Fred Cohen & Associates

Specializing in Information Protection Since 1977

2.1 - A Short History of Cryptography

Cryptography is one of the oldest fields of technical study we can find records of, going back at least 4,000 years. It is quite noteworthy that of all the cryptosystems developed in those 4,000 years of effort, only 3 systems in widespread serious use remain hard enough to break to be of real value. One of them takes too much space for most practical uses, another is too slow for most practical uses, and the third is widely believed to contain serious weaknesses.

We begin with a classification scheme for ciphers given by Gary Knight [Knight78] in the first of a series of articles which posed ciphers to the reader, and after a given period of time demonstrated reader solutions along with explanations of how they solved the ciphers. Versions of the solutions attained by the author were also given along with many mathematical techniques for "attacking the unknown cipher".

```
Substitution
    Polyalphabetic
        Periodic
            Non-Interrelated Alphabets
            Interrelated Alphabets
            Pseudorandom Key
        Non-periodic
            Non-Random Key, Random Key
    Polygraphic
        Digraphic, Algebraic
    Monoalphabetic
        Standard, Mixed Alphabet, Homomorphic,
        Incomplete Mixed Alphabet, Multiplex, Double
    Fractionating
        Bifid, Trifid, Fractionated Morse, Morbit
Transposition
    Geometrical - Rail-fence, Route, Grille
    Columnar
        Complete - Cadenus, Nihilist
        Incomplete - Myskowski, Amsco
    Double - U.S. Army Transposition Cipher

   A Classification Scheme for Ciphers
```

With the exception of the random-key cipher (which is provably unbreakable), examples from each of the systems listed above have yielded to cryptanalysis (analytical attack on secret writing).
Cryptography probably began in or around 2000 B.C. in Egypt, where hieroglyphics were used to decorate the tombs of deceased rulers and kings. These hieroglyphics told the story of the life of the king and proclaimed the great acts of his life. They were purposefully cryptic, but not apparently intended to hide the text. Rather, they seem to have been intended to make the text seem more regal and important. As time went by, these writings became more and more complicated, and eventually the people lost interest in deciphering them. The practice soon died out.

Cryptology was (and still is to some extent) enshrouded in a vail of mystique to most people. It was because of this that the public began to acquaint cryptography with the black arts. It was often thought to be concerned with communication with dark spirits, and developed a bad image because of it's mentors. Most early cryptographers were scientists, but the common people were often convinced that they were also followers of the devil.

The ancient Chinese used the ideographic nature of their language to hide the meaning of words. Messages were often transformed into ideographs for privacy, but no substantial use in early Chinese military conquests are apparent. Genghis Khan, for example, seems never to have used cryptography.
In India, secret writing was apparently more advanced, and the government used secret codes to communicate with a network of spies spread throughout the country. Early Indian ciphers consisted mostly of simple alphabetic substitutions often based on phonetics. Some of these were spoken or used as sign language. This is somewhat similar to "pig latin" (igpay atinlay) where the first consenant is placed at the end of the word and followed by the sound "ay".

The cryptographic history of Messopotamia was similar to that of Egypt, in that cuneiforms were used to encipher text. This technique was also used in Babylon and Asyria. In the Bible, a Hebrew ciphering method is used at times. In this method, the last letter of the alphabet is replaced by the first, and vice versa. This is called 'atbash'. For example, the following table gives a translation of this sort for English. The word "HELLO" becomes "SVOOL". Try to decrypt the word "WVXIBKG" and see what you get.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZYXWVUTSRQPONMLKJIHGFEDCBA
```

Figure 2.1 - An ATBASH Cipher

In the famous Greek drama the 'Iliad', cryptography was used when Bellerophon was sent to the king with a secret tablet which told the king to have him put to death. The king tried to kill him by having him fight several mythical creatures, but he won every battle.

The Spartans used a system which consisted of a thin sheet of papyrus wrapped around a staff (now called a "staff cipher"). Messages were written down the length of the staff, and the papyrus was unwrapped. In order to read the message, the papyrus had to be wrapped around a staff of equal diameter. Called the 'skytale' cipher, this was used in the 5th century B.C. to send secret messages between greek warriors. Without the right staff, it would be difficult to decode the message using the techniques available at that time. The following version of the alphabet demonstrates the technique. First we see the wrapped version of the alphabet, then the unwrapped version.

```
            ADGJMPSVY
            BEHKNQTWZ
            CFILORUX

        ADGJMPSVYBEHKNQTWZCFILORUX
```

Figure 2.2 - A Skytale Cypher

Another Greek method was developed by Polybius (now called the "Polybius Square"). The letters of the alphabet would be laid out in a five by five square (similar to the later Playfair method) with i and j occupying the same square. Rows and columns are numbered 1 to 5 so that each letter has a corresponding (row,column) pair. These pairs could easily be signaled by torches or hand signals. Decryption consists of mapping the digit pairs back into their corresponding characters. This system was the first to reduce the size of the symbol set, and in a loose sense it might be considered the forerunner of modern binary representations of characters. Try decoding the message on the right.

```
        \ 1 2 3 4 5
         \_________
        1|A B C D E        T=54
        2|F G H I J        H=32     5344 44 4435
        3|K L M N O        I=42     4224 24 3211
        4|P Q R S T        S=44
        5|U V W X Y/Z
```

Figure 2.3 - The Polybius Square (slightly modified)

Julius Ceasar used a system of cryptography (i.e. the 'Caesar Cipher') which shifted each letter 2 places further through the alphabet (e.g. Y shifts to A, R shifts to T, etc.). This is probably the first cipher used by most school children. In figure 2.4, the first row is plaintext, while the second row is the equivalent ciphertext. The distance of the displacement is not important to the scheme, and in fact, neither is the lexical ordering chosen. The general case of this sort of cipher is the "monoalphabetic substitution cipher" wherein each letter is mapped into another letter in a one to one fashion. Try decoding VJKU.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
CDEFGHIJKLMNOPQRSTUVWXYZAB
```

Figure 2.4 - The Caesar Cypher

Cryptanalysis is the practice of changing ciphertext into plaintext without complete knowledge of the cipher. The Arabs were the first to make significant advances in cryptanalysis. An Arabic author, Qalqashandi, wrote down a technique for solving ciphers which is still used today. The technique is to write down all the ciphertext letters and count the frequency of each symbol. Using the average frequency of each letter of the language, the plaintext can be written out. This technique is powerful enough to cryptanalyze ANY monoalphabetic substitution cipher if enough cyphertext is provided.

During the Middle Ages, cryptography started to progress. All of the Western European governments used cryptography in one form or another, and codes started to become more popular. Ciphers were commonly used to keep in touch with ambassadors. The first major advances in cryptography were made in Italy. Venice created an elaborate organization in 1452 with the sole purpose of dealing with cryptography. They had three cipher secretaries who solved and created ciphers that were used by the government.

Leon Battista Alberti is was known as "The Father of Western Cryptology" in part because of his development of polyalphabetic substitution. Polyalphabetic substitution is any technique which allows different ciphertext symbols to represent the same plaintext symbol. This makes it more difficult to interpret ciphertext using frequency analysis. In order to develop this technique, Alberti analyzed the methods for breaking ciphers, and devised a cipher which would try to render these techniques invalid. He designed two copper disks that fit into each other, each with the alphabet inscribed upon it. To start enciphering, a predetermined letter on the inner disk is lined up with any letter on the outer disk, which is written as the first character of the ciphertext. The disks are kept stationary, with each plaintext letter on the inner disk aligned with a ciphertext letter on the outer disk. After a few words of ciphertext, the disks are rotated so that the index letter on the inner disk is aligned with a new letter on the outer disk, and in this manner, the message is enciphered. By rotating the disk every few words, the cipher changed enough to limit the effectiveness of frequency analysis. Even though this technique in its stated form is very weak, the idea of rotating the disks and therefore changing the cipher many times within a message was a major breakthrough in cryptography.

The next major step was taken in 1518, by Trithemius, a German monk who had a deep interest in the occult. He wrote a series of six books called 'Polygraphia', and in the fifth book, devised a table that repeated the alphabet with each row a duplicate of the one above it, shifted over one letter. To encode a message, the first letter of the plaintext is enciphered with the first row of the table, the second letter with the second row, and so on. This produces a message where all available ciphers are used before being repeated. Figure 2.5 shows a changing key cipher of this sort. Notice that the assignment of code symbols to plaintext symbols changes at each time step (T1,T2,...). In this system, the key repeats every 26 letters of ciphertext.

```
        ABCDEFGHIJKLMNOPQRSTUVWXYZ Plaintext
        FGUQHXSZACNDMRTVWEJBLIKPYO T00
        OFGUQHXSZACNDMRTVWEJBLIKPY T01
        YOFGUQHXSZACNDMRTVWEJBLIKP T02
        PYOFGUQHXSZACNDMRTVWEJBLIK T03
            ...
        GUQHXSZACNDMRTVWEJBLIKPYOF T25
```

Figure 2.5 - A Changing Key Cipher

In 1553, Giovan Batista Belaso extended this technique by choosing a keyword that is written above the plaintext, in a letter to letter correspondence. The keyword is restarted at the beginning of each new plaintext word. The letter of the keyword above the letter of the plaintext is the first letter of the cipher line to be used. In other words, if the plaintext letter is 'b', and it's keyword letter is 'r', then the line of the Trithemius cipher beginning with 'r' is used to encipher the letter 'b'.

The most famous cryptographer of the 16th century was Blaise de Vigenere (1523-1596). In 1585, he wrote 'Tracte des Chiffres' in which he used a Trithemius table, but changed the way the key system worked. One of his techniques used the plaintext as it's own key. Another used the ciphertext. The manner in which these keys are used is known as key scheduling, and is an integral part of the "Data Encryption Standard" (DES) [DESDOC77] which we will discuss later.

In 1628, a Frenchman named Antoine Rossignol helped his army defeat the Huguenots by decoding a captured message. After this victory, he was called upon many times to solve ciphers for the French government. He used two lists to solve his ciphers: "one in which the plain elements were in alphabetical order and the code elements randomized, and one to facilitate decoding in which the code elements stood in alphabetical or numerical order while their plain equivalents were disarranged." When Rossignol died in 1682, his son, and later his grandson, continued his work. By this time, there were many cryptographers employed by the French government. Together, they formed the "Cabinet Noir" (the "Black Chamber").
By the 1700's, "Black Chambers" were common in Europe, one of the most renown being that in Vienna. It was called 'The Geheime Kabinets-Kanzlei' and was directed by Baron Ignaz de Koch between 1749 and 1763. This organization read through all the mail coming to foreign embassies, copied the letters, resealed them, and returned them to the post-office the same morning. The same office also handled all other political or military interceptions, and would sometimes read as many as 100 letters a day. The English Black Chamber was formed by John Wallis in 1701. Until that time, he had been solving ciphers for the government in a variety of unofficial positions. After his death in 1703, his grandson, William Blencowe, who was taught by his grandfather, took over his position and was granted the title of Decypherer. The English Black Chamber had a long history of victories in the cryptographic world.

In the colonies, there was no centralized cryptographic organization. Decryption was done predominantly by interested individuals and men of the cloth. In 1775, a letter intercepted from Dr. Benjamin Church was suspected to be a coded message to the British, yet the American revolutionaries could not decipher it. Their problem was solved by Elbridge Gerry, who later became the fifth Vice-President, and Elisha Porter. The message proved Church guilty of trying to inform the Tories, and he was later exiled. Benedict Arnold used a code wherein each correspondent has an exact copy of the same 'codebook'. Each word of plaintext is replaced by a number indicating its position in the book (e.g. 3.5.2, means page 3, line 5, word 2). Arnold's correspondent was caught and hung, so the codebook wasn't used very much. The revolutionaries also employed ciphers during the war. Samuel Woodhull and Robert Townsend supplied General George Washington with much information about British troop strength and movements in and around New York City. The code they used consisted of numbers which replaced plaintext words. This code was written by Major Benjamin Tallmadge. For further assurance, they also used invisible ink.

The father of American cryptology is James Lovell. He was loyal to the colonies, and solved many British ciphers, some which led to Revolutionary victories. In fact, one of the messages that he deciphered set the stage for the final victory of the war.

Former Vice-President Aaron Burr and his assistant General James Wilkinson were exploring the Southwest for possible colonization at the expense of Spain, and there was some confusion as to whether this colony would belong to the United States or Aaron Burr. Wilkinson was a Spanish agent, and changed one of Burr's encrypted letters home to make it appear as if Burr's intentions were to carve out his own country. This letter fell into the hands of President Thomas Jefferson. Burr was tried and acquitted, but his name was tainted forever.

The 'wheel cipher' was invented by Thomas Jefferson around 1795, and although he never did very much with it, a very similar system was still in use by the US navy only a few years ago. The wheel cipher consisted of a set of wheels, each with random orderings of the letters of the alphabet. The key to the system is the ordering in which the wheels are placed on an axle. The message is encoded by aligning the letters along the rotational axis of the axle such that the desired message is formed. Any other row of aligned letters can then be used as the ciphertext for transmission. The decryption requires the recipient to align the letters of the ciphertext along the rotational axis and find a set of aligned letters that makes linguistic sense as plaintext. This will be the message. There is a very small probability that there will be two sensible messages from the decryption process, but this can be checked simply by the originator. Without knowing the orderings of symbols on the wheels and the ordering of wheels on the axle, any plaintext of the appropriate length is possible, and thus the system is quite secure for one time use. Statistical attacks are feasible if the same wheels are used in the same order many times.

```
        GJTXUVWCHYIZKLNMARBFDOESQP
 W1
        IKMNQLPBYFCWEDXGZAJHURSTOV
 W2
        HJLIKNXWCGBDSRVUEOFYPAMQZT
 W3
                   ...
        BDFONGHJIKLSTVUWMYEPRQXZAC
 Wn
```

Figure 2.6 - A Wheel Cipher

In 1817, Colonel Decius Wadsworth developed a set of two disks, one inside the other, where the outer disk had the 26 letters of the alphabet, and the numbers 2-8, and the inner disk had only the 26 letters. The disks were geared together at a ratio of 26:33. To encipher a message, the inner disk is turned until the desired letter is at the top position, with the number of turn required for this result transmitted as ciphertext. Because of the gearing, a ciphertext substitution for a character will not repeat itself until all 33 characters for that plaintext letter have been used. Unfortunately, Wadsworth never got credit for his design, because Charles Wheatstone invented an almost identical machine a few years after Wadsworth, and got all the credit.

In 1844, the development of cryptography was dramatically altered by the invention of the telegraph. Communication with the telegraph was by no means secure, so ciphers were needed to transmit secret information. The public's interest in cryptography blossomed, and many individuals attempted to formulate their own cipher systems. The advent of the telegraph provided the first instance where a base commander could be in instant communication with his field commanders during battle. Thus, a field cipher was needed. At first, the military used a Vigenere cipher with a short repeating keyword, but in 1863, a solution was discovered by Friedrich W. Kasiski for all periodic polyalphabetic ciphers which up until this time were considered unbreakable, so the military had to search for a new cipher to replace the Vigenere.

The Black Chambers of Europe continued to operate and were successful in solving most American ciphers, but without a war underway, their usefulness was diminished, and by 1850 they were dissolved.

The 'Playfair' system was invented by Charles Wheatstone and Lyon Playfair in 1854, and was the first system that used pairs of symbols for encryption. The alphabet is laid out in a random 5 x 5 square, and the text is divided into adjacent pairs. The two letters of the pair are located, and a rectangle is formed with the two letters at opposite corners. The letters at the other two corners are the two letters of ciphertext. This is very simple to use, but is not extremely difficult to break. The real breakthrough in this system was the use of two letters at a time. The effect is to make the statistics of the language less pronounced, and therefore to increase the amount of work and the amount of ciphertext required to determine a solution. This system was still in limited use in world war 2, and was very effective against the Japanese.

```
    IKMNQ
    LPBYF
 PLAINTEXT =  PL AI NT EX TZ
    CWEDX       =              =
    GZAHU
 LPMGMOXEAS = LP MG MO XE AS
    RSTOV
```

Figure 2.7 - A Playfair System

In 1859, Pliny Earle Chase, developed what is known as the fractionating or tomographic cipher. A two digit number was assigned to each character of plaintext by means of a table. These numbers were written so that the first numbers formed a row on top of the second numbers. The bottom row was multiplied by nine, and the corresponding pairs are put back in the table to form the ciphertext.

Kasiski developed a cryptanalysis method in 1863 which broke almost every existing cipher of that time. The method was to find repetitions of strings of characters in the ciphertext. The distance between these repetitions is then used to find the length of the key. Since repetitions of identically ciphered identical plaintext occur at distances which are a multiple of the key length, finding greatest common divisors of repetition distances will lead to the key length. Once the key length (N) is known, we use statistics on every Nth character and the frequency of use implies which character it represents in that set of ciphertext symbols. These repetitions sometimes occur by pure chance, and it sometimes takes several tries to find the true length of the key using this method, but it is considerably more effective than previous techniques. This technique makes cryptanalysis of polyalphabetic substitution ciphers quite straight forward.

During the Civil War (1861-1865), ciphers were not very complex. Many techniques consisted merely of writing words in a different order and substituting code words for proper names and locations. Where the Union had centralized cipher control, the Confederacy tended to let field commanders decide their own forms of ciphers. The Vigenere system was widely used by field commanders, and sometimes led to the Union deciphering messages faster than their Confederate recipients. The Confederacy used three keywords for most of its messages during the War, "Manchester Bluff", "Complete Victory", and "Come Retribution". They were quickly discovered by three Union cryptanalysts Tinker, Chandler, and Bates, and messages encoded using them were regularly deciphered by the Union. The use of common words as keys to cryptosystems has caused many plaintext messages to be discovered. In fact, the use of common words for passwords is the most common entry point in modern computer system attacks.

In 1883, Auguste Kerckhoffs wrote 'La Cryptographie Militaire' in which he set forth six basic requirements of cryptography. We note that the easily remembered key is very amenable to attack, and that these rules, as all others, should be questioned before placing trust in them.

ciphertext should be unbreakable in practice
the cryptosystem should be convenient for the correspondents
the key should be easily remembered and changeable
the ciphertext should be transmissible by telegraph
the cipher apparatus should be easily portable
the cipher machine should be relatively easily to use

In the beginning of the 20th century, war was becoming likely in Europe. England spent a substantial effort improving its cryptanalytic capabilities so that when the war started, they were able to solve most enemy ciphers. The cryptanalysis group was called 'Room 40' because of its initial location in a particular building in London. Their greatest achievements were in solving German naval ciphers. These solutions were greatly simplified because the Germans often used political or nationalistic words as keys, changed keys at regular intervals, gave away intelligence indicators when keys were changed, etc.

Just as the telegraph changed cryptography in 1844, the radio changed cryptography in 1895. Now transmissions were open for anyone's inspection, and physical security was no longer possible. The French had many radio stations by WW1 and intercepted most German radio transmissions. The Germans used a double columnar transposition that they called 'Ubchi', which was easily broken by French cryptanalysts.

In 1917, the Americans formed the cryptographic organization MI-8. It's director was Herbert Osborne Yardley. They analyzed all types of secret messages, including secret inks, encryptions, and codes. They continued with much success during and after WW1, but in 1929, Herbert Hoover decided to close them down because he thought it was improper to "read others' mail". Yardley was hard pressed to find work during the depression, so to feed his family, he wrote a book describing the workings of MI-8. It was titled "The American Black Chamber", and became a best seller. Many criticized him for divulging secrets and glorifying his own actions during the War. Another American, William Frederick Friedman, worked with his wife, Elizebeth Smith, to become "the most famous husband-and-wife team in the history of cryptology". He developed new ways to solve Vigenere-like ciphers using a method of frequency counts and superimposition to determine the key and plaintext.

Up to 1917, transmissions sent over telegraph wires were encoded in Baudot code for use with teletypes. The American Telephone and Telegraph company was very concerned with how easily these could be read, so Gilbert S. Vernam developed a system which added together the plaintext electronic pulses with a key to produce ciphertext pulses. It was difficult to use at times, because keys were cumbersome. Vernam developed a machine to encipher messages, but the system was never widely used.

The use of cryptographic machines dramatically changed the nature of cryptography and cryptanalysis. Cryptography became intimately related to machine design, and security personnel became involved with the protection of these machines. The basic systems remained the same, but the method of encryption became reliable and electromechanical.

In 1929, Lester S. Hill published an article "Cryptography in an Algebraic Alphabet" in "The American Mathematical Monthly". Each plaintext letter was given a numerical value. He then used polynomial equations to encipher plaintext, with values over 25 reduced modulo 26. To simplify equations, Hill transformed them into matrices, which are more easily multiplied. This method eliminates almost all ciphertext repetitions, and is not broken with a normal frequency analysis attack. It has been found that if a cryptanalyst has two different ciphertexts from the same plaintext, and if they use different equations of the same type, the equations can be solved, and the system is thus broken. To counter charges that his system was too complicated for day to day use, Hill constructed a cipher machine for his system using a series of geared wheels connected together. One problem was that the machine could only handle a limited number of keys, and even with the machine, the system saw only limited use in the encipherment of government radio call signs. Hill's major contribution was the use of mathematics to design and analyze cryptosystems.

The next major advance in electromechanical cryptography was the invention of the rotor. The rotor is a thick disk with two faces, each with 26 brass contacts separated by insulating material. Each contact on the input (plaintext) face is connected by a wire to a random contact on the output (ciphertext) face. Each contact is assigned a letter. An electrical impulse applied to a contact on the input face will result in a different letter being output from the ciphertext face. The simple rotor thus implements a monoalphabetic substitution cipher. This rotor is set in a device which takes plaintext input from a typewriter keyboard and sends the corresponding electrical impulse into the plaintext face. The ciphertext is generated from the rotor and printed and/or transmitted.

The next step separates the rotor from previous systems. After each letter, the rotor is turned so that the entire alphabet is shifted one letter over. The rotor is thus a "progressive key polyalphabetic substitution cipher with a mixed alphabet and a period of 26". A second rotor is then added, which shifts it's position one spot when the first rotor has completed each rotation. Each electrical impulse is driven through both rotors so that it is encrypted twice. Since both rotors move, the alphabet now has a period of 676. As more rotors are added the period increases dramatically. With 3 rotors, the period is 17,576, with 4 it is 456,976, and with 5 it is 11,881,376. In order for a 5 rotor cipher to be broken with frequency analysis, the ciphertext must be extremely long.

The rotor system can be broken because, if a repetition is found in the first 26 letters, the cryptanalyst knows that only the first rotor has moved, and that the connections are changed only by that movement. Each successive set of 26 letters has this property, and using equations, the cryptanalyst can completely determine this rotor, hence eliminating one rotor from the whole problem. This can be repeated for each successive rotor as the previous rotor becomes known, with the additional advantage that the periods become longer, and thus they are guaranteed to have many repetitions. This is quite complex to do by hand. The first rotor machine was invented by Edward Hugh Hebern in 1918, and he instantly realized what a success it could be. He founded a company called Hebern Electric Code, which he promised would be a great financial success.

The company died in a bitter struggle, the Government bought some of his machines, and he continued to produce them on his own, but never with great success.

During Prohibition, alcohol was transported into the country by illegal smugglers (i.e. rum runners) who used coded radio communication to control illegal traffic and help avoid Coast Guard patrols. In order to keep the Coast Guard in the dark, the smugglers used an intricate system of codes and ciphers. The Coast Guard hired Mrs. Elizebeth Smith Friedman to decipher these codes, and thus forced the rum runners to use more complex codes, and to change their keys more often. She succeeded in sending many rum runners to jail.

During WW2, the neutral country Sweden had one of the most effective cryptanalysis departments in the world. It was formed in 1936, and by the time the war started, employed 22 people. The department was divided into groups, each concerned with a specific language. The Swedes were very effective in interpreting the messages of all the warring nations. They were helped, however, by bungling cryptographers. Often the messages that were received were haphazardly enciphered, or even not enciphered at all. The Swedes even solved a German cipher that was implemented on a Siemens machine similar to a Baudot machine used to encipher wired messages.

During WW2, the Americans had great success at breaking Japanese codes, while the Japanese, unable to break US codes, assumed that their codes were also unbreakable. Cryptanalysis was used to thwart the Japanese attack on Midway, a decisive battle in the South Pacific. The US had been regularly reading Japanese codes before the attack on Pearl Harbor, and knew of the declaration of war that was presented to the President just after the attack on Pearl Harbor, several hours before the Japanese embassy in Washington had decoded it. German codes in WW2 were predominantly based on the 'Enigma' machine, which is an extension of the electromechanical rotor machine discussed above. A British cryptanalysis group, in conjunction with an escaped group of Polish cryptanalysts, first broke the Enigma early in WW2, and some of the first uses of computers were for decoding Enigma ciphers intercepted from the Germans. The fact that these codes were broken was of such extreme sensitivity, that advanced knowledge of bombing raids on England was not used to prepare for the raids. Instead, much credit was given to radar, and air raids were given very shortly before the bombers arrived.

In 1948, Shannon published "A Communications Theory of Secrecy Systems" [Shannon49] . Shannon was one of the first modern cryptographers to attribute advanced mathematical techniques to the science of ciphers. Although the use of frequency analysis for solving substitution ciphers was begun many years earlier, Shannon's analysis demonstrates several important features of the statistical nature of language that make the solution to nearly all previous ciphers very straight forward. Perhaps the most important result of Shannon's famous paper is the development of a measure of cryptographic strength called the 'unicity distance'.

The unicity distance is a number that indicates the quantity of ciphertext required in order to uniquely determine the plaintext of a message. It is a function of the length of the key used to encipher the message and the statistical nature of the plaintext language. Given enough time, it is guaranteed that any cipher can be broken given a length of ciphertext such that the unicity distance is 1. The unicity distance is computed as:

H(K)/(|M|-H(M))
where H(K) is the information content [Shannon48] of the key, H(M) is the information content per symbol of the message, and |M| is the information content per symbol of the message assuming that all symbols are equally likely. If K is chosen at random, H(K)=|K|, so for randomly chosen letters in English, H(K)=|K|=log2(26)=4.7 bits. For a 26 letter alphabet, |M|=4.7 bits. After a lot of statistical analysis of text, H(M) was imperically found to be 2.9 bits for English, and thus the unicity distance for English is 1 when |M| is (4.7/1.8)*|K|. In other words, any time the length of all messages sent under a particular key in English exceeds 2.6 times the length of that key, the key and plaintext can eventually be determined.

Shannon noted that in a system with an infinite length random key, the unicity distance is infinite, and that for any alphabetic substitution cipher with a random key of length greater than or equal to the length of the message, plaintext cannot be derived from ciphertext alone. This type of cipher is called a "one-time-pad", because of the use of pads of paper to implement it in WW2 and before.

The story of cryptography would be at an end if it weren't for the practical problem that in order to send a secret message, an equal amount of secret key must first be sent. This problem is not severe in some cases, and it is apparently used in the hot line between Moscow and Washington [Kahn67] , but it is not the ultimate solution for many practical situations.

For most human (and computer) languages, a key of a given length can only be guaranteed safe for 2-3 times the length of the key. From this analysis, it appears that any system with a finite key is doomed to failure, but several issues remain to be resolved before all hope for finite key cryptography is abandoned. By looking at Shannon's equation, we may find ways out of our delema.

The first line of exploration is to reduce the redundancy of the language to extend the length of ciphertext required for solution. From Shannon's equation, we see that as the content of a message approaches its actual length, the divisor goes to 0, and thus the length of ciphertext required to determine the plaintext goes to infinity. Data compression techniques [Huffman52] may be practically used to remove 99.9% of the redundancy of plaintext with a reasonable degree of efficiency, and we can thus easily generate systems in which the unicity distance goes to |K|/|M|*0.001 which is 1 when |M|=1000*|K|. For a key of 64 bits in length, we could expect to safely encipher up to 64,000 bits of information, or about 8 pages of double spaced text before the system becomes theoretically breakable. We could easily replace a 64 bit key every 4 pages of text to make breaking the system nearly impossible, assuming we can store and distribute a sequence of truly random keys.

Shannon assures us that systems are breakable with sufficient ciphertext, but also introduces the concept of "workload", which embodies the difficulty in determining plaintext from ciphertext given the availability of enough ciphertext to theoretically break the system. An alternative to increasing unicity distance is the use of systems that tend to increase the workload required to determine solutions to cryptograms. Two important concepts due to Shannon's paper are the "diffusion" and "confusion" properties. These form the basis for many modern cryptosystems because they tend to increase the workload of cryptanalysis.

Diffusion is the dissipation of the statistical structure behind the language being transmitted. As an example, making a different symbol for each English word makes statistical occurance rates for many words difficult to detect in the short run. It also increases the quantity of data needed to decode messages because each word is treated as a symbol, and increases the difficulty of analysis once sufficient data is gathered because meaningful words are rarely repeated and the possible number of sentences with 'the', 'and', 'or', and other similar oft repeated words, is very large. Similarly, the random use of obscure synonyms for recurrent words tends to dissipate the ability to make statistical attacks against this system since it tends to equalize the chances of different words in the language occurring in the plaintext and thus tends to delay the statistical analysis of word occurance. Strange sentence structures have a similar effect on the cryptanalysis process.

Confusion is the obscuring of the relationship between the plaintext, the key, and the ciphertext. As an example, if any bit of the key has a 50% chance of affecting any bit of the ciphertext, statistical attacks on the key require solving a large number of simultaneous equations. In a simple XOR encoding, where each bit of plaintext is XORed with a single bit of key to give a single bit of ciphertext, each key bit only effects a single ciphertext bit. For addition in a modulus, each key bit and input bit potentially effect each output bit (although not with 50% probability in this case). Multiplication or exponentiation in a modulus tends to increase confusion to a higher degree than addition, and is the basis for many ciphers.

Extensions to Shannon's basic theories include the derivation of an "index of coincidence" that allows approximations of key length to be determined purely from statistical data [Knight78] , the development of semi-automated techniques for attacking cryptosystems, and the concept of using computational complexity for assessing the quality of cryptosystems [Diffie76] .