PAST, PRESENT, AND FUTURE METHODS OF CRYPTOGRAPHY AND DATA ENCRYPTION

A Research Review

by

Nicholas G. McDonald

Nicholas G. McDonald
Department of Electrical and Computer Engineering
University of Utah

PAST, PRESENT, AND FUTURE METHODS OF CRYPTOGRAPHY AND DATA ENCRYPTION

Table of Contents

Abstract

Cryptography and encryption have been used for secure communication for thousands of years. Throughout history, military communication has had the greatest influence on encryption and the advancements thereof. The need for secure commercial and private communication has been led by the Information Age, which began in the 1980's. Although the Internet had been invented in the late 1960's, it did not gain a public face until the World Wide Web was invented in 1989. The World Wide Web is an electronic protocol which allows people to communicate mail, information, and commerce through a digital medium. This new method of information exchange has caused a tremendous need for information security. A thorough understanding of cryptography and encryption will help people develop better ways to protect valuable information as technology becomes faster and more efficient.

Introduction and Terminology

Cryptography

Cryptography is the science or study of techniques of secret writing and message hiding (Dictionary.com 2009). Cryptography is as broad as formal linguistics which obscure the meaning from those without formal training. It is also as specific as modern encryption algorithms used to secure transactions made across digital networks. Cryptography constitutes any method in which someone attempts to hide a message, or the meaning thereof, in some medium.

Encryption

Encryption is one specific element of cryptography in which one hides data or information by transforming it into an undecipherable code. Encryption typically uses a specified parameter or key to perform the data transformation. Some encryption algorithms require the key to be the same length as the message to be encoded, yet other encryption algorithms can operate on much smaller keys relative to the message. Decryption is often classified along with encryption as it's opposite. Decryption of encrypted data results in the original data.

Encryption is used in everyday modern life. Encryption is most used among transactions over insecure channels of communication, such as the internet. Encryption is also used to protect data being transferred between devices such as automatic teller machines (ATMs), mobile telephones, and many more. Encryption can be used to create digital signatures, which allow a message to be authenticated. When properly implemented, a digital signature gives the recipient of a message reason to believe the message was sent by the claimed sender. Digital signatures are very useful when sending sensitive email and other types of digital communication. This is relatively equivalent to traditional handwritten signatures, in that, a more complex signature carries a more complex method of forgery.

Cipher

A cipher is an algorithm, process, or method for performing encryption and decryption. A cipher has a set of well-defined steps that can be followed to encrypt and decrypt messages. The operation of a

cipher usually depends largely on the use of an encryption key. The key may be any auxiliary information added to the cipher to produce certain outputs.

Plaintext vs. Ciphertext

Plaintext and ciphertext are typically opposites of each other. Plaintext is any information before it has been encrypted. Ciphertext is the output information of an encryption cipher. Many encryption systems carry many layers of encryption, in which the ciphertext output becomes the plaintext input to another encryption layer. The process of decryption takes ciphertext and transforms it back into the original plaintext.

Cryptanalysis

In efforts to remain secure, Governments have employed staff for studying encryption and the breaking thereof. Cryptanalysis is the procedures, processes, and methods used to translate or interpret secret writings or communication as codes and ciphers for which the key is unknown (Dictionary.com 2009). Even though the goal has been the same, the methods and techniques of cryptanalysis have changed drastically through time. These changes derive from an attempt to adapt to the increasing complexity of cryptography.

Due to the tremendous advantage of knowing an enemies thoughts, war is the main driving force of cryptanalysis. Throughout history many governments have employed divisions solely for cryptanalysis during war time. Within the last century, governments have employed permanent divisions for this purpose.

Historical Cryptography

Ancient Egypt

The earliest known text containing components of cryptography originates in the Egyptian town Menet Khufu on the tomb of nobleman Khnumhotep II nearly 4,000 years ago. In about 1900 B.C. Khnumhotep's scribe drew his master's life in his tomb. As he drew the hieroglyphics he used a number of unusual symbols to obscure the meaning of the inscriptions. This method of encryption is an example of a substitution cipher, which is any cipher system which substitutes one symbol or character for another.

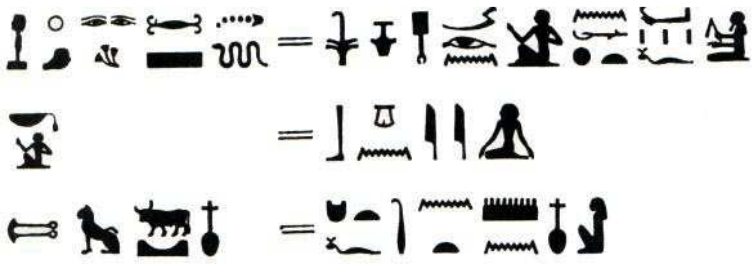


Figure 1. Symbols taken from the tomb of Khnumhotep II.

As the Egyptian culture evolved, hieroglyphic substitution became more common. This method of encryption was relatively easy to break for those who could read and write. There are several possibilities why the Egyptians would use this encryption system. It is likely that they wished to preserve the sacred nature of their religious rituals from common people. Another interpretation of Egyptian cryptography is that the scribes wanted to give a formal appearance to their writings. This seems to be very similar to formal complicated language used in any modern legal document. Egyptian cryptography could also have been a way for a scribe to impress others by showing that he could write at a higher level.

Greece

In about 500 B.C. the Spartans developed a device called Scytale, which was used to send and receive secret messages. The device was a cylinder in which a narrow strip of parchment was wound. The message was then written length-wise on the parchment. Once it was unwound the message on the strip of parchment became unreadable. To receive the message an identical cylinder was needed. It was only then that the letters would line up resulting in the original message.

Figure 2. Scytale example

The Scytale is an example of a transposition cipher, which is any cipher system that changes the order of the characters rather than changing the characters themselves. In today's standards, the Scytale would be very easy to decipher, however, 2,500 years ago the percent of people would could read and write was relatively small. The Scytale provided the Spartans a secure method of communication.

Rome

The earliest recorded military use of cryptography comes from Julius Caesar 2,000 years ago. Caesar, being commander of the Roman army, solved the problem of secure communication with his troops. The problem was that messengers of secret military messages were often overtaken by the enemy. Caesar developed a substitution cipher method in which he would substitute letters for different letters. Only those who knew the substitution used could decipher the secret messages. Now when the messengers were overtaken the secret messages were not exposed. This gave the Roman army a huge advantage during war.

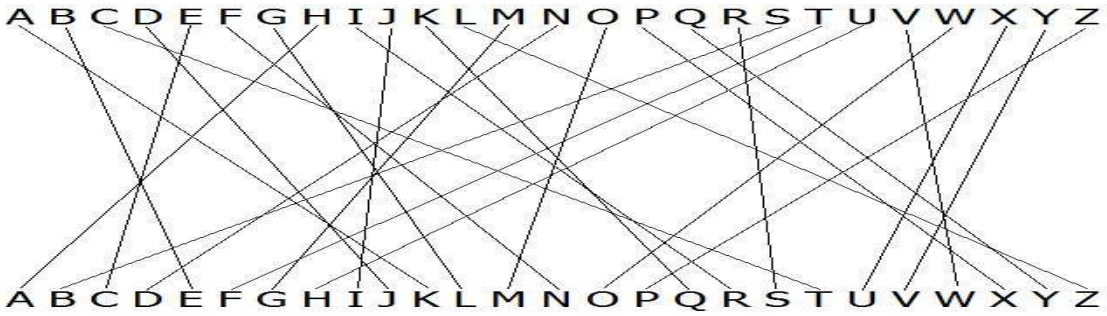


Figure 3. Example of a substitution cipher

Unlike the example found in Figure 3, Caesar typically just shifted his letters by some predetermined number. This number was the cipher key of his algorithm. A randomized order of substitution yields a much larger amount of security due to the larger amount of possible orderings.

Alberti-Vigenere Cipher

During the mid 1400's a man named Leon Battista Alberti invented an encryption system using a cipher disk. This was a mechanical device with sliding disks that allowed for many different methods of substitution. This is the base concept of a poly alphabetic cipher, which is an encryption method which switches through several substitution ciphers throughout encryption. In his book "The Codebreakers", David Kahn calls Alberti "the father of western cryptography" (Kahn 1967). Alberti never developed his cipher disk concept.

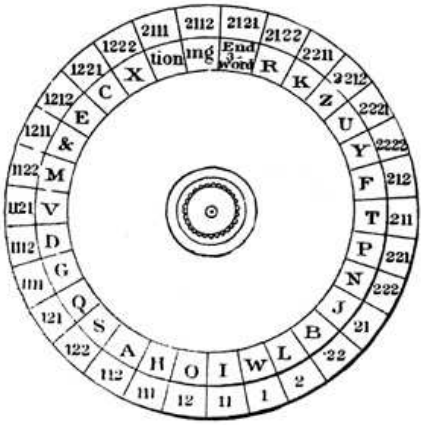


Figure 4. Cipher disk

In the 1500's Blaise De Vigenere, following Alberti's poly alphabetic cipher style, created a cipher that came to be known as the Vigenere Cipher. The Vigenere Cipher works exactly like the Caesar except that it changes the key throughout the encryption process. The Vigenere Cipher uses a grid of letters that give the method of substitution. This grid is called a Vigenere Square or a Vigenere Table. The grid is made up of 26 alphabets offset from each other by one letter.

	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

Figure 5. Vigenere Square

The method of changing from one key to another follows one simple pattern. The encryption key was chosen as a special secret word. The first character of the plaintext can be substituted using the table as follows: The substituted letter for the first plaintext character is found by lining up the plaintext character on the x-axis and the first letter of the special secret word on the y-axis. The corresponding letter is then substituted for the plaintext character. This method is repeated through all characters of the key word. After all characters of the key word are used, the word is just repeated.

For example, suppose that the plaintext to be encrypted is :

```
ATTACKATDAWN
```

The person encrypting the message chooses a keyword and repeats it until its length matches the plaintext. For example "LEMON."

```
LEMONLEMONLE
```

The first letter of the plaintext is enciphered using the alphabet in row *L*, which is the first letter of the keyword. The substitution is made by finding the letter in row *L* and column *A*, which is *L*. Moving to the next letter, the substitution is made by finding the letter in row *E* and column *T*, which is *X*. This is repeated until each plaintext character has been substituted. The results are:

Plaintext: `ATTACKATDAWN`
Keyword: `LEMONLEMONLE`
Ciphertext: `LXFOPVEFRNHR`

The decryption algorithm is the exact same except that the person finds the column that corresponds to the ciphertext's character in the keyword's row.

Jefferson Wheel Cipher

In the late 1700's, Thomas Jefferson came up with a cipher system very similar to the Vigenere Cipher except with higher security. His invention was 26 wheels with the alphabet randomly scattered on each wheel. The wheels were numbered and ordered with a specified order. This order is the key to the encryption algorithm.

Figure 6. Jefferson Wheel Cipher

To message to be encrypted is made on the wheels by lining up the wheels such that the message is present. The ciphertext is any other line besides the line containing the original message. The person decrypting the ciphertext must have the wheels in the proper order. As the ciphertext is made on the wheels, the plaintext is lined up somewhere else on the wheels. A visual scan can quickly result in finding the original text. There is an extremely small chance that two non-gibberish messages will emerge on the disk during decryption.

Similar to Alberti, Jefferson never developed his encryption system. During the early 1900's, the United States Army reinvented Jefferson's Wheel Cipher without any knowledge about Jefferson's invention. Jefferson was over a hundred years before his time. The United States Army used this system from 1923 to 1942 (Thinkquest.org 1999).

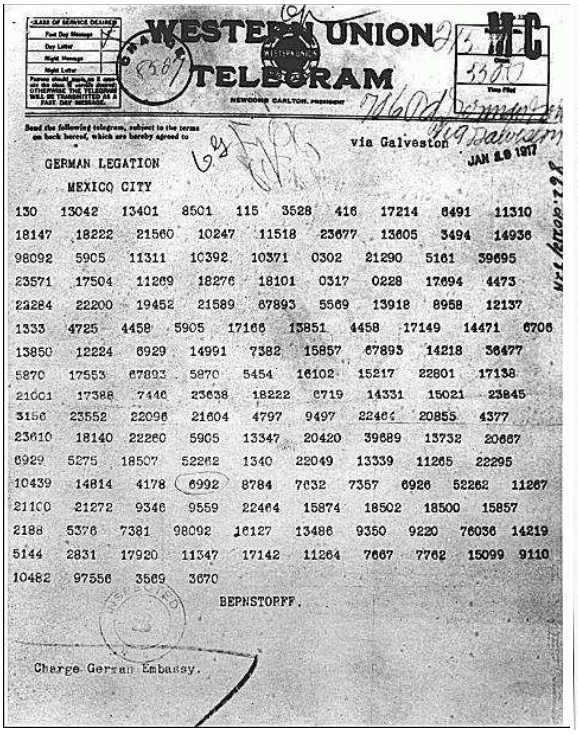
War Driven Cryptography - WWI

Zimmerman Telegram

In early 1917, during the early stages of World War I, British cryptographers encountered a German encoded telegram. This telegram is often referred to as the Zimmerman Telegram. These cryptographers were able to decipher the telegram, and in doing so they changed cryptanalysis history. Using this deciphered message, they were able to convince the United States to join the war.

The Zimmerman Telegram was a secret communication between the Foreign Secretary of the German Empire, Arthur Zimmerman, to the German ambassador in Mexico, Heinrich von Eckardt. The telegram contained an offer for Mexico to reclaim its territory of New Mexico, Texas, and Arizona if it joined the German cause. In spite of this offer, Mexico concluded that it would not be feasible or even desirable to take over their former territories.

At the time when the telegram was sent, World War I was at its height. Until that point, the United States had attempted to remain neutral. British, and other allies, had begged for help from the U.S., and attitudes in the US were slowly shifting towards war. The British gave the U.S. the decoded telegram on February 24, 1917 and on April 6, 1917 the U.S. officially declared war against Germany and its allies.


WESTERN UNION TELEGRAM

via Galveston

JAN 19 1917

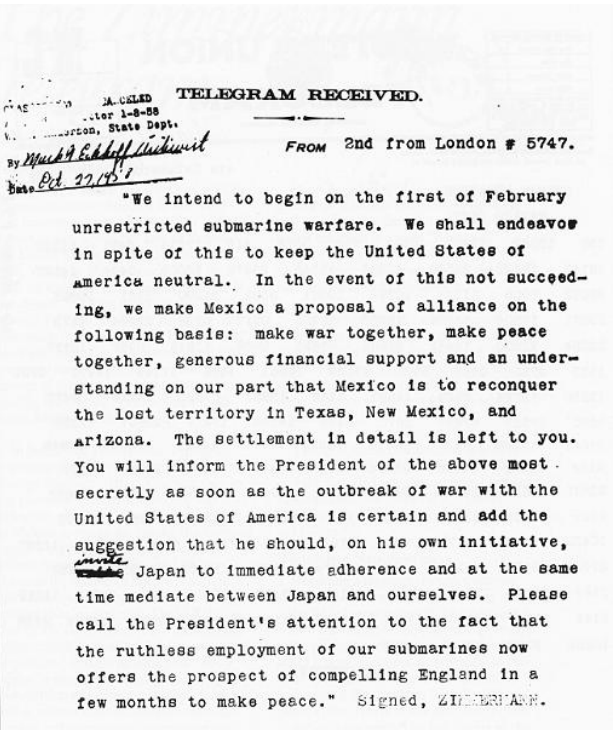
GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTORFF.

Charge German Embassy.


TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

Figure 7. Encoded Zimmerman Telegram

Figure 8. Decoded Zimmerman Telegram

Choctaw Codetalkers

As WWI went on, the United States had the continuing problem of the lack of secure communication. Almost every phone call made was intercepted by the Germans, leaving every move made by the allies known to the Germans. Army commander, Captain Lewis devised a plan that utilized American Indian languages. He found eight Choctaw men in the battalion and used them to talk to each other over radio and phone lines. Their language was valuable because ordinary codes and ciphers of a shared language can be broken, whereas codes based on a unique language must be studied extensively before beginning to decode them. Within 24 hours of using the Choctaw language as encryption, the advantage fell in favor of the United States. Within 72 hours, the Germans were retreating and the allies were in full attack.

War Driven Cryptography - WWII

Enigma Encryption Machine

At the end of World War I, Arthur Scherbius invented the Enigma, an electro-mechanical machine that was used for encryption and decryption of secret messages. The Enigma had several rotors and gears that allowed up to 10^{114} possible configurations. Because of the numerous configurations, the Enigma was virtually unbreakable with brute force methods. The first commercially available versions were available in the 1920's.

Figure 9. Enigma encryption machine used by Nazi Germany

It wasn't until World War II that the Enigma gained it's fame. Due to the Enigma's statistical security, Nazi Germany became overconfident about their ability to encrypt secret messages. This overconfidence caused the downfall of the Enigma. Along with numerous German operator errors, the Enigma had several built in weaknesses that Allied cryptographers exploited. The major weakness was that it's substitution algorithm did not allow any letter to be mapped to itself. This allowed the Allied cryptographers to decrypt a vast number of ciphered messages sent by Nazi Germans.

Purple

While the Allied forces were focusing on cracking the German Enigma, the Japanese developed an encryption machine called Purple. In contrast to the Enigma's rotors, Purple was made using stepping switches commonly used for routing telephone signals. During the war, the Japanese were most efficient in destroying their encryption machines. Currently, not one complete Purple machine has been discovered.

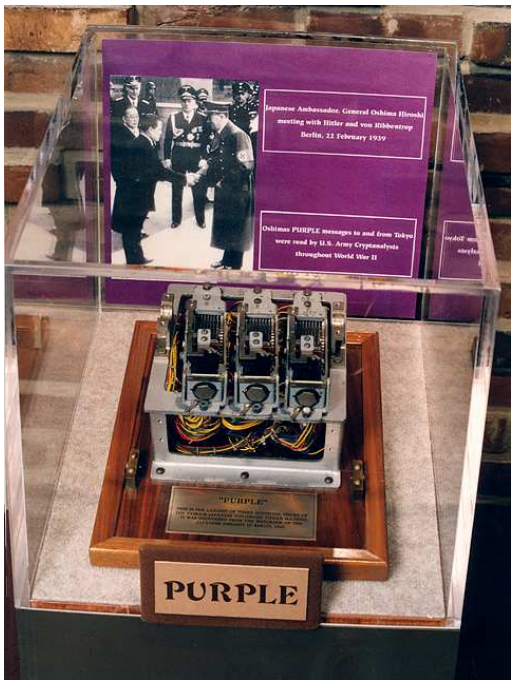


Figure 10. Purple encryption machine used by Japanese during WWII.

Because the Japanese were so good at keeping their encryption methods secret, the United States cryptographers had a hard time decrypting their messages. William Friedman, a renowned cryptographer, and his team built a replica of Purple based only on the encrypted messages recovered. Because they had never seen a Purple machine and didn't know how it worked, this proved to be very difficult. Eventually the team figured out the encryption method used by Purple, and were able to build a different machine for the decryption of it. This advancement allowed the United Stated access to Japanese diplomatic secrets in World War II.

Modern Encryption - Part 1

One-Time Pad

The "one-time pad" encryption algorithm was invented in the early 1900's, and has since been proven as unbreakable. The one-time pad algorithm is derived from a previous cipher called Vernam Cipher, named after Gilbert Vernam. The Vernam Cipher was a cipher that combined a message with a key read from a paper tape or pad. The Vernam Cipher was not unbreakable until Joseph Mauborgne recognized that if the key was completely random the cryptanalytic difficultly would be equal to attempting every possible key (Kahn 1996). Even when trying every possible key, one would still have to review each attempt at decipherment to see if the proper key was used. The unbreakable aspect of the one-time pad comes from two assumptions: the key used is completely random; and the key cannot be used more than once. The security of the one-time pad relies on keeping the key 100% secret.

The one-time pad is typically implemented by using a modular addition (XOR) to combine plaintext elements with key elements. An example of this is shown in Figure 11. The key used for encryption is also used for decryption. Applying the same key to the ciphertext results back to the plaintext.

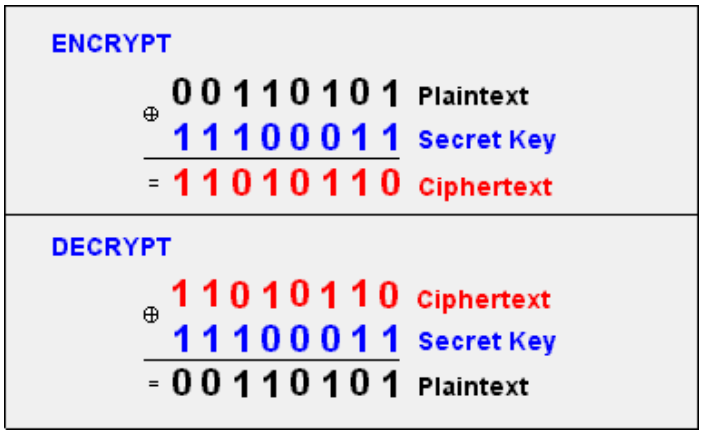


Figure 11. Example of a One-Time Pad implementation using modular addition.

Pseudo-Random Number Generator

If any non-randomness occurs in the key of a one-time pad, the security is decreased and thus no more unbreakable. Numerous attempts have been made to create seemingly random numbers from a designated key. These number generators are called Pseudo-Random Number Generators (PRNGs) because they cannot give a completely random number stream. Even though the security of a PRNG is not 100% unbreakable, it can provide sufficient security when implemented correctly. PRNGs that have been designated secure for cryptographic use are called Cryptographically Secure Pseudo-Random Number Generators (CSPRNGs). CSPRNGs have qualities that other PRNGs do not. CSPRNGs must pass the "next-bit test" in that given the first k bits, there is no polynomial-time algorithm that can predict the $(k+1)^{th}$ bit with probability of success higher than 50% (Knuth 1981). CSPRNGs must also withstand "state compromises." In the event that part or all of its state is revealed, it should be impossible to reconstruct the stream of random numbers prior to the revelation.

Symmetric Key Encryption (Private-Key)

Up to this point in the discussion, every method of encryption requires a special secret key to be previously and securely established. This is the nature of symmetric key encryption. A symmetric key, sometimes called private-key, encryption cipher is any algorithm in which the key for encryption is trivially related to the key used for decryption. An analogy of this is a typical mechanical lock. The same key that engages the lock can disengage it. To protect anything valuable behind the lock, the key must be given to each member securely. If an unintended person obtains access to the key, he or she will have full access to what is being secured by the lock.

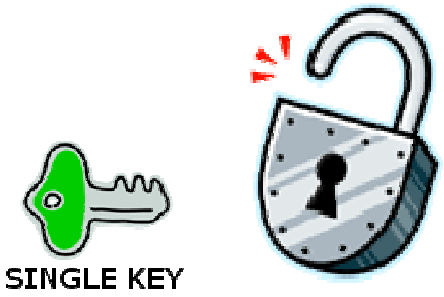


Figure 12. A lock that is engaged and disengaged by the same key.

Implementations of Symmetric Key Encryption

There are several modern algorithms that implement a symmetric key encryption scheme. One method of symmetric key encryption is a stream cipher, where a stream of random, or pseudo-random, numbers are combined with the original message. Specific stream ciphers include: One-Time Pad, Linear Feedback Shift Register (LFSR), Linear Congruential, and RC4. RC4 is the most widely-used stream cipher and is used in Secure Socket Layer (SSL) and Wired Equivalent Privacy (WEP).

Another method of symmetric key encryption is a block cipher, which operates on a fixed-length groups of bits. When encrypting, a block cipher takes a set amount of bits (i.e. 128-bit block) of plaintext and outputs a corresponding same size (i.e. 128-bit) block of ciphertext. The exact transformation of a block cipher is controlled by the encryption/decryption key. Popular block ciphers include: Blowfish, Twofish, DES, and AES . AES is an encryption standard adopted by the U.S. government and has been approved by the National Security Agency (NSA) for encryption of "top secret" information. Many current methods of symmetric key encryption employ both stream and block schemes.

Modern Encryption - Part 2

Asymmetric Key Encryption (Public-Key)

The digital era of the 1970's caused a need for an encryption system that would rely on a predetermined key. Cryptographers of this era realized that in order to send a message securely without previously meeting with the recipient, they would need a system that uses a different key for encryption than it does for decryption. In comparison with symmetric key encryption, this system would compare to a lock that has one key for engaging the lock and a different key for disengaging the lock.

Figure 13. A lock that is engaged and disengaged by different keys.

Diffie-Hellman Key Exchange

The Diffie-Hellman Key Exchange is a cryptographic protocol that allows two parties with no prior knowledge of each other to establish a shared secret key, which typically is used in a symmetric key cipher. The Diffie-Hellman Key Exchange was first published by Whitfield Diffie and Martin Hellman in 1976. The GCHQ, the British signals intelligence, announced that this scheme had been invented by Malcolm Williamson years before Diffie and Hellman's publication, but was kept classified.

The Diffie-Hellman Key Exchange relies on exponential functions computing much faster than discrete logarithms. When used properly, the Diffie-Hellman Key Exchange protocol gives two parties the same key without actually transmitting it. The strength of this algorithm depends on the time it takes to compute a discrete logarithm of the public keys transmitted (Diffie, Hellman 1976).

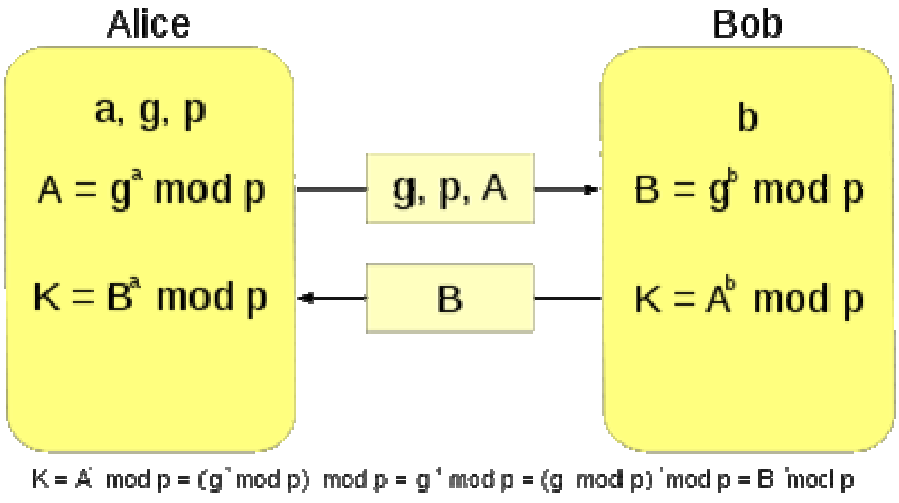


Figure 14. Diffie-Hellman Key Exchange protocol.

Figure 14 shows the steps for establishing a key through the Diffie-Hellman Key Exchange. Alice, wanting to establish a key with Bob, first sets up the variables "*a*", "*g*", and "*p*." Bob decides "b". After sending the public keys, or numbers, each party can compute "*K*." Notice that "*K*" is never sent through

the medium. Also notice that "*K*" was not previously determined, rather it was a result to both Alice and Bob's computations. This allows each party access to the same key without ever having to see each other. A disadvantage of the Diffie-Hellman key exchange is that it does not contain the function of encryption. A predetermined message cannot be inserted into the algorithm. The transmitted number is simply the result of computation, of which is purposely hard to decompose. In order for "*K*" to be discovered by someone besides Alice and Bob, a logarithm of "*A*" or "*B*" must be computed. When extremely large numbers for "*a*", "*b*", and "*p*" are chosen, it could take billions of years to compute the logarithm of "*A*" or "*B.*"

RSA Encryption

Noticing the inability of the Diffie-Hellman Key Exchange to transmit a secret message, Ron Rivest, Adi Shamir, and Leonard Adleman developed a system similar to the Diffie-Hellman protocol except that a message could be embedded and transmitted.

Figure 15. Ron Rivest, Adi Shamir, and Leonard Adleman

RSA encryption, named for the surnames of the inventors, relies on multiplication and exponentiation being much faster than prime factorization. The entire protocol is built from two large prime numbers. These prime numbers are manipulated to give a public key and private key. Once these keys are generated they can be used many times. Typically one keeps the private key and publishes the public key. Anyone can then encrypt a message using the public key and sent it to the creator of the keys. This person then uses the private key to decrypt the message. Only the one possessing the private key can decrypt the message. One of the special numbers generated and used in RSA encryption is the modulus, which is the product of the two large primes. In order to break this system, one must compute the prime factorization of the modulus, which results in the two primes. The strength of RSA encryption depends on the difficultly to produce this prime factorization. RSA Encryption is the most widely used asymmetric key encryption system used for electronic commerce protocols.

Breaking RSA Keys

The patent holder of RSA Encryption, RSA Security or RSA Laboratories, issued a challenge to encourage research into the practical difficulty of factorizing large integers. The motivation behind the challenge was to credit RSA Encryption to be a super power in the cryptography field. In 2007, RSA Laboratories ended the challenge stating: "Now that the industry has a considerably more advanced understanding of the cryptanalytic strength of common symmetric-key and public-key algorithms, these challenges are no longer active" (RSA Laboratories 2007).

During the activity of the RSA factoring challenge, RSA Laboratories published a list of semi-primes (numbers with exactly two prime factors) known as RSA numbers. Several of these numbers had cash prizes if they were successfully factored. Many of the smaller numbers were factored during the 1990's. During the early 2000's, a few decently large RSA numbers were factored, one of which took 80 computers 5 months to compute, and had a cash prize of $20,000. Some of the numbers that were never factored were worth $100,000 and $200,000. These larger numbers are estimated to take billions of years to factor on a single computer. In contrast, they can be generated in less than a minute.

Steganography

Security Through Obscurity

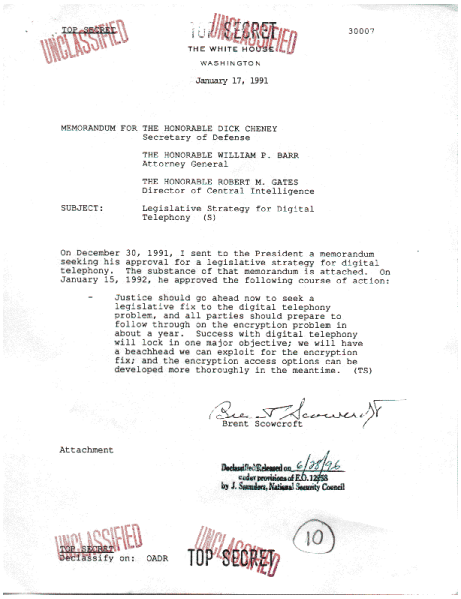
Steganography is a form of cryptography that embeds data into other mediums in an unnoticeable way, instead of employing encryption. Mediums used for steganography are typically human viewable objects such as picture, audio, and video files. Other steganographic mediums can include web pages, communication protocols, data streams, and many more. A very simple implementation of steganography could be invisible ink written between visible lines of text in a document.

Large scale steganography, performed with computers, is typically based on human undeterminable numbers. For example, the typical audio WAV file represents one audio sample with a 16-bit number ranging from 0 to 65535. A person could split up the secret message into it bits and embed them one at a time into each audio sample, thus only changing the amplitude of the sample by 1. This means that if an actual audio sample was represented by 12345 it could only change by one. The human ear is very far from hearing this change. In this way, the secret message is put into the audio file without noticeable change and without altering the file's size. A random person would not be able to tell that an embedded message even exists. This is where the phrase "security through obscurity" comes from. An encrypted message is easily seen as encrypted and a cryptographer can begin working on decrypting it. In comparison, a message embedded into a picture, audio, or video file can pass right by without being noticed.

Many people claim that the terrorist attack of September 11th 2001, among many, was planned using steganographic cryptography and the internet. Previous to the attack, USA Today said: "Lately, al-Qaeda operatives have been sending hundreds of encrypted messages that have been hidden in files on digital

photographs on the auction site eBay.com" (USA Today Feb. 5 2001). If this allegation is true, it seems it would be an effective way to hide secret information without more advanced countries discovering their work. Al-Qaeda would know that the U.S. could probably break any encryption they used, so the alternative method of steganography was a clever choice.

Steganographic Embedding



TOP SECRET UNCLASSIFIED

THE WHITE HOUSE
WASHINGTON

January 17, 1991

MEMORANDUM FOR THE HONORABLE DICK CHENEY
Secretary of Defense

THE HONORABLE WILLIAM P. BARR
Attorney General

THE HONORABLE ROBERT M. GATES
Director of Central Intelligence

SUBJECT: Legislative Strategy for Digital Telephony (S)

On December 30, 1991, I sent to the President a memorandum seeking his approval for a legislative strategy for digital telephony. The substance of that memorandum is attached. On January 15, 1992, he approved the following course of action:

- Justice should go ahead now to seek a legislative fix to the digital telephony problem, and all parties should prepare to follow through on the encryption problem in about a year. Success with digital telephony will lock in one major objective; we will have a beachhead we can exploit for the encryption fix; and the encryption access options can be developed more thoroughly in the meantime. (TS)

Brent Scowcroft

Attachment

Declassified/Released on 6/25/96
under provisions of E.O. 12958
by J. Saunders, National Security Council

TOP SECRET UNCLASSIFIED
Declassify on: OADR

TOP SECRET

Figure 16. Sample secret document to be embedded into Figure 17.

Figure 17. Before embedding of Figure 15.

Figure 18. After embedding of Figure 15.

Figure 16 shows a sample top secret document that is wished to be hidden. Figure 17 is the original picture and Figure 18 shows that picture after is has been embedded with the top secret document. As can be seen, the picture looks exactly the same to the human eye. If an analysis of the pictures binary

codes were compared, the differences would be seen. The inability to see precision in a given medium is the basis for steganography.

Future Methods of Encryption

Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) has technically already been invented but is considered by the author to be a future technique of cryptography because its advantages and disadvantages are not yet fully understood. ECC is an approach to encryption that utilizes the complex nature of elliptic curves in finite fields. ECC typically uses the same types of algorithms as that of Diffie-Hellman Key Exchange and RSA Encryption. The difference is that the numbers used are chosen from a finite field defined within an elliptic curve expression.

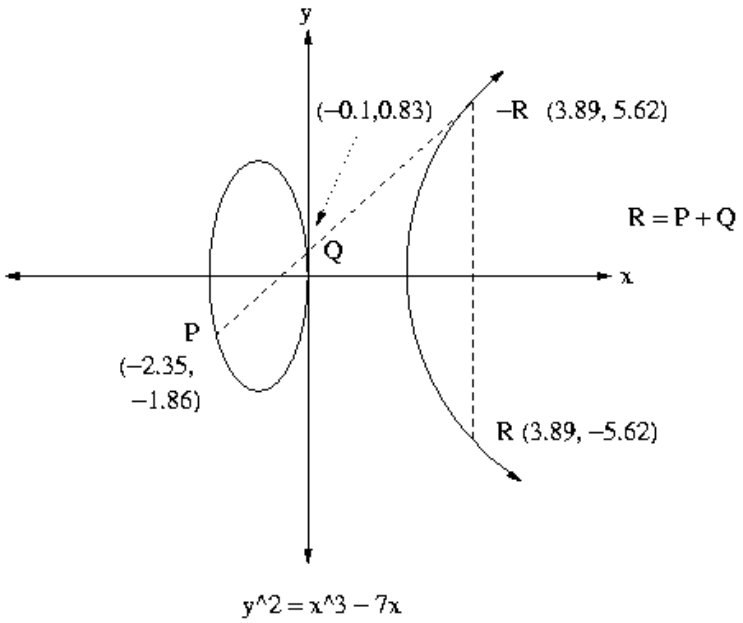


Figure 19. An elliptic curve graph

Figure 19 shows an example of an elliptic curve. This example could be used in conjunction with an RSA type algorithm in which two primes, "*P*" and "*Q*", are chosen. When the primes are chosen using a predefined elliptic curve in a finite field, the key sizes can be much smaller and still yield the same amount of security. This allows the time it takes to perform the encryption and decryption to be drastically reduced, thus allowing a higher amount of data to be passed with equal security. Just as other methods of encryption have, ECC must also be tested and proven secure before the it gets accepted for commercial, governmental, and private use.

Quantum Computation

Quantum computation is performed in a quantum computer or processor, which is a processor that makes use of quantum mechanical phenomena, such as quantum superposition and quantum entanglement. Modern computers store data using a binary format called a "bit" in which a "1" or a "0" can be stored. The computations in modern computers typically work in a bit by bit fashion. Quantum computers store data using a quantum superposition of multiple states. These multiple valued states are stored in "quantum bits" or "qubits." Depending on the quantum design, each qubit can store a set number values simultaneously (Jones 2009). This allows the computation of numbers to be several orders of magnitude faster than traditional transistor processors.

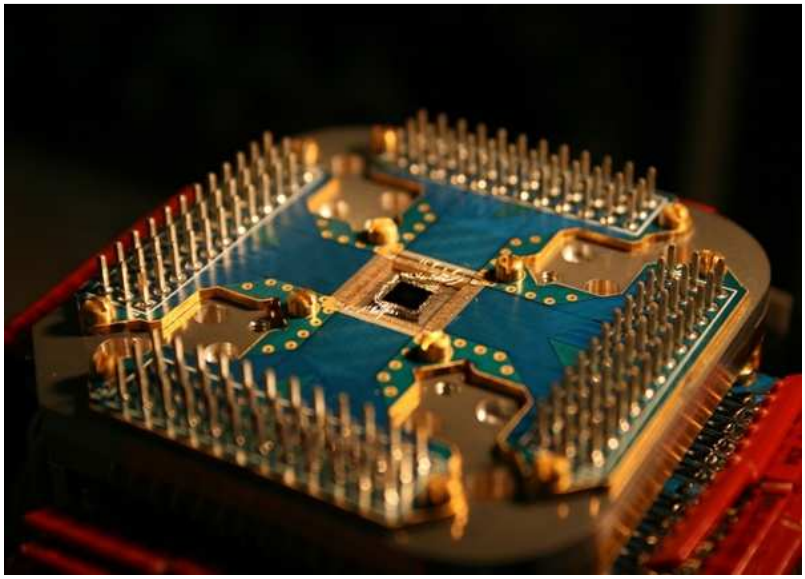


Figure 20. First commercially available quantum processor (D-Wave Systems)

Figure 20 shows the world's first commercially available quantum processor. It's capabilities are approximately 1000 times less than that of a modern transistor processor. Quantum computing is still in its infancy. Quantum processors manufactured today are very small and do not have the computational size that transistor processors have. Some fear that a successful and practical quantum computer would devastate the world's financial system by breaking every encryption system known (Jones 2009). As mentioned earlier, public-key cryptography relies on computer being slow to compute discrete logarithms and prime factorizations.

$$e^{\left[\left(\frac{64}{9}*b\right)^{\frac{1}{3}}(\log b)^{\frac{2}{3}}\right]}$$

Equation 1. GNFS algorithm time.

$$b^3$$

Equation 2. Shor's algorithm time.

Equation 1 shows the time it takes to run the fastest known algorithm (GNFS) to compute a prime factorization on a binary formatted processor. Equation 2 shows the algorithm discovered by Peter Shor that computes a prime factorization on a quantum computer. In both cases, "*b*" is the number of bits in the number. It's easily viewed that Shor's algorithm runs much faster. To comprehend the power of a

theoretical quantum computer, consider the RSA numbers previously mentioned. RSA-640, a number with 193 digits, was factored by 80 2.2GHz computers over the span of 5 months. If this RSA number was applied to one quantum computer of equal size, Shor's algorithm shows that it would be factored in less than 17 seconds. Numbers that would typically takes billions of years to compute could only take a matter of hours or even minutes with a fully developed quantum computer.

Conclusion

There has been a historical pattern that shows the country with the strongest encryption has been a leader in military power. By studying cryptography and encryption, a country could strengthen its defenses and have the necessary means to survive in a hostile world. An understanding of encryption can also help individuals with securing private data and information. Even though it is severely unethical, our communication with one another is constantly being monitored. Those who monitor our communication can include governments, internet service providers, hackers, identity thieves, and more. By learning to use cryptography for secure communication, we can safe guard ourselves from being compromised by those who could steal our information. Cryptography is illegal in many countries because the local government wishes to be able to read any transmission sent. Many people speculate that the United States does not need these laws because the NSA has developed methods of cryptanalysis that break all encryption methods currently known.

References

Brodney A, Asher J. Tales of the Encrypted [home page on the Internet]. Team 28005; 199. [cited 2009 May 5].

Available from: http://library.thinkquest.org/28005/flashed/index2.shtml.

Kahn D. The Codebreakers: The Story of Secret Writing. Scribner; 1996. 1181 p.

Knuth D E. The Art of Computer Programming: Semi-numerical Algorithms. Addison-Wesley; 1981. 688 p.

Diffie W, Hellman M. New Directions in Cryptography. Stanford University; 1976. 40 p.

Merkle R C. Secrecy, Authentication, and Public Key Systems. UMI Research Press; 1982. 104

RSA Laboratories. The RSA Factoring Challenge FAQ; [Internet] 2007. [cited 2009 May 2].

Available from: http://www.rsa.com/rsalabs/node.asp?id=2094.

Jones A Z. What Is a Quantum Computer? [Internet]. About.com-Physics; 2009 Mar. 11. [cited 2009 May 3].

Available from: http://physics.about.com/od/quantumphysics/f/quantumcomp.htm.