,m]) \equiv x\uparrow u \bmod(m)$. It follows that $x\uparrow(u+w+cyc[x,m]) \equiv x\uparrow(u+w) \bmod(m)$ for every nonnegative integer w. This ends the proof.

Proof of Corollary 3.2: Let A = cyc[x,m], and let B = cyc[x↑u,m]. Then we know that $x\uparrow(um + uB) \equiv x\uparrow u(m + B) \equiv x\uparrow um \bmod(m)$. Consequently uB is a multiple of A. If B were to have a factor which A lacked there would be a prime p such that uB/p is also a multiple of A. But then $x\uparrow u(m + B/p) \equiv x\uparrow um \bmod(m)$ whence $B \neq \text{cyc}[x\uparrow u,m]$ contrary to assumption. This ends the proof.

Proof of Lemma 3.7: Suppose m is prime, if an integer a is not a multiple of m then (a,m) = 1, whence [4, p. 42] $a\uparrow\phi(m) \equiv 1 \bmod(m)$. Hence ord[a,m] exists. Conversely if pq is a factor of m, where p and q are (not necessarily distinct) primes, then the congruence $p\uparrow e \equiv 1 \bmod(m)$ has no positive integer solutions e because $p\uparrow e - 1$ is not divisible by p. E. Hewitt [8] proved the second statement.

Proof of Lemma 3.8: Since m is a square free positive integer, every integer x has a multiplicative period modulo m. We know that $x\uparrow c \equiv x\uparrow(1+(c-1)) \equiv x \bmod(m)$ if and only if c-1 is a multiple of per[x,m]. But $\lambda(m)$ is necessarily a multiple of per[x,m]. Hence the equality holds if and only if c-1 and $\lambda(m)$ are multiples of per[x,m].

Proof of Theorem 3.5: The only positive common divisors of c-1 and $\lambda(m)$ are 1 and 2. So the result follows immediately from Lemma 3.8.

Proof of Lemma 3.9: If c is relatively prime to $\lambda(m)$ then the congruence $cd \equiv 1 \bmod(\lambda(m))$ has a solution d. Hence we know from Theorem 3.2 that $(x\uparrow c)\uparrow d \equiv x \bmod(m)$ for every integer x. The operation of raising to the cth power is therefore a permutation of the residue classes modulo m. The proof that c is relatively prime to $\lambda(m)$ whenever the operation of raising to the cth power effects a permutation of the residue classes modulo m can be found in [1].

Proof of Theorem 3.6: If c is a deranging exponent for m then $\text{per}[x,m] \in \{1,2\}$ for every integer x such that $x\uparrow(1+(c-1)) \equiv x\uparrow c \equiv x \bmod(m)$. But all divisors of $\lambda(m)$ occur as multiplicative periods modulo m. This implies that no divisor of $\lambda(m)$ other than 1 or 2 is a factor of c-1. To verify the converse assume that there is an integer x such that $x\uparrow c \equiv x \bmod(m)$ and $3 \leq \text{per}[x,m]$. But per[x,m] is a factor of $\lambda(m)$, as well as of c-1. Hence $3 \leq \text{per}[x,m] \leq \text{GCD}\{\lambda(m),c-1\}$. This completes the proof. Corollary 3.3 is an immediate consequence.

Proof of Lemma 4.1: Evidently

$$m-1 = pq - 1 = (2a(p) + 1)(2a(q) + 1) - 1 = 4a(p)a(q) + 2a(p) + 2a(q).$$

Therefore $4 < (m-1)/a(p)a(q)$. On the other hand, 7 is the smallest safe prime and a(7) = 3. Therefore if s is any safe prime then $s/a(s) \leq 7/3$. Thus

$$(m-1)/a(p)a(q) < pq/a(p)a(q) \leq 49/9.$$

This completes the proof.

Proof of Lemma 4.2: In this case $\lambda(m) = 2a(p)a(q)$. Because of Lemma 4.1 we know that

$$0 < 1 < 1 + \lambda(m) < 1 + 2\lambda(m) < m < 3\lambda(m).$$

Evidently the congruence

$$x\uparrow 1 \equiv x\uparrow(1+\lambda(m)) \equiv x\uparrow(1+2\lambda(m)) \equiv x \bmod(m)$$

is an identity in x. But the congruence $x\uparrow(1+g) \equiv x \bmod(m)$ is an identity in x if and only if g is a multiple of $\lambda(m)$. This completes the proof.

Proof of Theorem 4.1: Recall that $2a+1 = p$. Obviously $per[0,p] = 1$. Moreover $ord[1,p] = 1$ and $ord[p-1,p] = ord[-1,p] = 2$. So it only remains to prove the last two equalities. Euler's criterion [3, p. 46] states that for each quadratic residue b the congruence $b\uparrow a \equiv 1 \bmod(p)$ holds. If $2 \leq x \leq a$ and $b \equiv x\uparrow 2 \bmod(p)$, then b is not congruent to 1 or -1. Since a is prime it follows that

$$per[x\uparrow 2,p] = ord[x\uparrow 2,p] = ord[b,p] = a.$$

Euler's criterion also states that for every quadratic nonresidue n the congruence $n\uparrow a \equiv 1 \bmod(p)$ fails. For every n we know that $ord[n,p]$ is a divisor of $\lambda(p) = p-1 = 2a$. But the nonzero residue classes modulo p form a field. So the congruence $x\uparrow 2 \equiv 1 \bmod(p)$ has only two solution classes modulo p, namely the class of 1 and the class of -1. Thus, throwing away 1, 2 and a as divisors of $2a$, we see that the nontrivial quadratic nonresidues must all have multiplicative order $2a$ modulo p. This ends the proof.

Proof of Theorem 4.2: The formula for $\lambda(m)$ is obvious. Evidently $cyc[x,p] = cyc[x,2a(p) + 1]$ is a factor of $2a(p)$ for every x, and every factor p of m. It follows from Theorem 3.1 that

$$cyc[x,\Pi\{p \mid p \in T\}] = LCM\{cyc[x,p] \mid p \in T\}$$

is a factor of $LCM\{2a(p) \mid p \in T\} = \lambda(m)$ for every x. This ends the proof. Corollary 4.1 is the special case in which T contains exactly two primes.

Proof of Theorem 4.3: It is immediate from Theorems 3.1 and 4.1. To establish Corollary 4.2 one needs merely to sort the integers into invertible and noninvertible residue classes modulo m.

Proof of Theorem 4.4: If $x(x-1) \equiv 0 \bmod(pq)$ and if x is not congruent to 0 or 1 modulo pq then there are two possibilities:

$$\text{I)} \quad x \equiv 0 \bmod(p) \quad \text{and} \quad x-1 \equiv 0 \bmod(q);$$

or

$$\text{II)} \quad x \equiv 0 \bmod(q) \quad \text{and} \quad x-1 \equiv 0 \bmod(p).$$

Thus $GCD\{x,pq\}$ is either p or q. Moreover if $x(x-1)(x+1) \equiv 0 \bmod(pq)$ but $x(x-1) \not\equiv 0 \bmod(pq)$ then either p is not a factor of $x(x-1)$ or q is not a factor of $x(x-1)$. Since x is not congruent to 0, 1 or -1 modulo pq, it follows that either p or q (but not both) is a factor of $x + 1$. Hence $GCD\{x+1,pq\}$ is either p or q. This ends the proof.

Proof of Lemma 5.1: Since b is the smallest member of $\{a(p) \mid p \in T\}$ it follows that $2 \leq x \leq 2a(p)-1$ for every $p \in T$. Therefore x is not congruent to 0, 1 or -1 modulo p for any $p \in T$. It follows that $per[x,p] \in \{a(p),2a(p)\}$ for every $p \in T$. But

$$per[x,m] = cyc[x,m] = LCM\{cyc[x,p] \mid p \in T\} = LCM\{per[x,p] \mid p \in T\}.$$

The word *set* implies distinct elements. No two members of T are equal. For each $p \in T$ either $per[x,p] = a(p)$ or $per[x,p] = 2a(p)$. Hence this least common multiple $per[x,m]$ is equal to $\Pi\{a(p) \mid p \in T\}$ if $per[x,p] = a(p)$ for every $p \in T$. Otherwise $per[x,p] = 2a(p)$ for some $p \in T$, in which case the least common multiple, $per[x,m]$, is $2\Pi\{a(p) \mid p \in T\}$. This ends the proof.

Proof of Theorem 5.1: Since $per[x,m] < \Pi\{a(p) \mid p \in T\}$ there must be some $q \in T$ and some $r \in \{-1,0,1\}$ such that $x \equiv r \bmod(q)$. Since $x \notin \{-1,0,1\}$ it follows that x belongs to one of the sets

$$A = \{\pm q, \pm 2q, \pm 3q, \ldots\}$$

$$B = \{1 \pm q, 1 \pm 2q, 1 \pm 3q, \ldots\}$$

$$C = \{-1 \pm q, -1 \pm 2q, -1 \pm 3q, \ldots\}.$$

This completes the proof. Corollary 5.1 is the special case in which T contains exactly two members.

Proof of Theorem 5.2: If per[x,m] = a(p) then x is congruent to 0 or 1 modulo q. But x is not 0 or 1. So it is at least as large as a positive integer multiple of q. If per[x,m] = a(q) then x is congruent to 0 or 1 modulo p. But p is not congruent to 0 or 1 modulo q. So x is unequal to p. Hence x is either of the form 2p, 3p, 4p,... or of the form p+1, 2p+1, 3p+1,... . This ends the proof.

Proof of Theorem 5.3: Evidently x is not congruent to 0, 1, -1 modulo p. Thus $x \notin \{0,1\}$. But x is congruent to 0, 1, or -1 modulo q. Therefore the smallest possible positive integer value x can have is q-1.

Proof of Theorem 5.4: If, on the one hand, per[x,m] = 1 then per[x,p] = 1 for every $p \in T$. But the integers modulo any prime p form a field. In such a field the congruence $x\uparrow 2 \equiv x \bmod(p)$ has only 0 and 1 for solutions. If, on the other hand, per[x,m] = 2 and $p \in T$ then $\text{per}[x,p] \in \{1,2\}$. Moreover there is at least one $q \in T$ for which per[x,q] = 2. For any prime p, the equation $x\uparrow 3 \equiv x \bmod(p)$ has only 0, 1 and -1 for solutions. Since per[x,q] ≠ 1 it follows that x is not congruent to 0 or 1 modulo q. So $x \equiv -1 \bmod(q)$. It follows from the Chinese remainder theorem [4, p. 35] that there are $2\uparrow k$ solutions of the congruence $x\uparrow 2 \equiv x \bmod(m)$, since 0 and 1 are the only solutions of the congruence $x\uparrow 2 \equiv x$ modulo any prime p. It also follows from the Chinese remainder theorem that these $2\uparrow k$ residue classes modulo m are all to be found among the $3\uparrow k$ solutions of the congruence $x\uparrow 3 \equiv x \bmod(m)$, since 0, 1 and -1 are the only solutions of the congruence $x\uparrow 3 \equiv x$ modulo any prime p. From these facts follow all the statements in the theorem. Corollary 5.2 is its specialization to the case in which m is the product of k = 2 primes.

Proof of Lemma 5.2: Clearly $(A+B)p \equiv Ap + Bp \equiv 0 \bmod(q)$. Hence A + B is a positive integer multiple of q. Evidently $0 < A < q$ and $0 < B < q$. Consequently $0 < A + B < 2q$. Therefore A + B = q. This ends the proof. Lemma 5.3 is an immediate corollary.

Proof of Lemma 5.4: Evidently $0 < A < q$, and $0 < B < p$, and $0 < C < q$, and $0 < D < p$. There are two cases to consider. If $A < q/2$ then

$$B = Ap/q - 1/q < Ap/q < p/2.$$

If, on the other hand, $A \geq q/2$ then $A > q/2$. Let C and D be defined by setting C = q-A, and D = p-B. Then

$$Cp + 1 = qp - Ap + 1 = qp - Bq = Dq$$

$$0 < C = q - A < q - q/2 = q/2$$

$$0 < D = p - B = Cp/q + 1/q < p/2 + 1/q.$$

But D and p are integers, and $1/q \leq 1/3$. It follows that $D < p/2$. This ends the proof.

Proof of Theorem 5.5: Let A, B, C, D be the smallest nonnegative integers such that Ap = Bq + 1, and Cp + 1 = Dq. It follows from Corollary 5.2 that x is the smaller of the two numbers Ap and Dq. Either way it is clear from Lemma 5.4 that $x < pq/2$.

Proof of Theorem 5.6: Recall Corollary 5.2. If $x \equiv 0 \bmod(p)$, and $x \equiv 1 \bmod(q)$ then $x = Ap = Bq + 1$ where A and B are positive. If $x \equiv 1 \bmod(p)$, and $x \equiv 0 \bmod(q)$ the argument is similar.

Proof of Lemma 5.5: It is obvious that A, C, E, and G are positive. Clearly $Ap + Ep \equiv 0 \bmod(q)$, and $Cp + Gp \equiv 0 \bmod(q)$. Of course p and q are relative prime. Hence $A + E$ and $C + G$ are both positive integer multuples of q. Evidently $0 < A < q$, and $0 < C < q$, and $0 < E < q$, and $0 < G < q$. Consequently $0 < A + E < 2q$, and $0 < C + G < 2q$. Therefore $A + E = q$, and $C + G = q$. This ends the proof. Corollary 5.3 follows immediately.

Proof of Theorem 5.7: Let $m = pq$. The four nontrivial numbers y, z, t, s with multiplicative period 2 modulo m are the smallest positive integers which satisfy the following four pairs of simultaneous congruences:

$y \equiv 0 \bmod(p)$, and $y \equiv -1 \bmod(q)$;

$z \equiv 1 \bmod(p)$, and $z \equiv -1 \bmod(q)$;

$t \equiv -1 \bmod(p)$, and $t \equiv 0 \bmod(q)$;

$s \equiv -1 \bmod(p)$, and $s \equiv 1 \bmod(q)$.

Note that $2t + 1$ is congruent to s modulo both p and q, whence modulo their product m. Similarly $2y + 1$ is congruent to z modulo m. Now let A, B, C, D, E, F, G and H be the smallest nonnegative integers such that

$y = Ap = Bq - 1$, $z = Cp + 1 = Dq - 1$,

$t = Ep - 1 = Fq$, and $s = Gp - 1 = Hq + 1$.

Then the integers A, B, C, D, E, F, G and H are all positive. Moreover we can employ the argument which established Lemma 5.3 to show that either both the inequalities

$0 < A < q/2$, and $0 < B < p/2$

hold, or else both the inequalities

$0 < E < q/2$, and $0 < F < p/2$

hold. It follows from Corollary 5.3 that

$$y/p + (t+1)/p = A + E = q$$

$$(z-1)/p + (s+1)/p = C + G = q.$$

Hence $y + t + 1 = pq = m$, and $z + s = pq = m$. The remainder of the proof has two parts. Suppose, first that $0 < y < m/2$. If $y < m/3$ we have the desired result. If $m/3 \leq Ap = y < m/2$ then $m/2 < t + 1 \leq 2m/3$. It follows that $m-1 < 2t+1 \leq 4m/3-1$. But $2t + 1 \equiv s \bmod(m)$ and s is not congruent to zero modulo m. Therefore $0 < s \leq m-1$, whence $s = 2t + 1 - m$. It follows that $0 < s < m/3$. If $0 < t < m/3$ we have the desired result. So all that remains is to assume that $m/2 \leq Ap = y < m$ and $m/3 \leq Ep - 1 = t$. Since $0 < y + t < m$ it is clear that $t < m/2$. Consequently

$$2m/3 + 1 \leq 2t + 1 < m + 1$$

and

$$m + 1 \leq 2y + 1 < 2m + 1.$$

Therefore $z = 2y + 1 - m$. We also know that $y + t + 1 = m$, whence

$$(2y + 1) + (2t + 1) = 2m$$

so that

$$(2y + 1) - m = m - (2t + 1).$$

From the inequalities $2m/3 < 2t + 1 < m + 1$ it follows that $-1 < m - (2t + 1) < m/3$, *i.e.* that $-1 < z < m/3$. Since z is not congruent to 0 or -1 modulo (m) it is thus clear that $0 < z < m/3$. This ends the proof.

Proof of Lemma 5.6: Obviously 2 is not congruent to 0, 1 or -1 modulo either p or q since they are safe primes. So it follows from Theorem 4.3 that

$$per[2,m] \in \{a(p)a(q), 2a(p)a(q)\}.$$

Evidently $6 \leq p-1 \leq q-3$. Therefore $p-1$ is not congruent to 0, 1 or -1 modulo q. It follows from Theorem 4.3 that

$$per[p-1,m] = 2a(q) = q-1.$$

Since p and q are distinct primes we know that $q \not\equiv 0 \bmod(p)$. Since p and q are both odd it is clear that q is not congruent to either 1 or -1 modulo p. It is a consequence of Theorem 4.3 that

$$per[q,m] \in \{a(p), 2a(p)\}.$$

To repeat the foregoing, we know that $q-1 \not\equiv 0 \bmod(p)$, and that $q-1 \not\equiv -1 \bmod(p)$. If, additionally, $q \not\equiv 2 \bmod(p)$ then $q-1 \not\equiv 1 \bmod(p)$. It follows from Theorem 4.3 that $per[q-1,m] = 2a(p)$ when $q \not\equiv 2 \bmod(p)$. This ends the proof.

Proof of Theorem 5.8: Recall Corollary 5.2. Every number x with multiplicative period 2 satisfies one of the five pairs of congruences:

$$x \equiv 0 \bmod(p), \text{ and} \qquad x \equiv -1 \bmod(q);$$

or

$$x \equiv 1 \bmod(p), \text{ and} \qquad x \equiv -1 \bmod(q);$$

or

$$x \equiv -1 \bmod(p), \text{ and} \qquad x \equiv 0 \bmod(q);$$

or

$$x \equiv -1 \bmod(p), \text{ and} \qquad x \equiv 1 \bmod(q);$$

or

$$x \equiv -1 \bmod(p), \text{ and} \qquad x \equiv -1 \bmod(q).$$

The smallest positive solution x of any of these pairs of congruences satisfies the inequalities $p-1 \leq x$, and $q-1 \leq x$. This ends the proof.

Proof of Theorem 5.9: Neither $x-1$ nor $x+1$ is divisible by any prime $p \in T$. Therefore $2 < per[x,p]$ for every $p \in T$. But p is a safe prime for every $p \in T$. Hence $a(p) = (p-1)/2$ is a prime for every $p \in T$. Therefore, if $p \in T$, then the only positive divisors of $\phi(p) = \lambda(p) = p-1$ are 1, 2, $a(p)$, and $2a(p)$. It follows that the prime $a(p)$ is a divisor of $per[x,p]$ for every $p \in T$. If $p \in T$ and $q \in T$ and $p \neq q$ then

$$LCM\{a(p) \mid p \in T\} = \Pi\{a(p) \mid p \in T\}.$$

Therefore $\Pi\{a(p) \mid p \in T\}$ is a divisor of

$$per[x,m] = LCM\{per[x,p] \mid p \in T\}$$

which is, in turn, a divisor of t. This completes the proof.

Proof of Theorem 5.10: The positive integer m is the product of two distinct primes, p and q. So if $2 \leq h \leq m-1$ and $GCD\{h,m\} \neq 1$ then the greatest common divisor is either p or q. This proves the first assertion. So now suppose that $F = G = H = 1$. It follows from Theorem 5.9 that ab is a factor of t. We know from Lemma 4.1 that $t/ab < m/ab < 6$. We also know from the hypotheses that $\{a,b\} \cap \{2,3,5\} = \emptyset$. So let s be the largest positive integer less than 6 such that s is a factor of t. It follows that $f = t/s = ab$. Thus we know that $f = ab$, and $m = (2a + 1)(2b + 1)$. But then we calculate, successively, that

$$\begin{aligned} m - 4f &= 2a + 2b + 1 \\ 2b &= m - 4f - 2a - 1 \\ 2f &= 2ab = a(m - 4f - 2a - 1) \\ 0 &= 2a\uparrow 2 + (1 + 4f - m)a + 2f. \end{aligned}$$

It is a consequence of the quadratic formula that either

$$\begin{aligned} 2p - 2 = 4a &= (m - 4f - 1) + ([1 + 4f - m]\uparrow 2 - 16f)\uparrow 1/2 \\ &= m - 4f - 1 + (1 + 16f\uparrow 2 + m\uparrow 2 - 8f - 2m - 8mf)\uparrow 1/2. \end{aligned}$$

or

$$2p - 2 = 4a = m - 4f - 1 - (1 + 16f\uparrow 2 + m\uparrow 2 - 8f - 2m - 8mf)\uparrow 1/2.$$

Recall the definition of i and j in the statement of the theorem. $2i$ and $2j$ differ by 2 from the last two right hand sides above. Since a and b enter symmetrically we see that $\{i,j\} = \{p,q\}$. This ends the proof.

We thank N. W. Naugle for the integral estimates in Section 5, R. L. Rivest for bringing the attack on RSA by means of exponents to our attention, and I. Borosh for many incisive comments and many improvements of proofs. We close with two minor errata. The inequality in the last line in Section 2 should now read $0 < \log(p) < 21701$, since a new Mersenne prime [13] was discovered after the proofs of I were read. A comma was omitted from $cyc[x\uparrow u,m]$ in the statement of Corollary 3.2.

REFERENCES

1. Blakley, G. R. and Borosh, I., Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages, Computers and Mathematics with Applications, 5(1979) 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.

8. E. Hewitt, Certain congruences that hold identically, American Mathematical Monthly, 83(1976), 270-271.

9. A. E. Livingstone and M. L. Livingstone, The congruence $a^{r+s} \equiv a^{r} (\text{mod } m)$, American Mathematical Monthly, 85(1978), 79-100.

10. G. L. Miller, Riemann's hypothesis and tests for primality, Research Report CS-75-27, Department of Computer Sciences, University of Waterloo, Waterloo, Ontario, Canada (1975).

11. L. Monier, Evaluation and comparison of two efficient probabilistic primality testing algorithms Rapport de Recherche no. 20, June (1978), Equipe de Recherche Associee Au C.N.R.S. no. 452 "Al Khowarizmi", Laboratoire de Recherche en Informatique.

12. M. O. Rabin, Probabilistic algorithms (in the book Algorithms and Complexity, edited by J. Traub), Academic Press, New York (1976).

13. Scientific American, 240, January(1979), 88.