

Cryptography: The Science and Art of Secure Communications

by
Ahmet Eskicioglu and Louis Litwin

WHY DO WE NEED CRYPTOGRAPHY?

The desire to transmit messages securely is not new. For centuries, people have had a desire for keeping their communications private. Two examples that immediately come to mind are letters to a secret lover and military correspondence¹. Although there has been a need for secure communications for hundreds of years, recent technological and social developments have resulted in a drastic increase in both the number of applications requiring secure communications and the level of security required. Today, modern digital communications systems, particularly those related to the Internet, are being used to carry vast amounts of sensitive data. Sending credit card information to a website in an e-commerce transaction or exchanging confidential trade secrets by email are typical examples.

The field of *cryptography* deals with the techniques for conveying information securely. The goal of a secure communications system is to allow the intended recipients of a message to receive the message properly while preventing eavesdroppers from understanding the message. The message in its original form is called *plaintext*. The transmitter in a secure system will encrypt the plaintext in order to hide its meaning. This reversible mathematical process produces an encrypted output called *ciphertext*. The algorithm used to encrypt the message is a *cipher*. *Cryptanalysis* is the science of breaking ciphers, and *cryptanalysts* try to defeat the security of cryptographic systems.

A ciphertext can be transmitted openly across a communications channel. Because of the encrypted nature of the ciphertext, eavesdroppers who may have access to the ciphertext will ideally be unable to uncover the meaning of the message. Only the intended recipient can decrypt the message to recover the plaintext for interpretation. The above processes are shown in Figure 1.

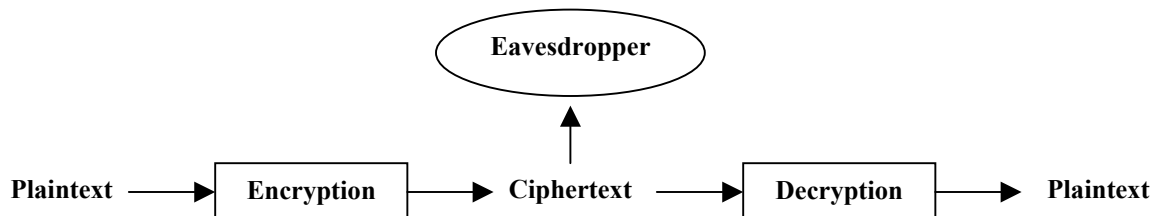


Figure 1: Block diagram of a cryptographic system.

¹ The question of which example requires greater secrecy will be left as an exercise for the reader!

CLASSIFICATION OF CIPHERS

Ciphers can be classified using several criteria. According to one criterion, two important types of ciphers exist: symmetric key and asymmetric key.

Symmetric Key (Secret Key) Ciphers

In symmetric key ciphers, the same key is used for both encryption and decryption. A major problem with such a system is that the sender and receiver must have knowledge of the key prior to transmission. This requirement makes such a system difficult to use in practice. The key cannot be openly transmitted since that would compromise the security of the system. One possibility is for the two parties to meet and exchange the keys prior to transmitting their messages. However, this exchange becomes difficult when many parties are involved in a communications network.

Asymmetric Key (Public Key) Ciphers

An asymmetric key cipher uses different keys for encryption and decryption. These two keys are mathematically related, but it is very difficult to obtain one from the other. The key used for encryption is called the public key and the key used for decryption is called the private key. The public key can be made available without compromising the security of the system. The corresponding private key, however, must not be revealed to any party.

CLASSICAL CIPHERS

We will start with the classical ciphers. Developed and used prior to the Computer Age, these ciphers are not secure against the present techniques of cryptanalysis. They are included for their historical importance and educational value.

Statistics of English Language Text

A plaintext message written in English (or any other language) has certain statistical characteristics. The letter *E* is the most frequent in the English language. The next most frequent is *T*, followed by *O*, *A*, *N*, *I*, *R*, *S*, *H*, and so on with *Z* being the least frequent. All ciphers modify the plaintext in order to change its statistics. A cipher is considered to be “weak” if it generates ciphertext that still contains significant statistical information about the original plaintext. Cryptanalysis of classical ciphers is made possible because of the redundancy in the linguistic structure of natural languages.

Simple (Monoalphabetic) Substitution Ciphers

Simple substitution ciphers replace each letter in the plaintext with another letter in order to form the ciphertext. This class of ciphers is easy to implement and use. Nevertheless, they are not difficult to break, and thus do not offer much security. An eavesdropper can decrypt a ciphertext by performing frequency analysis on the letters in the ciphertext. Because of the substitution, the letter frequencies will be different than the frequencies for normal English text. The eavesdropper can still exploit this frequency information in order

to break the cipher. If, for example, *Z* is the most frequent letter in the ciphertext, then it was probably substituted in for *E*. The next most frequent letter in the ciphertext may correspond to a *T* or an *O*, and so on. By trial and error, the entire plaintext message can be revealed. Simple substitution ciphers are also called monoalphabetic substitution ciphers because they define a mapping from the plaintext alphabet to a ciphertext alphabet.

Although simple substitution ciphers by themselves are not actually used in modern encryption systems, powerful modern ciphers use the operation of substitution in combination with other operations (transposition, Boolean algebra, modular arithmetic, etc.). This is a very important design criterion that results in an algorithm more secure than each of the components.

Caesar Cipher

A simple substitution cipher of historical interest is the Caesar cipher. The cipher gets its name because Julius Caesar (100 B.C. – 44 B.C.) used it to send secret messages. The ciphertext is formed by replacing each letter in the plaintext by the letter three positions to the right in the alphabet. This shift is performed modulo 26. Thus, the plaintext letter *A* becomes *D*, *B* becomes *E*, and *Z* becomes *C*. Breaking this cipher is a trivial task as the statistical information of the plaintext is contained in the ciphertext with the exception that the letter frequencies are also shifted to the right by three. Instead of *E* being the most frequent letter, the letter *H* will be the most frequent in the ciphertext. Frequency analysis quickly reveals that the Caesar cipher is being used, and it is a simple matter to replace the ciphertext letters in order to uncover the plaintext message.

The amount of the shift $K = 3$ is defined to be the key for the Caesar cipher. Shifts by an amount other than three can also be used, but there are only 25 possible shifts for the English alphabet, and it is easy to try all possible combinations if necessary.

An Example of the Caesar Cipher

The example in Table 1 is an application of the Caesar cipher. The most frequent letters in the ciphertext are simply shifted versions of the most frequent letters in the plaintext. Because the cipher fails to significantly alter the statistical properties of the message, an eavesdropper can easily uncover the plaintext from the ciphertext.

	Message	Five Most Frequent Letters
Plaintext	THISISACAESARCIPHER	S, I, A, R, H
Ciphertext	WKLVLVDFDHVDUFLSKHU	V, L, D, U, K

Table 1: Example of the Caesar cipher.

The ciphertext alphabet used in the Caesar cipher is very orderly since it is only a shifted version of the plaintext alphabet. Some simple substitution ciphers use a scrambled alphabet that has no apparent order. These ciphers are slightly harder to break than the Caesar cipher because there is not such an obvious pattern to the ciphertext alphabet. For example, *A* might be substituted with *Q*, *B* with *D*, and *C* with *R*. The letters in the English

alphabet can be rearranged in $26!$ (over 4×10^{26}) different ways, allowing for a large number of possible ciphertext alphabets. It would, of course, take a significantly long time to try all possible combinations. However, all simple substitution ciphers can be easily broken by using frequency analysis.

Polyalphabetic Substitution Ciphers

Polyalphabetic substitution ciphers use multiple alphabets to conceal the single letter frequency distribution of the plaintext letters in the ciphertext. In its simplest form, they are based on a period d that determines the number of the alphabets. Using the alphabets sequentially results in a given plaintext character being encrypted to different ciphertext characters. For a monoalphabetic cipher, d is equal to 1.

Example of a Polyalphabetic Substitution Cipher

The simple Vigenère cipher is representative of polyalphabetic substitution ciphers with a period. The letter k_i in the key $K = k_1 \dots k_d$ determines the amount of shift in the i th alphabet. The application in Table 2 shows the repeated use of the encryption keyword *CODE*. For example, the first letter of the ciphertext is obtained by shifting the plaintext letter *P* by two positions where *C* represents a right shift of two.

Plaintext	POLY ALPH ABET IC
Key Sequence	CODE CODE CODE CO
Ciphertext	RCOC CZSL CPHX KQ

Table 2: Example of a simple Vigenère cipher.

Periodic substitution ciphers can be cryptanalyzed in two steps. First, the period d is estimated. The Kasiski method and the Index of Coincidence are two useful tools for this purpose. The work is then reduced to the cryptanalysis of a set of monoalphabetic substitution ciphers.

Transposition Ciphers

Transposition ciphers are a different family of ciphers for which frequency analysis does not provide any useful information about the plaintext. In fact, transposition ciphers produce ciphertext that has the exact same letter frequencies as the original plaintext. The reason is that they work by rearranging, or transposing, the letters in the plaintext. Thus the ciphertext contains the same letters as the plaintext, but the order of the letters will be changed. A common method of transposition is to insert the plaintext into a matrix in some known way (e.g., by inserting the text by rows), and forming the ciphertext by reading the letters out in another known way (e.g., by reading out the columns). This information determines the key for the cipher. More complicated transposition ciphers can be formed by building upon this basic idea.

An Example of a Transposition Cipher

The example in Table 3 is for an application of a transposition cipher. The cipher uses the transposition matrix shown in Table 4. Note that the frequency analysis gives the same results for both the plaintext and the ciphertext.

	Message	Five Most Frequent Letters
Plaintext	ATranspositionCipher	I, T, S, R, P
Ciphertext	ANSOPTSINHRPTCEAOIIR	I, T, S, R, P

Table 3: Example of a transposition cipher.

The ciphertext in this example was formed by writing the plaintext into the rows of a 5x4 matrix, and then reading the text out by columns.

A	T	R	A
N	S	P	O
S	I	T	I
O	N	C	I
P	H	E	R

Table 4: Matrix used to create transposed ciphertext.

Transposition ciphers can be broken by restoring the original order of the letters. Column and row rearrangements, and frequency distributions of digrams (two-letter sequences) and trigrams (three-letter sequences) are commonly used in cryptanalysis of transposition ciphers.

MODERN CIPHERS

With the proliferation of high-speed digital computing machines, classical ciphers have become inadequate for providing information security. After World War II, a need emerged for a stronger cipher that could be used for non-military applications. Modern ciphers have been designed as an attempt to resist cryptanalytic attacks which use the huge processing and storage capabilities of today's computer systems.

The Data Encryption Standard (DES)

The Data Encryption Standard (DES), the well-known symmetric key cipher, was developed as a result of the efforts initiated by the National Security Agency (NSA). In their public request for proposals, where a set of design criteria was specified, the NSA argued that the security of the algorithm must reside in the key. In 1977, DES was adopted as a federal standard for use in commercial and unclassified U.S. government applications. In later years, both hardware and software implementations became widely available, and were used in many sectors of industry, including banking.

DES is a product cipher, i.e., it is a composition of substitutions and transpositions. Like all other modern ciphers, the algorithm is published in full detail. There are two major

arguments for not keeping a cryptographic algorithm secret: (1) It is very difficult to keep the algorithm secret, especially if it is to be used in a standard. (2) Publication leads to open discussions and cryptanalysis to evaluate the real strengths and weaknesses.

DES operates on 64-bit blocks of plaintext to produce 64-bit ciphertext blocks. The length of the encryption key is 56 bits. Since DES is a symmetric cipher, this key is also used for decryption. DES keys are generated as 64-bit numbers, but in each key every eighth bit is used for error (parity) checking.

A summary of the DES algorithm is shown in

Figure 2. The output of the Initial Permutation (IP) is divided into two 32-bit halves L_0 and R_0 . After 16 “rounds” of identical operations, the inverse permutation IP^{-1} gives the ciphertext. The subkeys

K_1, K_2, \dots, K_{16} are derived from the 56-bit encryption key. A combination of substitution and transposition operations define the function f .

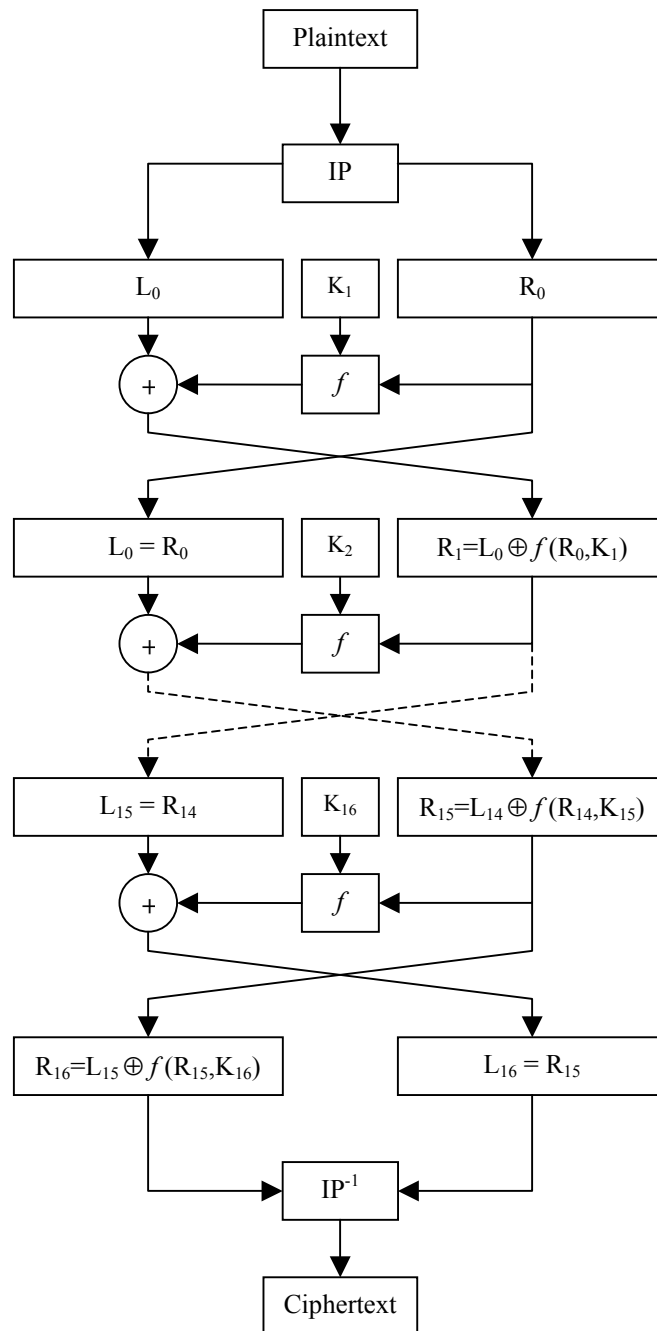


Figure 2: DES encryption.

The length of the DES key and some other design aspects have been the subject of a lot of controversy. After more than 20 years of use, the original key length is no longer sufficient if high security is needed. Several DES variations have been proposed to increase the robustness of the algorithm. One popular implementation is triple DES (TDES) which uses three different keys (Figure 3).

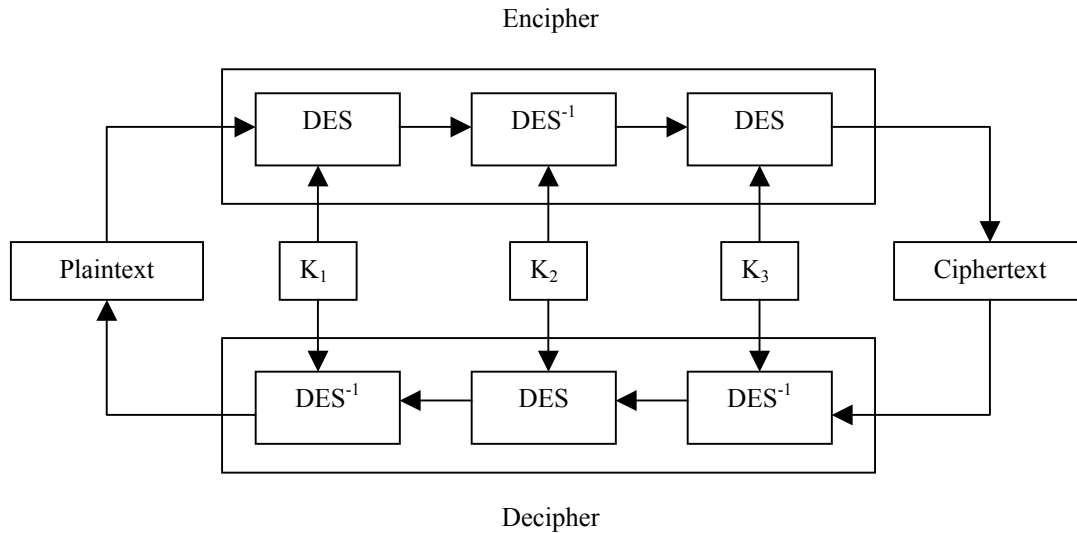


Figure 3: Triple-DES encryption and decryption.

There is a recent collaborative effort to develop a new algorithm, Advanced Encryption Standard (AES), to replace DES. The National Institute of Standards and Technology (NIST) has been working with industry and cryptology experts to develop a Federal Information Processing Standard (FIPS). It is expected that the standard, which is needed by the U.S. Government, will be completed by the summer of 2001. The AES candidate algorithms that are under public review are MARS, RC6, Rijndael, Serpent, and Twofish.

One-Time Pads

As surprising as it seems, an encryption scheme that is perfectly secure actually exists (at least in theory!). It is known as a one-time pad. The scheme gets its name from a pad that is used only once. The pad consists of a non-repeating random sequence of letters with a length equal to the plaintext length. Both the sender and the receiver will have a copy of the pad. Encryption works by adding each letter of the plaintext with the next letter on the pad. This addition is performed modulo 26 (so that the result is also a letter in the alphabet). The decryption process is just the reverse, and is performed by adding the letters of the ciphertext with the letters on the pad modulo 26. If the pad is generated in a truly random fashion, the cipher cannot be broken as there is no pattern or statistics to exploit. Each letter of the alphabet has an equal probability of occurring in the ciphertext. The scheme is very cumbersome to implement. The pad can only be used once, and thus it needs to be replaced frequently. One-time pads are best suited for sending low bit rate data that requires absolute security.

KEY AGREEMENT

As mentioned earlier, the strength of a modern cipher lies in its key, since the algorithm itself is typically published and thus well-known. Because of the importance of cipher key secrecy, key management is one of the most critical issues in secure communications. A number of schemes have been developed to allow the communicating parties to establish a shared key. They are based either on symmetric or public key ciphers.

Diffie-Hellman Public Key Exchange Algorithm

Diffie and Hellman developed the first practical key exchange algorithm. Two parties, Alice and Bob, agree on numbers g and n which satisfy certain mathematical conditions. These numbers do not need to be kept secret and can be posted publicly.

1. Alice randomly selects a large number x as her private key, and sends Bob her public key $X = g^x \bmod n$.
2. Bob randomly selects a large number y as his private key, and sends Alice his public key $Y = g^y \bmod n$.
3. Alice computes $k_A = Y^x \bmod n$.
4. Bob computes $k_B = X^y \bmod n$.

Note that $k_A = (g^y)^x \bmod n$ and $k_B = (g^x)^y \bmod n$. Thus, $k_A = k_B = g^{xy} \bmod n$, and this value becomes the shared key that will be used to encrypt and decrypt the message. Although g , n , X and Y are publicly available, it is very difficult to determine the private keys x and y based on these values.

An Example of the Diffie-Hellman Algorithm

Small numbers will be used to keep the example simple. In real life, much larger numbers are used to provide a greater level of security.

Assume that Alice and Bob publicly agree to use $g = 5$ and $n = 11$. Alice chooses her private key to be $x = 3$ and Bob chooses his private key to be $y = 4$. These numbers are kept private. The two parties compute their shared keys as follows. Alice computes

$$X = g^x \bmod n = 5^3 \bmod 11 = 125 \bmod 11 = 4$$

and Bob computes

$$Y = g^y \bmod n = 5^4 \bmod 11 = 625 \bmod 11 = 9$$

These values are then transmitted openly. Based on the received value, Alice computes the shared key as

$$k_A = Y^x \bmod n = 9^3 \bmod 11 = 729 \bmod 11 = 3$$

and Bob computes the shared key as

$$k_B = X^y \bmod n = 4^4 \bmod 11 = 256 \bmod 11 = 3$$

This algorithm has allowed the two parties to decide on a key value that is known only to them. Eavesdroppers will know the values of g , n , X , and Y , but it will be difficult for them to determine the shared key value.

CONCLUSIONS

This article provided the reader with a basic introduction to the field of cryptography. Descriptions and examples of simple ciphers were used to present the concept of substitution and transposition. These operations form the building blocks for powerful modern ciphers such as DES. The interested reader can learn more about this fascinating subject by starting with the references listed below.

ACKNOWLEDGEMENTS

The authors would like to acknowledge their two favorite cryptographers: Julius Caesar and Secret Agent #98470982.

READ MORE ABOUT IT

- D. Denning, *Cryptography and Data Security*, Addison-Wesley Publishing Company, 1983.
- B. Schneier, *Applied Cryptography*, John Wiley & Sons, Inc., 1996.
- A. J. Menezes, P. C. Van Oorschot, and S. A. Van Stone, *Handbook of Applied Cryptography*, CRC Press, 1997.
- AES Website: <http://csrc.nist.gov/encryption/aes/>

ABOUT THE AUTHORS

Ahmet M. Eskicioglu received the B.S. degree from the Middle East Technical University, Ankara, Turkey, and the M.S. and Ph.D. degrees from the University of Manchester Institute of Science and Technology (UMIST), England. Dr. Eskicioglu is a Principal Member Technical Staff with Thomson Multimedia Corporate Research, and is working on conditional access and copy protection projects. He has participated in the development of several national and international standards, including the Advanced Television Systems Committee (ATSC) conditional access system, the Electronics Industries Alliance (EIA) National Renewable Security Standard (NRSS) and the Content Scramble System (CSS) for DVD players. His interests include text, image and video compression, system simulation, data security and conditional access.

Louis Litwin is a Member Technical Staff with Thomson Multimedia Corporate Research where he is working on wireless digital home networking technology. Mr. Litwin received his M.S. degree in Electrical Engineering from Purdue University in 1999, and his B.S. degree in Electrical Engineering with distinction from Drexel University in 1997. He was named by Eta Kappa Nu as the Alton B. Zerby and Carl T. Koerner Outstanding Electrical Engineering Student for 1997. His professional interests include digital communications with a particular focus on adaptive equalization and error control coding. For fun, he likes to SLKUWNSUOUA while wearing QEOMDNEY and drinking LXUOUEME.