

Modular Arithmetic For RSA Cryptography

by

**John Kennedy
Santa Monica College
1900 Pico Blvd.
Santa Monica, CA 90405**

rkennedy@ix.netcom.com

Except for this comment explaining that it is blank for some deliberate reason, this page is intentionally blank!

Modular Arithmetic For RSA Cryptography

1 Definition. **Congruence Modulo n .** Let a and b and n denote any three integers. To say a is congruent to b modulo n , written $a \equiv b \pmod{n}$, means there exists an integer k such that $a - b = k \cdot n$.

2 Theorem. If j denotes any integer and if $a \equiv b \pmod{n}$ then $(a + j) \equiv (b + j) \pmod{n}$ and $(a - j) \equiv (b - j) \pmod{n}$.

In other words, the same integer may be added or subtracted from both sides of a congruence to create a new congruence.

Proof: Since $a \equiv b \pmod{n}$ there exists an integer k such that $(a - b) = k \cdot n$. Next, $(a + j) - (b + j) = a + j - b - j = a - b = k \cdot n$. This last equation implies $(a + j) \equiv (b + j) \pmod{n}$.

Similarly, $(a - j) - (b - j) = a - j - b + j = a - b = k \cdot n$ and this implies $(a - j) \equiv (b - j) \pmod{n}$.

3 Theorem. If j denotes any integer and if $a \equiv b \pmod{n}$ then $a \cdot j \equiv b \cdot j \pmod{n}$.

In other words, the same integer may be multiplied on both sides of a congruence to create a new congruence.

Proof: Since $a \equiv b \pmod{n}$ there exists an integer k such that $(a - b) = k \cdot n$. Next, $(a \cdot j) - (b \cdot j) = (a - b) \cdot j = kn \cdot j = (kj) \cdot n$. This last equation implies $a \cdot j \equiv b \cdot j \pmod{n}$.

4 Corollary. If j denotes any integer and if k denotes a nonnegative integer and if $a \equiv b \pmod{n}$ then $a \cdot j^k \equiv b \cdot j^k \pmod{n}$.

Proof: Apply Theorem **3** k times with the multiplier equal to j each time.

5 Corollary. If k denotes a positive integer and if $a \equiv b \pmod{n}$ then

$$a^k \equiv b^k \pmod{n}.$$

Proof: Note that $(a - b)$ is always a factor of $a^k - b^k$ so that there exists an integer j such that we may write $a^k - b^k = (a - b) \cdot j = (kn) \cdot j = (kj) \cdot n$. Now this last equation implies $a^k \equiv b^k \pmod{n}$.

6 Corollary. If $p(x)$ denotes any polynomial with integer coefficients and if $a \equiv b \pmod{n}$ then $p(a) \equiv p(b) \pmod{n}$.

In other words, the same polynomial may be applied to both sides of any congruence.

Proof: Apply Theorems **2** and **3** and Corollary **5** multiple times to build up to the polynomial on both sides of the congruence.

7 Theorem. Modular arithmetic is reflexive, symmetric and transitive so it is an equivalence relation.

- 1) $a \equiv a \pmod{n}$.
- 2) If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.
- 3) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.

Proof: 1) Note that $a - a = 0 = 0 \cdot n$.
 2) Assume $(a - b) = k \cdot n$. Then $(b - a) = (-k) \cdot n$.
 3) There exist integers k and j such that $(a - b) = k \cdot n$ and $(b - c) = j \cdot n$. Now, $a - c = (a - b + b - c) = (a - b) + (b - c) = k \cdot n + j \cdot n = (k + j) \cdot n$ and this last equation implies $a \equiv c \pmod{n}$.

8 Theorem. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $(a + c) \equiv (b + d) \pmod{n}$ and $(a - c) \equiv (b - d) \pmod{n}$.

In other words, modular equivalences may be added or subtracted.

Proof: $(a - b) = k \cdot n$ and $(c - d) = j \cdot n$ so that
 $(a + c) - (b + d) = (a - b) + (c - d) = k \cdot n + j \cdot n = (k + j) \cdot n$ and this last equation implies what we need to establish the first part of the theorem. The second part is similar; $(a - c) - (b - d) = (a - b) - (c - d) = k \cdot n - j \cdot n = (k - j) \cdot n$.

9 Theorem. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a \cdot c \equiv b \cdot d \pmod{n}$.

In other words, modular equivalences may be multiplied.

Proof: $(a - b) = k \cdot n$ and $(c - d) = j \cdot n$.
 $(a - b) \cdot c + (c - d) \cdot b = ac - bc + cb - bd = ac - bd$.
 But we may also write $(a - b) \cdot c + (c - d) \cdot b = (kn) \cdot c + (jn) \cdot b = (kc + jb) \cdot n$ which means $ac - bd$ is a multiple of n .

10 Theorem. If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$ and if m and n are relatively prime then $a \equiv b \pmod{mn}$.

Proof: We can assume there exist integers j and k such that $a - b = jm$ and $a - b = kn$. Since m divides into $a - b$, we know m divides into kn , but since m and n are relatively prime we conclude m divides into k . Thus there exists an integer l , such that $k = ml$. Finally, $a - b = kn = (ml)n = l(mn)$. This last equation implies $a \equiv b \pmod{mn}$.

11 Theorem. Every integer n is congruent modulo 9 to the sum of its own digits.

Proof: Consider that $3548 = 3 \cdot 10^3 + 5 \cdot 10^2 + 4 \cdot 10 + 8$ which shows this integer can be written as a special polynomial value. Next, note that $10 \equiv 1 \pmod{9}$ and this in turn implies $10^k \equiv 1 \pmod{9}$ by Corollary **5**. Thus by Theorem **3** $3 \cdot 10^3 \equiv 3 \pmod{9}$ and $5 \cdot 10^2 \equiv 5 \pmod{9}$ and $4 \cdot 10 \equiv 4 \pmod{9}$. Also, $8 \equiv 8 \pmod{9}$. Now applying Theorem **8** we just add congruences to get $3548 \equiv (3 + 5 + 4 + 8) \pmod{9}$. What has just been demonstrated with the integer 3548 could be done with any integer.

12 Theorem (**Cancellation Law for Modular Arithmetic**)

If $ac \equiv bc \pmod{n}$ and if c and n are relatively prime then $a \equiv b \pmod{n}$.

Proof: There exists an integer k such that $ac - bc = kn$. $c(a - b) = kn$. Since n divides the right side of this last equation it also divides the product $c(a - b)$ on the left. Since c and n are relatively prime we conclude that n divides into $(a - b)$ alone. There exists an integer j such that $a - b = jn$. This means $a \equiv b \pmod{n}$.

13 Theorem. **Fermat's Little Theorem.**

If p is prime and p is not a factor of a then $a^{p-1} \equiv 1 \pmod{p}$.

Proof: Consider the special set $\{a \cdot 1, a \cdot 2, a \cdot 3, \dots, a(p-1)\}$. We claim that this set of $p-1$ integers consists of distinct representatives of nonzero equivalence classes modulo p . First we show that if $1 \leq k \leq p-1$, then we cannot have $ak \equiv 0 \pmod{p}$. For this would imply that $ak - 0 = np$ for some integer n . $ak = np$. Since a and p are relatively prime this last equation implies that p divides into k . But this is impossible because $1 \leq k \leq p-1$. So none of the integers in the above special set is equivalent to 0 modulo p .

Next we will establish that no two of the elements in this special set are congruent to each other modulo p . For suppose j and k are such that $1 \leq k < j \leq p-1$ where $aj \equiv ak \pmod{p}$. Then for some n , $aj - ak = np$. $a(j - k) = np$. Since a and p are relatively prime this last equation implies p divides into $(j - k)$. But this is impossible because $1 \leq j - k < p - 1$.

As a set of representatives of equivalence classes, the above special set could be replaced by the simpler set $\{1, 2, 3, \dots, (p-1)\}$. Now let's write $\{r_1, r_2, r_3, \dots, r_{p-1}\}$ for these simplest of $p-1$ remainders in a possibly different order where for all i , $1 \leq r_i \leq p-1$, and

$$\begin{aligned} a \cdot 1 &\equiv r_1 \pmod{p} \\ a \cdot 2 &\equiv r_2 \pmod{p} \\ a \cdot 3 &\equiv r_3 \pmod{p} \\ &\vdots \\ a \cdot (p-1) &\equiv r_{p-1} \pmod{p} \end{aligned}$$

Note that $\prod_{i=1}^{p-1} r_i = (p-1)!$. Finally, taking products and applying Theorem **9** multiple times we have

$$\begin{aligned} (a \cdot 1)(a \cdot 2)(a \cdot 3) \cdots (a(p-1)) &\equiv r_1 \cdot r_2 \cdot r_3 \cdots r_{p-1} \pmod{p} \\ a^{p-1}(1 \cdot 2 \cdot 3 \cdots (p-1)) &\equiv \prod_{i=1}^{p-1} r_i \pmod{p} \\ a^{p-1} \cdot (p-1)! &\equiv (p-1)! \pmod{p} \end{aligned}$$

Now apply Theorem **12** and divide by $(p-1)!$ after noting that $(p-1)!$ is relatively prime to p . Then we have $a^{p-1} \equiv 1 \pmod{p}$.

14 Corollary. If n is not a multiple of q and $n^{q-1} \not\equiv 1 \pmod{q}$ then q must be composite.

Proof: By contradiction. Assume q is prime. Then by Fermat's Little Theorem 13 we would have $n^{q-1} \equiv 1 \pmod{q}$ which is a contradiction to the second hypothesis.

15 Definition **Euler's Phi Function**. Let n denote any positive integer. $\phi(n)$ denotes the number of integers not exceeding n that are relatively prime to n .

16 Remark: We would normally just say $\phi(n)$ is the number of integers less than n that are relatively prime to n . The reason for saying "not exceeding n " is so that $\phi(1) = 1$.

17 Theorem. (Euler ϕ -function Evaluation #1)

If p is prime then $\phi(p) = p - 1$.

Proof: Since p is prime, every integer less than p is relatively prime to p .

18 Theorem. (Euler ϕ -function Evaluation #2)

If p is a prime then $\phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right) = p^{k-1}(p - 1) = p^{k-1}\phi(p)$.

Proof: All the integers less than or equal to p^k are relatively prime to p^k except those that are multiples of p . Consider $1p, 2p, 3p, \dots, p^{k-1}p$. Thus there are p^{k-1} of these. Thus we have $\phi(p^k) = p^k - (\# \text{ multiples of } p \text{ less than } p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right) = p^{k-1}(p - 1) = p^{k-1}\phi(p)$.

19 Theorem. (Euler ϕ -function Evaluation #3)

If p and q are distinct primes then

$$\phi(p^{k_1} \cdot q^{k_2}) = \phi(p^{k_1}) \cdot \phi(q^{k_2}) = p^{k_1} q^{k_2} \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right)$$

Proof: Let $n = p^{k_1} q^{k_2}$. Note that p and q are the only prime factors of n . Except for the multiples of p and the multiples of q and the multiples of pq , all the integers less than n are relatively prime to n . Note that $\frac{n}{p} = \#$ of multiples of p that are less than n . $\frac{n}{q} = \#$ of multiples of q that are less than n . $\frac{n}{pq} = \#$ of multiples of pq that are less than n . Now the only two complications are that some of the multiples of p also include all the multiples of pq and some of the multiples of q also include all the multiples of pq . So we calculate $\phi(n) = n - \frac{n}{p} - \frac{n}{q} + \frac{n}{pq}$. We have subtracted all the multiples of pq twice and we have added all the multiples of pq back once, so the net effect is to subtract all the multiples of pq once. Now we can factor out n and write $\phi(p^{k_1} q^{k_2}) =$

$$n \left[1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{pq}\right] = n \left[\left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right)\right] = p^{k_1} q^{k_2} \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right).$$

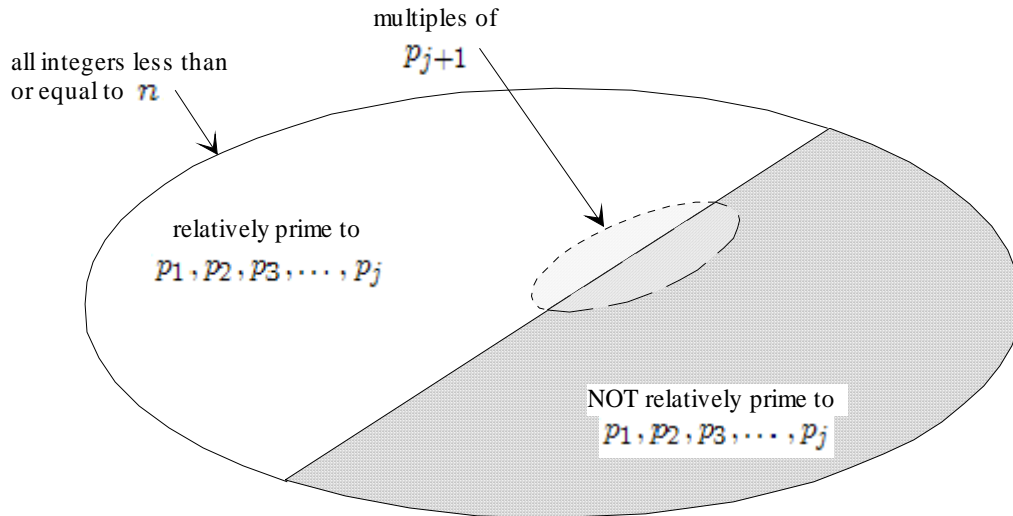
20 Theorem. (Euler ϕ -function Evaluation #4)

Let $p_1, p_2, p_3, \dots, p_k$ be some of the primes that divide evenly into any positive integer n . Then the number of positive integers less than or equal to n that are not divisible by any of $p_1, p_2, p_3, \dots, p_k$ is given by $n \cdot \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$.

Proof: Use induction on k . If $k = 1$ we only assume n is divisible by the prime p . Now all integers less than n can be considered to be not divisible by p , except those integers that are multiples of p . However, $\frac{n}{p}$ is the number of multiples of p that are less than or equal to n . So $n - \frac{n}{p} = n \left(1 - \frac{1}{p}\right)$ is the number of integers less than or equal to n that are not divisible by p . This establishes the result when $k = 1$.

Now assume that when any integer is divisible by the primes $p_1, p_2, p_3, \dots, p_j$, then the number of positive integers less than or equal to that integer that are not divisible by any of $p_1, p_2, p_3, \dots, p_j$ is given by the product of that integer with $\prod_{i=1}^j \left(1 - \frac{1}{p_i}\right)$. That is, we assume the result is true whenever $j \leq k$.

Let n denote any integer that is divisible by $p_1, p_2, p_3, \dots, p_j, p_{j+1}$. All the integers less than or equal to n can first be split into two disjoint subsets, those that are relatively prime to $p_1, p_2, p_3, \dots, p_j$ and those that are NOT relatively prime to $p_1, p_2, p_3, \dots, p_j$. Next, consider all the multiples of p_{j+1} that are split across the two main subsets just described.



To determine all the integers less than or equal to n that are relatively prime to all of $p_1, p_2, p_3, \dots, p_j, p_{j+1}$ we first count the number of integers less than or equal to n that are relatively prime to $p_1, p_2, p_3, \dots, p_j$. This count is too high for $\phi(n)$ because it includes multiples of p_{j+1} . So we simply subtract from this first count the multiples of p_{j+1} that are also relatively prime to $p_1, p_2, p_3, \dots, p_j$. See the above figure.

The first count, by the induction assumption, is $n \cdot \prod_{i=1}^j \left(1 - \frac{1}{p_i}\right)$. Next, the multiples of p_{j+1} may be listed as: $1 \cdot p_{j+1}, 2 \cdot p_{j+1}, 3 \cdot p_{j+1}, \dots, \frac{n}{p_{j+1}} \cdot p_{j+1}$. Now the positive integers among those just listed that are not multiples of any of $p_1, p_2, p_3, \dots, p_j$ are the ones in which the coefficients of p_{j+1} , that is, $1, 2, 3, \dots, \frac{n}{p_{j+1}}$ are not divisible by any of $p_1, p_2, p_3, \dots, p_j$. But by the induction assumption this number is

$$\frac{n}{p_{j+1}} \cdot \prod_{i=1}^j \left(1 - \frac{1}{p_i}\right). \text{ Finally, } \phi(n) = n \cdot \prod_{i=1}^j \left(1 - \frac{1}{p_i}\right) - \frac{n}{p_{j+1}} \cdot \prod_{i=1}^j \left(1 - \frac{1}{p_i}\right) =$$

$$n \cdot \prod_{i=1}^j \left(1 - \frac{1}{p_i}\right) \cdot \left\{1 - \frac{1}{p_{j+1}}\right\} = n \cdot \prod_{i=1}^{j+1} \left(1 - \frac{1}{p_i}\right).$$

21 Theorem (Euler ϕ -function Evaluation #5)

If $p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_m^{k_m}$ is the unique prime factorization of n then $\phi(n) = n \cdot \prod_{i=1}^m \left(1 - \frac{1}{p_i}\right)$

$$= \prod_{i=1}^m (p_i^{k_i} - p_i^{k_i-1}).$$

Proof: Apply Theorem **20** after noting that $p_1, p_2, p_3, \dots, p_m$ are all and the only primes that divide into n . The second equation is established by writing $\phi(n) = \prod_{i=1}^m p_i^{k_i} \left(1 - \frac{1}{p_i}\right)$ and applying the distributive law.

22 Theorem (Euler ϕ -function Evaluation #6)

If m and n are relatively prime then $\phi(mn) = \phi(m) \cdot \phi(n)$.

Proof: Let $p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_a^{k_a}$ denote the unique prime factorization of m and let $q_1^{j_1} q_2^{j_2} q_3^{j_3} \cdots q_b^{j_b}$ denote the unique prime factorization of n . Then by Theorem **20** we may write

$$\phi(m \cdot n) = \phi(p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_a^{k_a} \cdot q_1^{j_1} q_2^{j_2} q_3^{j_3} \cdots q_b^{j_b}) =$$

$$p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_a^{k_a} \cdot q_1^{j_1} q_2^{j_2} q_3^{j_3} \cdots q_b^{j_b} \cdot \prod_{i=1}^a \left(1 - \frac{1}{p_i}\right) \cdot \prod_{i=1}^b \left(1 - \frac{1}{q_i}\right) =$$

$$p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_a^{k_a} \cdot \prod_{i=1}^a \left(1 - \frac{1}{p_i}\right) \cdot q_1^{j_1} q_2^{j_2} q_3^{j_3} \cdots q_b^{j_b} \cdot \prod_{i=1}^b \left(1 - \frac{1}{q_i}\right) =$$

$$\phi(m) \cdot \phi(n).$$

23 Theorem. (**Euler**) If a and n are relatively prime then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof: Note that this Theorem is a generalization of Fermat's Little Theorem in light of Theorem **13** when n is a prime number.

The set $\{0, 1, 2, \dots, n-1\}$ contains representatives for distinct equivalence classes that exist modulo n . From this set we remove 0 and we keep only the positive integers that are relatively prime to n and less than n . There are $\phi(n)$ of these and we may write (label) the new reduced set as $\{r_1, r_2, r_3, \dots, r_{\phi(n)}\}$.

Now consider the special set $\{a \cdot r_1, a \cdot r_2, a \cdot r_3, \dots, a \cdot r_{\phi(n)}\}$. We claim that no two members in this last set are congruent to each other modulo n . For if $j \neq k$ but $a \cdot r_j \equiv a \cdot r_k \pmod{n}$ then $a \cdot r_j - a \cdot r_k = bn$ for some integer b . Then $a(r_j - r_k) = bn$. n is a factor of the right side of this last equation which means n is a factor of the left side. But since a and n are relatively prime we conclude that $r_j - r_k = cn$ for some integer c . This of course means $r_j \equiv r_k \pmod{n}$ and this is impossible because the r_i represent distinct equivalence classes.

Now since all the r_i as well as a are relatively prime to n , so are the $\phi(n)$ integers $\{a \cdot r_1, a \cdot r_2, a \cdot r_3, \dots, a \cdot r_{\phi(n)}\}$ all relatively prime to n . But this implies that as a set of representatives of equivalence classes the set $\{a \cdot r_1, a \cdot r_2, a \cdot r_3, \dots, a \cdot r_{\phi(n)}\}$ could be replaced by the simpler set $\{r_1, r_2, r_3, \dots, r_{\phi(n)}\}$.

Lets write $\{s_1, s_2, s_3, \dots, s_{\phi(n)}\}$ as a possible re-ordering of the set $\{r_1, r_2, r_3, \dots, r_{\phi(n)}\}$ where

$$\begin{aligned} a \cdot r_1 &\equiv s_1 \pmod{n} \\ a \cdot r_2 &\equiv s_2 \pmod{n} \\ a \cdot r_3 &\equiv s_3 \pmod{n} \\ &\vdots \\ a \cdot r_{\phi(n)} &\equiv s_{\phi(n)} \pmod{n} \end{aligned}$$

Note that $\prod_{i=1}^{\phi(n)} r_i = \prod_{i=1}^{\phi(n)} s_i$. Finally, taking products and applying Theorem **9** multiple times we have

$$(a \cdot r_1)(a \cdot r_2)(a \cdot r_3) \cdots (a \cdot r_{\phi(n)}) \equiv s_1 \cdot s_2 \cdot s_3 \cdots s_{\phi(n)} \pmod{n}$$

$$a^{\phi(n)}(r_1 \cdot r_2 \cdot r_3 \cdots r_{\phi(n)}) \equiv \prod_{i=1}^{\phi(n)} s_i \pmod{n}$$

$$a^{\phi(n)} \cdot \prod_{i=1}^{\phi(n)} r_i \equiv \prod_{i=1}^{\phi(n)} r_i \pmod{n}$$

Now apply Theorem **12** and divide by $\prod_{i=1}^{\phi(n)} r_i$ after noting this product is relatively prime to n because each r_i is relatively prime to n . Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

24 Theorem. (**Wilson**) If p is prime then $(p - 1)! \equiv -1 \pmod{p}$.

Proof: By Fermat's Little Theorem 13 $a^{p-1} \equiv 1 \pmod{p}$ where p is not a factor of a .

By Theorem 2 we can subtract 1 from both sides to get $a^{p-1} - 1 \equiv 0 \pmod{p}$.

Now if $a = 1, 2, 3, \dots, p - 1$ then

$$a^{p-1} - 1 \equiv (a - 1)(a - 2)(a - 3) \cdots (a - (p - 1)) \pmod{p}.$$

$$\text{Now let } a = 0 \text{ to get } -1 \equiv \prod_{i=1}^{p-1} -i \pmod{p}$$

$$-1 \equiv (-1)^{p-1} \cdot (p - 1)! \pmod{p}$$

Now since p is prime, p is odd, or $p = 2$. If p is odd, then $p - 1$ is even and then we have $-1 \equiv (p - 1)! \pmod{p}$. If $p = 2$ then we have $(2 - 1)! = 1 \equiv -1 \pmod{2}$ because $1 - (-1) = 2$. So in either case we get $(p - 1)! \equiv -1 \pmod{p}$.

25 Remark: For any integer a and a large integer n , it is easy to compute $a^{n-1} \pmod{n}$ by using what is called a fast exponential algorithm that is based on repeated squaring. For an example of this technique, go to the author's homepage web site and download the paper titled *An Efficient Algorithm For Computing Large Integer Powers of any Base*.

26 Remark: For any large integer n that has only two large prime factors of nearly the same size it is extremely time-consuming and difficult to find the prime factors of n .

27 Remark: The RSA cryptographic system may be described as follows.

- 1) Generate at random two 100+ digit prime numbers, call them p and q .
- 2) Calculate $n = p \times q$.
- 3) Calculate $\phi(n) = (p - 1)(q - 1) = pq - p - q + 1 = n - (p + q) + 1$.
- 4) Forget the values of p and q that were used to generate n .
- 5) Generate at random a large integer $e < \phi(n)$ such that e is relatively prime to $\phi(n)$.
- 6) Calculate the multiplicative inverse of e modulo $\phi(n)$ and call this number d . Note that $de \equiv 1 \pmod{\phi(n)}$. Since e and $\phi(n)$ are relatively prime, by Euler's Theorem we know $e^{\phi(n)} \equiv 1 \pmod{\phi(n)}$. This result guarantees there exists a positive integer k such that $e^k \equiv 1 \pmod{\phi(n)}$. We can then let $d = e^{k-1}$. Note that k can be found by simply calculating powers of e using the fast exponential algorithm until the first one is found that is equivalent to $1 \pmod{\phi(n)}$.
- 7) The public enciphering key is the pair (n, e) .
- 8) The secret deciphering key is the pair (n, d) .
- 9) The plain text P is broken down into a sequence of block numbers B_i , all the same size. If this size is M then we require $1 \leq M \leq n$. The simple table shown on the next page is an example of how to encode letters as numbers.

A simple table for converting letters to numbers.

| Letter | encoded number |
|--------|----------------|
| A | 01 |
| B | 02 |
| C | 03 |
| D | 04 |
| E | 05 |
| F | 06 |
| G | 07 |
| H | 08 |
| I | 09 |
| J | 10 |
| K | 11 |
| L | 12 |
| M | 13 |
| N | 14 |
| O | 15 |
| P | 16 |
| Q | 17 |
| R | 18 |
| S | 19 |
| T | 20 |
| U | 21 |
| V | 22 |
| W | 23 |
| X | 24 |
| Y | 25 |
| Z | 26 |
| space | 27 |

- 10) The enciphering transformation is $C_i = (B_i)^e \pmod n$ where each B_i is a block number of plain text and each C_i is a block number of cyphertext. Note that anyone can encipher any text since both e and n are part of the public key and the enciphering algorithm is also publicly known.
- 11) The deciphering transformation is $B_i = (C_i)^d \pmod n$ where each B_i is a plaintext block and each C_i is a cyphertext block. Note that only the holder of the private key pair (n, d) can decode cyphertext.

28 Remark: The following explains how and why the RSA deciphering algorithm works.

First we will prove that for all integers I we must have $I^{ed} \equiv I \pmod{n}$.

Since $ed \equiv 1 \pmod{\phi(n)}$ we know there exists an integer k such that

$$ed - 1 = k \cdot \phi(n) = k(p-1)(q-1).$$

We claim that for all integers I we must have $I^{ed} \equiv I \pmod{p}$ and that

$I^{ed} \equiv I \pmod{q}$. We will first establish this claim for the prime p . A similar argument can be used to establish the claim for the prime q .

Let I denote any integer. By Fermat's Little Theorem **13** we know $I^{p-1} \equiv 1 \pmod{p}$

provided I is relatively prime to p . This implies $I^p \equiv I \pmod{p}$ because we can multiply both sides of the congruence by I . Now if I is not relatively prime to p then

we would have $I = kp$ for some integer k . Then,

$$I^p - I = (kp)^p - kp = [k^p p^{p-1} - k] \cdot p \text{ which is a multiple of } p \text{ so that}$$

$$I^p \equiv I \pmod{p} \text{ whether } I \text{ and } p \text{ are relatively prime or not.}$$

We have shown that for all integers I , $I^p \equiv I \pmod{p}$. Now divide both sides

by I to get $I^{(p-1)} \equiv 1 \pmod{p}$. Now raise both sides to the power of $k(q-1)$

and we have $[I^{(p-1)}]^{k(q-1)} \equiv 1^{k(q-1)} \pmod{p}$. Simplifying both sides yields

$$I^{ed-1} \equiv 1 \pmod{p}. \text{ Finally, multiply both sides by } I \text{ to get } I^{ed} \equiv I \pmod{p}.$$

Now having established for all integers I that $I^{ed} \equiv I \pmod{p}$ and $I^{ed} \equiv I \pmod{q}$

we next use the fact p and q are relatively prime to each other to conclude by Theorem

10 that $I^{ed} \equiv I \pmod{n}$ where $n = pq$.

Now under the encyphering algorithm, if $C_i = (B_i)^e \pmod{n}$ and then if this same C_i is sent to the deciphering algorithm then we would calculate

$$(C_i)^d \equiv ((B_i)^e)^d = (B_i)^{de} \equiv B_i \text{ where all calculations are carried out modulo } n \text{ and the last congruence is based on the above identity that } I^{ed} \equiv I \pmod{n} \text{ for all integers } I.$$

29 Remark: The security of the RSA cryptographic system is based on two facts. The first is that knowing n and e do not allow you to determine the value of d . Second, since you know n , it would be relatively easy to find d if you could just factor n to determine the primes p and q . However, no one has found a time-efficient way to factor n when n has only two very large prime factors.