

CHAPTER 11

Cryptography

Contents

11.1 Classical Cryptography	197
11.2 Modern Cryptography	201
11.3 Private-Key Cryptography	202
11.4 Public-Key Cryptography	204
11.5 The RSA Cryptosystem	205

Governments for military intelligence and diplomatic purposes over the past couple of millennia have been protecting information through secret messaging. In view of the advent of the Internet, there is an indispensable need to protect the information, in its transmission as well as its storage from unauthorized access and malicious actions. Cryptography is the field to keep information secret and offer protection of data from unwanted access and from any manipulation, impersonation, and forgery. An overview of cryptography is briefly presented in this chapter.

11.1 Classical Cryptography

Cryptography is about making secret communication to make messages secure in the presence of adversaries. By **encryption**, an original message, called **plaintext**, is transformed into a coded message, called **ciphertext**. This transformation is performed before the plaintext is transmitted or stored. The reverse process is called **decryption** and is performed after the ciphertext is received or retrieved. The algorithm used for encryption and decryption is often called a **cipher**, and the process of encryption and decryption requires a **secret key**. A key is a number (value) that the cipher operates on, without which the unauthorized parties must not be able to recover the original message.

In **classical cryptography**, symbols, characters, letters, and digits were directly manipulated with the sole goal to provide secrecy through obscurity. It appears that encrypted messages were first developed in ancient Egypt using **disordered hieroglyphics**, which consisted of visual symbols and characters. There were then other forms of message concealment, which were developed by the Greeks, namely **steganography**, through which a secret message was hidden within an ordinary nonsecret message, and by the Spartans, namely **scytale**, by which a narrow strip of parchment was wound on a rod and the message written across the adjoining edges.

A well-known classical cryptography technique, which was developed by Romans, was the **Caesar cipher**, a simple encryption method based on substitution. The Caesar cipher shifts each letter in the alphabet by three letters forward, for instance, the letter G becomes J. It thus requires a letter three places further along, while wrapping the letters at the end of the alphabet around to the letters at the beginning of the alphabet that is X wraps around to A, Y to B, and Z to C.

Mathematically described, in the Caesar cipher, each letter is coded by its position relative to others. To this effect, an integer $i \in \{0, 1, \dots, 24, 25\}$ replaces a letter whose position in the alphabet $\{A, B, \dots, Y, Z\}$ is the i th; for instance, D is the fourth letter in the alphabet, that is $i = 3$, D is thus replaced by 3. Assuming the nonnegative integer $p \leq 25$, the functions providing the encrypted message and the decrypted message are $f(p) = (p+3) \bmod 26$ and $f^{-1}(p) = (p-3) \bmod 26$, respectively.

A slight generalization of the Caesar cipher called the **shift cipher** or the **additive cipher**, is when 3 is replaced by the integer b , called a **key**. In other words, the numerical equivalent of each letter is shifted by b , thus yielding the following functions:

$$\begin{cases} \text{Encryption} \rightarrow f(p) = (p + b) \bmod 26 \\ \text{Decryption} \rightarrow f^{-1}(p) = (p - b) \bmod 26 \end{cases}$$

Example 11.1

Using the shift cipher with key $b = 7$, encrypt the message DESTROY ALL THE EVIDENCE.

Solution

The following steps, shown in Table 11.1, must be taken to encrypt the message:

- (i) Break the message DESTROY ALL THE EVIDENCE into a set of individual letters.
- (ii) Translate each letter to the corresponding number.
- (iii) Apply $f(p) = (p+7) \bmod 26$ to each number in part (ii).
- (iv) Translate the new set of numbers to get a set of encrypted letters.

The encrypted text is thus KLZAYVFHSSAOLLCPKLUJL.

Example 11.2

Using the shift cipher with key $b = 11$, decrypt the message LEELNVHTESH SLEJZFSLGP.

Solution

The following steps, shown in Table 11.2, must be taken to decrypt the message:

- (i) Break the message “LEELNVHTESH SLEJZFSLGP” into a set of individual letters.

Table 11.1 Steps in shift cipher for Example 11.1.

(i)	D	E	S	T	R	O	Y	A	L	L	T	H	E	E	V	I	D	E	N	C	E
(ii)	3	4	18	19	17	14	24	0	11	11	19	7	4	4	21	8	3	4	13	2	4
(iii)	10	11	25	0	24	21	5	7	18	18	0	14	11	11	2	15	10	11	20	9	11
(iv)	K	L	Z	A	Y	V	F	H	S	S	A	O	L	L	C	P	K	L	U	J	L

Table 11.2 Steps in shift cipher for Example 11.2.

(i)	L	E	E	L	N	V	H	T	E	S	H	S	L	E	J	Z	F	S	L	G	P
(ii)	11	4	4	11	13	21	7	19	4	18	7	18	11	4	9	25	5	18	11	6	15
(iii)	0	19	19	0	2	10	22	8	19	7	22	7	0	19	24	14	20	7	0	21	4
(iv)	A	T	T	A	C	K	W	I	T	H	W	H	A	T	Y	O	U	H	A	V	E

- (ii) Translate each letter to the corresponding number.
- (iii) Apply $f^{-1}(p) = (p - 11) \bmod 26$ to each number in part (ii).
- (iv) Translate the new set of numbers to get a set of decrypted letters.

The decrypted text is thus ATTACK WITH WHAT YOU HAVE.

A generalization of the shift cipher, called the **affine cipher**, is when for the given alphabet size n , the encryption function is $f(p) = (mp + b) \bmod n$, where $0 \leq p \leq n - 1$, b , m , and n are all integers, and $\gcd(m, n) = 1$ to ensure $f(p)$ is a one-to-one correspondence. To decrypt a message using an affine cipher, we need to find p using $p \equiv (\bar{m}(f(p) - b)) \bmod n$, where $\bar{m}$ is an inverse of m modulo n , that is, $\bar{m}m \equiv 1 \pmod{n}$.

Example 11.3

Consider the affine cipher $f(p) = (11p + 4) \bmod 26$.

- (i) Encrypt the letter N.
- (ii) Decrypt the letter S.

Solution

- (a) We first translate the letter N to the corresponding number; we therefore have $p = 13$. We then apply $f(p) = (11p + 4) \bmod 26$ for $p = 13$ to obtain $f(13) = (11 \times 13 + 4) \bmod 26 = 17$. We then translate 17 to get the letter R, the encrypted letter of N.
 - (b) We first translate the letter S to the corresponding number, and therefore obtain $f(p) = 18$. With $m = 11$, we find $\bar{m} = 19$ as $\bar{m}m \equiv 1 \pmod{26}$. We thus have $p \equiv (19(18 - 4)) \bmod 26 \equiv (19)(14) \bmod 26 \equiv 266 \bmod 26 \equiv 6$. Having $p = 6$, we translate 6 to get back the letter G, the decrypted letter of S.
-

Both shift ciphers and affine ciphers replace a letter by another letter; hence they are called **monoalphabetic ciphers**. In a **polyalphabetic cipher**, each occurrence of a character may have a different substitute; for instance, T could be enciphered as P at the beginning or the end of the text but as M in the middle. Therefore each character in the ciphered message depends on both the corresponding original text character and its position in the message.

Monoalphabetic ciphers and even polyalphabetic ciphers are simple methods of encryption and easy to break, thus being very vulnerable to attacks. This vulnerability led the way to the introduction of block ciphers, which are significantly more effective methods of encryption. A **block cipher** breaks up the original text into fixed blocks of letters and then replaces blocks of letters by other blocks of letters using a one-to-one correspondence transformation. A type of block ciphers is the **transposition cipher**, in which the order of letters in a block of letters are rearranged (reordered) according to a fixed permutation rather than being substituted with other letters of the alphabet. In other

words, the letters of a block do not change, but instead they are just shuffled in a deterministic way to encrypt the block.

Example 11.4

Using the transposition cipher based on the permutation of the set $\{1, 2, 3\}$ with $1 \rightarrow 3$, $2 \rightarrow 1$, and $3 \rightarrow 2$, encrypt the message HELP IS COMING.

Solution

As the given set for the permutation consists of three integers, the plaintext message is then split into blocks of three letters, we thus need to encrypt HEL, PIS, COM, and ING. In order to encrypt each block based on the given mapping, the first letter replaces the third letter, the second letter replaces the first letter, and the third letter replaces the second letter. The encrypted message is thus ELH ISP OMC NGI.

11.2 Modern Cryptography

To encrypt a message, an encryption algorithm, an encryption key, and the plaintext are needed, and to decrypt a message, a decryption algorithm, a decryption key, and the ciphertext are required. The encryption and decryption algorithms are public (i.e., anyone can access them), but the keys are secret and thus need to be protected.

Number theory uniquely plays a pivotal role in modern cryptography. Cryptography has become increasingly complex and its applications more varied. The major requirements for a system employing cryptography are as follows:

- To provide an easy and inexpensive means of encryption and decryption to all authorized users in possession of the appropriate key.
- To ensure that the task of producing the plaintext without the key is made extremely difficult and time-consuming.

Relying on the processing power and speed of modern computers, original messages are no longer encoded in characters in a specified language, nor are they encoded one at a time. **Modern cryptography** operates on binary bit sequences and relies on publicly known algorithms for encoding the message. Secrecy is obtained through a secret key, which is used as the seed for the algorithms. In modern cryptography, encryption and decryption can be carried out rapidly using complicated functions that are designed to be resistant to attack. The computational difficulty of algorithms in conjunction with the fact that only the parties interested in secure communication possess the secret key makes it extremely difficult for anyone else to obtain the original information.

The underlying need for modern cryptography stems from the fact there are essential applications in today's world that require sensitive information to be fully protected. Some of the widely popular applications requiring cryptography are electronic and

mobile commerce transactions, email privacy, secure remote surveillance, file transfers of confidential data, secure e-voting, banking data, secure cloud computing, medical records, and secure remote access.

There are numerous threats that can arise in transmission and storage of data, the array of attacks is constantly widening, and network security is continually becoming more challenging. The notion of security is tied to computing power, as a coded message is only as safe as the amount of computing power needed to break it. In short, the goal is to make undecipherability by an adversary as difficult as possible. Protecting information in its storage and retrieval as well as in transactional and messaging services is always of paramount importance.

The primary reasons to make messages secure through cryptographic mechanisms are as follows:

- **Confidentiality:** ensuring the transmitted message containing confidential data is hidden from unauthorized parties.
- **Authentication:** verifying the communicating parties are those they claim to be.
- **Integrity:** confirming that the message content has not been tampered with.
- **Nonrepudiation:** not being able to deny the transmission between the two parties has taken place.

There are fundamentally two types of adversaries. *Passive adversaries* are a threat to confidentiality, as they do not interrupt, alter, or insert any data. *Active adversaries* additionally threaten integrity and authentication. In any event, potential adversaries may have powers and resources ranging from minimal to unlimited.

There are two broad categories of cryptography: *private-key cryptography*, also known as *secret-key cryptography* or *symmetric-key cryptography*, and *public-key cryptography*, also referred to as *asymmetric-key cryptography*. Public-key cryptography is growing, but private-key cryptography is more common. They often complement each other, as there are applications in which both public-key cryptography and private-key cryptography are used.

11.3 Private-Key Cryptography

Private-key cryptography is based on sharing secrecy by permuting or substituting characters in the plaintext. All classical ciphers with no exception fall into private-key cryptography. The private-key cryptography is often used for long messages, for they require less time to encrypt. In private-key cryptography, an n -bit block of plaintext is encrypted and an n -bit block of ciphertext is decrypted. If a message block has fewer than n bits, padding must be added to make it an n -bit block. The common values of n are 64, 128, 256, and 512 bits. Private-key cryptography uses the same k -bit key for both the encryption at the transmitter and the decryption at the receiver, as shown in Fig. 11.1.

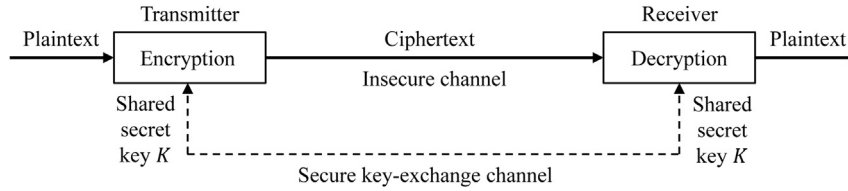


Fig. 11.1 Private-key Cryptography.

In private-key cryptography, once the key is known, both encryption and decryption can be carried out.

In private-key cryptography, the decryption algorithm is the inverse of the encryption algorithm, and the number of private keys for N users to communicate is $\frac{N(N-1)}{2}$, as each pair must have a unique private key. The number of keys grows quadratically, thus making these systems infeasible for larger-scale use. In private-key distribution, a trusted third party, referred to as a **key distribution center** (KDC), is used. In private-key cryptography, each user establishes a shared secret key with KDC. The secret keys, created by KDC, are used exclusively between KDC and the users and not among the users themselves. When a user wants to transmit secretly with another one, the transmitter then asks KDC for a session (temporary) secret key to be used between the two users. A session private key between two parties is used only once.

A widely known example of private-key cryptography is the **Data Encryption Standard** (DES), which has a block cipher structure. DES was developed in the 1970s, and for over 25 years, DES was used by the US government to protect binary data during transmission and storage in computer systems and by the banking industry and businesses to protect financial transactions for commercial data security. At the transmitter, a 64-bit plaintext is created into a 64-bit ciphertext, and at the receiver, a 64-bit cipher text is converted back to a 64-bit plaintext, noting that in DES, the same 56-bit key is used for both encryption and decryption. The key in fact consists of 64 bits. However, only 56 of these are actually used by the algorithm. Eight bits are used solely for error detection and are thereafter discarded. Despite its deprecation as an official standard, DES remains popular; it is used across a wide range of applications, including ATM encryption, email privacy, and secure remote access.

Another widely known example of private-key cryptography is the **Advanced Encryption Standard** (AES), which was established in 2001 as a replacement for DES. The highly complex structure of AES yields a high degree of protection against cryptanalysis. AES has a block size of 128 bits but with three different key lengths of 128, 192, and 256 bits. AES has been adopted by the US government and supersedes DES. AES is based on block ciphers and is efficient in both software and hardware.

11.4 Public-Key Cryptography

Public-key cryptography is based on personal secrecy rather than sharing secrecy. In public-key cryptography, the plaintext and ciphertext are numbers that are manipulated by mathematical functions. In public-key cryptography, a public key and a private key are used (see Fig. 11.2). It is a salient requirement that it must not be possible to determine the private key from the public key. In general, the public key is small, and the private key is large. A pair of keys can be used many times. The number of keys for N users to communicate is $2N$. The algorithm is complex and more efficient for short messages.

In public-key distribution, an organization, known as a **certification authority** (CA), is used. In public-key cryptography, public keys, like secret keys, need to be distributed securely; otherwise, the process can be subject to forgery. CA first checks the identification of a user, asks the user's public key, and writes it on the certificate. To prevent the certificate itself from being forged, CA signs the certificate with its own private key, which is difficult to be forged. The user uploads the signed certificate. Anyone who wants a user's public key downloads the user's signed certificate and then uses the CA's public key to obtain the user's public key.

Message authentication protects two communicating parties from any third party; it does not, however, protect the two parties against each other. In situations where something more than authentication is needed, the digital signature is the most attractive solution; in addition, it can also prevent denial and forgery. Public-key cryptography can be used to provide nonrepudiation by producing a digital signature. A **digital signature** uses a pair of private-public keys belonging to the sender to provide message integrity and message authentication. In short, a digital signature is reminiscent of an ordinary signature, as they both have the benefit of being easy to produce but difficult enough for anyone else to forge. A digital signature can be permanently tied to the content of the message being signed, and it cannot be moved then from one digital file to another, for any attempt will be detected.

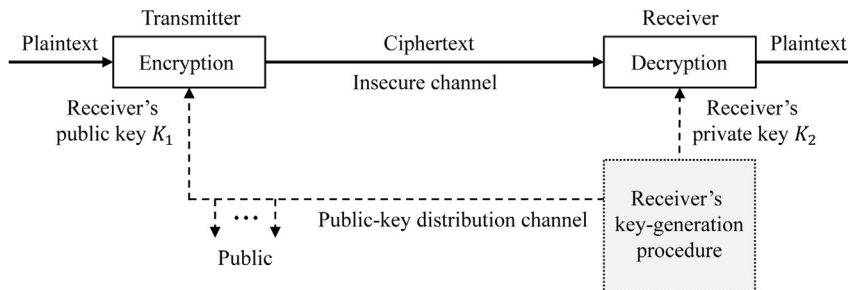


Fig. 11.2 Public-key Cryptography.

In a digital signature system, on the one hand, the messages are normally long, but on the other hand, we must use public-key cryptography systems that are very inefficient when dealing with long messages. The solution is to create a **digest** of a message through a hashing function, for instance, a checksum is produced that is much smaller than the message. Therefore the transmitter first produces a digest, then encrypts it using its own private key to produce the signature, and then sends the signature along with the message to the receiver. At the receiver, the signer's public key is applied to the signature to get the transmitted digest, and the digest is also directly determined from the message. If both digests are the same, then only the given transmitter could have issued the message and that the message has maintained its integrity.

It is important to highlight the distinction between how private and public keys are used in digital signature, vis-à-vis in cryptography for confidentiality. In digital signature, the signer (transmitter) signs the message digest with the signer's private key and the verifier (receiver) verifies with the signer's public key. In contrast, in cryptography, the public and private keys of the receiver are used in the process.

Another important application of public-key cryptography is the digital envelope. A **digital envelope** is a framework for data encryption, in which the data is encrypted under a secret key using a private-key cryptography, such as DES or AES, while this secret key is encrypted using a public-key cryptography such as RSA, and sent to the other party. In short, a public key cryptography can be used to distribute private keys to pairs of individuals wishing to communicate.

11.5 The RSA Cryptosystem

The RSA, named after the initials of its inventors, is the most widely used public-key cryptography for secure data transmission. Its effectiveness is based on the fact that very large prime numbers are fairly easy to produce on a computer, but it is enormously difficult (i.e., extremely time-consuming) to factor a product of two large unknown prime numbers. Digital envelopes and digital signatures are two important applications of RSA. However, these two security functions are mutually independent (i.e., neither, either, or both can be applied to a message). A digital envelope is the electronic equivalent of putting the message into a sealed envelope to provide privacy and prevent unauthorized alterations. A digital signature is the electronic equivalent of signing and sealing the letter. The digital envelope protects the digital signature.

The following steps show how the RSA keys can be generated:

- (i) Choose two very large prime numbers p and q at random, on the order of a couple of hundred digits each, often using probabilistic computer algorithms, and calculate $n = pq$. As the number of digits in n is approximately equal to the sum of digits in p and q , no computer currently can factor it in a reasonable length of time. Note that due to the nature of factoring algorithms, p and q need to be of similar size to keep

the RSA system secure. In addition, the large numbers are stored in binary form and generally 2048 to 4096 bits are needed for n to ensure a reasonably high degree of security.

- (ii) Compute $\varphi(n) = (p-1)(q-1)$, and choose an arbitrary integer e satisfying $1 < e < \varphi(n)$, which is relatively prime to $\varphi(n)$. In other words, $\gcd(e, \varphi(n)) = 1$. Although for some applications, such as making encryption faster on small devices like smart cards, it is desirable to have small values of e , it is best not to choose a small value for e , as the secrecy of the cipher may then be compromised.
- (iii) Find the positive integer d , an inverse of e modulo $\varphi(n)$, that is, find an integer d such that $ed \equiv 1 \pmod{\varphi(n)}$. Note that as $\gcd(e, \varphi(n)) = 1$, we have $de + c\varphi(n) = 1$, where the integers c and d can be found using the extended Euclidean algorithm, with the condition that $0 < d < \varphi(n)$.

The **public key** is $\{n, e\}$, which is widely distributed, and thus anyone with the public key can encrypt a message to send. The **private key** is $\{n, d\}$, where the security of the system depends on d being very difficult to calculate if only n and e are known. Because d is not publicly available, only someone in possession of that value can correctly decrypt the message.

The correctness of the RSA cryptosystem follows from the elementary number theory, in particular from Euler's theorem. The RSA cryptosystem is a block cipher and the following steps reflect how to encrypt using the public key and decrypt using the private key:

- (i) Translate each letter in the plaintext message M into a two-digit number because the RSA cipher works only on numbers while noting that A is translated into 00, B is translated into 01, ..., and Z is translated into 25.
- (ii) Concatenate the two-digit numbers into a sequence of digits representing the plaintext message, and then divide the sequence of digits into the largest possible equally sized blocks of even number of digits. Note that a block of digits is represented by m , where $0 < m < n$, and $\gcd(m, n) = 1$.
- (iii) Pad the plaintext message with a number of random characters at the beginning and the end of the message to foil some potential code breaking attacks (if needed) or if a block is not full, additional characters need to be filled in to make the last block the same size as all other blocks or to ensure $\gcd(m, n) = 1$.
- (iv) Determine the ciphertext C block by block using $c = m^e \bmod n$, which is the encryption of m in the RSA cryptosystem.
- (v) Determine the plaintext M block by block using $m = c^d \bmod n$, which is the decryption of c in the RSA cryptosystem.

Example 11.5

Assuming $p = 101$, $q = 103$, and the message is PASSION. Determine the blocks of integers that are encrypted using the RSA cryptography.

Solution

We have $n = pq = 101 \times 103 = 10,403$. The translation of the seven letters in PASSION into their numerical equivalents is 15001818081413. We now need to divide this sequence of fourteen digits into the largest possible equally sized blocks of even number of digits, where each block is less than 10,403. This results in blocks of four digits, as a block of six digits is greater than 10,403. Therefore the sequence of 14 digits are groups into 4 blocks of 4 digits, where we have padded the end of the sequence, say, with 24, so as to make the sequence into 16 digits, a multiple of 4. The four blocks of integers to be encrypted block by block are thus as follows: 1500 1818 0814 1324.

Example 11.6

Show how the message 19 can be encrypted using the RSA cryptography by the sender and how accordingly the encrypted message can be decrypted by the receiver.

Solution

Suppose the sender arbitrarily chooses the two prime numbers $p = 83$ and $q = 53$ and thus has $n = pq = 83 \times 53 = 4399$ and $\varphi(n) = (p-1)(q-1) = 82 \times 52 = 4264$. The sender then chooses an arbitrary $e = 23$, which is relatively prime to 4264, because we have $\gcd(4264, 23) = 1$. Therefore $(4399, 23)$ is a valid public key. The encrypted message using fast modular multiplication is then as follows: $c = m^e \bmod n = 19^{23} \bmod 4399 = 2556$.

The valid private key is thus $(4399, 927)$, which the receiver possesses. Note that $d = 927$, as it is an inverse of e modulo $\varphi(n) = 23$ modulo 4264 while noting that $de + c\varphi(n) = 23d + 4264c = 1$. The decrypted message using fast modular multiplication is then as follows: $m = c^d \bmod n = 2556^{927} \bmod 4399 = 19$.

Example 11.7

Suppose in an RSA cryptosystem, we have $p = 23$ and $q = 31$. Encrypt $M = 572$ to get C and then decrypt C to get M back.

Solution

$$\text{Given } \begin{cases} p = 23 \\ q = 31 \end{cases} \rightarrow n = pq = 713 \rightarrow \varphi(n) = (p-1)(q-1) = 660.$$

$$\text{Having } \begin{cases} e < \varphi(n) \\ \gcd(e, \varphi(n)) = 1 \end{cases} \rightarrow \begin{array}{l} \text{Choosing } e = 29 \\ \text{as an arbitrary choice,} \\ \text{while meeting both requirements.} \end{array}$$

$$\text{Having } \begin{cases} d < \varphi(n) \\ de \equiv 1 \pmod{\varphi(n)} \end{cases} \rightarrow \text{Using the Euclidean algorithm} \rightarrow d = 569.$$

$$\text{Having } \begin{cases} \text{Public key: } \{713, 29\} \\ \text{Private key: } \{713, 569\} \end{cases} \rightarrow \text{Obtaining } \begin{cases} C = 572^{29} \bmod 713 = 113 \\ M = 113^{569} \bmod 713 = 572 \end{cases}$$

Note that by replacing each exponent by its binary expansion and then using the modular exponentiation algorithm, C and M were calculated.

Example 11.8

Suppose in an RSA cryptosystem, we have $p = 53$ and $q = 61$. Encrypt $M = 1717$ to get C and then decrypt C to get M back.

Solution

$$\text{Given } \begin{cases} p = 53 \\ q = 61 \end{cases} \rightarrow n = pq = 3233 \rightarrow \varphi(n) = (p-1)(q-1) = 3120.$$

$$\text{Having } \begin{cases} e < \varphi(n) \\ \gcd(e, \varphi(n)) = 1 \end{cases} \rightarrow \begin{array}{l} \text{Choosing } e = 17 \\ \text{as an arbitrary choice,} \\ \text{while meeting both requirements.} \end{array}$$

$$\text{Having } \begin{cases} d < \varphi(n) \\ de \equiv 1 \pmod{\varphi(n)} \end{cases} \rightarrow \text{Using the Euclidean algorithm} \rightarrow d = 2753.$$

$$\text{Having } \left\{ \begin{array}{l} \text{Public key: } \{3233, 17\} \\ \text{Private key: } \{3233, 2753\} \end{array} \right. \rightarrow \text{Obtaining } \left\{ \begin{array}{l} C = 1717^{17} \bmod 3233 = 2460 \\ M = 2460^{2753} \bmod 3233 = 1717 \end{array} \right.$$

Note that by replacing each exponent by its binary expansion and then using the modular exponentiation algorithm, C and M were calculated.

Exercises

(11.1)

Encrypt HELLO using the shift cipher with $b = 15$.

(11.2)

Encrypt the message BEWARE OF MARTIANS using the transposition cipher with blocks of four letters, and the permutation $1 \rightarrow 3$, $2 \rightarrow 1$, $3 \rightarrow 4$, and $4 \rightarrow 2$.

(11.3)

Propose a method to decrypt a ciphertext message if a transposition cipher was used.

(11.4)

Suppose the alphabet in a language consists of n letters. Assuming the shift cipher is employed, determine a key b for which the enciphering function and deciphering function are the same.

(11.5)

Determine an inverse of 43 modulo 660, that is, find an integer s such that $43s \equiv 1 \pmod{660}$.

(11.6)

Show why the RSA cryptography works, that is, for the cyphertext C and plaintext M we have

$$C = M^e \bmod n \rightarrow M = C^d \bmod n.$$

(11.7)

In a trivial, certainly unrealistic, example of the RSA cryptosystem, we have $p = 3$ and $q = 13$. Encrypt 20.

(11.8)

Suppose in an RSA cryptosystem, we select two prime numbers $p = 17$ and $q = 11$. After determining a private key and a public key, determine the encryption of 88 and show how 88 can be obtained back from the encrypted number.

(11.9)

Suppose in an RSA cryptosystem, we select two prime numbers $p = 59$, $q = 43$, and $e = 13$. Assuming the encrypted message is 0667 1947 0671, determine the original message.

(11.10)

Show that in the RSA cryptography, when $n = pq$, with p and q being primes, and $\phi(n) = (p-1)(q-1)$ are both known, we can easily factor n to find p and q .
