A Historical Overview of Secret Communication and an Introduction to Modern Encryption Methods

Lee Seemann

Follow this and additional works at: https://louis.uah.edu/honors-capstones

Recommended Citation
https://louis.uah.edu/honors-capstones/565

This Thesis is brought to you for free and open access by the Honors College at LOUIS. It has been accepted for inclusion in Honors Capstone Projects and Theses by an authorized administrator of LOUIS.
A Historical Overview of Secret Communication and an Introduction to Modern Encryption Methods

by

Lee Seemann

An Honors Capstone submitted in partial fulfillment of the requirements for the Honors Diploma to The Honors College of The University of Alabama in Huntsville

April 27, 2016

Honors Capstone Director: Dr. Tommy Morris Director of Center for Cybersecurity Research and Education Associate Professor of Electrical and Computer Engineering

Property rights reside with the Honors College, University of Alabama in Huntsville, Huntsville, AL
Honors Thesis Copyright Permission

This form must be signed by the student and submitted as a bound part of the thesis. In presenting this thesis in partial fulfillment of the requirements for Honors Diploma or Certificate from The University of Alabama in Huntsville, I agree that the Library of this University shall make it freely available for inspection. I further agree that permission for extensive copying for scholarly purposes may be granted by my advisor or, in his/her absence, by the Chair of the Department, Director of the Program, or the Dean of the Honors College. It is also understood that due recognition shall be given to me and to The University of Alabama in Huntsville in any scholarly use which may be made of any material in this thesis.

Lee Seemann
Student Name (printed)

Lee Seemann
Student Signature

4/27/16
Date
Table of Contents

Abstract

Introduction
    The Need for Secret Communication
    The Tools of the Trade

Chapter 1: The History of Secret Communication
    The Substitution Cipher
        Ancient Egypt
        Ancient Rome
    The Transposition Cipher
    The Poly Alphabetic Cipher
        Alberti-Vigener Cipher
        Jefferson Wheel Cipher
    The First Mechanical Methods
        The Enigma Machine
        The Purple Machine

Chapter 2: Current Methods of Encryption
    Symmetric Encryption
        Data Encryption Standard
        Diffie-Hellman
    Asymmetric Encryption
        RSA Encryption
    Hashing
        Cryptographic Hash Functions
        Digital Signatures
    Steganography

Chapter 3: The Future of Encryption
    Elliptic Curve Cryptography
    Quantum Computation
Abstract

Throughout history, people have sought to control access to valuable information. Although encryption is viewed as a modern invention, the concept of disguising information to prevent unauthorized access has been around for thousands of years. There is evidence from the Egyptian town of Menet Khufu that hieroglyphic substitution was used to obscure the meaning of inscriptions nearly 4000 years ago. While the methods are quite different, the goal of modern encryption algorithms is the same; to prevent vital information from falling into the hands of unintended recipients. From ancient Egypt to the present, sensitive information has always been protected in one way or another. The goal of this paper is to provide a brief history of the methods used to communicate secretively for centuries and to introduce modern methods of data encryption, such as symmetric encryption, asymmetric encryption, and steganography.
Introduction

The Need for Secret Communication

Sir Francis Bacon is often attributed with the phrase “knowledge is power” (“Knowledge is Power”). Throughout history, people have sought to control access to valuable information in an attempt to protect the power that it provides. Although methods of communicating secretively (such as data encryption) are viewed as modern inventions, the concept of disguising information to prevent unauthorized access has been around for thousands of years. As long as wars have been fought, there has been a need to communicate with allies while hiding such communication from the enemies. As a result, military communication has been one of the major driving forces behind the advancement of secret communication methods throughout history. In addition to militaries and their corresponding governments, private businesses also seek to protect vital information from their competitors. Many modern methods of protecting data were created as a result of the Information Age, which began in the 1980s. With the advancement of the internet and new ways of rapidly transmitting information, a need to verify the security of these transmissions arose (McDonald, 3). From Julius Caesar’s military strategy to personal financial transactions, the need for secret data transfer and communication is not only alive and well today, but has been vital throughout history.

The Tools of the Trade

In order to discuss and study the history of secret communication, becoming familiar with some basic terminology is necessary. The terms “cryptography,” “cryptology,” and “cryptanalysis” are often used interchangeably, but they have different meanings within the world of security. The term “cryptography” refers to the historical or forensic approach concerned with the writing of secret messages (Pelling). Cryptanalysis has the opposite purpose
of cryptography. Instead of writing secret messages, cryptanalysis is concerned with interpreting those secret messages. Finally, cryptology is the study of the math and science that is behind the methods used to disguise and interpret secret messages (“Difference Between Cryptography, Cryptanalysis, Cryptology”). If cryptography is the input to an equation and cryptanalysis is the output of the equation, cryptology is concerned with the equation itself.

A term that appears frequently when discussing data security is “encryption.” Often associated with secret data transmission, encryption is a single area within cryptography. Encryption is the process of converting readable information, called the plaintext, into an unreadable form, which is called the ciphertext. A key, often referred to as public or private depending upon the application, is the variable used by an encryption algorithm to convert plaintext into ciphertext (Rouse). Decryption works in the opposite direction by converting the ciphertext into the original, readable plaintext. A term often used with encryption and decryption is “cipher.” A cipher refers to the process used to encrypt or decrypt a message (McDonald, 3). With a basic understanding of these commonly used terms, a discussion of the history of secret communication can begin.
Chapter 1: The History of Secret Communication

The Substitution Cipher

Ancient Egypt

One of the earliest and simplest ciphers ever created is the substitution cipher. A substitution cipher protects information by substituting one character or symbol for another. The earliest recorded use of cryptography occurred in approximately 1900 B.C. in an Egyptian town called Menet Khufu. In the tomb of Khnumhotep II, a scribe depicted the life of his master by using hieroglyphics. However, a number of unusual symbols were used by the scribe to obscure the meaning of the images resulting in the first recorded use of a substitution cipher (McDonald, 4).

Ancient Rome

The military has always been a driving force behind secret communication, and Julius Caesar’s substitution cipher provided the first recorded use of cryptography by a military force. In order to communicate with his troops while avoiding interference from Rome’s enemies should his message be intercepted, Caesar implemented a substitution cipher which involved shifting each letter by a predetermined number of letters. This number of letters served as the key to Caesar’s substitution cipher (McDonald, 5). For example, if the cipher used a key of three, every ‘a’ would be replaced with a ‘d’ and every ‘b’ would be replaced with an ‘e.’ Although simple, this method of communication was sufficient during an age where only a small portion of the population could read at all (“History of Encryption”). This ability to communicate freely gave Rome a significant advantage in war. A substitution cipher key that is slightly more complex than that used by Caesar is shown in figure 1. This figure illustrates how one letter may be randomly mapped to another for a more complex substitution cipher.
Substitution ciphers provide a simple way of obscuring messages that is both easy to implement and quick to decipher if the method used to encode the message is known. However, this simplicity makes it insufficient for modern use because of the speed at which modern computing can break such encryption methods.

**The Transposition Cipher**

Transposition ciphers are similar to substitution ciphers except transposition ciphers modify the order of the characters in a message instead of changing them. The Greek Scytale, which was used by the Spartans for secure communication beginning around 500 B.C., is an example of how a transposition cipher may be used. The Scytale consisted of a piece of parchment which was wrapped around a cylinder. A message was then written along the parchment. This message became unreadable as soon as the parchment was removed from the cylinder. In order to read the secret message, an individual would need to wrap the parchment around an identical cylinder to the one used to create the message (McDonald, 5). An example of what a Scytale might have looked like is shown in figure 2.
Similar to Caesar’s substitution cipher, the transposition cipher is simple to implement but also easily decoded with modern computing. However, as with the Roman’s substitution cipher, the transposition cipher was sufficient for the Spartans during a period when the majority of the population was illiterate.

**The Poly Alphabetic Cipher**

Alberti-Vigener Cipher

Poly alphabetic ciphers provide an increased level of security by utilizing multiple substitution ciphers throughout the process of encrypting a message. Leon Battista Alberti developed a method of encryption in the mid-1400s using a series of movable disks to accomplish this task. Even though Alberti’s idea remained only a concept and was never put into practice, Blaise De Vigenere created the Vigenere Cipher in the 1500s using the concept of Alberti. Unlike Caesar’s substitution cipher, the Vigenere Cipher changes the key constantly during the process of encryption. The Vigenere Square shown in figure 3 is used. This table contains a series of 26 alphabets that are offset by one letter (McDonald, 6).
For example, assume the sender would like to transmit the message “CHARGER” using the Vigenere Cipher. Also, assume “UAH” has been chosen as the keyword for the encryption. The keyword is repeated until each letter in the message has a corresponding letter in the keyword.

First, find row U since that is the first letter in the keyword. In row U, find column C since that is the first letter in the message to be encrypted. In row U, column C, find the letter “W” which will be the first letter in the encrypted message. This process is repeated until all letters of the original message have been encoded. This process results in the following:

<table>
<thead>
<tr>
<th>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</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>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</td>
</tr>
</tbody>
</table>

Figure 3 (McDonald, 7)

Plaintext: CHARGER
Keyword: UAHUAHU
Ciphertext: WHHLGLL

To decrypt the message, the receiver of the transmission would find the ciphertext’s character in the keyword’s row. The column where the character is found is the corresponding letter of the plaintext. For the example above, row U would be searched for a ‘W’ which would be found in
column C, which becomes the first letter of the decrypted message. This process is repeated for each letter to obtain the original plaintext.

Jefferson Wheel Cipher

Thomas Jefferson improved upon the Vigenere Cipher when he developed the wheel cipher in the late 1700s. Jefferson’s method included 26 wheels that each contained a randomly ordered version of the alphabet. To encrypt a message, the wheels were aligned so that the original message could be read across the wheels. The ciphertext was any other line of text that was present when the original message was created using the wheels. The recipient of the message would place the wheels in the proper order, rotate the wheels until the ciphertext was present, and then quickly scan the other rows to discover the original message. Although Jefferson never actually developed his invention, a similar system was invented and used by the United States Army supposedly without the knowledge of Jefferson’s cipher. This method of encryption remained in use by the U.S. Army from 1923 to 1942 (McDonald, 8). An example of what the Jefferson Wheel Cipher may have looked like is shown in figure 4.
While poly alphabetic ciphers are still easily cracked with modern computing, they offered increased security compared to the standard substitution ciphers. In addition, they were easy to use and required minimal special equipment to utilize.

**The First Mechanical Methods**

The Enigma Machine

As decryption methods improved throughout history, it soon became necessary to develop encryption methods with greater security. The Enigma, a mechanical machine developed by Arthur Scherbius near the end of World War I, had $10^{114}$ possible configurations due to a series of rotors and gears that modified the way a message was encrypted. The Enigma became commercially available in the 1920s and was almost impossible to decrypt by hand due to the possible number of ways to encrypt a message (McDonald, 10). An example of how the Enigma worked is shown in figure 5. In the figure, the process of encrypting the letter ‘T’ using the Enigma is shown. After the user presses the letter ‘T,’ the signal created travels into the plugboard. Inside the plugboard, the ‘T’ input is connected to the ‘K’ output. As a result, the ‘K’ signal enters the series of rotors. With the exception of the first static wheel, these rotors are designed to scramble the signal. The mobility of these rotors results in a large variety of ways a message can be encrypted. In addition, these rotors move each time an individual letter is pressed. This ensures, for example, that if a message contains two identical letters, the letter will be encrypted differently each time it is entered. The signal’s last stop before making the return trip is the reflector. This reflector modifies the signal before sending it back through the other rotors which work the same way in reverse. If the reflector did not modify the incoming signal, it would simply be decrypted on the return trip resulting in an unencrypted message. After the signal leaves the static rotor as a ‘W,’ it returns to the plugboard. In this case, the ‘W’ is
connected to the ‘G’ which is the final letter that is output to the user. Decryption simply involves matching the settings used for encryption and entering the ciphertext.

Figure 5 (Dade)

The Enigma created such secure messages that it was used by the Nazis during World War II for military communication. However, the Enigma had one, ultimately fatal flaw. Because of the reflector, the Enigma never mapped a letter to itself. If the plaintext began with an ‘a,’ the ciphertext created by the Enigma would never begin with an ‘a.’ Therefore, by adjusting the rotors, all letters would be possible with one exception: the original plaintext letter. This flaw, along with the use of common phrases and operator error by the Germans, allowed the Allies to decrypt a number of German messages during the war. This eventually led to the demise of the Enigma (Hern 2014). The Enigma, which resembled a typewriter, is shown in figure 6.
The Purple Machine

While the Germans were placing their trust in the Enigma to protect communication, the Japanese were using their own encryption machine called the Purple. The Purple was actually a modified version of the Enigma. However, unlike the Enigma, which used rotors and gears, the Purple used a series of switches, such as those for routing a telephone signal, to modify the input signal (McDonald, 10). Despite much difficulty, William Friedman, the creator of the U.S. Army’s Signal Intelligence Service (SIS), and his team of American cryptographers were able to build a Purple replica by analyzing encrypted messages. This advancement eventually led to the construction of a machine capable of decrypting Purple messages. By 1940, the SIS had constructed eight of these machines which gave the United States a significant advantage against the Japanese during World War II (McDonald, 11). Figure 7 shows what a Purple machine may have looked like. The Japanese were incredibly careful to protect their secrets, and as a result, no complete Purple machine was ever found (McDonald, 10).
As with many conflicts, World War I and World War II resulted in the creation of new methods of hiding messages out of necessity. The Enigma and Purple machines’ methods were eventually decrypted, and they became obsolete as a result. However, both of these machines were responsible for helping to advance message encryption technology.
Chapter 2: Current Methods of Encryption

As decryption techniques improved and the Information Age introduced new ways of transmitting information, more advanced methods of data encryption became necessary. Symmetric encryption techniques, such as the Advanced Encryption Standard (AES), and asymmetric encryption techniques, such as RSA encryption, were created to fill this void and to provide greater security for data transmission.

Symmetric Encryption

Symmetric encryption, also called private-key encryption, uses a single key to both encrypt and decrypt a message. In a sense, symmetric encryption is not new. The cylinder used in the Greek Scytale or the keyword used in a Vigenere Cipher can be viewed as keys, and the same one must be used to encrypt and decrypt the message. However, symmetric encryption is often used in reference to more modern approaches such as the Data Encryption Standard (DES). When symmetric encryption is implemented, the creator of the message encrypts the data using a key, and that same key is used by the receiver of the message to decrypt the data. Because the same key works in both directions, the key must be protected to ensure security (“3 Different Data Encryption Methods”). This type of encryption is particularly useful when the person encrypting the data is also the person who needs to decrypt the data, such as encrypting a computer’s hard drive or backing up vital documents using the cloud (Behrens 2014). However, this can also be the biggest drawback to symmetric encryption. If an individual obtains the key being used, they can read your information, and send false data on your behalf. Therefore, symmetric encryption has a wide variety of uses and is extremely effective as long as proper precautions are taken to protect the private key.
Data Encryption Standard

The Data Encryption Standard (DES), one form of symmetric encryption, groups data into 64-bit blocks and encrypts all bits in each block simultaneously. Such encryption methods are referred to as block ciphers because the encryption algorithm is applied to blocks of data simultaneously instead of bit by bit. Sixteen rounds of encryption are used by DES and the blocks of data can be encrypted individually or can be made dependent on the encryption of all previous blocks. A single round is sufficient to transform the original plaintext into ciphertext, but each additional round provides an additional layer of complexity that prevents messages from easily being decrypted. The secret key used for the encryption is 64 bits, with 8 bits used for error checking. The key, which is effectively 56 bits long not including the error checking bits, provides $2^{56}$ or 72,057,594,037,927,936 possible keys (Cobb, “Data Encryption Standard (DES) Definition”). This 56-bit key is used to create 16 subkeys of 48 bits each. Each of these subkeys is responsible for one of the sixteen rounds of encryption. To create these subkeys, the original 56-bit key is divided into two pieces of 28 bits each. This original pair, which will be called $A_0$ and $B_0$, is used to create the second pair, $A_1$ and $B_1$, by shifting the bits of the original pair. Each subsequent pair is obtained by manipulating the previous pair. For example, $A_2$ and $B_2$ are used to create $A_3$ and $B_3$, which are then used to create $A_4$ and $B_4$. This is repeated until sixteen pairs are obtained. To create the sixteen subkeys, each of these pairs are combined to form a 56-bit set. Finally, a permutation table is used to manipulate the bits and obtain the final sixteen 48-bit subkeys from these 56-bit sets. Each 64-bit set of data is now encrypted with each of the sixteen keys with the output of the first round of encryption serving as the input for the second round and so on (Grabbe). Although, the DES process is quite complex, this is a simplified overview of the encryption method. DES was used extensively until the mid-1990s. However, in 1998 the
Electronic Frontier Foundation (EFF) built a computer that could find the correct key by trying all possible keys in just 56 hours. Attempting to decrypt a message by trying all possible keys is called a “brute force approach” and is a common method of attempting to break encryption methods. This time was reduced to 22 hours when the EFF utilized a large network of computers to perform the decryption. This advancement effectively ended the useful life cycle of the DES.

Triple DES (3DES), which is currently approved for use with government information until 2030, performs DES three times to improve security. Although the key length of 3DES is 168 bits (56 + 56 + 56), the effective security is considered to be equal to that of a 112-bit key due to potential attacks by third parties. While more secure than DES, 3DES also requires significantly more time to implement. To decrypt messages encrypted using DES and 3DES, “encrypt” the ciphertext using the same key to retrieve the plaintext. DES and 3DES are no longer the most advanced methods of encryption available, but they served as an important stepping stone in the advancement of cryptographic techniques (Cobb, “Data Encryption Standard (DES) Definition”).

Advanced Encryption Standard

When it became necessary to select a successor to the DES and 3DES, a number of possible algorithms were considered. The Rijndael cipher, created by two Belgians, Joan Daemen and Vincent Rijmen, was ultimately selected as the algorithm for the Advanced Encryption Standard (AES). In 2002, the AES became a federal government standard, and its successful government use led to increased usage by private companies. Three versions of AES are currently in use. The AES-128, AES-192, and AES-256 encrypt 128-bit blocks of data using 128-bit, 192-bit, and 256-bit keys and 10, 12, and 14 rounds of encryption respectively. In the case of AES-128, ten different 128-bit keys are created from the original key (“How does the encryption algorithm Rijndael (also called AES) work?”). As in DES, each of these keys is used
for one of the rounds of encryption. After each round, the ciphertext created becomes the plaintext for the next round of encryption. Even though fewer rounds of encryption take place compared to DES, the keys used are much longer which results in a higher degree of security. As with DES/3DES, AES decryption involves applying the same key to the ciphertext to obtain the original plaintext. Unlike DES, AES has not been successfully attacked using brute force methods. The only successful attack against AES was the result of the improper implementation of the standard (Cobb, “Advanced Encryption Standard (AES)”). Current estimates suggest that it would take billions of years to successfully break AES-128 using a brute force approach (Arora 2012). When implemented correctly, AES provides exceptional protection for sensitive information that is essentially unbreakable given current computing capabilities.

**Diffie-Hellman**

Symmetric encryption is only as secure as the level of access to the key used in the encryption. Therefore, special care must be taken to restrict access to this key. One protocol used to protect keys is the Diffie-Hellman Key Exchange protocol. Whitfield Diffie and Martin Hellman created this protocol in 1976. It is designed to provide both parties, the sender and receiver, with the key without ever actually sending the key itself. Figure 8 shows the transmissions involved. For example, if Alice and Bob want to establish communication, Alice first assigns a value to ‘a’, ‘g’, and ‘p.’ These variables are then used by Alice to calculate ‘A.’ Alice then sends ‘g’, ‘p’, and ‘A’ to Bob. Bob then assigns a value to ‘b’ and uses ‘b’, ‘g’, and ‘p’ to calculate ‘B’ which is then sent back to Alice. Both parties now have the necessary information to calculate ‘K’, the key that will be used to perform the encryption/decryption. The “mod” function used here returns the remainder of a division operation. For example, 8 mod 5 would return 3 since 8 divided by 5 is 1 with a remainder of 3. Even if a third party is able to
intercept the transmitted values, the logarithm of ‘A’ or ‘B’ still must be determined. Depending upon the size of the values for ‘a’, ‘b’, and ‘p’ that are selected by Alice and Bob, this calculation could take billions of years even with modern computing (McDonald, 15).

![Diagram of asymmetric encryption](image)

**Figure 8 (McDonald, 14)**

**Asymmetric Encryption**

Asymmetric encryption, also referred to as public-key encryption, differs from symmetric encryption in that one key is used for encryption and another key is used for decryption. The key used to encrypt messages is made public for those wishing to send messages. However, only the individual with the correct decryption key can decode and read the message (“3 Different Data Encryption Methods”). While secure, asymmetric encryption can be subject to man-in-the-middle attacks. These attacks occur when a third party is standing between you and the entity you think you are communicating with. The third party provides a public key to use and provides the intended recipient with a different public key. As a result, the third party has the necessary decryption keys and is able to decrypt messages, read them, and re-encrypt them before sending them to their destination without anyone noticing. As with symmetric encryption, the security provided by asymmetric encryption is dependent upon the level of trust that can be placed in the
keys being used. Man-in-the-middle attacks can be prevented by using digital signatures, which will be discussed later (Behrens 2014).

RSA Encryption

RSA encryption, named after its creators, Ron Rivest, Adi Shamir, and Leonard Adleman, follows protocol similar to those used by the Diffie-Hellman Key Exchange. However, unlike the Diffie-Hellman Key Exchange, RSA encryption allows the actual message to be included as part of the transmission. RSA encryption consists of manipulating two large prime numbers to create a public and private key which can be used for asymmetric encryption. A prime number is a number whose only divisors are one and itself. The modulus, which is the product of the two large prime numbers, provides the only way to break RSA encryption. By finding the prime factorization of the modulus, someone could obtain the private and public keys used. However, for larger numbers, this could take billions of years using a single computer. However, these large numbers can be generated in less than a minute, making RSA encryption a secure and efficient method of transmitting sensitive messages (McDonald, 15). The following example provides a very simple overview of the RSA encryption process. Assume that the two prime numbers, p and q, have been assigned the values of 3 and 7 respectively. The modulus, which is the product of p and q, is 21. The function f(n) = (p-1) * (q-1) will use p and q to calculate the public encrypt key. In this case, the result of this function is f(n) = (3-1) * (7-1) = 2 * 6 = 12. The next step is to select a public encrypt key that is relatively prime to 12. When factored, relatively prime numbers share no common factors other than one. For this example, the numbers 5, 7, or 11 could be chosen. For this example, the number 5 will be selected as the public encrypt key, also called the encryption exponent. The public encrypt key, 5, and the modulus, 21, can now be
provided to anyone wishing to send a message. The private decrypt key, also called the
decryption exponent, can now be calculated by using the following equation:

\[
\text{private decrypt key} = (\text{public encrypt key})^{-1} \mod f(n)
\]

As previously mentioned, the mod function used here returns the remainder of a division
operation. After the necessary algebra, the equation can be rearranged to the following:

\[ l = (\text{private decrypt key} \times 5) \mod 21 \]

Solving this equation yields a private decrypt key of 17. The private decrypt key, 17, and the
modulus, 21, are now ready to be used for decryption.

For the example transmission, assume the plaintext is the number 4. The ciphertext is
determined using the following equation:

\[
\text{ciphertext} = \text{plaintext} \times \text{public encrypt key} \mod \text{modulus}
\]

Therefore, the ciphertext = 4⁵ Mod 21 = 16. The plaintext has now been encrypted, and the
transmission will contain the number 16. To decrypt the transmission, the following equation is
used by the receiver:

\[
\text{plaintext} = \text{ciphertext} \times \text{private decrypt key} \mod \text{modulus}
\]

As a result, the plaintext = 16¹⁷ Mod 21 = 4. The only way to break such an encryption method is
to determine the prime factorization of the modulus. When incredibly large prime numbers are
used, the time needed to try all possible prime number combinations is not practical (“A Basic
Public Key Example”).

**Hashing**

Cryptographic Hash Functions

Digital signatures were previously mentioned as a way to verify that a transmitted
message has not been accessed and altered without permission from the creator. Hashing is used
to create digital signatures by creating a unique signature for a message (“3 Different Data Encryption Methods”). A hash function is designed to produce a fixed-size output given an input. Most importantly, this output, called the message digest, will always be the same given the same input. Also, knowing the output of a hash function does not provide the information needed to reverse it and to determine the original input message. The most powerful hash functions, known as cryptographic hash functions, have one additional property not present in traditional hash functions. It is difficult, if not impossible, to generate the same digest for different messages if a cryptographic hash function is being used. A collision occurs when the same digest is generated for two different messages, and this occurrence greatly weakens the security of the cryptographic hash function. Cryptographic hash function collisions cannot be found by any means other than brute force. As is the case with most encryption algorithms, brute force attacks would likely take thousands of years at a minimum to successfully find a collision (Silva 2003). Although these functions are not actually methods of encryption themselves, the uniqueness of the message digests allows them to be used to detect any changes to a message (“3 Different Data Encryption Methods”). Two popular cryptographic hash functions are the Message Digest (MD) and the Secure Hash Algorithm (SHA). Numbers often follow these two functions to indicate the revision of the algorithm being used, such as MD5 and SHA3. An example MD5 message digest is shown below:

Message: UAH Chargers!

Message Digest: ac48777e902435827a69053285d0d0e8

It is important to reiterate that the message digest is a representation of a message not an encrypted version of the message. In other words, the message digest cannot be used to
determine the original message. The digest can only be used to determine if the original message has been modified.

Digital Signatures

Cryptographic hash functions provide a way to check a message for modifications, but they are just one part of the process of creating a digital signature. Digital signatures are a popular way to verify whether or not a message has been manipulated, and they are often used with asymmetric encryption. A digital signature is created by first using a cryptographic hash function to determine the message digest of the transmission. This digest is then encrypted using the public key being used for the transmission. This encrypted message digest, along with the cryptographic hash function and other information, becomes the digital signature. A digital signature is not only unique to the message, but also to the sender. Whether or not the actual message is encrypted, this digital signature can be used by the receiver to verify that a message has not been modified by a third party before reaching its destination. To do this, the receiver uses the public key to decrypt the message digest included with the message and then computes the message digest of the actual message that was received. If they match, no tampering has occurred (Cobb, “Digital Signature Definition”). Unfortunately, digital signatures do have a potential weakness. If a third party can gain access to the location where the message digest is stored, it is possible for the message to be modified and a new digest created to replace the digest that corresponds to the unmodified message. Therefore, it is wise to also store the message digests in a secure location, such as a protected database that can only be accessed by the authorized parties (Silva 2003).
Secret Communication

Steganography

Steganography is a part of cryptography that involves hiding data by placing it inside another medium, such as an audio file or image. For example, the bits of a secret data file could be broken up and spread throughout an audio file. If a WAV audio file is used, audio is represented by a 16-bit number. Changing a single bit in the 16-bit number will not change the way the audio file sounds to the human ear, but is an excellent way to conceal information. The same could be done using an image. The binary representation of the image could be modified to include the secret data without changing the way the picture appears. Figure 8 shows the same image before (left) and after (right) steganography has taken place. Only when the binary representation is analyzed is the foreign data seen.

![Figure 8](image_url)

Figure 8 (McDonald, 17)

Steganography has proven to be a very secure way to transmit data because of the difficulty involved with determining if data is even being transmitted at all. In fact, the Al-Qaeda operatives that carried out the terrorist attacks in New York City on September 11, 2001, likely used steganography and the internet to exchange information prior to the attacks (McDonald, 17).
Chapter 3: The Future of Encryption

As demonstrated throughout history, there is no doubt that modern decryption techniques will eventually catch up to even the most secure encryption techniques. The need for new and more advanced data concealment techniques will continue to grow, and those with the ability to develop these new techniques will have a significant advantage over those restricted to using outdated methods.

Elliptic Curve Cryptography

Though already invented, Elliptic Curve Cryptography (ECC) is not fully understood and could provide an improved method of encryption in the future. ECC has similar characteristics to the Diffie-Hellman Key Exchange and RSA encryption, except the numbers used are selected from the finite field of an elliptic curve. Figure 9 shows an example of an elliptic curve where P and Q represent the numbers selected as the public and private keys. If the prime numbers used for RSA encryption are selected from the field of an elliptic curve, the keys can be smaller and still be just as secure (McDonald, 18). This can be done because the math required to solve elliptic curve logarithms is much more involved than the math involved with factoring a prime number. For example, the amount of energy needed to boil a teaspoon of water is greater than the amount of energy needed to break a 228-bit RSA key. On the other hand, determining a 228-bit elliptic curve key would require enough energy to boil all of the water on earth. A 228-bit elliptic curve key is equivalent to an RSA key with 2,380 bits. ECC can ultimately result in more efficient encryption by reducing the time it takes to encrypt a message without sacrificing security (Sullivan 2013). More testing is needed before ECC is used for government and commercial purposes, but this method is showing promise as an improved component of encryption (McDonald, 18).
Quantum Computation

We have seen that many of the more secure methods of encryption use keys that could take billions of years to determine by brute force. Quantum computation could provide a much faster way to break these encryption keys. Quantum computation utilizes quantum processors which use the principles of quantum mechanics. The first quantum processor available commercially is shown in figure 10. While traditional computers store information in bits which can have a value of ‘0’ or ‘1’, quantum computers store information in “quantum bits.” These bits can have multiple values at the same time which allows calculations to complete in exponentially less time. For example, an RSA key of 193 digits was factored in approximately five months using eighty computers running at 2.2 GHz, which means the processor of each computer is performing 2,200,000,000 calculations per second. Estimates indicate that the same number could be factored in approximately 17 seconds using quantum computation. The billions of years needed to break some encryption methods could be reduced to just a few hours.
Fortunately, quantum computation is currently far behind existing methods of computation. However, should a fully developed quantum computer be developed, many of the world’s systems, including financial industries, could be devastated as their security measures are thwarted (McDonald, 19).

Figure 10 (McDonald, 19)
Conclusion

Data concealment has been vital to military and economic success throughout history. Early methods of secret communication, such as Caesar’s substitution cipher and Jefferson’s wheel cipher, were sufficient to allow secret communication during a time when all decryption techniques had to be performed by hand. As decryption techniques have improved as a result of increased knowledge and improved computing techniques, methods of encryption have been forced to adapt and advance. Such advances resulted in the modern encryption techniques now in use, such as the Advanced Encryption Standard. Whether the result of quantum computing or some other new and advanced technique of breaking modern encryption algorithms, this pattern of progress is sure to continue into the future.
Bibliography


Difference Between Cryptography, Cryptanalysis, Cryptology. Study Notes and
The DES Algorithm Illustrated. Technical University of Berlin.


How does the encryption algorithm Rijndael (also called AES) work? AceBit. Web.


Knowledge is Power (Quotation). Thomas Jefferson Foundation, Inc. Web. 6 Apr.


http://searchsecurity.techtarget.com/definition/key.


