International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 2, Issue 4, April 2013 **ISSN 2319 - 4847**

The Art of Cryptology: From Ancient Number System to Strange Number System

Debasis Das[1], U. A. Lanjewar[2] and S. J. Sharma[3]

[1]Assistant Professor, MCA Department, VMV Commerce, JMT Arts & JJP Science College, Nagpur, Maharashtra, India

[2]Professor, MCA Department, VMV Commerce, JMT Arts & JJP Science College, Nagpur, Maharashtra, India

[3]Reader and Head, Department of Electronics and Computer Sc., RTM Nagpur University, Nagpur

ABSTRACT

From the Rosetta stone to cryptography using Strange Number System, the art and science of cryptology has been used to unlock the vivid history of ancient cultures, to turn the tide of warfare, and to thwart potential hackers from attacking computer systems. The paper begins by tracing the development of cryptology from that of an arcane practice used, for example, ancient Egyptian hieroglyphics, to the modern scientific method that is cryptography using Strange Number System. This paper explores the depth and breadth of the ancient cryptology and the modern aspects and applications of cryptography, covering ancient Greece, Roman, Egypt, India, China Mesopotamia Cryptology, cryptology of the early modern Era to Computer age and the cryptography using Strange Number System, which is recently developed. By analyzing these areas, we hope to provide a more complete picture of where the field has been and where it is headed.

Keywords: Cryptology, Ancient Cryptology, Medieval Cryptology, Strange Number System.

1. INTRODUCTION

Cryptology is a subject that has been studied and applied since ancient Roman times, and research into better encryption methods continues to this day. The word cryptology is derived from two Greek words: kryptos, which means "hidden or secret," and logos, which means, "word or description." Cryptology means secret speech or communication. Cryptology encompasses two competing skills – concealment and solution.

- The concealment portion of cryptology is called cryptography. The aim of cryptography is to render a message incomprehensible to the unauthorized reader. Cryptography is often called “code making.”
- The solution portion of cryptology is called cryptanalysis. Cryptanalysis is often called “code breaking.”

Knowledge of cryptology can be traced back to ancient times. It's not difficult to understand why: as soon as three people had mastered the art of reading and writing, there was the possibility that two of them would want to send letters to each other that the third could not read.

Some experts argue that cryptography appeared spontaneously sometime after writing was invented. The first documented use of encryption was in 1900 BC. And after that, developments are started and this field is growing more, more and more…

However, cryptography is one of the oldest fields of technical study we can find records of, going back at least 4,000 years. Messages were already being encrypted in the archaic period of Greece. One of these, dating from the sixth century BC, consisted of wrapping a roll of paper around a cylinder and then writing the message on the paper. The unrolled paper was then sent off to the receiver, who could easily decrypt the message if he knew the diameter of the original cylinder [4].

Nineteenth century scholars decrypted ancient Egyptian hieroglyphics when Napoleon's soldiers found the Rosetta stone in 1799 near Rosetta, Egypt. Its inscription praising King Ptolemy V was in three ancient languages: Demotic, hieroglyphics, and Greek. The scholars, who could read ancient Greek, decrypted the other languages by translating the Greek and comparing the three inscriptions.

The earliest forms of secret writing required little more than pen and paper. The main classical cipher types are transposition ciphers, which rearrange the order of letters in a message (e.g. 'help me' becomes 'ehpl em'); and substitution ciphers, which systematically replace letters or groups of letters with other letters or groups of letters (e.g. 'fly at once' becomes 'gmz bu podf' by replacing each letter with the one following it in the alphabet). Simple versions of either offered little confidentiality. An early and simple substitution cipher was the Caesar cipher, in which each letter in the plaintext was replaced by a letter some fixed number of positions further down the alphabet. It was named after Julius Caesar who used the cipher with a shift of 3 in order to communicate with his generals during his various military campaigns [6].

Before the modern era, cryptography was concerned solely with message confidentiality (i.e. encryption) — conversion of messages from a comprehensible form into an incomprehensible one and back again at the other end, rendering it unreadable without secret knowledge (namely, the key). In recent decades, the field has expanded beyond

confidentiality concerns to include techniques for authentication, digital signatures, interactive proofs, and secure computation.

For many years, Cryptography was the exclusive reserve of military and diplomatic circles. Literature on the subject was very limited. During the 20th century, cryptography began a rapid change. One reason was the rise of computers, which lead to the mechanization of cryptography. Another reason was Claude Shannon's groundbreaking paper formed the foundations information theory and modern cryptography. The paper outlined the basic tenets of cryptography and allowed cryptography to be studied formally in the computer age. Developments henceforth have led us to be able to send messages securely over networks today.

Modern cryptography is heavily based on mathematical theory and computer science practice. More recently, cryptography using strange number system can provide a real physical security to data—allowing only authorized users to delete or update data. Nowadays when more and more sensitive information is stored on computers and transmitted over the Internet, people need to ensure information security and safety. Security of network communications is arguably the most important issue in the world today given the vast amount of valuable information that is passed around in various networks. Cryptography using strange number system is a better data encoding and decoding strategy, which will offer better security towards all possible ways of attacks while transmission. The most prominent feature of strange number system is its full fleshed Cryptography that provides techniques of encryption and decryption while hiding all the technical details.

In this paper we describe the history and evolution of cryptography starting from the beginning of the 20th century and continuing into the current day. Specifically, the following topics are addressed: ancient cryptology (covering ancient Greece, Roman, Egypt, India, China, Mesopotamia, Hebrew, and Arab Cryptology), medieval cryptology, the early modern era (1500-1900) cryptology, the twentieth century cryptology including World War I and World War II, cryptography in computer age and at last cryptography using strange number system. By analyzing these areas, we hope to provide a more complete picture of where the field has been and where it is headed.

2. ANCIENT CRYPTOLOGY

Early examples of cryptology can be found in the work of Mesopotamian, Egyptian, Chinese, and Indian scribes. In those four cradles of civilization, which emerged during the period between 3500 and 2000 B.C., few people could read and write, therefore, written language was a secret code in itself. Further concealment of meaning behind opaque hieroglyphs, cuneiform, or ideograms served to narrow the intended audience even further.

2.1 Ancient Egypt

Cryptography probably began in or around 2000 B.C. in Egypt. In the tomb Khnumhotep, a nobleman of about 1900 BC, the scribe used a simple code of hieroglyphic substitution, changing one symbol for another, less well-known one. However, this scribe did not use a comprehensive system of encryption; he just substituted hieroglyphs here and there, mostly at the end of his document. As time went on, Egyptians continued to use transformed hieroglyphs in their writings, in fact they became more common as the civilization matured. The Egyptians had several letters which commonly changed around in written communications. However, the interesting thing about the Egyptians' cryptography is that any viewer could figure out what the transcriptions read in a relatively short time, as compared to the millions of years needed to break modern cryptograms.

At the beginning of the second century BC, some stonework was created in Egypt that would prove to be, some 2000 years later, the gateway to an understanding of virtually all Egyptian hieroglyphs that came before it. It was discovered in August 1779 by a Frenchman named Bouchard near the town, known to the Europeans as Rosetta, which is 56 kilometers (35 miles) northeast of Alexandria. It is called the Rosetta Stone, an irregularly shaped black basalt stone about 114 centimeters (3 feet 9 inches) long by 72 centimeters (2 feet 4.5 inches) wide, and 28 centimeters (11 inches) thick. It was discovered with three of its corners broken [7].

When the French surrendered to the British in Egypt in the spring of 1801, it came into British possession and now sits in the British Museum. On it are three different writing systems: Greek letters, hieroglyphics, and demotic script, the language of the people, which is a cursive form of writing derived from hieratic, a simplified form of Egyptian hieroglyphics. Hence, this provided an opportunity to decipher Egyptian hieroglyphic writing on a scale not seen before.

2.2 Ancient Greece

In ancient Greece, the Spartan generals used a form of cryptography so that the generals could exchange secret messages: the messages were written on narrow ribbons of parchment that were wound spirally around a cylindrical staff called a scytale. After the ribbon was unwound, the writing on it could only be read by a person who had a matching cylinder of exactly the same size. This primitive system did a reasonably good job of protecting messages from interception and from the prying eyes of the message courier as wel [8]l.

In his writings, Herodotus reports the use of other forms of secret writing in the Grecian war to repel the Persian invasion. He writes of Greek soldiers cleanly shaving their heads, and then writing messages on their bare skin before allowing their hair to grow back. Although this more accurately describes stenography, it was often used in conjunction

with the simple substitution ciphers that were common at the time. Despite the fact that this method did now allow for the quick transmission of message, it was still widely used against the Persian Empire to communicate information of relatively low classification or importance.

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.

2.3 Ancient Roman

Although many examples of cryptography, secret transmission of messages, and the protection of information through encryption existed before the dawn of the Roman Empire, the cryptography used in Rome was the first such example that led to widespread military conquest. Julius Caesar was famous for using the so-called Caesar cipher, which consisted of a simple alphabetic shift by two characters to the right. 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 cipher text. The distance of the displacement is not important to the scheme, and in fact, neither is the lexical ordering chosen.

ABCDEFGHIJKLMNOPQRSTUVWXYZ
CDEFGHIJKLMNOPQRSTUVWXYZAB

Table 2.1 - The Caesar Cypher

For example, using the English word CAESAR would become:

C	A	E	S	A	R
E	C	G	S	C	T

Decoding a message encrypted with the Caesar cipher follows a similar process, but decryption is possible by shifting an encoded message two characters to the left, in an exact reversal of the encryption process.

By encoding his battle plans, as well as the instructions to the commanders in the field, Caesar was able to hide his objectives from regional enemies and further the expansion of the Roman Empire.

2.4 Ancient Mesopotamia

The cryptographic history of Mesopotamia was similar to that of Egypt, in that cuneiforms were used to encipher text. This technique was also used in Babylon and Asyria. From ancient Mesopotamia, one of the oldest extant examples of cryptography was found in the form of an enciphered cuneiform tablet, containing a formula for making pottery glazes. This tablet, found on the site of Selucia on the banks of the Tigris river, dates back to about 1500 BC. Mesopotamian scribes used cuneiform symbols in these formulas to encrypt their secret recipes. However, later, when the knowledge of the formulas for glaze making they were trying to protect became widespread common knowledge, their cryptographic sleights of hand became unnecessary and so later inscriptions were written in plaintext. The Mesopotamian civilization actually exceeded that of Egypt in its cryptographic evolution after having matched it in its early stages of development.

2.5 Ancient China

One of those great civilizations, China, did not develop any meaningful cryptography. Perhaps the reason is that most messages were memorized and sent in person to be delivered orally. Sometimes, if written, usually on rice paper, the message was concealed by covering it with wax, then either swallowing it, or concealing it elsewhere on the body. These techniques are examples, not of cryptography, but rather of steganography, the concealment of the existence of the message, sometimes called covert secret writing, whereas cryptography is overt secret writing. Due to the ideographic nature of the Chinese language, ciphers are ruled out as unworkable.

2.6 Ancient India

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. We mention two of the outstanding contributions from this civilization. One of them is still used today, namely finger communications. Ancient India called this kind of communication “nirabhasa”, where joints of fingers represented vowels and the other parts used for consonants. The second contribution of Indian civilization of antiquity is that they are responsible for the first reference in recorded history for the use of cryptanalysis for political purposes. Although no mechanisms are given for carrying out such suggestions, there is some cryptographic maturity seated in the knowledge that such cryptanalysis could indeed be achieved.

2.7 Hebrew Ciphers

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".

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZYXWVUTSRQPONMLKJIHGFEDCBA

Figure 2.1 - An ATBASH Cipher

2.8 Ancient Arab

The Arabs were the first people to clearly understand the principles of cryptography and to elucidate the beginning of cryptanalysis. Cryptanalysis is the practice of changing cipher text 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 cipher text 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 cipher text is provided.

3. MEDIEVAL CRYPTOLOGY

Progress in cryptology—as with most other areas of study—came to a virtual standstill between the decline of the Roman Empire in the third century and the rise of Islam in the seventh. Arab scholars pioneered cryptanalysis, the solving of ciphers or codes without the aid of a key, from the eighth century onward. In 1412, al-Kalka-shandi published a treatise in which he introduced the technique, later made famous to popular audiences by Edgar Allan Poe in "The Gold Bug," of solving a cipher based on the relative frequency of letters in the language.

By that time, cryptology had begun to advance again in Europe, where the Italian city states used secret codes for their diplomatic messages in the fourteenth century. Messages were carried on horseback, and even in peacetime, the roads of Europe were plagued with highway robbers, so secrecy in communication was of the utmost importance.

Progress in mathematical learning from the twelfth century onward aided these advances. In the early thirteenth century, Italian mathematician Leonardo Fibonacci introduced the Fibonacci sequence, wherein each number is the sum of the previous two: 1, 1, 2, 3, 5, 8, and so on. Fibonacci's sequence would prove highly influential in cryptology: even in the late twentieth century, some cryptologic systems relied on an electronic machine called a Fibonacci generator, which produced numbers in a Fibonacci sequence.

In the late fifteenth century, another influential Italian mathematician, Leon Battista Alberti, published a work in which he introduced the idea of a cipher disk. The latter is a device for encoding and decoding messages by use of concentric wheels imprinted with alphabetic and numeric characters. Even in the late nineteenth century, cryptographers were using cipher disks based on the model pioneered by Alberti.

4. THE EARLY MODERN ERA (1500-1900)

Due to its secret nature, cryptography—a word based on Greek roots meaning "secret writing"—had long been associated with the occult, and one occultist who advanced the art was the early sixteenth-century German monk Trithemius. Trithemius developed a table in which each row contained all the letters of the alphabet, but each successive row was shifted over by one letter. The first letter of plain text would be encrypted using the first line, the second letter using the second line, and so on. Late in the 1500s, French cryptographer Blaise de Vigenère adapted the Trithemius table for his own Vigenère table, which in the twentieth century became the basis for the widely used data encryption standard, or DES.

In 1518, another major breakthrough in the advancement of cryptography occurred in 1518 with the German monk Trithemius's publication of his six volumes "Polygraphia". He developed a system for repeating a key every 26 letters, so in essence, his encryption system consisted of 26 different, albeit basic, cipher alphabets.

In 1553, Giovan Batista Belaso extended Trithemius' technique by restarting the keyword after every individual letter in the original message. This varied the size of the text between the lengths of each text, so without prior knowledge of the beginning text, decryption by the means available at the time became virtually impossible.

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 its 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).

The event that thrust cryptography into the modern age, however, and caused governments and armies around the world to take notice occurred in 1628, with the Frenchman Antoine Rossignol's defeat of a Hugenot army by decoding a captured message that detailed their coming deployment plans. Soon after his victory, the French government began asking him to solve numerous ciphers, and other nations and city-states began forming dedicated organizations to break ciphers and protect information [11].

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 [13].

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.

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 [1].

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.

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.

5. THE TWENTIETH CENTURY

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.

World War I marked a watershed in cryptography. Not only was it the first major conflict in which radio was used, it was the last in which a great power failed to employ cryptographic communications. On the Eastern Front, the Russians sent uncoded messages that were easily interpreted by Russian-speaking intelligence officers on the German and Austrian side, leading to a massive victory for the Central Powers at Tannenberg in 1914.

The war also marked the debut of the Germans' ADFGX cipher, which was so sophisticated that French cryptanalysts only deciphered it for one day, after which the Germans again changed the key. But the cryptographic dimension of the war did not belong entirely to the Central Powers. British signal intelligence cracked the German cipher, and intercepted a message from German foreign minister Arthur Zimmermann to the Mexican president, promising to return territories Mexico had lost to the United States in the Mexican War if the country attacked the United States. Informed of the Zimmermann telegram, President Woodrow Wilson declared war on Germany.

In 1915, two Dutch navy officers invented the rotor machine; which is a combination of electrical and mechanical systems. The simple view of rotor machine is an electrical system with twenty-six switches pressed by the plaintext, These switches attached by a wire to a random contact letter on the output, for example if the plaintext letter is pressed, the wiring is placed inside a rotor, and then rotated with a gear every time a letter was pressed.

Also in 1917, American engineer Gilbert S. Vernam developed the first significant automated encryption and decryption device when he brought together an electromagnetic ciphering machine with a teletypewriter. A year later, Major Joseph O. Mauborgne of the U.S. Army devised the one-time pad, whereby sender and received possess identical pads of cipher sheets that are used once and then destroyed—a virtually unbreakable system. World War I also saw the development of a cipher machine by Edward Hebern, who tried to sell his idea to the U.S. Navy. The Navy rejected Hebern's system, which was later taken by the Japanese and used in World War II. By the time of that war, Hebern had developed Mark II (SIGABA), which became the most secure U.S. cipher system during the conflict.

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 [17].

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 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 [16].

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.

5.1 World War I

5.1.1 Zimmermann Telegram

In the opening days of World War I, the British navy severed every German and Austrian telecommunications line leading through the Atlantic, thus forcing the Germans to send all messages destined for the states, including diplomatic communications, through American-owned cables. This caused significant problems for the German high command later in the war, because without their own dedicated cables, their messages were subjected to American interception and cryptanalysis. In January, 1917, two cryptanalysis working for Room 40, the American equivalent of the European "black chambers," successfully deciphered the majority of a telegram from the German State Secretary of Foreign Affairs, Arthur Zimmermann, asking the Mexican president to intervene in the war on the German side, as well as request the same from the Japanese military [18]. The decipherment of this message convinced the United States to enter into the war against the Germans, dramatically shifting the odds against Germany.

5.1.2 The One Time Pad and Perfect Cryptography

Coinciding with the final days of World War I, United States Army Major Joseph Mauborgne, the current head of Room 40 and all cryptographic research for the United States, suggested the possibility of encrypting a message using a truly random key. By printing two identical pads with a random key, then using that key to encrypt one message and one message alone, this cipher obliterated the past problems with poly-alphabetic ciphers: the repetition of the key. Assuming that each random key, and therefore each set of pads, were only used one time, this encryption system formed the first and to this day only known cryptographic algorithm, or cryptosystem, that provides perfect secrecy.

5.2 World War II

5.2.1 Pacific Theater

After seeing the unbridled success of the cryptographic sciences in the First World War, more and more governments began investing considerable effort in the study, both to decipher information intercepted from foreign nations and to make their own messages more secure against these tactics.

A significant example of the power of decipherment and the benefits derived from research into cryptography came on April 13, 1943, during the height of America's war against Japan. The visiting commander in chief of Japanese naval forces in the Pacific, Admiral Yamamoto, forwarded his itinerary to the Japanese naval fleet. When an American listening station in Hawaii intercepted the message and decoded it, the United States seized the opportunity, and less than a week later, downed Yamamoto's plane as it prepared to leave a Japanese runway. Through a direct application of cryptography, the American Navy had killed one of the most powerful and beloved figures in the Japanese military, thus striking a critical blow to the morale of the Japanese [19].

The Japanese continued to use a similar cryptographic system, however, still blissfully unaware of the fact that the American researchers had long since broken it completely. Because of this overwhelming American advantage in both

knowledge and warning of attacks, the United States was able to fend off a massive Japanese assault near the Midway Islands, now infamous as the site of the Battle of Midway.

5.2.2 European Theater

In the European theater of World War II, a British-run group of cryptanalysts, consisting mostly of Polish mathematicians that had fled their home country before the outbreak of the war, enjoyed great success in 1942 when they first broke the codes of the German Enigma machines. Although the decoded information often revealed crucial parts of the German war strategy to the Allies, the paranoia and overly suspicious nature of the Nazi commanders led them to practice extreme security with their codes and ciphers alike.

6. THE COMPUTER AGE

American cryptologic work during World War II had contributed to the development of a machine, the computer, which would revolutionize cryptology to an even greater extent than the telegraph or radio had previously. Most cryptologic advances since the war have involved, or made use of, computers. A quarter-century after the war's end, in the early 1970s, American electrical engineers Martin Hellman and Whitfield Diffie introduced the idea of asymmetric or public-key ciphers, which are extremely hard to crack. This led to the development of the RSA algorithm (named for its creators, Rivest, Shamir, and Adelman) at the Massachusetts Institute of Technology in 1977.

Also in 1977, the U.S. federal government introduced DES, a transposition-substitution algorithm so complex that it seemed a safe means of guarding computer data. Given the fact that DES had some 2 56 possible keys (a number roughly equivalent to a 1 followed by 17 zeroes), it had seemed unbreakable at the time. By the early 1990s, however, vast increases in the processing speed of computers had made it possible for hackers to break DES using "brute-force" means—that is, trying every possible value for a given cipher until finding a solution. To guard against these attacks, new Advanced Encryption Standard (AES) algorithms were developed to replace DES.

Advances in computers and in communication by electronic means over the Internet, have both enabled and necessitated progress in cryptology. For example, electronic commerce requires sophisticated encryption systems to protect users' credit card information. Similarly, digital communication via cellular telephones requires encryption to prevent easy interception of phone calls. Developments of the 1990s include Phil Zimmermann's PGP (Pretty Good Privacy) to protect e-mail communications.

7. CRYPTOLOGY USING STRANGE NUMBER SYSTEM

Cryptology using Strange Number System is a novel concept to secure the data. Data encryption using strange number system is the process of converting information into an encrypted form, so that it is intelligible only to someone who knows how to ‘decrypt’ it to obtain the original text [5].

7.1 Encryption and Decryption using Octovicentimal SNS

This technique can be used as an encoding converter in text files. In the present network system, to increase security, every encryption algorithm is to make it as difficult as possible to decrypt the generated cipher text without using the key. This technique fulfils all such requirements as this technique use the concept of data encryption and decryption. This algorithm is based on the concept of base encryption in which a word of text is converted into ASCII number and after that it converted into pentaoctagesimal number. Finally after encryption, result is again an ASCII number; this number is converted into original string and sends to the receiver [3].

7.2 Encryption and Decryption using Pentaoctagesimal SNS

It provides an excellent data encryption and decryption technique to increases the data security and transfer rate during data communication. The most prominent feature of strange number system is its full fleshed Cryptography that provides techniques of encryption and decryption while hiding all the technical details. Cryptography with pentaoctagesimal SNS, a base conversion routine, symbol remapping, and a dynamic algorithm is the only encryption algorithm that is as secure as one-time pad.

8. CONTROVERSY IN MODERN CRYPTOLOGY

There has been considerable debate recently centering on the notion of key escrow. The usual context is during debate over the ability of private citizens to have access to strong cryptography. Many government officials and prominent scientists advocate a form of escrowed encryption as a good compromise between law enforcement needs and privacy concerns. In such schemes, a copy of the decryption key for each user is escrowed by one or more trusted parties, and is available if a warrant is issued for it.

In recent years, encryption has gone from being an arcane science and the stuff of James Bond movies, to being the subject of debate in several nations. In the U.S. that debate is playing itself out on the front pages of newspapers such as The New York Times and the San Jose Mercury News. On one side of the debate are a large number of computer professionals, civil libertarians, and perhaps a majority of the American public, who are rightly concerned about their privacy and the secrecy of their communications. These people want the right and the ability to protect their data with the most powerful encryption systems possible. On the other side of the debate are the United States Government,

members of the nation's law enforcement and intelligence communities, and (apparently) a small number of computer professionals, who argue that the use of cryptography should be limited because it can be used to hide illegal activities from authorized wiretaps and electronic searches.

MIT Professor Ronald Rivest has observed that the controversy over cryptography fundamentally boils down to one question: Should the citizens of a country have the right to create and store documents which their government cannot read?[20] Rivest, Ronald, speaking before the MIT Telecommunications Forum, Spring 1994.

This chapter does not address this question. Nor do we attempt to explore the U.S. Government's[4] claimed need to eavesdrop on communications, the fear that civil rights activists have of governmental abuse, or other encryption policy issues.

9. CONCLUSION

This paper discussed the technical history of cryptography: its definition, its historical development, the current state of the art, its significance for Information Systems Managers, and future tendencies and development. Section 2 detailed the history of ancient cryptology covering ancient Greece, Roman, Egypt, India, China, and Mesopotamia Cryptology. Section 3, 4 and 5 detailed the history of medieval cryptology before the advent and the early modern era and general computing with a focus on the beginning of the twentieth century. Section 6 and 7 detailed the cryptography in computer age and the cryptography using strange number system. It would seem that cryptographic algorithms and applications are secured for the time being against modern cryptanalyst attacks, however as they are all only computationally secure, their life span is limited. Cryptography as a field has a bright future, with new research and development prompting new algorithms and methods. Cryptography using strange number system, perhaps the next, largest step in computing, also provides the newest hopes for cryptography, creating the potential for new cryptographic methods algorithms, obsolescing modern applications and algorithms at the same time. By looking at modern and past methods cryptographers can look to the future with experience, creating better, more efficient algorithms without recreating the mistakes of the past.

References

[1] Mohammed Abutaha, Mousa Farajallah, Radwan Tahboub, Mohammad Odeh, “Survey Paper: Cryptography Is the Science of Information Security”, International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (3): 2011.

[2] Hinsley, Harry. "The Enigma of Ultra." History Today 43 (1993). EBSCOHost. Georgia Tech Library, Metz. 16 July 2006.

[3] Debasis Das, Dr U A Lanjewar, “Strange Number System: An Enhancing Tool for Data Encryption and Decryption”, International Journal of Advanced Research in Computer Science, Volume 3, No. 2, March-April 2012.

[4] Kartalopoulos, Stamatios V. "A Primer on Cryptography in Communications." IEEE Communications Magazine (2006): 146-151. EBSCOHost. Georgia Tech Library, Metz. 16 July 2006.

[5] Debasis Das, Dr. U A Lanjewar, “Exploring Strange Number System: Latent Talent to be used in place of Traditional Number System,” International Journal of Advances in Science and Technology, vol. 3, No. 1, pp. 102–150, January 2012.

[6] Beutelspacher, Albrecht. Cryptology: An Introduction to the Art and Science of Enciphering, Encrypting, Concealing, Hiding, and Safeguarding Described Without Any Arcane Skullduggery But Not Without Cunning Waggery for the Delectation and Instruction of the General Public. Washington, D.C.: Mathematical Association of America, 1994.

[7] Nicolas Courtois, Josef Pieprzyk, "Cryptanalysis of Block Ciphers with over defined Systems of Equations". The Association for Computer Machinery. Lecture Notes in Computer Science; Vol. 2501. pg. 267 – 287. 2002.

[8] Haldane, Robert A. The Hidden War. New York: St. Martin's Press, 1978.

[9] Kahn, David. Kahn on Codes: Secrets of the New Cryptology. New York: Macmillan, 1983.

[10] Lubbe, J. C. A. van der. Basic Methods of Cryptography. New York: Cambridge University Press, 1995.

[11] Lateiner, D. “Signifying Names and Other Ominous Accidental Utterances in Classical Historiography.” Greek, Roman, and Byzantine Studies 45.1 (2010): 35–57.

[12] Konheim, Alan G. Cryptography, a Primer. New York: Wiley, 1981.

[13] Ibrahim A. Al-Kadi (April 1992), "The origins of cryptology: The Arab contributions”, Cryptologia 16 (2): 97–126.

[14] "New Directions in Cryptography." Diffie, Whitfield and Hellman, Martin. IEEE Transactions on Information Theory Vol. IT-22. 6 Nov. 1976.

[15] Berlekamp, Elwyn; Solomon W. Golomb, Thomas M. Cover, Robert G. Gallager, James L. Massey, and Andrew J. Viterbi (January 2002).

[16] "A Brief History of Cryptography." CYCOM Cypher Research Laboratories.24 Jan. 2006.

[17] Monica Pawlan, "Cryptography: The Ancient Art of Secret Messages", www.pawlan.com, February 1998. Available: http://www.pawlan.com/monica/articles/crypto. [Accessed: Sept 12, 2012].
[18] P. K. Mohapatra. "Public Key Cryptography." The Association for Computer Machinery. Available: http://www.acm.org/crossroads/xrds7-1/crypto.html. [Accessed: Dec 12, 2012].
[19] "National Security Agency." University of San Diego. Dept. of History, U. of San Diego. 18 July 2006. Available: http://history.sandiego.edu/gen/20th/nsa.html. [Accessed: Mar 26, 2013].
[20] Derek J. Smith, " Codes and Ciphers in History," www.smithsrisca.co.uk, Part 1 - To 1852, 14th January 2010. Available: http://www.smithsrisca.co.uk/crypto-ancient.html. [Accessed: Jan. 15, 2013].
[21] Fred Cohen &Associates, "A Short History of Cryptography", 2.1, 1995. Available: http://web.itu.edu.tr/~orssi/dersler/cryptography/Chap2-1.pdf. [Accessed: Feb. 11, 2013].
[22] Rubin, J., "Vigenere Cipher", 2008. Available: http://www.juliantrubin.com/encyclopedia/mathematics/vigenere_cipher.html. [Accessed: Feb. 13, 2013].

AUTHOR

Name - Debasis Das
Qualification - M Phil, MCA, M. Sc (Comp. Sc.), MBA
About research - Around 7 years teaching Experience to Post-Graduate students.
Member of IETE
Around 7 research papers are published in International peer reviewed journals.
Research interest includes Number System, Network Security, Cryptography, Data Compression, Image Processing, and Mobile Computing.

Name - Ujwal A. Lanjewar
Qualification - Ph.D., MCA, M. Sc (Stats.), MBA, Diploma in Industrial Engineering and Diploma in Export Management
About research - Around 16 years teaching and Research experience to Graduate, Post-Graduate and Doctoral degree students.
Post doctoral research work is submitted in RTM Nagpur University for Doctor of science.
Around 35 research papers are published in International peer reviewed journals.
Four students have already awarded doctoral degree.
Research guide for five universities in the research area of Computer science and technology, Business management and applications, and statistics
Worked on various advisory committee of National and International Conferences

Name - Satish J. Sharma
Qualification - B.Sc., M.Sc., M. Phil., Ph.D
About research - Around 25 years teaching and Research experience to Graduate, Post-Graduate and Doctoral degree students.
Research guide in Electronics and Physics
Life member of professional organizations: Instrument society of India, Ultrasonic society of India, Materials Research Society
Presented two of his research papers at the International Conference on Materials for Advanced Technology, held at Suntec City, Singapore on Dec. 4-10, 2007
Visited Italy, Singapore and Oman as a visiting scientist
Worked on various advisory committee of National and International Conferences