CYBERTECH PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-pub.com
ITB15190

This paper appears in the publication, **Cryptography and Security Services: Mechanisms and Applications**
authored by **M. Mogollon © 2008, IGI Global**

Chapter I

Classic Cryptography

Classic Cryptography

Chapters 1 and 2 cover information on classic cryptography and the aspects of information security related to security services and mechanisms. The history of cryptography and code-breaking is very interesting and, in this chapter, some of the types of implementation employed over the centuries to attempt to code information are covered. These implementations are not very sophisticated by today's standards and are considered too weak for serious applications. Some early crypto machines and the Vernam Cipher developed by Gilbert Vernam in 1917 are discussed in this chapter.

Objectives

- Gain an historical perspective of cryptography
- Become familiar with terms used in cryptography and network security

Introduction

The purpose of cryptography is to render information unintelligible to all but the intended receiver. The sender enciphers a message into unintelligible form, and the receiver deciphers it into intelligible form. The word "cryptology" is derived from the Greek ***kryptos*** (hidden) and ***logos*** (word) (*The American Heritage College Dictionary*, 1987).

- **Cryptology:** The scientific study of cryptography and cryptanalysis
- **Cryptography:** The enciphering and deciphering of messages into secret codes by means of various transformations of the plaintext
- **Cryptanalysis:** The process of deriving the plaintext from the ciphertext (breaking a code) without being in possession of the key or the system (code breaking)

The history of codes and ciphers goes back almost 4,000 years to a time during the early Egyptian civilization when scribes told the story of their masters' lives using unusual hieroglyphics (Khan, 1976, p. 71). The inscriptions were not secret writing, but incorporated one of the essential elements of cryptography: an intentional transformation of writing so that only certain people could read it.

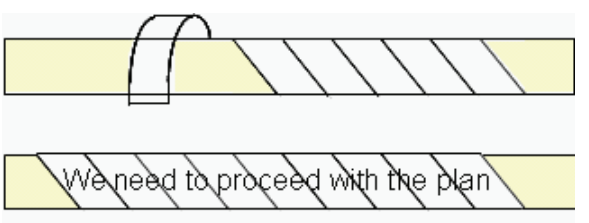
The Spartans were probably the first to use cryptography for military purposes. Their crypto device, called the *scytale* (stick), consisted of a wooden stick around which a narrow piece of papyrus, leather, or parchment was wrapped in a spiral. The secret message was inscribed on the parchment over the whole length of the shaft, and the ribbon was then sent to its destination. The ribbon alone was useless to all but the recipient, who had a cylinder of the same diameter as the sender. The diameter of the cylinder determined the key.

The Arab civilization, with its advanced mathematics, was the first to establish specific rules to cryptoanalyze written messages (Khan, 1976, p. 97). The rules were the following:

- The cryptanalyst must know the language in which the crypto message is written and its linguistic characteristics.
- In every language, there are letters that are never found together in one word, letters that rarely come together in a word, and combinations of letters that are not possible.
- All letters are not used equally in any language, and the proportions in which the letters occur remain constant.

Unfortunately, with the decline of the Arab civilization, this knowledge of cryptology also vanished.

Figure 1-1. The Spartan Scytale



Classic Cipher Techniques

Many of the techniques employed over the centuries to attempt to **code** information were not very sophisticated. By today's standards, most of these techniques are considered too weak for serious applications; however, many of their basic principles are still used in modern cryptography and, therefore, it is worthwhile to review them.

These techniques include the following (Davies & Price, 1984, pp. 17-35):

- The Caesar substitution cipher
- Monoalphabetic substitution
- Polyalphabetic substitution (the Vigenere cipher)
- Transposition ciphers

Caesar Substitution Cipher

In his book, *The Gallic Wars*, Julius Caesar described the use of a military code in which a plaintext alphabet is shifted by three positions (Khan, 1976, p. 84).

Plain a b c d e f g h i j k l m n o p q r s t u v w x y z

Cipher d e f g h i j k l m n o p q r s t u v w x y z a b c

This type of code, called a *Caesar substitution cipher*, is very weak because if the amount of displacement is known, there is no secret. Even if the displacement is not known, it can be discovered very easily because the number of possible cipher solutions is only 25.

Monoalphabetic Substitution

If the substitution of each letter is done at random, the cipher technique is called a *monoalphabetic substitution*.

Plain a b c d e f g h i j k l m n o p q r s t u v w x y z

Cipher h o s b r g v k w c y f p j t a z m x i q d l u e n

The number of possible substitutions is 26! or 4.0329×10^{26}. With so many substitutions, monoalphabetic substitution might appear as a very strong cipher technique but, in reality, it is a very weak cipher. Cryptanalysis of a message enciphered using a monoalphabetic substitution takes into consideration that each plain letter is always transformed into the same encipher equivalent, and that in any language there are some letters that occur more often than others.

Polyalphabetic Substitution

In the 16th century, the Frenchman Blaise de Vigenere wrote the book, *Traite des Chiffres*, which described cryptology up to his day, and introduced a polyalphabetic substitution using one alphabet for each of the plain letters. Using Caesar's basic idea, he formed a square, the Vigenere Table, consisting of 25 horizontal alphabets, one below the other, with each shifted to the right by one letter. A vertical alphabet was used to define the key and, at the top, an additional alphabet was used for the plaintext letters (Khan, 1976, p. 149).

The Vigenere encryption could also be expressed as a modulo-26 addition of the letters of the key word, repeated as many times as necessary into the plaintext.

The Vigenere Tableau

(Plain Text)

	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A	a b c d e f g h i j k l m n o p q r s t u v w x y z
B	b c d e f g h i j k l m n o p q r s t u v w x y z a
C	c d e f g h i j k l m n o p q r s t u v w x y z a b
D	d e f g h i j k l m n o p q r s t u v w x y z a b c
E	e f g h i j k l m n o p q r s t u v w x y z a b c d
F	f g h i j k l m n o p q r s t u v w x y z a b c d e
G	g h i j k l m n o p q r s t u v w x y z a b c d e f
H	h i j k l m n o p q r s t u v w x y z a b c d e f g
I	i j k l m n o p q r s t u v w x y z a b c d e f g h
J	j k l m n o p q r s t u v w x y z a b c d e f g h i
K	k l m n o p q r s t u v w x y z a b c d e f g h i j
L	l m n o p q r s t u v w x y z a b c d e f g h i j k
M	m n o p q r s t u v w x y z a b c d e f g h i j k l
N	n o p q r s t u v w x y z a b c d e f g h i j k l m
O	o p q r s t u v w x y z a b c d e f g h i j k l m n
P	p q r s t u v w x y z a b c d e f g h i j k l m n o
Q	q r s t u v w x y z a b c d e f g h i j k l m n o p
R	r s t u v w x y z a b c d e f g h i j k l m n o p q
S	s t u v w x y z a b c d e f g h i j k l m n o p q r
T	t u v w x y z a b c d e f g h i j k l m n o p q r s
U	u v w x y z a b c d e f g h i j k l m n o p q r s t
V	v w x y z a b c d e f g h i j k l m n o p q r s t u
W	w x y z a b c d e f g h i j k l m n o p q r s t u v

X x y z a b c d e f g h i j k l m n o p q r s t u v w
Y y z a b c d e f g h i j k l m n o p q r s t u v w x
Z z a b c d e f g h i j k l m n o p q r s t u v w x y

In his book, Vigenere listed several key methods, such as words, phrases, and the progressive use of all the alphabets, as well as a running key in which the message itself is its own key —the so-called *autokey*.

All the possible keys can be grouped into three systems:

1. A key word or key phrase is used, thus defining not only the key length (key period), but also the number of alphabets being used.

   Example:

   Key D A L L A S D A L L A S
   Plain N O W I S T H E T I M E
   Cipher Q O H T S L K E E T M W

2. A primary key consisting of a single letter is provided to encipher the first plaintext letter, and the plaintext is then used as a running key.

   Example:

   Key D N O W I S T H E T I M
   Plain N O W I S T H E T I M E
   Cipher Q B K E A L A L X B U Q

3. As in (2), the prime letter is used to encipher the first plaintext letter, but the ciphertext is used as a running key.

   Example:

   Key D Q E A I A T A E X F R
   Plain N O W I S T H E T I M E
   Cipher Q E A I A T A E X F R V

It becomes apparent that example 1 uses only four alphabets (A and L are repeated), while B and C use all 26 alphabets, assuming that all 26 letters of the alphabet occur in the plaintext or in the cryptogram respectively.

Transposition Ciphers

With transposition ciphers, the successive letters of the plaintext are arranged according to the key. The key is a group of sequential numbers arranged at random. The plaintext is separated into groups of letters in which each group has the same number of letters as the number chosen as a key.

Plaintext	n o w i s / t h e t i / m e f o r / a l l x x /
Key	5 1 3 4 2
	s n w i o
	i t e t h
	r m f o e
	x a l x l
Ciphertext	s n w i o i t e t h r m f o e x a l x l

Early Cipher Machines

In the end, encryption without a cipher machine was too complex, the enciphering and deciphering processes were too slow, and the risk of making a mistake too high.

At the beginning of the 18th century, cryptographers started using mechanical aids to encipher information. The following were some of the most famous cipher devices used (Davies & Price, 1984, pp. 17-25):

- The Saint-Cyr Slide
- The Jefferson Cylinder
- The Wheatstone Disk
- The Vernam Cipher
- The Enigma (the rotor machine used by the German forces in World War II)
- The M-209 (used by the U.S. Army until the early 1950s)

The Saint-Cyr Slide

The construction, compilation, and use of complete enciphered tables in the polyalphabetic cipher system were inconvenient. This problem disappeared with a device called the *Saint-Cyr Slide*, invented by Kerckhoffs and named after the French military academy (Khan, 1976, p. 238). With this device, the process of modulo-26 addition could be conducted conveniently.

The Jefferson Cylinder

In the 1790's, Thomas Jefferson developed a device for polyalphabetic substitution that consisted of 36 discs or cylinders with their peripheries divided into 26 equal parts (Khan, 1976, pp. 192-195). Each of the discs was numbered and carried in its peripheral an alphabet with the letters placed, not alphabetically, but randomly. The discs were mounted on a shaft,

Figure 1-2. The Saint Cyr Slide

and the order was specified and agreed to between the correspondents. The discs' order constituted the key, and the number of possibilities was 36! or 3.72×10^{41}.

The message was enciphered by rotating the discs until the message letters stood in the same row. The ciphertext was any of the other 26 positions around the cylinder in which the letters appeared jumbled and meaningless. To decipher the message, the correspondent set the discs in the same specified order and rotated them to present a row with the same ciphertext; the correspondent then moved the wheel cipher device around until a meaningful row of letters was found.

The Wheatstone Disc

In the 19th century, the British scientist Sir Charles Wheatstone (Khan, 1976, p. 197) invented another famous cipher machine. The Wheatstone cryptograph machine consisted of two concentric discs that carried the letters of the alphabet in their peripheries. The outer disc contained the letters of the alphabet in alphabetic order, plus a symbol for a blank space after the letter **z**, while the inner disc had 26 letters at random. Over the discs, two clock-like hands were geared together in some way, so that when the larger hand completed one revolution, the smaller hand would move ahead only one letter. For enciphering, the two hands were first aligned at the blank space on the outer circle; then the outer hand was used to spell out the plaintext (always moving clockwise and including the space as a character), while the shorter hand automatically selected the cipher text equivalent from the inner disc. Whenever a double letter occurred, some unused letter (for example, q or x) was substituted for the repeated letter.

This cipher is a type of polyalphabetic substitution with a change of alphabet after each word because of the blank space. The variation in length of the alphabets means that as the larger hand is completing a revolution, the smaller is already one letter into its second revolution. This cipher has the property that the ciphertext representing a word depends on the preceding plaintext. This is called *chaining* and has great importance in today's applications.

The Vernam Cipher

In 1917, Gilbert Vernam (Kahn, 1976, pp. 94-97), an employee of AT&T, designed a security device for telegraphic communications that revolutionized modern cryptography: the bit-by-bit combination of random characters (keystream) with characters of plaintext using modulo-2 addition (the XOR function) —the *stream cipher*. Vernam's system, based upon

the Baudot code, required punching a tape of random characters (chosen by picking numbers out of a hat) and electronically adding them to the plaintext characters.

A new tape, the ciphertext, was thus produced in a simple and reversible operation; all that was necessary to obtain the message was to subtract the ciphertext pulses from the keystream pulses.

Vernam decided to use the Baudot code pulses for his electronic addition so that if both pulses were mark or space, the result was space; if one was mark and the other was pulse, the result was mark. The four possibilities were the following:

Plaintext		**Keystream**		**Ciphertext**
Mark	+	Mark	=	Space
Space	+	Space	=	Space
Mark	+	Space	=	Mark
Space	+	Mark	=	Mark

The addition can be better visualized if, instead of using the Baudot code of mark and space, the mark is represented by a 1 and a space by a 0.

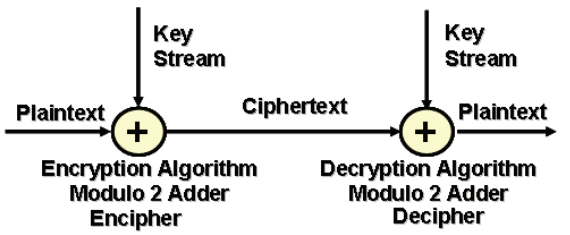
Plaintext		**Keystream**		**Ciphertext**
1	+	1	=	0
0	+	0	=	0
1	+	0	=	1
0	+	1	=	1

In accordance with this rule, and since in the Baudot code each character had five pulses, either a mark (pulse) or a space (no pulse), Vernam combined five pulses from the keystream with five pulses from the plaintext to obtain the ciphertext. For example:

Encipher		
Plaintext	1 1 0 0 0 (letter A)	1 1 0 0 0 (letter A)
Keystream	1 0 1 0 1	1 1 0 0 1
Ciphertext	0 1 1 0 1 (letter P)	0 0 0 0 1 (letter T)

Decipher		
Ciphertext	0 1 1 0 1 (letter P)	0 0 0 0 1 (letter T)
Keystream	1 0 1 0 1	1 1 0 0 1
Plaintext	1 1 0 0 0 (letter A)	1 1 0 0 0 (letter A)

Figure 1-3. Vernam's cipher



Vernam's addition, the modulo-2 (XOR), together with the use of the same keystream to encipher and decipher, are the basis of modern cryptography. Thanks to his contribution, enciphering and deciphering a message was made easy, simple, and fast.

Vernam's cipher required the sender to provide the receiver with identical tapes of keystream characters. Vernam's keystream consisted of a loop of tape with the alphabet on it, which was used over and over until the complete message was enciphered. The system was a polyalphabetic substitution, a 32 x 32 table, which permitted a Kasiski solution. To increase the difficulty of a Kasiski solution, which is the conjunction of a repeated portion of the key with a repetition in the plaintext producing a repetition of the ciphertext, the group of AT&T engineers working with Vernam at first made the keystream tapes extremely long. These tapes were difficult to handle, and they later decided to combine two short keystream tapes of different lengths to generate a longer number of keystream characters. For example, if one loop tape of 1000 keystream characters were combined with a keystream loop tape of 999 characters, the result would provide 999,000 combinations before the sequence would repeat.

If the keystream tapes are different for each message, and if each keystream tape is used only one time to encipher one message, then the cipher is perfect and unbreakable. Because of the randomness and the nonrepetition of the keystream, this system is called the *one-time system*.

The Rotor Crypto Machines

Rotor machines implemented polyalphabetic substitution ciphers with long periods (Davies & Price, 1984, p. 31; Kahn, 1976, p. 411; Way, 1977, p. 89). The body of the machine consisted of several *t* rotary discs made of insulated material, normally two to four inches in diameter, and half an inch thick. On each side of each disc were 26 electrical contacts in the form of metal studs. Each stud on one side of the disc was connected by wire to another stud on the other side of the disc. The wire did not go directly from one stud to the immediate opposite stud, but to a stud at random. For example, the stud from the letter *G* was connected internally not to *G*, but to another letter.

If the discs were immovable, an alphabet could be changed only to another alphabet. However, if after each letter were enciphered, one or more of the rotors were rotated one step, a new alphabet would be created to encipher each letter with a different ciphertext alphabet.

A machine with *t* rotors would not return to its starting position until after 26^t successive steps; a three-rotor machine would go through $26^3 = 17{,}576$ different alphabets before repeating itself; a five-rotor machine has a period of $26^5 = 11{,}881{,}376$ different alphabets before repeating itself.

After World War I, four men, all from different countries, independently created a crypto machine based on the wired code wheel, the rotor. The inventor of the first rotor machine in the United States was Edward Hugh Herbert who, in the 1920's, founded the Herbert Electric Code, the first cipher machine company in the U.S. By 1923, the firm had closed after selling only 12 machines (Kahn, 1976, p. 415).

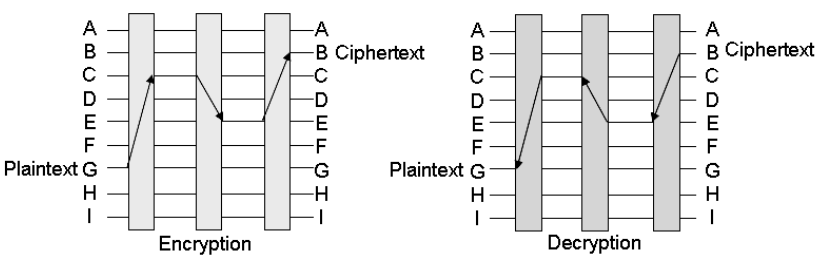
In the Netherlands, Hugo Alexander Koch filed a patent for a secret writing machine and established a company called *Securitas*, but no machines were ever produced. In 1927, Kock transferred the patent rights to the German inventor of a rotor device (Kahn, 1976, p. 420).

In Germany, Arthur Scherbious designed a device with multiple switchboards. These boards connected each arriving lead with one of the outgoing leads and were adapted to make this connection with great facility and variation (Kahn, 1976, p. 421). This operation was the basis of a rotor machine. The first apparatus, which had only 10 contacts, was used to encipher code numbers into code words. In subsequent machines, Scherbious expanded the contacts from 10 to 26, so the machine could be used to encipher letters. He called his machine *Enigma*. Scherbious formed a company called *Cipher Machine Corporation*, which started operating in 1923. His advertisement, "One secret, well protected, may pay the whole cost of the machine ...," did not convince either commercial or military customers. The company survived 11 years before its dissolution and never paid a dividend. Scherbious went bankrupt and died prior to World War II before Germany decided to adopt the machine. When Hitler started rearming Germany, his cryptology experts chose the Enigma as the crypto machine for top army, navy, and air force communications.

These early inventors tried to commercialize their crypto machines too soon. Nations during the 1920's, after World War I, were not interested in crypto devices. In the 1930's, when European countries were rearming for World War II, the interest in crypto machines was renewed. At that time, Boris Caesar Wilhelm Hagelin, the only person who became a multimillionaire from the cipher machine business, was able to capitalize on the need for secure communications.

In 1916, Arvid Gerhard Damm founded in Stockholm a company called *Cryptograph, Inc.*, with money invested by Emanuel Nobel, nephew of Alfred Nobel, and K. W. Hagelin, man-

Figure 1-4. Rotor machine



ager of the Nobel brothers' oil production in Russia. In October 1919, Damm applied for a patent for a rotor crypto machine (Kahn, 1976, p. 422). During the following years, Damm designed several crypto machines based on the rotor concept and even won some orders for a prototype, but the machines were not reliable, and he was not able to establish a market. In 1922, Boris Caesar Wilhelm Hagelin started to work in the factory to represent his father's and Emanuel Nobel's investments. With his degree in mechanical engineering, Hagelin had the technical background to enable him to modify and simplify the Damm mechanism; he was also able to get a large contract from the Swedish Army in 1926.

After Damm's death in 1927, Hagelin bought the company at a very good price and fulfilled the contract with the Swedish Army. By 1934, Hagelin had designed a more compact crypto machine, which was probably the first of its kind to print ciphertext in five-letter groups and the plaintext in normal word-lengths. In 1935, after witnessing a successful demonstration, the French government placed an order for 5,000 units. When World War II began, Hagelin packed blueprints and two dismantled ciphering machines and headed for the United States. The U.S Army, after exhaustive tests, adopted the crypto machine for medium-level cryptographic communications from divisions to battalions, and more than 140,000 units were manufactured by L.C. Smith & Corona Typewriters Inc. The Army's designation of Hagelin's crypto machine was the M-209 (Kahn, 1976, pp. 425-427).

The M-209

The M-209 was used by the U.S. Army until the early 1950's. A full description of the M-109 is given by Beker and Piper (1982).

The M-209 had six rotors, but not all the rotors had the complete alphabet. The following sequences of letters were engraved around the rotors' circumference:

Rotor	I	or	"26 wheel":	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Rotor	II	or	"25 wheel":	ABCDEFGHIJKLMNOPQRSTUVXYZ
Rotor	III	or	"23 wheel":	ABCDEFGHIJKLMNOPQRSTUVX
Rotor	IV	or	"21 wheel":	ABCDEFGHIJKLMNOPQRSTU
Rotor	V	or	"19 wheel":	ABCDEFGHIJKLMNOPQRS
Rotor	VI	or	"17 wheel":	ABCDEFGHIJKLMNOPQ

The numbers 26, 25, 23, 21, 19, and 17 do not have common factors, so the rotors produced the following individual periods: 26 25, 23, 21, 19, and 17. Therefore, the ciphertext that the M-209 produced was polyalphabetic with a period of 26 x 25 x 23 x 21 x 19 x 17 = 101,405,850, nearly ten times greater than a five-rotor machine.

Cryptanalysis in World War II

The rotor machines used by Germany and Japan generated long keystreams, but they were not as random as they may have seemed. In August 1939, one month before World War II started, the British, with the help of some Polish ex-employees of the German factory that manufactured the Enigma, had somehow obtained a working replica of the machine. Getting the machine was only the first step, however; solving the mathematical computations involved was more difficult.

The head of the British Government's Codes and Cipher School, Alastair Denniston, hired the best mathematicians in Britain to work with him on a project called *ULTRA*, whose objective was to break the German Enigma machine. By early April 1940, Denniston and his personnel, using probably the first electronic computational machine, were able to decipher a short message from the Luftwaffe. During the rest of the war, the British were able to decipher all German messages. Churchill referred to ULTRA as "my most secret source."

In 1934, the Imperial Japanese Navy purchased several German Enigma machines. After making some modifications to the machine, they introduced it in 1937 with the name, *Alphabetic Typewriter 2597* (2597 was the Japanese year which corresponded to 1937). The *J machine*, as it was called by the Japanese Navy, was lent to the Foreign Office for its use. There it was adopted for the highest level, State Secret, diplomatic communications.

In the United States, this machine was called *PURPLE*, according to the color progression established by two previous Japanese codes, ORANGE and RED, which the Americans had solved (Way, 1977, p. 68). The task to break the PURPLE code was assigned directly to William Frederick Friedman, Chief Cryptanalyst of Signal Intelligence Service (S.I.S.). He and his team of codebreakers were able to put together a complicated maze of multicolored wires, contacts, switches, and relays, a perfect clone of the Japanese cipher machine. On September 25, 1940 (Bamford, 1982, p. 35), this replica issued its first totally clear, ungarbled text of a message from a PURPLE machine.

The British had an Enigma working model when they broke the German codes, but the Americans duplicated the PURPLE machine sight-unseen. Later on, the Americans were able to find out that the keys the Japanese were using were not random but did indeed have a special order, a terrible mistake in any crypto organization. The S.I.S found out that the keys used in a period of ten days were related, so after breaking the key used the first day, they were able to predict the keys for the next nine days. **They found the key to the keys!** Inexplicably, the Americans were able to break the highest level of messages from Japan, but sometimes they were not able to break low-level crypto messages.

Summary

The Saint-Cry Slide, the Jefferson Cylinder, the Wheatstone Disk, and the rotor machines, Enigma and M-209, used substitution and transposition techniques, which are still used in modern cryptography. However, the way these techniques were originally implemented made the encryption algorithms very vulnerable when today's computer power was utilized.

The number of possible substitutions in a monoalphabetic substitution is 26! or 4.0329 x 10^{26}, but, in reality, it is a very weak cipher technique because each plain letter is always transformed into the same encipher equivalent.

Rotor machines are based on substitution. A letter in one of the rotors is substituted for another letter in the following rotor. The technique is excellent; the only problem is that it is necessary to select many rotors and to make the rotors step in an unpredictable way. Today, some crypto companies are implementing rotors in electronic form by using an S-Box for each of the rotors. See Chapter 4 for more on the S-Box.

The one-time pad Vernam cipher is still used in ultra-secret communications for short messages. Furthermore, the XOR cipher algorithm used by Vernam, also called *modulo-2 addition*, is the most used cipher algorithm today.

In several places in this book, comparisons are made between encryption algorithms in order to make a determination about which one is more secure or more robust. If two encryption algorithms use the same techniques, it doesn't mean that both have the same ability to resist an attack or have the same cipher strength.

When talking about the strength of an encryption algorithm and to determine the minimum effort needed to break a crypto system, it is necessary to take into consideration the following:

- The cryptanalyst's processing capabilities
- The cryptanalyst's ability to find a weakness, that is, a fault in the design that allows circumventing the algorithm security
- Number of possible key combinations

A secure encryption algorithm is one in which it is not possible to use a short-cut attack because there is no fault in the design, and the only possible way of breaking the crypto algorithm is by brute force, trying all possible keys. If key exhaustion is the best attack, then the strength of an encryption algorithm is determined by its key size.

Learning Objectives Review

1. Cryptography is the art or science of rendering plaintext unintelligible and converting encrypted messages into intelligible form. (T/F)
2. The Calsar substitution cipher is very weak because there are only 25 different substitutions. (T/F)
3. The monoalphabetic cipher system has 4 x 1026 possible substitutions; therefore, it is a very strong cipher technique. (T/F)
4. The security of the Vernam cipher is based on its keystream randomness. (T/F)
5. A perfect cipher (unbreakable) is a cipher system in which:
   a. The cipher stream is random

b. The keystream is used to encipher only one message

c. A and B

6. Make a histogram that shows the relative frequencies of alphabetic characters in the English language for one, two, and three letters

References

Bamford, J. (1982). *The puzzle palace: A report on NSA America's most secret agency*. Boston: Houghton, Mifflin Co.

Beker, H., & Piper, F. (1982) *Cipher system, the protection of communications*. New York: John Wiley and Sons.

Davies, D. W., & Price, W. L. (1984). *Security for computer networks*. New York: John Wiley & Sons.

Khan, D. (1976). *The codebreakers*. New York: Macmillan Publishing Co., Inc.

The American heritage college dictionary (3rd ed.). (n.d.). Boston: Houghton Mifflin Company.

Way, P. (1977). *The encyclopedia of espionage codes and ciphers*. London: The Danbury Press.