Power	40 Bit	56 Bit	64 Bit	128 Bit
Individual	1.4 Min	73 Days	50 Years	10^{20} Year
Corporate	2 Sec	35 Hours	1 Year	10^{19} Year
Government	0.2 Sec	3.5 Hours	37 Days	10^{18} Year

Table 1-1 Times to Break a Key of a Given Length on Different Types of Hardware

Looking at Table 1-1 and 1-2, it would seem that a longer key would automatically equal a greater amount of protection, and in many cases this is true. However, there are tradeoffs in the name of performance. A longer key generally equates to longer encrypt and decrypt times. Additionally, the old axiom that says "more is better" is proven wrong here in relation to key length and protection. In fact, the length of the key will only result in a stronger algorithm up to a point, and anything after that will slowly plateau and result in the aforementioned increased processing time.

One more factor that enhances the effectiveness and security of a key is a technique known as a *cryptoperiod,* the objective of which is to define the specific period of time a cryptographic key may be used before it is pulled from usage in favor of a new key. The cryptoperiod, when used as intended, dictates that after a defined period has expired, the key is no longer to be used to encrypt or decrypt any information, and will either be relegated to an archive or discarded altogether.

When a cryptoperiod is in use, the actual timeframe for key usage is defined by a myriad of factors, dependent on the organization itself. Factors that can impact the time a

Key Length	Value
40	Of no use to companies and governments; effective at stopping casual attackers.
56	Used for privacy. Vulnerable and has been broken. DES is the best example of a broken 56-bit encryption scheme.
64	Considered safe, but still is vulnerable and has been broken.
128	Considered generally unbreakable, but some newer technologies and implementations have been vulnerable.
256	Impossible to break with today's technology.

Table 1-2 Subjective Values of Each Key Length

In Actual Practice

Key lengths may also be impacted by export laws that fall outside the scope of the cryptographer—and the scope of this book for that matter. When we discuss key lengths and export laws, we'll refer to the United States and the laws that were in place for a period of time. In the United States the laws that were in play for a while absolutely forbad the export of any encryption technology that exceeded 40 bits in length. Anyone who chose to run afoul of this would quickly find themselves in trouble with the U.S. government and in the same category as those who would export weapons technology to foreign powers. Although these laws were intended to prevent the technology from getting into the hands of hostile powers, it also impacted, tremendously, the flow of strong encryption technology outside the U.S. Although such controls still exist, they have been substantially relaxed, and the export of stronger encryption is allowed more than it was before—but restrictions still exist.

key is valid are key compromises of any type, cost of replacing a key to include decrypting and re-encrypting with a new key and business requirements. Factors that effect the cryptoperiod include incidents such as the loss of a key or other types of compromise.

Putting It All Together

Now that you know the key players and terms, let's put everything together to form a complete picture of the encryption/decryption process. First, it is important to clearly understand what is needed prior to the encryption or decryption process occurring.

In the case of encryption, here's what's needed:

- **Plaintext** In other words, you need to have the information on hand that you are going to put through the encryption process.
- **Encryption algorithm** This is the mechanism that will perform that actual encryption process and is responsible for being the "mechanism" that transforms the information.
- **Key** The item responsible for setting the specific options or configuration, if you will, of the mechanism at a specific point in time.

In the case of decryption, here's what's needed:

- **Ciphertext** This is the previously encrypted information that needs to be manipulated to once again reveal its original contents.
- **Decryption algorithm** This is a mechanism capable of reversing the encryption process, allowing the original information to be viewed, provided the right key is used.
- **Key** This is the item responsible for configuring the decryption process to allow the ciphertext to be viewed.

Note

The key is not any random key—it must be the corresponding key or the same key used to encrypt the data in the first place. If a random key or incorrect key is used, the result will be information that is not useful.

Let's now look at the encryption process again. Let's say that, hypothetically, Link wants to send Zelda another message. Knowing what you know now, the process would look like what's shown in Figure 1-6.

In Figure 1-6, the original message would be represented by the plaintext being fed into the algorithm as input. Together with the plaintext into the algorithm is a key selected out of the keyspace defined by the algorithm in use. Along with the plaintext and algorithm, a key is also selected after which they are combined to produce ciphertext.

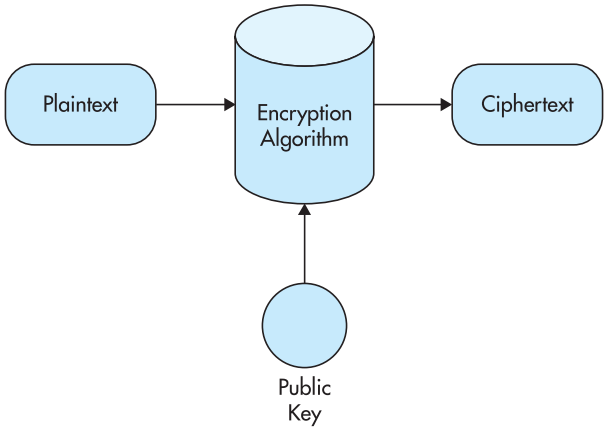

Figure 1-6 Encryption process using a key

Note

In Figure 1-6, the keyspace looks like it is separate from the algorithm when in fact it is defined by the algorithm, and the user is free to choose whatever key they wish from the keyspace. In the diagram, the two (the keyspace and algorithm) are illustrated separately to make things a little clearer to visualize.

So the encryption process is simple; nothing that we haven't seen before or discussed. Let's look at the decryption process, as defined in Figure 1-7.

In Figure 1-7, the decryption process is shown, which is simply a reverse of the encryption process, but with a little tweak here and there. First, if we assume that the message from Figure 1-6 is being decrypted here, then it means that Zelda received the message from Link and had the instructions (the algorithm) and the combination (the key) provided to reverse the encryption operation. Because Zelda already would know the key as provided by Link, she doesn't have to worry about selecting a new one; in fact, a new key wouldn't help. All Zelda needs is the ciphertext, the key, and the algorithm to begin the process.

Both encryption and decryption, as defined in Figures 1-6 and 1-7, are simple and effective, but they are only a small part of the process. In fact, the process shown here only covers symmetric, as the same key is used to encrypt and decrypt. What about asymmetric encryption? Let's look at that process as well.

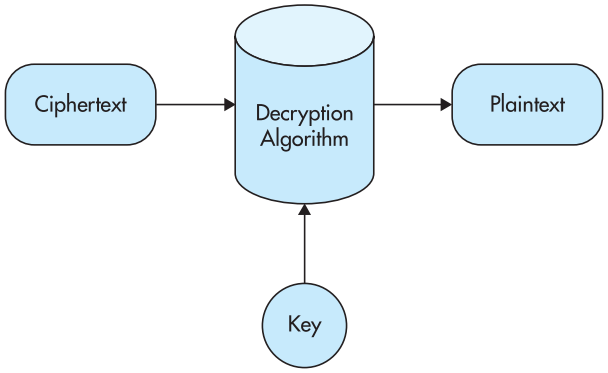

Figure 1-7 The decryption process

Note

In this opening chapter, we will only discuss the basic functioning of asymmetric encryption just to set the stage for later discussions. If the details seems a little confusing, don't worry. We will clear this up later—just note the differences between the two types, symmetric and asymmetric, right now.

In asymmetric encryption, the process changes just a little because two keys exist that cannot be used to encrypt and decrypt the same piece of information. With this in mind, let's look at the process a little more closely to understand how this works.

Suppose Link and Zelda wish to exchange information once again. This time, Link wants to send information to Zelda that only she can view. With symmetric encryption algorithms, this is trickier because Link not only has to encrypt the information, but he also has to send the encrypted data to Zelda along with the key used to decrypt. This presents some interesting problems because Link must now figure out a way to get both to Zelda without the key being compromised. This is where asymmetric encryption comes in. In Figure 1-8, you see how asymmetric encryption works.

Note

Further explanation of asymmetric encryption will come in later chapters; however, just remember from our previous explanation that the "public" key is readily available and not a secret part of the process.

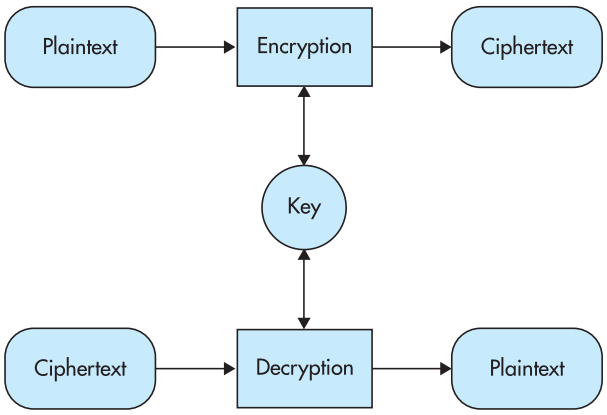

Figure 1-8 The encryption process using asymmetric methods. Note the public key.

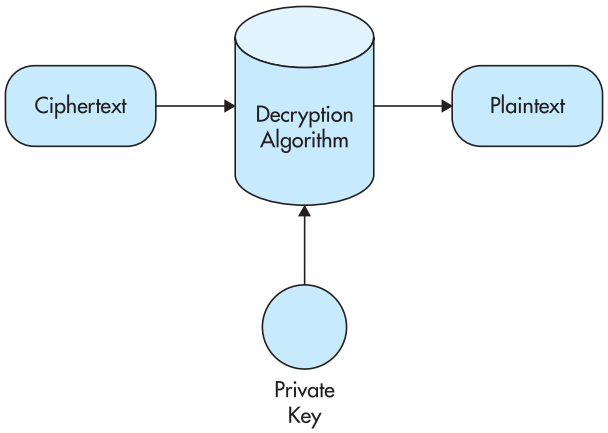

Figure 1-9 The decryption process in an asymmetric system. Note the private key.

Of course, every encryption process must have a decryption process (see Figure 1-9).

Asymmetric decryption is simple in concept. However, keep in mind that the private key is a critical and sensitive piece of this process. You will realize just how important when we dig deeper into the nuts and bolts of this methodology.

As you can see, two different encryption methods can be used to protect the secrecy of information. Both of these methods will be discussed more in depth later in the book.

We've Covered

Fundamentals of cryptography

- Cryptography is used to secure the integrity and confidentiality of information.
- Cryptography is the science of protecting information in all its forms from prying eyes and unauthorized modification.
- Cryptography is applied in everything from cell phones to hard drives.

Key concepts in cryptography

- Keys are used to determine the settings used for a particular encryption or decryption sequence.
- Algorithms are formulas used to determine the mechanism of encryption and decryption.
- Plaintext is information that has not been encrypted.
- Ciphertext is information after an encryption sequence has been performed.

Key terms and terminology

- Asymmetric cryptography is a cryptographic process which uses a public and private key.
- Symmetric cryptography is a cryptographic process which uses a single key for encryption and decryption.
- Hashing is also known as one way encryption that creates a message digest.
- Legal issues prevent particular applications and export of cryptosystems.

CHAPTER 2

History of Cryptography

We'll Cover

- History of cryptography
- Cryptography in the ancient world
- Modern cryptography
- Future directions for cryptography
- Historical users of cryptography

Cryptography is the body of knowledge that relates to the safeguarding of information either by keeping it secret or by keeping unwanted changes from being detected. Contrary to what many think, the art has been around for a very long time and has evolved much over the years, moving from a curiosity to a science that is in found in many aspects of technology. Although it may never be known exactly when the art appeared, it is almost assuredly sometime after man learned to write down information that the need to conceal a meaning arose. Since the time the science came on the scene, changes have been made to how it's done, and the mechanisms have advanced to a high degree.

The science of cryptography provides unique abilities not attainable otherwise or as easily. Crypto provides three key fundamental functions: confidentiality, integrity, and non-repudiation. *Confidentiality* is the concept of safeguarding data or information from any unauthorized outside party viewing or accessing it in any way. In addition, *integrity* is provided through a mathematically complex and intensive mechanism known as *hashing*. Finally, *non-repudiation* is also provided by the art of cryptography and gives us the ability to prevent a party from denying their part in initiating an activity.

LINGO
Hashing is a process that converts a message or input into a fixed-length encrypted string of information typically in an alphanumeric format. The length of a hash will always be the same no matter what the input may happen to be, although the actual characters in the hash will be different.

For most, cryptography is an unknown and is something that is the stuff of secret agents, spies, puzzles, and games and mentioned in areas such as national security matters. Heck, most of the public would not understand the role that cryptography plays in their

lives when they perform online banking or store their health records online, for example. Consider for a moment the individual who writes a letter to his friend; this individual puts the letter in an envelope then drops it in a mailbox. This individual typically considers the envelope all the protection he needs, but does not think of the fact that someone may be able to see the letter through the envelope or even go through the extra step of replacing the letter with one of their own. Although this may seem far fetched with a traditional letter, such things are possible with the new generation of e-mail. The general public usually doesn't think about possible security problems with e-mail and that there may be many mechanisms at work behind the scenes to keep their messages private and confidential in cyberspace.

Cryptography Overview

Let's start with a brief overview of what cryptography is offering us as users and readers of this text. Simply put, the goal of cryptography is to preserve confidentiality, integrity, and non-repudiation by performing each individually or in combination. When applied with the appropriate skill and knowledge, cryptography provides levels of protection that would be near impossible to achieve using other basic methodologies. Confidentiality is the ability to protect information from unauthorized disclosure; information is prevented from being viewed by those not authorized to view it, which is the primary function of encryption. In addition, integrity is provided through the cryptographic mechanism known as hashing, which employs a robust mechanism for allowing detection of changes to the information's original form. Finally, non-repudiation is provided via the science of cryptography and enables the prevention of the sending party denying the origin of the information in question. Through the application of cryptographic protocols, information can be protected both in transit and in storage.

IMHO

I think it is always helpful to consider one of the cornerstones of security when talking about cryptography, which is the CIA triad. CIA refers to Confidentiality, Integrity, and Availability, which are the three central areas in security. Although cryptography only indirectly supports availability, it deals heavily with the other two components—and non-repudiation as well. Using these elements as a set of guideposts—for they apply to cryptography—helps me (and hopefully you) focus on the true impact of cryptography on you and your data.

Note

You may be picking up this text because you are a security professional or just because you are interested in the topic. For those who are professionals in the security field, understanding how cryptography works is essential to being able to properly carry out your job. Although you do not need to know all the nuts and bolts that may exist under the hood, the basic functions and how they are applied are important. If you are one of those who are just interested in the field, you will find an exploration of the topic stimulating and perhaps exciting and intriguing.

What Is Cryptography?

Let's put a finer point on what cryptography is and what it does for us before we move on to how it has evolved. Cryptography is the science and practice of safeguarding information through the use of special tools, techniques, and other methods. This has evolved over time, as you will soon see, to not only describe how information is changed from one form to another but also how to create new systems and defeat existing ones. In fact, the field of cryptography has broadened substantially through necessity and has continued to increase in complexity, covering older traditional methods and the new high-technology digital methods and systems.

Encryption is what gets the most attention and may be considered the nice "romantic" technology that everyone thinks about when they hear the word *cryptography.* Encryption is the heavyweight of cryptographic processes in terms of frequency of use, but it is not the only one. Within the field are numerous technologies and protocols that work to keep information secret as well as detect possible modifications to the original data.

This study, cryptanalysis, has been used almost as long as encryption and cryptography itself, largely due to the fact that whenever something has been written in code by one party there have been other parties trying to find out hidden secrets. The ability to break these codes is known as *cryptanalysis* and is a hot issue for every government as well as those seeking protected information because it allows secrets to be uncovered.

Early cultures have shown us some of the fundamentals of cryptography, but not everything that we need to know. So what is cryptography anyway? Well, when the science and art is carefully applied, it is extremely useful and is an effective tool in protecting all sorts of information from compromise. Cryptography can keep information secret through the careful and thoughtful application of seemingly simple techniques that together form more than the sum of the individual parts. Such systems can be designed to be relatively simple or can quickly evolve into the complex variety based on what is being protected. Some simple and ancient applications include the protection of information

such as hunting routes and messages to the gods, as the Egyptians did. Other more current applications are more complex and involved, such as those used to protect credit card information, e-mail, and other similar types of information.

As with the Egyptians, one of the most widely used applications of cryptography is in the safeguarding of communications between two parties wanting to share information. Guaranteeing that information is kept secret is one thing, but in the modern world it is only part of the equation. In today's world, information must be kept secret, and provisions to detect unwelcome or unwanted modifications are just as important. In the days of Julius Caesar and the Spartans, keeping information secret was not as challenging a task as it is today and in fact was substantially difficult. In the days of yore, keeping a message secret could be as simple as writing it in a language the general public didn't understand or was unlikely to understand. Later forms of encryption required that elaborate systems of management and security be implemented in order to safeguard information.

Is the body of knowledge relating to cryptography only concerned with protecting information? Well, for the first few generations of its existence the answer was yes, but that has changed with the knowledge being used in systems such as those for authenticating individuals and validating that someone who sent a message or initiated an action is indeed the right party.

The knowledge contained in the field has even made some of the everyday technologies you use possible. In fact, one area that owes its existence to cryptography is e-commerce. The practice has reaped tremendous benefits from the field, allowing for the secure exchange of financial information as well as preventing exposure of and authenticating access to that information. In fact, the case could be made that e-commerce would not exist in anything resembling its current form without the backing of cryptographic science.

Now you may be tempted to think of cryptography as operating strictly within the domain of computing, but this is simply not true. It is used in many other areas very different from what the Egyptians, Greeks, and others had ever even thought of. One area that has benefited tremendously is that of cell phones and mobile technologies. The evolution and advancement of cryptographic science and its processes in these fields has led to a number of threats being thwarted, such as the cloning of devices and the decrease of identity theft. Specific to cloning, mobile technology has implemented increasingly advanced cryptographic measures to prevent malicious duplication of a device, the potential for running up thousands of dollars in fraudulent charges, and eavesdropping on another party.

So what are the key concentrations of cryptography? We've touched on a few of them already, but there are more you should be aware of. There exists the possibility for this knowledge to be applied in any one or more of five areas, including those relating to confidentiality, integrity, authentication, non-repudiation, and key distribution. Each of these benefits is something that must be understood to put the tools and techniques in their proper context. Some additional protections and usage are

- A prominent role of authentication can be found within the actual authentication process used to log in to most systems and services. Authentication has become commonplace in many of our normal, daily activities. Consider the information used to authenticate and validate a credential such as an ATM card or a computer login at work. Our PINs and passwords must be kept absolutely secret and protected to prevent inadvertent disclosure to unauthorized parties. Another fundamental example of cryptography's role in authentication is in the hashing of passwords, which allows a method of authenticating a party without the need to transmit the password itself over a network (the hashes themselves are instead).
- Non-repudiation is another area that the science of cryptography provides to the modern world. Non-repudiation, simply stated, is the ability to have positive proof that a particular party or entity is the one who originated an action. For example, in many corporate environments the application of a digital signature to e-mail is used as a potent means of asserting that a certain party transmitted the message. The possibility of the specific party not being the one who transmitted the message or carried out the action raises other legitimate security concerns, such as the compromise of the sender's system access (for example, did they lose control of their credentials and not say anything?). With this mechanism in place, it is possible now to have strong accountability for every action within an organization, allowing for the tracing of actions back to whomever initiated them. Non-repudiation should also, in theory, eliminate or substantially cut down on what is known as *spoofing* (impersonating) another party if the system is kept secure.
- Finally, one other critical aspect of any effective cryptosystem is key distribution. Arguably one of the most valuable components of a cryptosystem is the key, which represents the specific combination or code used to encrypt or decrypt data. This "combination" must be kept absolutely secret and accessible only to authorized parties; failure to do so severely weakens and many times compromises the entire system.

Consider this example: If an individual is required in their work environment to set a 12-character complex password, but then writes that password on a sticky note and places it on the lid of their laptop, the system is compromised no matter how strong the password may be otherwise. Another example would be the soon to be covered Caesar's system : If a message encrypted with this system is considered secure, that security is severely compromised if the key is sent along with the message, kind of like locking the front door to a house and then taping the key to the it.

History of Cryptography

While cryptography may seem like a new technology to many, it is in fact much longer lived than many realize. Cryptography has been around for a long time and has a rich and interesting history that goes back at least 4,500 years, if not more. So let's set the "Wayback Machine" and take a look at the origins of cryptography and trace it up through modern times.

Cryptography is more than likely one of the oldest bodies of knowledge that we can find evidence of. Although the original systems may not actually be in use for the most part anymore, each one adds something to today's technology and body of knowledge. The knowledge associated with encoding and hiding information is still very much considered mysterious and much like a "black art," as few truly understand all the logic and mathematics behind the scenes. In fact, it is this veil of mystery that led the science to be considered a black art and, by some, a way to communicate with spirits or the devil itself.

For many of you, it is possible that the first time you saw an encrypted message was when you set eyes on Egyptian hieroglyphics. This intricate and complex system of writing was used for religious and spiritual purposes. Although 4,500+ years ago the Egyptians most likely were not trying to keep secrets for the same reasons we are today, there is evidence that suggests they were trying to keep the ability to commune with their pantheon of gods somewhat controlled. In fact, it is believed that only members of the royal family and members of the religious orders could fully understand how to read and write the complex designs (although this has not been proven either way). The knowledge needed to read and write this beautiful and complex system was so restricted that when the last person capable of writing it died, over a thousand years ago, the knowledge was lost until a French soldier unwittingly uncovered the key to deciphering hieroglyphics in 1799. Figure 2-1 shows an example of hieroglyphics in an Egyptian tomb.

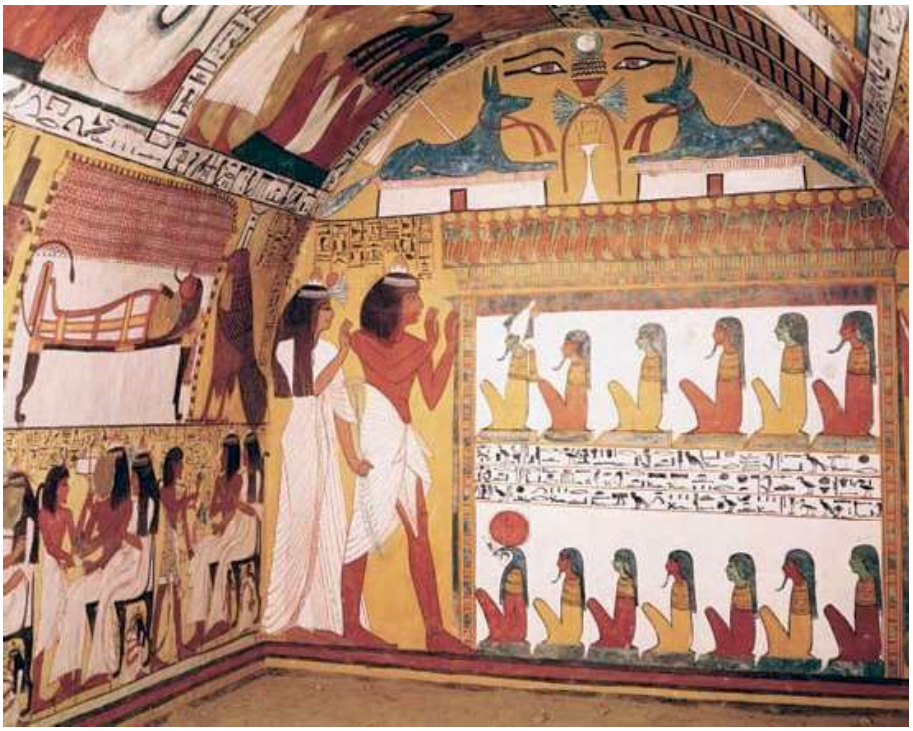

Figure 2-1 Egyptian hieroglyphics in a nobleman's tomb

In Actual Practice

Hieroglyphics, and arguably the best example of cryptography, began in or around 2000 B.C. in Egypt, where they were commonly used to decorate the tombs of deceased rulers and kings as well as other VIPs. The pictures served as a way to illustrate the story of the life of the deceased and proclaimed the great acts of their lives. It seems that the writing was intended by its designers to be purposefully cryptic; however, they did not intend to hide the text. To researchers now it seems that the writing system was designed to provide an additional sense of importance or regal appearance. As time went by, the developed writings became ever more complicated, and eventually the public turned to other pursuits and lost interest in deciphering them.

(continued)

In the eighteenth century, scholars in Europe were in the midst of making several attempts to decode the ancient Egyptian language. The common belief at the time was that the ancient culture held secrets both scientific and mystical that were encoded in the language represented by these strange writings. Confusion about decoding them was abound, with the prevailing wisdom being that the glyphs represented actual ideas as opposed to sounds as in other languages. The symbols, despite the work of scholars, stubbornly held onto their secrets for many more years, much as they had for a thousand years and more before.

The missing piece to understanding hieroglyphics turned out to be the famous Rosetta Stone. This stone was discovered by a soldier in the French Army in 1799. The stone was eventually transferred to English control after they defeated the French Army in Egypt. Due to the work of experts, and 20+ years of hard work, the ancient language was decoded and reintroduced to the world. The language could be read once again, and the world could enjoy the culture that had been lost. The Rosetta Stone went on to become a household name, even today, with the stone itself having a home in the British Museum. Figure 2-2 shows the Rosetta Stone.

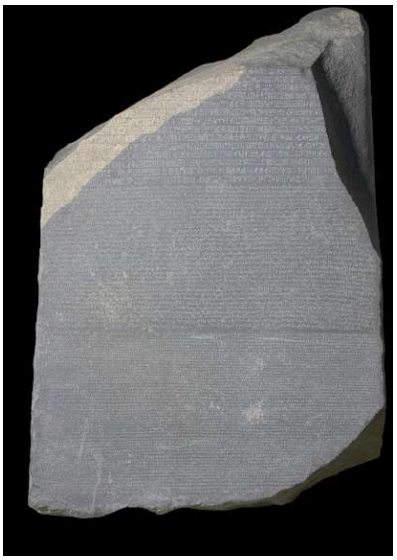

Figure 2-2 The Rosetta Stone

One of the earliest examples of the art is considered by some to be the paintings that early man used to render ideas on cave walls. Although this may be a bit of a stretch, it is not hard to see how anyone looking at a cave painting would assume that only the ones who drew them knew the meaning behind them. Because it is likely that only members of a tribe or clan would be the ones in the know, all outsiders would be barred from gathering any knowledge because they would not know how to read them.

IMHO

On a recent trip with my girlfriend to the Valley of Fire State Park in the great state of Nevada, I observed many petroglyphs on rock faces within the park. The glyphs were drawn by the inhabitants of the Valley one thousand to two thousand years ago, and now their meanings are lost. It isn't hard to imagine them in the same context as an intentionally encrypted message in today's world. Looking at these glyphs, I could only wonder what the ancient people were saying and whether there is a key someplace that would unlock the meanings of the pictures.

Of course, not all encryption techniques were meant to hide secrets relating to life, death, or military information. Others were meant to hide more taboo pieces of information, such as those that were sexual in nature. Although the text is known as containing a lot of information relating to the erotic arts, there is other information contained in the text that recommends how to live a life with a family and other aspects of love. Past all this information is a section on what is known as the mlecchita-vikalpa, or the art of secret writing, which was put forth to assist women in the concealment of the details of their liaisons. One of the techniques, in fact, involves a process that has come to be known as a substitution cipher, which is still in common usage today.

Another ancient civilization that was excellent at hiding information in creative and unique ways comes from China. The Chinese were known to use the unique nature of their language to obscure and transform the meaning of messages for those not intended to see them. Such transformation of messages through language could easily hide the meaning of a message to those not privy as to its true meaning, thus keeping privacy intact. However, although the practice of transforming the content of messages was known to the Chinese, it never saw widespread use, and evidence indicates that it never saw major use outside of private purposes. In fact, although it may seem logical that leaders such as Genghis Khan would have used such techniques during their conquests, no evidence has ever shown this to be the case.

IMHO

I'll add that the prevailing wisdom seems to indicate that Genghis Khan not only didn't use encryption to obscure messages, he really didn't need to. Why use cryptography when you have a fast moving army that can descend upon a city quickly? In other words, why send an encoded message when you have an army that could be on top of an enemy so fast it wouldn't matter anyway.

Other civilizations such as India made use of cryptography and did so more than the Chinese people did at the same time in history. In India, it was known that the government at various times used special codes and ciphers to communicate with their spies who were part of their early intelligence network. Although the codes were simplistic compared to those in use today for the same purpose, they were very effective at concealing the meaning of messages from outsiders.

Note

It is fascinating to note that the early Indian ciphers consisted largely of what are now known as simple substitutions based on phonetics. Essentially, this method is similar to what is now known as "Pig Latin," where the first consonant is placed at the end of the word and followed by the sound "ay." This method may seem simple to any child who has spoken Pig Latin on the playground with friends, but it still was effective at the time.

Another one of the more well-known encryption techniques from the ancient world comes by way of the Mesopotamians. Much like in Egypt of old, this culture used specialized symbols (known as cuneiform) to convey information, and after this knowledge was lost, the writings stood as an enigma to travelers in the Middle East. Complicating the deciphering of the language was the lack of a key which meant incorrect assumptions were being made. In the case of cuneiform, the deciphering process was simpler than that of the earlier example involving the Egyptians, but it still took some time.

Potentially complicating the picture even more was that the writing technique was around for so long. For the many centuries the script was in use, it evolved dramatically, meaning that the symbology changed and reflected different meanings in some cases. Figure 2-3 shows an example of cuneiform writing.

A little known example of cryptography known as ATBASH comes courtesy of the Hebrew language and the Bible. This cipher was simple in design and concept, but in implementation it was straightforward compared with later ciphers. Essentially the design of the technique flipped the characters of the alphabet, with the characters at the

Figure 2-3 Sample of cuneiform writing

end replacing the ones at the beginning. Once this was done, the letters were substituted accordingly. The following shows how this process looks in the English language:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

ZYXWVUTSRQPONMLKJIHGFEDCBA

IMHO

Some have cited the ATBASH cipher as the possible inspiration for what is known as the Bible Code. The Bible Code is purported to be the way the creators of the Bible hid messages and prophecy within the work. Whether or not this is the actual case is still the source of some debate, but the idea is intriguing, to say the least.

One of my personal favorites comes from the Spartans and Scytale (rhymes with *Italy)*. This method is markedly different and unique among all the methods mentioned so far. It approaches the problem of how to encrypt by replacing an algorithm with a wooden dowel. To use this encryption method, all parties would have to agree on the diameter of

the dowel prior to exchanging messages. Next, the sender would take a strip of leather or parchment and wrap it around their dowel and inscribed the message in several lines across the parchment, rotating the dowel as each line was completed. After the message was inscribed, the parchment was unwrapped and sent to the intended recipient, who would wrap the parchment around their dowel, which is of the same diameter, and read the message. This method of encoding messages, although simple, was popular in a handful of ancient civilizations, including the Greeks and in particular the Spartans, who used it to transmit messages on the battlefield. Figure 2-4 shows a diagram of Scytale.

Another personal favorite, and one we will revisit later, is the Caesar Cipher, which is a simple-but-effective process that has been around for over 2000 years. Julius Caesar used this process to encrypt or encode his messages to his commanders in the field for the same reason the military today does—to keep sensitive information private. Although the cipher is simple, it is still in use today, and in fact is the one that most school children would be familiar with because it has appeared in countless puzzle game books and cereal boxes over the years.

Simply put, the process Caesar used shifted each letter three places further in the alphabet (for instance, Y becomes B, and R shifts to U). Although the process could use any shift amount, Caesar settled on a shift of three spaces. Although simple, it was effective at keeping secrets at the time because anyone encountering the message would most likely assume it was in a foreign language—if they could read at all. As shown here, the first row represents what is known as plaintext, and the second row is the equivalent ciphertext if a shift of two was used instead of three:

ABCDEFGHIJKLMNOPQRSTUVWXYZ
CDEFGHIJKLMNOPQRSTUVWXYZAB

Figure 2-4 A diagram of a Scytale system

Let's move forward a bit in time to take a look at some of the techniques that emerged during the Middle Ages. Much like before, and definitely like the times that came after, cryptography was mainly focused on protecting the secrets of diplomats and military types. During this time period, the first truly new ciphers came from Italy, specifically Venice, where a new organization was created in 1452 to deal with the issues involving cryptography.

One figure who emerged from this time period is Leon Battista Alberti, who later became known as the Father of Western Cryptology. Alberti was responsible for the development of a technique known as polyalphabetic substitution. This technique is still widely utilized by many modern-day processes and mechanisms. Essentially, this process relies on substituting different characters for the same unencrypted symbol. This technique came into being after Alberti reviewed how other existing ciphers were compromised or broken and then envisioned a technique that could thwart these methods. Don't worry too much about polyalphabetic substitution at this point because it will be discussed further in a later chapter.

LINGO
Leon Battista Alberti is known as a **polymath**, or an expert in many fields. In Alberti's case, he was an author, artist, architect, poet, priest, linguist, philosopher, cryptographer, and humanist polymath.

Alberti's technique was essentially simple in concept, but powerful in practice. The initial mechanism as designed was simple, being nothing more than two copper disks with the entire alphabet written upon each of them. To encrypt a message, the encrypting party chose a letter on the outer ring and lined it up with the inner ring. The outer ring represented the letters in the unencrypted message, and the inner the encrypted message. By matching up the unencrypted letters with the ones on the inner ring, one could quickly translate a message into another form that was unreadable without knowing the settings used. Making the process even more complicated is the fact that the settings were redone after every so many letters in order to make the mechanism that much more robust. Because the settings were changed every few words, the cipher changed enough to blunt the overall effectiveness of known code-breaking methods. Even though this technique, when explained, seems very weak, at the time it was considered to be very strong. Also, the idea of rotating the disks to change the process every so often was a major step in the field of cryptography, one that is also still used today (albeit in a different form).

Of course, Alberti and the Italians didn't come up with all the advances in the field of cryptography: There were many others, one of which was made by the German Abbott Trithemius. Trithemius was responsible for authoring a series of books that came to be known as *Polygraphia.* At the time, the books were viewed by some to be heretical and related to the occult due to their extensive use of tables and codes. It wasn't until much later that research showed that what had been documented and devised was a complex and effective method of encrypting information. The process worked like so: To encode and convert a message, each letter of the plaintext in the first row of the table is swapped with the letter in the same position in the second row, with the same process being repeated for the each letter within the message. The result of this process is a message where each letter is replaced at least once before a letter is reused.

Note

Much like other ciphers in use, the Trithemius technique was improved by later followers, such as Giovan Belaso in 1553. The technique that Belaso introduced used whole phrases to encrypt plaintext instead of a single letter. This technique will be visited more later, but I wanted to mention it now just to put it into context.

A later development, and a significant one at that, is known as the Vigenère cipher. The Vigenère cipher is much more complex than Alberti's cipher in that is uses 26 unique and distinct alphabets as opposed to Alberti's two. Each alphabet is the same, except each one is shifted by one letter. Essentially, each row is a representation of the Caesar cipher and represents a shift of some given number, with row number 1 representing a shift of 1, row number 2 representing a cipher alphabet with a shift of 2, and so on.

To use this method, a different row is used to encrypt each letter in a message. In other words, the sender of the message would encrypt their message, with each letter being encrypted by a different row. In order to decode the message, the recipient must be aware of which row of the matrix was used to encrypt each letter. In turn, there must be a way to agree how the switch between rows will occur. This agreement is achieved via the selection of a keyword.

The evolutionary leap this represented was huge because it rendered the many forms of frequency analysis moot. In fact, it wasn't until much later that this cipher was routinely broken, albeit slowly.

In Actual Practice

In 2010, a glass vial was discovered that contained a message written during the Civil War. The coded message was authored by a Confederate commander outside Vicksburg the day the city fell to Union forces.

The message offered no hope to the Confederate officer, one Lt. Gen. John C Pemberton. It clearly and unambiguously stated that reinforcements would not be arriving. The message was a short six lines and was dated July 4, 1863, which also was the day the General surrendered to future U.S. President and then Union General Ulysses S Grant. The surrender represented a major turning point in the war in the favor of the Union.

The glass vial sat alone and undisturbed in a museum dedicated to the Confederacy in Richmond, Virginia until experts were able to recover the message and decrypt it. The message when it was decrypted stated the following:

> Gen'l Pemberton:
>
> You can expect no help from this side of the river. Let Gen'l Johnston know, if possible, when you can attack the same point on the enemy's lines. Inform me also and I will endeavor to make a diversion. I have sent some caps (explosive devices). I subjoin a despatch from General Johnston.

The significance to our story is that the message was rendered into its encrypted format via the Vigenère cipher.

But let's not focus just on techniques; let's also consider some of the historical events cryptography played a role in, such as the life, and death, of Mary Queen of Scots. Poor Mary, who was eventually executed in 1587 on the orders of her cousin Queen Elizabeth I of England, used cryptography in the events leading up to her eventual demise.

Prior to her execution, Mary had thrown herself upon the mercy of the Queen after she had been coerced to give up the Scottish thrown to her infant son James in 1567. Following the abdication, an inquiry had determined that she had colluded with her third husband, the Earl of Bothwell, to murder her second husband, Lord Darnley. As a result, Mary was held in prison as a long term "guest." Not content with this situation, Mary's

own supporters, and Mary herself, made other plans. In the years between 1571 and 1586, a handful of plots were put forth to free the Catholic Mary and place her on the throne, supplanting Protestant Elizabeth. Elizabeth was not naïve, however, and knew that such plots were in the works, but was reluctant to move against Mary and accuse her of treason without proof. As fate would have it, later events would unfold that provided the proof Elizabeth needed to seal Mary's fate.

In July of 1586, Mary was a prisoner under the ward of Protestant, Sir Amias Paulet, at Chartley Castle in Staffordshire when she received a letter from Sir Anthony Babington, asking for Mary to approve "the dispatch of the usurping Competitor," which meant that permission was being sought for the assassination of Elizabeth.

Mary was able to communicate with her network of allies by smuggling encrypted messages in and out Chartley within casks of ale. The messages were kept secret, or so Mary thought, through use of an encryption mechanism that relied on substitution. Mary's code substituted symbols for letters of the alphabet and also some words. The cipher also included some additional tricks known as "nulls," or symbols which represented nothing at all, to confuse any code breakers trying to decipher the letters.

Where did Mary's plan fall apart? Well, unbeknownst to Mary, the courier who carried the messages back and forth, Gilbert Gifford, was a double-agent who worked for Elizabeth—specifically, for Sir Francis Walsingham. Sir Walsingham, the head of intelligence at the time, had the messages intercepted and monitored in an effort to gain evidence, which was about to pay off. Everything that Mary sent to Babington was intercepted and later passed to Walsingham's expert code breaker Sir Thomas Phelippes. Phelippes was a master of his code-breaking craft and was fluent in six languages. He was able to see clues to break many a code. In this particular case, a method known as frequency analysis was used to look for patterns that could reveal the underlying message.

To make things even more interesting, the messages were not only broken, but they were altered. In an effort to root out all the conspirators in one swift stroke, Phelippes added a postscript to the message asking Babington to provide the names of others involved in the plot. With this resulting reply in hand from Babington to Mary, the conspirators were rounded up and their heads made an untimely separation from their bodies.

Elizabeth herself was presented the evidence by Sir Thomas Gorges with the following comment:

> "Madame, the Queen, my mistress finds it very strange that you, contrary to the pact and engagement made between you, should have conspired against her and her State, a thing which she could not have believed had she not seen proofs of it with her own eyes and known it for certain."

On the heels of the discovery, Mary found herself taken to Fotheringay Castle and subsequently tried in October 1586. Despite her denials, the evidence was too much, as Mary was done. Elizabeth now had what she needed and formally signed a death warrant calling for Mary's execution in February of 1587. Mary lost her head, and the case was closed on the tale.

Although she didn't actually live to see it, Mary did have the last "laugh" in the whole affair. Mary, of course, never replaced Elizabeth, but her son James VI of Scotland was crowned James I of England in 1603. The succession was the result of Elizabeth never having a child of her own to take the throne.

Interestingly enough, James himself was the target of a famous assassination plot known as the Gunpowder Plot, involving the famous conspirator Guy Fawkes.

At the same time all of this intrigue was going on, a new organization called "Black Chambers" showed up in Europe in many different countries. This entity was commonplace throughout Europe during the 1700s forward, but what did it do? Simply put, the Black Chambers were put in place to investigate and break codes as their primary responsibility. Many of these organizations were in place all over Europe, with one of the most famous in Vienna. In fact, this particular Black Chamber was so well organized and thought out that it was reportedly able to intercept mail destined for foreign embassies and then copy, alter, and reseal the contents before sending them back to the post office later the same morning.

Of course, the Austrians weren't the only ones involved in the code-breaking field: The British had something to say about it, too. The English had their own code breakers and had numerous victories in the field. They were known at times to decrypt and process over 100 letters a day—amazing considering that no computers were used. In fact, at least one individual was granted the title of "Decypherer" after demonstrating extreme skill in breaking foreign diplomatic codes.

The original 13 colonies were also involved in the code-breaking game, but without the centralized mechanisms that were present in Europe. In fact, the colonies' encryption efforts were carried out through the dedicated work of clergymen and other religious types. Significantly, the colonies had a major code-breaking coup early in the war when a coded message from Dr. Benjamin Church was intercepted. It was suspected of being a message sent to the British, but without it being deciphered, this could not be confirmed. Solving the code was a somewhat unlikely and little remembered individual by the name of Elbridge Gerry. Gerry provided the skills necessary to break the code and show that Church had tried to work with the Tories, a crime he was later exiled for. Later