EXERCISES 9.3

1. Find the numbers of letters grouped for an exponentiation cipher in a plaintext numeric block that is 12 digits long.
2. Find the smallest prime that can be used as the modulus in an exponentiation cryptosystem if the letters are grouped in blocks of two letters.
3. Show that the plaintext AB is left fixed by every exponentiation cipher.

With $p = 3037$ as the exponentiation modulus and $e = 31$ as the enciphering exponent, encipher each message.

4. ALL IS WELL.
5. HAVE A NICE DAY.

Using $p = 2549$ as the exponentiation modulus and $e = 11$ as the enciphering exponent, encrypt each message.

6. NO PAINS NO GAINS.
7. NOTHING TO EXCESS. (Solon)

Each ciphertext below was generated by an exponentiation cipher with $p = 3037$ and $e = 31$. Decipher each.

8. 0790 0778 1509 0499
9. 0624 1535 2669 0998

Each ciphertext below was created by an exponentiation cipher with $p = 2333$ and $e = 13$. Decrypt each.

10. 1194 1693 1453 2250 0008
11. 1560 1250 0522 0631 1505

Two persons would like to share secret messages by using a common key and an exponentiation cipher with $p = 131$. Using $x = 2$ as in the text, compute the common key e for the given pair of individual keys.

12. 11, 23
13. 7, 17

14–15. Determine the common deciphering key in Exercises 12 and 13.

9.4 The RSA Cryptosystem

In a conventional cipher system, the enciphering key is known only to the sender and the intended receiver, since once the enciphering key is known, an unauthorized individual can discover the deciphering key in a short time. Consequently, before coded messages are sent, the key must be transmitted over a secure communication channel.

However, in 1976, Whitfield Diffie and Martin E. Hellman of Stanford University proposed a revolutionary cipher system, called a **public-key cryptosystem**, that makes it unnecessary to keep the key away from unauthorized users. In a public-key system, the enciphering algorithm E of every user of the system is made public as in a telephone directory, while the corresponding decrypting algorithm D is known only to the intended user. Although the encryption key E is public knowledge, it is computationally infeasible to employ it to discover the decryption key D, so it is virtually impossible for a cryptanalyst to crack the system.

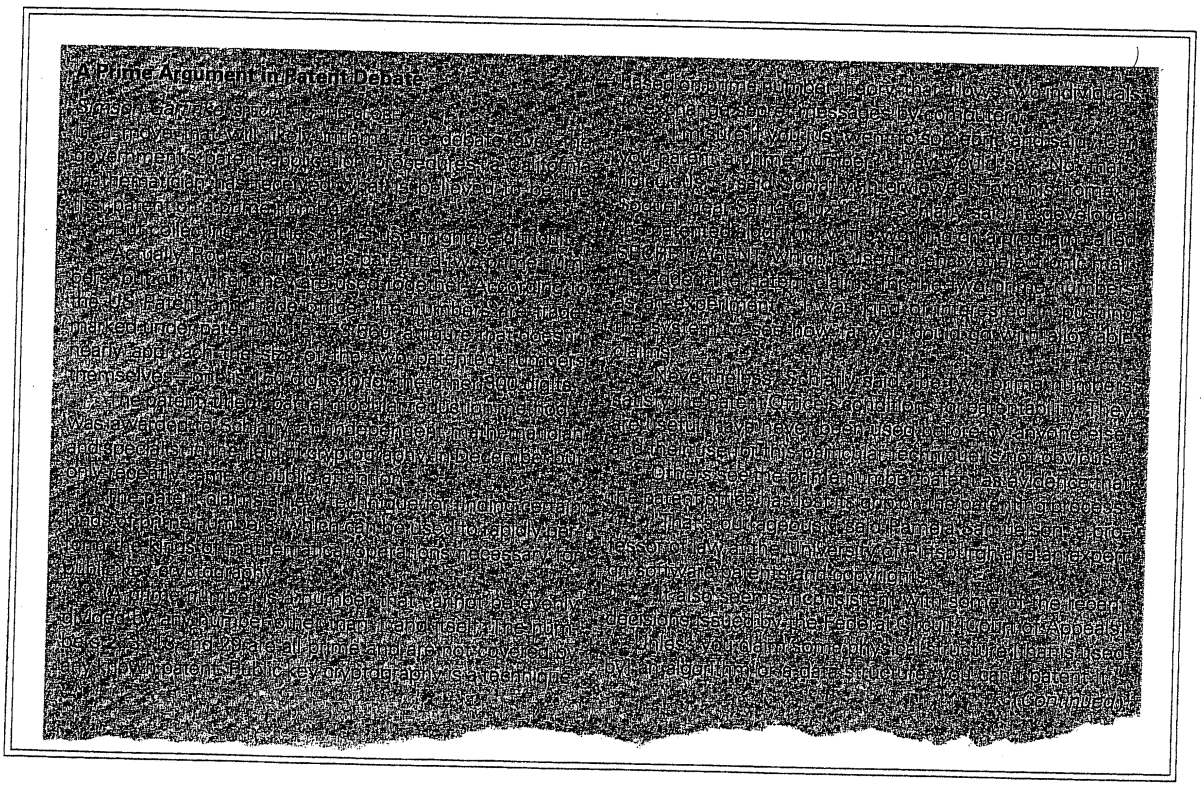
Although Diffie and Hellman did not provide a practical implementation of a public-key cipher system, they developed three properties such a cryptosystem must

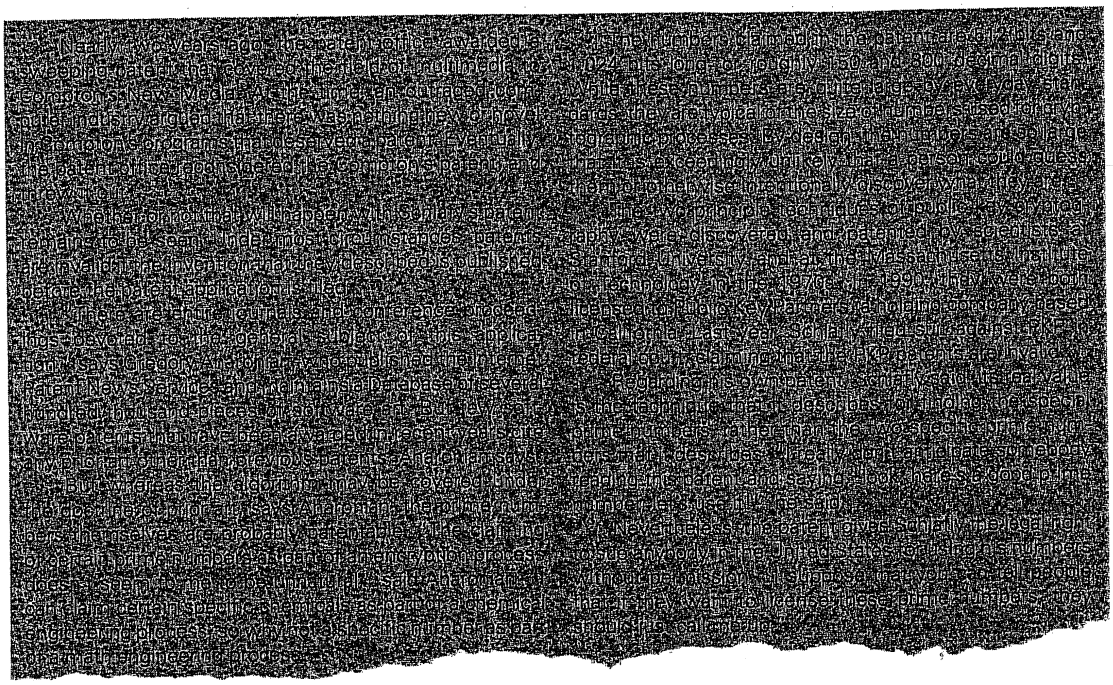
have. They are

- Each user must have an encryption key E (which is made public) and a decryption key D (which is kept secret) such that $M = E(D(M)) = D(E(M))$ for every message M. Thus the algorithms E and D are inverse operations.
- It is computationally easy for the user to compute the keys E and D.
- It is computationally infeasible for an unauthorized user to employ the encryption key E to develop the decryption key D, ensuring the security of the system.

How does such a cipher system work? Suppose there are n users of the system. Each person i has an encryption key E_i in the public directory, where $1 \leq i \leq n$. For him to send a message P to person j, he looks up j's encryption key E_j and then sends him the encrypted message $C = E_j(P)$. Then j applies his secret deciphering algorithm D_j to C to recover the original plaintext P, since $D_j(C) = D_j(E_j(P)) = P$. No other person k can crack the message C since $D_k(C) = D_k(E_j(P)) \neq P$, when $k \neq j$.

In 1978 Ronald L. Rivest, Adi Shamir, and Leonard Adelman of the Massachusetts Institute of Technology developed a practical way of implementing Diffie and Hellman's elegant concept. Popularly known as the **RSA cryptosystem**, this public key system is an exponentiation cipher system based on modular exponentiation and Euler's theorem. (RSA is an acronym for **R**ivest, **S**hamir, and **A**delman.)





The Enciphering Algorithm

In an RSA system, the enciphering key is a pair (e, n) of positive integers e and n, where the enciphering modulus n is the product of two very large and distinct primes p and q, each about 100 digits long, and $(e, \varphi(n)) = 1$. To encrypt a plaintext message, as in the exponentiation cryptosystem, we group the plaintext numeric equivalents into blocks of length $2m$, with padding at the end if necessary. Then we convert each block P into a ciphertext block C using the encrypting congruence

$$C = E(P) \equiv P^e \pmod{n} \tag{8}$$

where $0 < C < n$.

The following example illustrates this algorithm.

EXAMPLE 9.14 Using the RSA enciphering modulus $n = 2773$ and the enciphering key $e = 21$, encrypt the message SILENCE IS GOLDEN.

SOLUTION

First, notice that $n = 2773 = 47 \cdot 59$, the product of two primes, and $\varphi(n) = \varphi(47 \cdot 59) = 46 \cdot 58 = 2^2 \cdot 23 \cdot 29$, so clearly $(e, \varphi(n)) = 1$. (For practical purposes, we have chosen the primes to be small.)

As in Example 9.12, after the numeric translation and grouping into blocks, the plaintext yields

$$1808 \quad 1104 \quad 1302 \quad 0408 \quad 1806 \quad 1411 \quad 0304 \quad 1323$$

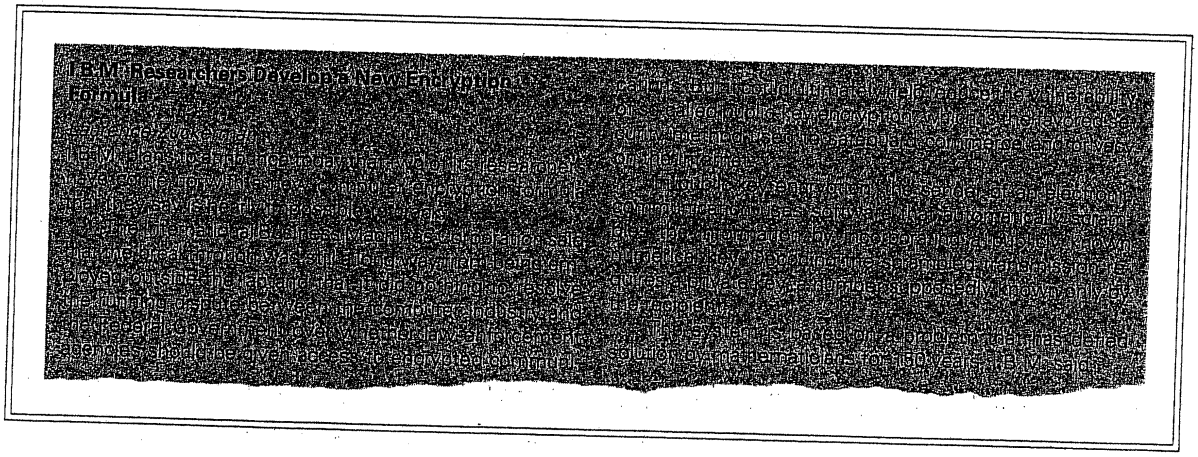
Now using modular exponentiation and formula (8), convert each block P into a ciphertext block C:

$$C \equiv P^e = P^{21} \pmod{2773}$$

For instance, when $P = 1808$,

$$C \equiv 1808^{21} \equiv 1808^{16+4+1} \equiv 1511 \cdot 666 \cdot 1808 \equiv 0010 \pmod{2773}$$

The other blocks can be found similarly. The ensuing ciphertext message is 0010 0325 2015 2693 2113 2398 2031 1857. ■



The Deciphering Algorithm

To decipher a ciphertext C generated by an RSA system, we need to compute the inverse d of the enciphering exponent e modulo $\varphi(n)$, which exists since $(e, \varphi(n)) = 1$. Then $de \equiv 1 \pmod{\varphi(n)}$; that is, $de = 1 + k\varphi(n)$ for some constant k. Knowing the deciphering exponent d, we can recover the plaintext P by raising both sides of

congruence (8) to the power d modulo n:

$$\begin{aligned} P &= D(C) \\ C^d &\equiv (P^e)^d = P^{ed} = P^{1+k\varphi(n)} \pmod{n} \\ &= P \cdot \left[P^{\varphi(n)}\right]^k \equiv P \cdot 1^k = P \pmod{n} \end{aligned} \tag{9}$$

where, by Euler's theorem, $P^{\varphi(n)} \equiv 1 \pmod{n}$, if $(P, n) = 1$. The pair (d, n) is the **deciphering key**.

In the highly unlikely event that $(P, n) \neq 1$, since $n = pq$, $(P, n) = p, q$, or pq. Since $P < n$, $(P, n) \neq n$. When $(P, n) = p$, $(P, q) = 1$, so by Fermat's little theorem, $P^{q-1} \equiv 1 \pmod{q}$. Since $de \equiv 1 \pmod{(p-1)(q-1)}$, $de = 1 + k(p-1)(q-1)$ for some integer k.

$$\therefore P^{de} = P \cdot (P^{q-1})^{k(p-1)} \equiv P \cdot 1^{k(p-1)} \equiv P \pmod{q}$$

That is,

$$C^d \equiv P \pmod{q}$$

When $(P, n) = p$, $C^d \equiv P^{de} \equiv 0 \equiv P \pmod{p}$. Thus $C^d \equiv P \pmod{p}$ and $C^d \equiv P \pmod{q}$, so $C^d \equiv P \pmod{n}$. The case $(P, n) = q$ yields the same conclusion.

Note that if p and q are 100-digit primes, the probability of such an occurrence of a plaintext block is extremely negligible, namely less than $2 \cdot 10^{-99}$. See Supplementary Exercise 6.

The following example demonstrates the decrypting algorithm D.

EXAMPLE 9.15 Decrypt the ciphertext message 0010 0325 2015 2693 2113 2398 2031 1857 that was created using the RSA enciphering key $(e, n) = (21, 2773)$.

SOLUTION

Because $\varphi(n) = \varphi(2773) = \varphi(47 \cdot 59) = 46 \cdot 58 = 2668 = 127 \cdot 21 + 1$, $(-127) \cdot 21 \equiv 1 \pmod{2668}$, that is, $2541 \cdot 21 \equiv 1 \pmod{2668}$, so the deciphering exponent is $d = 2541$. Because $P \equiv C^d \pmod{n}$, raise each ciphertext C to the power 2541 modulo 2773. For instance, when $C = 0010$,

$$\begin{aligned} P &\equiv 0010^{2541} \equiv 10^{2541} \pmod{2773} \\ &\equiv 10^{2048+256+128+64+32+8+4+1} \pmod{2773} \\ &\equiv 1024 \cdot 2431 \cdot 2500 \cdot 1366 \cdot 2127 \cdot 74 \cdot 1681 \cdot 10 \equiv 1808 \pmod{2773} \end{aligned}$$

as expected. The other blocks can be decrypted similarly. ■

Digital Signatures

The property $E(D(M)) = M$, found in public-key cryptosystems, can be effectively used to transmit "digitally signed" messages. This is a practical and highly desirable feature, since such a cipher system ensures authentication and protects against forgeries. Such digital signatures are widely used in electronic banking.

Interestingly, in June 2000, President William J. Clinton signed into law a bill allowing businesses and consumers to enter into legally binding arrangements with electronic rather than handwritten signatures. *E-signing*, as the new process is called, is expected to spur new technologies, accelerate electronic transactions, and save billions of dollars in administrative costs. See Figure 9.4.

To see how signed messages work in public-key cipher systems and, in particular, RSA systems, suppose that person i wishes to send person j a signed message P. First, person i applies his secret deciphering algorithm D_i to P. This yields $D_i(P) \equiv P^{d_i} \pmod{n}$; he then applies j's enciphering algorithm E_j to it, since E_j is public knowledge. This produces the message $E_j(D_i(P)) \equiv P^{d_i e_j} \pmod{n}$. Person i now sends this convoluted message to j.

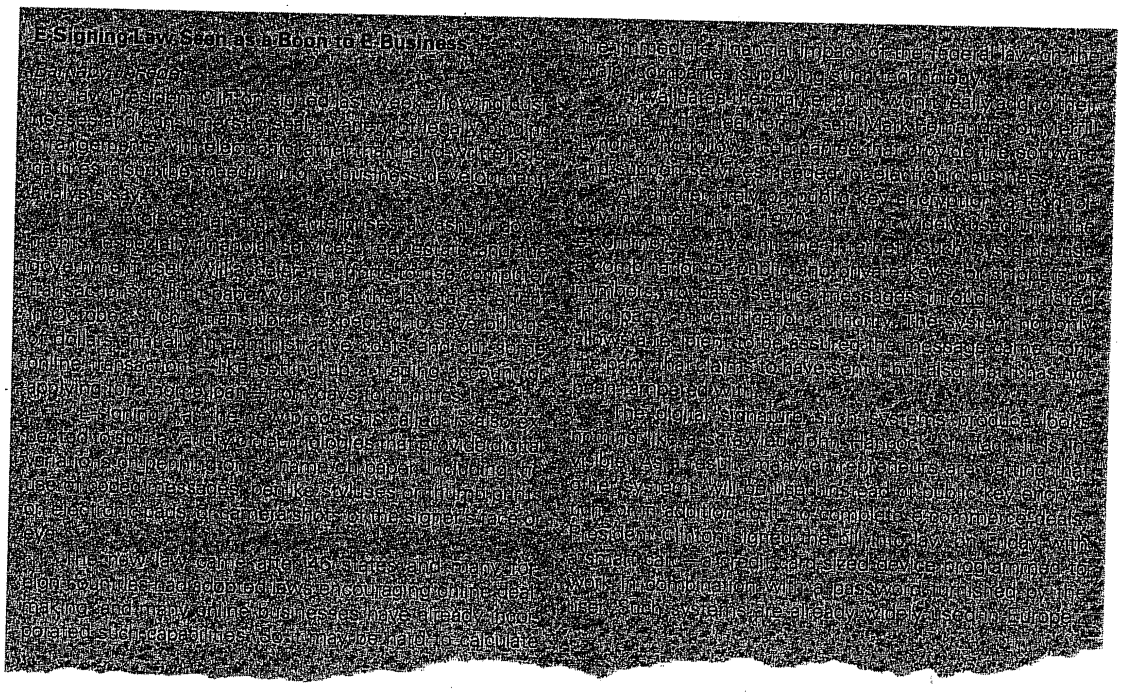


Figure 9.4

To decipher this message, allegedly sent by person i, first person j applies his deciphering key to it to yield

$$D_j(E_j(D_i(P))) \equiv (P^{d_i e_j})^{d_j} = (P^{e_j d_j})^{d_i} \equiv P^{d_i} \pmod{n} = D_i(P)$$

because D_j and E_j are inverse operations. He then applies person i's public encryption algorithm E_i to it to yield

$$E_i(D_i(P)) \equiv (P^{d_i})^{e_i} = P^{d_i e_i} \equiv P \pmod{n}$$

Once again, because E_i and D_i are inverse operations, this operation produces the original plaintext P. This ensures that the original message was in fact sent by person i and nobody else, since $E_i(D_k(P)) \neq P$ if $k \neq i$. Consequently, i can never claim that he did not send the plaintext P, since he is in sole possession of the secret key D_i.

As these two examples demonstrate, both encryption and decryption become tedious as n gets larger and larger, so for an RSA system to be realistically useful, n must be very large. Both processes require fast computers for implementation.

To find n, first find two large primes p and q, about 100 digits long. This requires only a few minutes of computer time. Then $n = pq$ is about 200 digits long. That the value of n is public information does not imply that its prime factors are publicly known. The factoring of a 200-digit number is an extremely time consuming proposition.

Once p and q have been selected, the enciphering exponent e can be chosen in such a way that $(e, \varphi(n)) = 1$. One way to do this is by choosing a prime greater than both p and q.

The exponent e must be chosen so that $2^e > n$; this ensures that every plaintext block, except 0 and 1, will be subjected to reduction modulo n. Otherwise, since $C \equiv P^e \pmod{n}$, P can be recovered by taking the eth root of C.

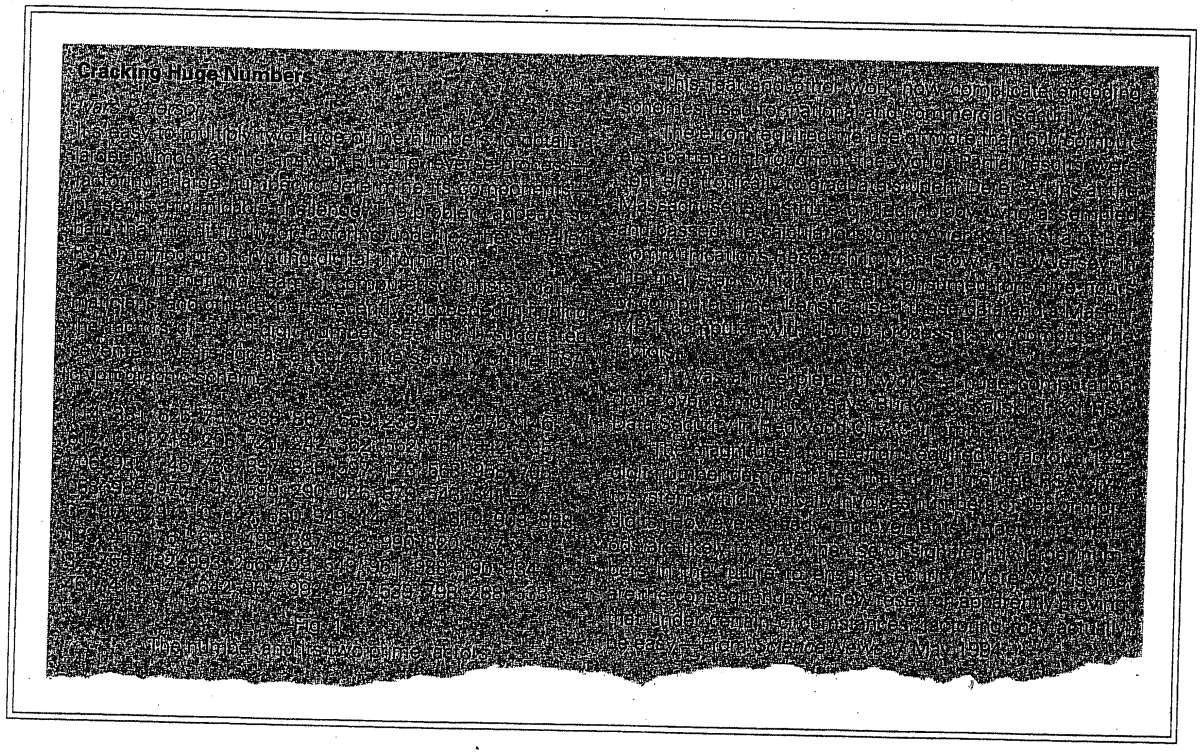
The deciphering exponent d can easily be computed using the euclidean algorithm, where $de \equiv 1 \pmod{\varphi(n)}$ and $\varphi(n) = (p-1)(q-1)$.

Publishing the enciphering key (e, n) does not compromise security, because a cryptanalyst must know the value of $\varphi(n)$ to compute the deciphering exponent d. Clearly, $\varphi(n)$ can be computed if p and q are known, since $\varphi(n) = \varphi(pq) = (p-1)(q-1)$. Since computing $\varphi(n)$ involves the factoring of n, it is as difficult as the factoring of n. Since p and q are 100 decimal digits long and $n = pq$ is about 200 decimal digits long, the fastest known factorization algorithm will take about four billion years of computing time on the fastest available computer, as Table 9.9† shows. Although this could change with time and technology, the RSA system is virtually secure at present. If faster factorization techniques and faster computers become available, then the size of the factors can be increased accordingly to maintain the security of the system.

† Based on R. L. Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, Vol. 21, (February 1978), pp. 120–126.

Number of Digits	*Time*
50	3.9 hours
75	104 days
100	74 days
200	3.8×10^9 years
300	4.9×10^{15} years
500	4.2×10^{25} years

Table 9.9



Note that the primes p and q can be computed from $\varphi(n)$. See Exercises 9 and 10.

Also, to prevent a cryptanalyst from resorting to special techniques to factor n, both p and q should be of about the same size, with $p - 1$ and $q - 1$ having large prime factors and $(p - 1, q - 1)$ small.

However, if d is known then $ed - 1$, a multiple of $\varphi(n)$ can be computed; knowing a multiple of $\varphi(n)$, n can be factored fairly easily using an algorithm developed in 1976 by G. L. Miller.

EXERCISES 9.4

Using the RSA enciphering key $(e, n) = (11, 2867)$, encrypt each message.

1. SEAFOOD
2. OPEN DOOR

3–4. Redo Exercises 1 and 2 using the RSA enciphering key $(e, n) = (17, 2867)$.

Each ciphertext below was generated by the RSA enciphering key $(e, n) = (11, 2867)$. Decipher each.

5. 1420 0614 1301 1694
6. 1959 1384 1174 2050

Decrypt each ciphertext below that was created by the RSA enciphering key $(e, n) = (17, 2867)$.

7. 0579 0341 0827 1511
8. 0592 2131 2584 2188

Let $n = pq$, where p and q are primes with $p > q$. [Exercises 9–11 show that if n and $\varphi(n)$ are known, then the prime factors of n can be determined.]

9. Show that $p + q = n - \varphi(n) + 1$.
10. Show that $p - q = \sqrt{(p+q)^2 - 4n}$.
11. Express p and q in terms of n and $\varphi(n)$.
12. Use Exercises 9–11 to determine the primes p and q if $n = pq = 3869$ and $\varphi(n) = 3744$.
13. Redo Exercise 12 if $n = 3953$ and $\varphi(n) = 3828$.

Anne and Betsey would like to send each other a signed message using an RSA cipher. Their encryption keys are (13, 2747) and (17, 2747), respectively. Find the signed cipher message sent by:

14. Anne if the plaintext message is MARKET.
15. Betsey if the plaintext message is INPUT.

With the enciphering keys as before, find the plaintext sent by:

16. Anne if her signed message to Betsey is 1148 0194 2715.
17. Betsey if her signed message to Anne is 1130 2414 2737.

9.5 Knapsack Ciphers

In 1978, Ralph C. Merkle and Martin E. Hellman, both electrical engineers at Stanford University, developed a public-key cryptosystem based on the **knapsack problem**, a celebrated problem in combinatorics. It can be stated as follows: *Given a knapsack of volume* S *and* n *items of various volumes* $a_1, a_2, \ldots, a_n$, *which of the items can fill the knapsack*? In other words, given the positive integers $a_1, a_2, \ldots, a_n$, called **weights**, and a positive integer S, solve the linear diophantine equation

$$S = a_1x_1 + a_2x_2 + \cdots + a_nx_n \tag{10}$$

where $x_i = 0$ or 1. [Note that S is the dot product of the vectors $(a_1, a_2, \ldots, a_n)$ and $(x_1, x_2, \ldots, x_n)$.] The knapsack problem may have no solutions, one solution, or more than one solution.

For example, the knapsack problem $3x_1 + 5x_2 + 9x_3 + 19x_4 + 37x_5 = 45$ has one solution (1, 1, 0, 0, 1), since $3 + 5 + 0 + 0 + 37 = 45$. On the other hand, the knapsack problem $3x_1 + 5x_2 + 8x_3 + 13x_4 + 21x_5 = 34$ has two solutions; they are (0, 0, 0, 1, 1) and (0, 1, 1, 0, 1), because $0 + 0 + 0 + 13 + 21 = 34 = 0 + 5 + 8 + 0 + 21$. But the problem $5x_1 + 14x_2 + 15x_3 + 27x_4 + 11x_5 = 23$ has no solutions.

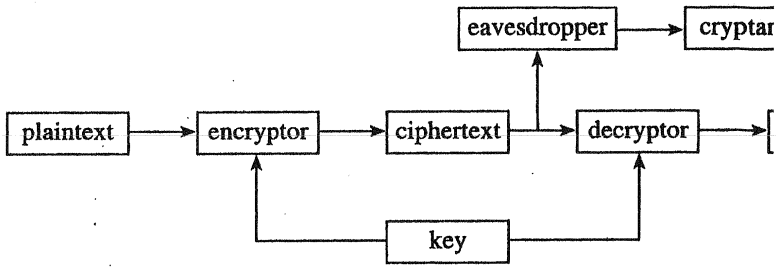


Figure 9.2

secret from unintended users of the system. In a public-key systen key is made public while only the intended receiver knows the deci

We now turn to our first cryptosystem.

9.1 Affine Ciphers

We will restrict our discussion to plaintext messages written in cap English alphabet, and ignore blank spaces and punctuation marks. tems we first translate each letter to a number. A convenient way o numbering the letters A through Z by their **ordinal numbers** 00 thr tively, as Table 9.1 shows. Using this scheme, we translate the th numeric message which is then enciphered into a numeric ciphertex then replaced by a letter. The recipient of the ciphertext substitutes th for each letter and uses the key to decipher the numeric message by s for the various numbers.

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
Ordinal Number	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21

Table 9.1

Substitution Ciphers

In a **substitution cipher**, we substitute a letter of the alphabet for plaintext. It is, in fact, a **permutation cipher**, since each substitutior of the letters of the alphabet. Since there are 26! permutations of th a total of 26! possible substitution ciphers; one of them is the trivial letter is substituted for itself.