**INTRODUCTION AND TERMINOLOGY**

**Cryptography:**

Cryptography is a form of technique used to convert the messages into format where only the creator(s) or the user(s) authorized, by creator, can understand. Since ages, it is commonly used to transmit messages to receiver, where only the receiver will understand the messages. Even if some other person gets the message, they cannot have an idea on what the message is. In modern days, it is highly vital to use cryptography as confidential messages are transmitted over the open medium, the internet.

**Encryption and Decryption:**

Encryption is the primary feature of cryptography, which is used to convent the normal/plain text to text that is not understood by unauthorized persons. Decryption is the reverse process, where the authorized users can get back the normal/plain text from the text that is converted to encryption process.

To encrypt the text, we are in need of some password or key that is defined by the creator. This aids to keep the message secret. The key can be of any length or type according to the cryptography that is used. In the present life cycle, the encryption key plays a major role on the level of security that is maintained. The larger length of the key is, greater the encryption. It is evident that in the technology influenced world, we need to have secure communication. This is influenced by the encryption level.

**Cipher:**

A cipher is an algorithm, method or process is used to perform encryption or decryption. The cipher has a structure on how to either encrypt or decrypt. A cipher depends on encryption key. The use of key, the additional information, in cipher is used to produce the respective encrypted output.

**Plaintext and Cipher text:**

Plaintext is the text that we have before encryption, and the text after the encryption is cipher text. In few encryptions, we will be having multiple layers of encryption. In decryption process, the cipher text is used as input and plaintext is obtained as output.

**Cryptanalysis:**

The process of converting the cipher text to plain text, without knowing the key is called cryptanalysis. It is seen that many governments have deployed a focused division for this purpose. It sometimes aids the government to gain command over wars.

HISTORICAL CRYPTOGRAPHY

**Ancient Egypt:**

One of the earliest known cryptography is from the Egyptian town Menet Khufu on the Tomb of noble man Khumhotep II, somewhere around 4000 years behind. Khnumhotep drew many different symbols to transcript the meaning of text in his master’s tomb at 1900 B.C. Generally the Egyptian had the idea of hiding their rituals in the transcripts in ciphered form, so that only they can read it. It was a basic substitution cipher.



**Greece:**

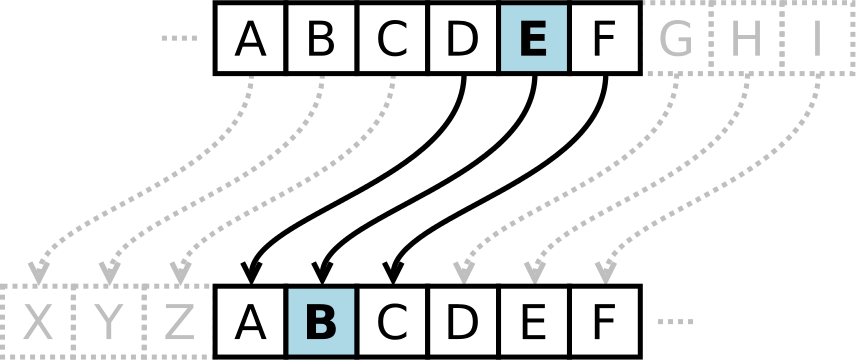
The Spartans used the Scytale around 500 B.C. to cipher and send and receive the messages. It was made such that only when it is winded on a particular shaped block, the message was revealed. When it is unwound or wound in any other block or shape, the message becomes unclear. This was a effective method of cipher at that time because, there were only few who could write or read at that time. It was a basic transposition cipher.



**Rome:**

The military use of cipher was established in the times of Julius Caesar, around 2000 years ago. Ceasar used basic substitution cipher, which shifted the letters by known number of letters.

Only those who knew the value for substitution were able to interpret the message. This made him to have a powerful communication to his base and thus providing a benefit over the enemy war head.

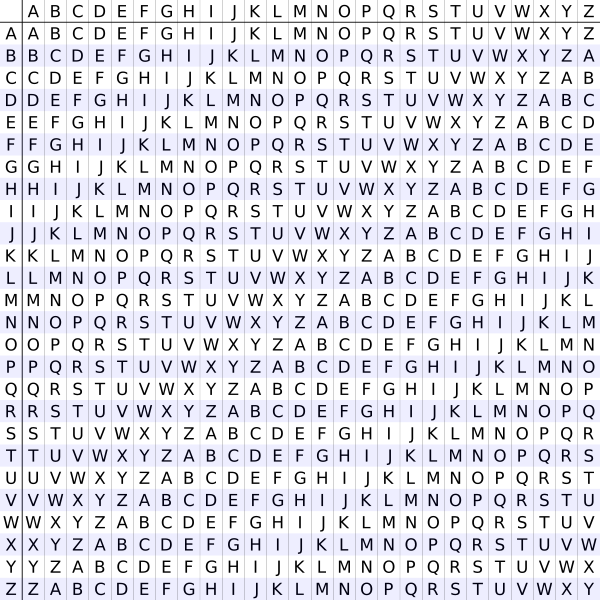


**Alberti-Vigenere Cipher:**

In 1400’s Leon Battista Alberti invented a cipher disk, which can revolve and form various forms of cipher. It was the base for poly alphabetic cipher.

In the 1500’s Blaise De Vigenere created Vigenere cipher, which the above as base idea. It had a grid of letters in a table and was called as Vigenere square. The grid has 26 alphabets which will have the first alphabet of a line to be shifted to the last position. Thus a substitution cipher was formed.

The substitution was formed such that the plain text letter was seen in the x axis and the corresponding key, which is repeated till the length of plain text, was seen on the y axis. The merging cell will for the corresponding cipher. The deciphering is similar but with a difference where the person finds the column corresponding to the cipher text.



**Jefferson Wheel Cipher:**

During 1700’s Thomas Jefferson invented a cipher system that is almost similar to Vigenere cipher but with improved security. The system had 26 wheels with alphabets that are randomly scattered on them. The key for the system is having the wheels in ascending order. The cipher text is any other line found by aligning the wheel with a line that has the plain text or message. While decrypting the message the cipher text are aligned first then the all other lines are scanned for finding a meaningful line. It is very rare to find two lines which make some sense.

Around 1900’s the US army found the same method without having knowledge about Jefferson’s invention.



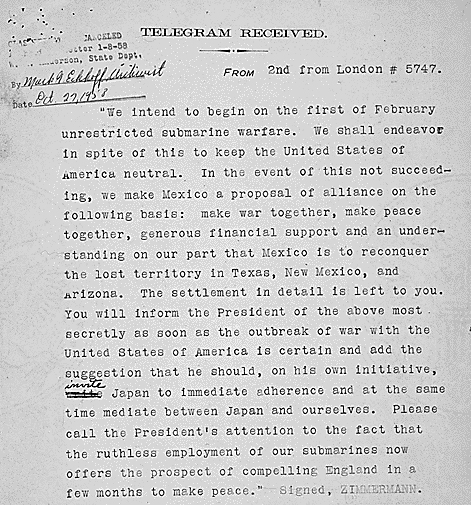
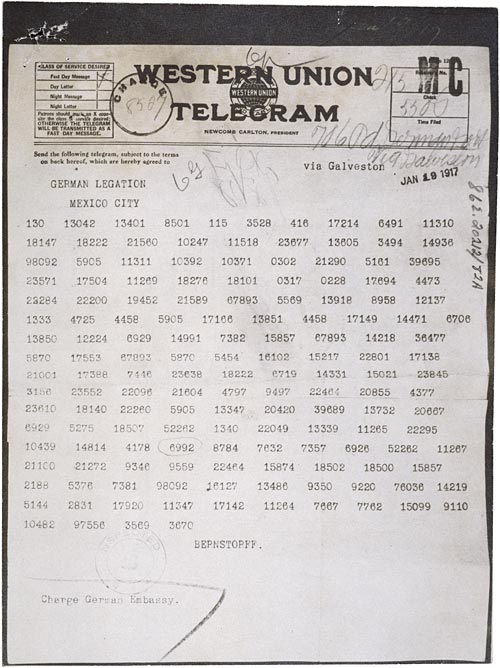
**WAR DRIVEN CRYPTOGRAPHY – WORLD WAR I:**

**Zimmerman Telegram:**

In the early stages of World War I, i.e. around 1917, the cryptanalysis history was impacted by British cryptographers, who encountered German encoded telegram called Zimmerman telegram. They are able to decipher the telegram which convinced United States for joining the war.

The foreign secretary of the German Empire, Arthur Zimmerman, sent a secret message to German ambassador in Mexico, Heinrich von Eckardt. The telegram was to make an offer for Mexico to get back its territory of New Mexico, Texas, Arizona if they joined the World War to help Germany. Even with regards to such big offer Mexico concluded that it would not be able to take over their former territories.

World War I was in full swing when this message was sent. The United Sates has been neutral until that point. British along with their team of other countries had requested help from United States. This message made United States to move towards war. On February 24, 1917 British gave their decoded telegram to United States. On April 6, 1917 the United States authorities officially declared war on Germany and allies to favor the British.



**Choctaw Code talkers:**

The United States was having problem with communication as it was not secure. Almost all the phone calls were intercepted by Germany which made Germany know every move of the United States. This made the army commander, Captain Lewis use eight Choctaw men who knew American and Indian languages. As they were in their battalion, they communicated over the radio signals and phone lines with each other. Using of such unique language was vital for United States because it was difficult for Germany to decipher codes of unknown language. Within a day of using this technique the United States had a comparative winning edge. Thus the Germany decided to retreat within 72 hours.

**WAR DRIVEN CRYPTOGRAPHY – WORLD WAR II:**

**Enigma Encryption Machine:**

During the end of World War I, Arthur Scherbius found enigma and electro mechanical that was used for message encryption and decryption. The enigma had 10114 possible combinations of ciphering as it has several rotors and gears. As it had many combinations it was virtually not easy to brake with brute force methods. The commercial version was only available at 1920’s.

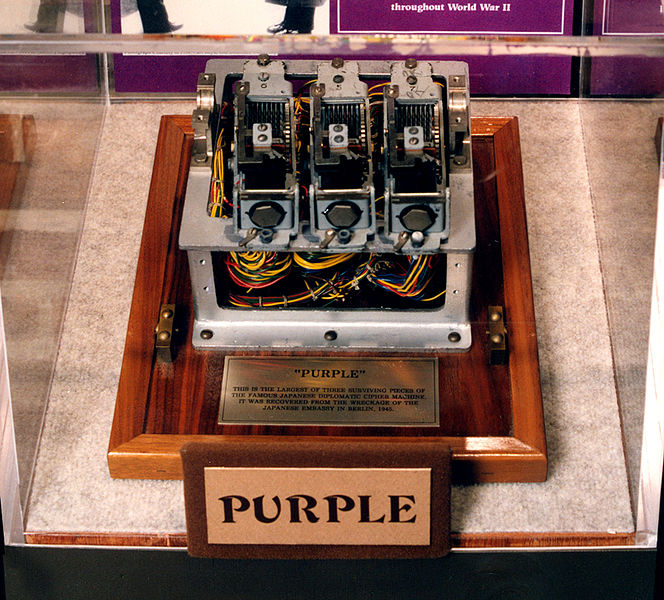
It was only during World War II that this machine gained popularity. It was only with this device that nazi Germany became over confident about sending their secret message. This made the allied cryptographers to find the several built in weakness of this device, which included the algorithm not to map a letter with itself while substituting. This caused the downfall of Enigma. This made allied cryptographers to decipher many cipher message sent Nazi Germans.



**Purple:**

While German Enigma was cracked by allied forces, the Japanese found an encryption device and named it purple. The purple was using the stepping switches that were commonly used by routing telephone signals. The Japanese were much efficient in destroying their encryption machines, as not even one complete machine has been discovered till date.

As the Japanese were efficient in keeping the secrets, the United States cryptographers had difficult time decrypting their message. Replica of the purple was built based on the encrypted messages recover by William Friedman, a famous cryptographer. As they have not seen a purple machine nor they know how it works, it was very difficult to build that machine. After sometime the team figured out encryption techniques used by purple and was able to build another machine for decryption. Thus the United State has access to Japanese secrets in World War II.



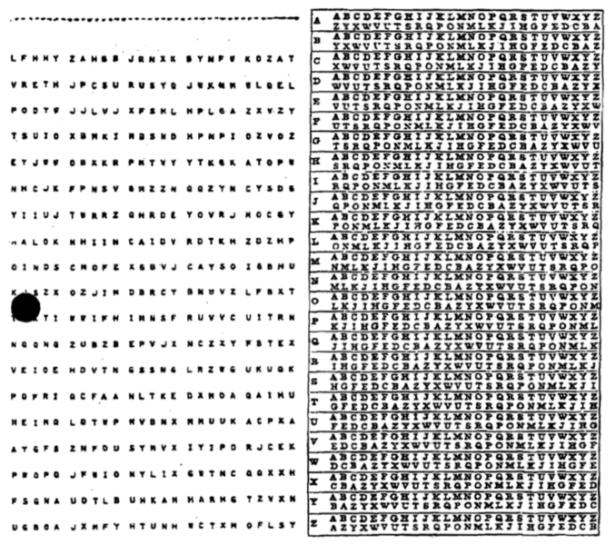
MODERN ENCRYPTION:

**One Time Pad:**

One Time pad encryption algorithm brought into existence around 1990’s and from then it is unbreakable. This algorithm derived from Vernam Cipher, which is named after Gilbert Vernam. Vernam cipher was mixed with a message and a key from a paper tape or pad. This was not breakable till Joseph Mauborgne found that whether the key was completely arbitrary. Cryptanalytic would be difficult in determining the right key from every possible key. During the process of using the possible key anyone should view back the decipherment. There are two assumptions for the unbreakable one time pad.

* The key is totally arbitrary.
* The key used ones can’t be used again.

The importance of security totally relies on keeping the key cent percent secret. The implementation of one time pad is the combination of plain text elements and key elements using modular addition. Here the key used in encryption is also used in decryption that implies a key used for cipher text encryption is also used for plain text decryption.



**Pseudo Random number generation:**

Any non-arbitrary number appears in the key of one tie pad, security is going to decrease which directly affects the un-breakability of one time pad. Huge attempts were made to create arbitrary numbers, from a key. All these arbitrary numbers are called Pseudo Random number generators. The reason for pseudo is that they can’t give an arbitrary cluster. Although the Pseudo random number generator is not fully unbreakable, it can provide efficient security when it is executed correctly. Pseudo random number generators that have been focused on security use are called crypto graphical secure Pseudo random number generators. Crypto graphical secure Pseudo random number generators have augmented advantages compared to Pseudo random number generators. Here crypto graphical secure Pseudo random number generators must pass the next bit test. For the given number of bits, the first part should not contain any polynomial algorithm that will guess the next bit. Here the probability is greater than fifty per cent. Crypto graphical secure Pseudo random number generators sees that if any state is revealed, it should not be possible to rebuild the set of random number, before the values are actually revealed.

**Symmetric Key Encryption (Private Key)**

Any encryption requires a secret key to maintain the secrecy, even this is used Symmetric Key Encryption. Here the symmetric key can also be called as private key. The key used in encryption cipher is also used in decryption. To compare it with a regular routine, let us consider a mechanical lock. So here the key which is used to close the lock is used to open the lock. Suppose if unknown person gets the key, then will be able to access the things inside the lock.



**Implementation of Symmetric Key Encryption:**

There are latest algorithms that utilizes key encryption scheme. The types of encryptions are Stream cipher and Block cipher.

* **Stream Cipher**

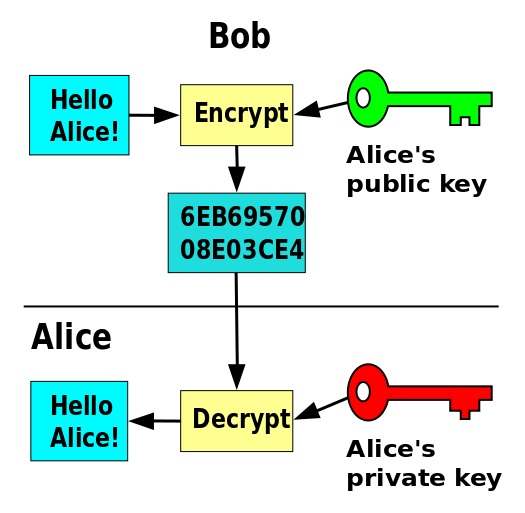
Stream cipher combines a group of random numbers or unreal numbers with the original text. Some special group cipher include ones time pad, linear feedback shift register, linear Congruential and RC4. RC4 is well known among all the cipher and it is used in security socket layer and wide equivalent privacy.

* **Block Cipher**

This is another process of symmetric key encryption using a block cipher. This works based on fixed lengths of bits. When encrypting a bock cipher takes a portion set of bits of original text and gives back same amount of cipher text. Here modification of block cipher is maintained by encryption or decryption key. Some of the famous block ciphers are Blowfish, Twofish, DES and AES. Advanced Encryption Standard (AES) is used by United States government and has an approval by the national security agencies, to encrypt highly secured and confidential information.

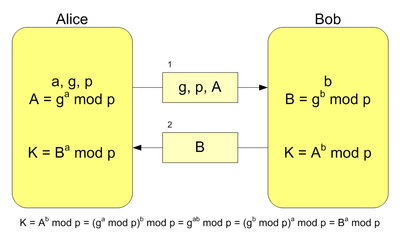
**Asymmetric Key Encryption:**

The period of 1970s encryption system required a previously known key. Cryptographers of 1970s are more cognizant to send a text securely without getting together with the sender and receiver. They had an idea of using different key for encryption and decryption. Here a key used for encryption is not useful to decrypt the lock. Similarly the key used for decryption is not used to encrypt the image.



**Diffie – Hellman Key Exchange:**

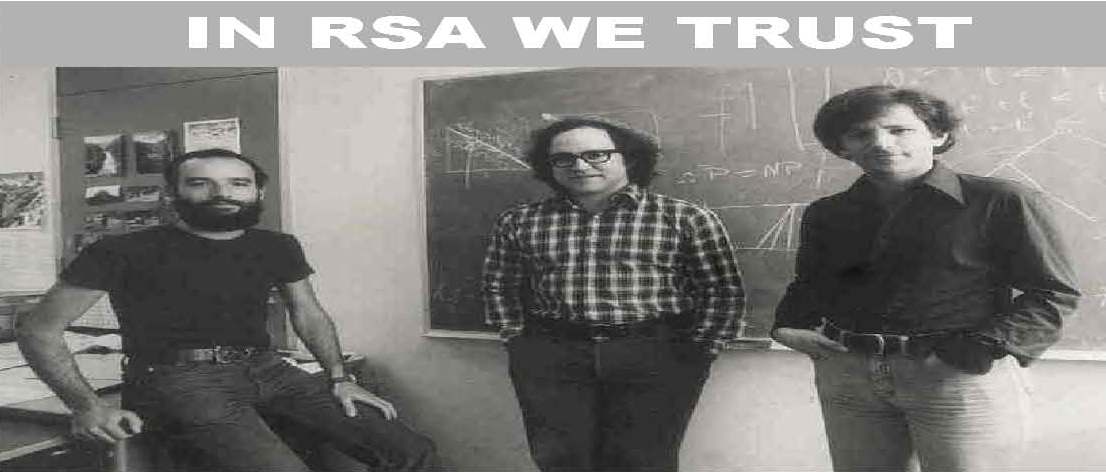
The Diffie Hellman Key Exchange is a cryptographic protocol that utilizes two people with no previous knowledge of each other to come up with a share secret key. Even this is used in symmetric key cipher. Diffie Hellman key exchange was first brought out by Whitfield Diffie and Martin Hellman in 1976. The British signal intelligence showed that this scheme was brought out by Malcolm Williamson which is prior to Whitfield Diffie and Martin Hellam’s publications. Diffie Hellman Key Exchange depends on exponential functions, which is faster compared to logarithms. When they are executed properly, Diffie Hellman key exchange protocol gives both people the same key, without actually sending the physical key. The capacity of the algorithm depends more on computing the discrete logarithms.



The above figure shows the generation of the key through Diffie Hellman Key Exchange. Here Alice wants to bridge with Bob, by using a key. First step is to come up with a variable. Here Alice came with a, g, p and Bob came up with b. Variables g, p, A and B public and are shared between Alice and Bob. After exchanging the variable, each person used to compute their own K. Important point here is that K is never shared between the Alice and Bob. Thus both Alice and Bob will be able to generate the same key K. The disadvantage of Diffie Hellman Key Exchange is that any message that is determined previously cannot be used in above algorithm. The transmissions are simply the result of computation, that makes it had to break it down. In order for K to bed is covered by someone besides Alice and Bob, a logarithm of A or B must be computed. When extremely large numbers for a, b, and p are chosen, it could take billions of years to compute the logarithm of A or B.

**RSA Encryption:**

To overcome the drawbacks in Diffie Hellman Key Exchange Ron Rivest, Adi Shamir, and Leonard Adleman developed an extension system to Diffie Hellman System. This RSA system embeds the message and transmits it. The RSA encryption is named from the surname of Ron Rivest, Adi Shamir, and Leonard Adleman.



RSA System depends on multiplication and exponentiation, which is faster than Prime factorization. Here the protection is built on 2 big prime numbers. These two numbers are used to build a public key and private key. Public key and private key are hold by one, to encrypt any message, one should use public key and he should send back to the one who created the key. Then the authorized person uses a private key and decrypts the text. Here the important thing is that one, who is having the private, can only decrypt the message. One of the encryption in RSA is modulus. Where this is the multiplication of two large prime numbers so to decrypt this any other person, should compute the factorization to the modulus, which intern gives two prime. The capability of the encryption mainly depends upon the factorization of prime numbe, this is widely used in electronic commerce protocol.

**Breaking RSA Keys:**

The authorized holder of RSA encryption of RSA laboratories had put a challenged to stimulate research into the field factoring large numbers. The main motto of this challenge is that to give advantage to the RSA encryption, which is considered to be ultimate power in cryptography. In 2007 RSA laboratories concluded that “Now that the industries have a considerably more advanced understanding of the cryptanalytic strength common symmetric key and public key algorithms. These challenges are now where active.”

Around these activities of RSA prime factoring challenge, RSA laboratories came up with a list of medium size prime numbers, known as RSA prime numbers. Which can also called as RSA numbers. All these numbers had price money, if every prime numbers was completely factorized. Many of the smaller numbers were factored around 1990s and during the beginning of 2000s, large RSA numbers were factorized which took a long time like 80 computers 5 months to calculate that. They had a price one of $20,000. Other numbers had price money of $100,000 to $200,000. The estimation time of factorization of these large prime numbers are billions of years, for a single computer. The time for creating such number is less than a minute.

**Steganography:**

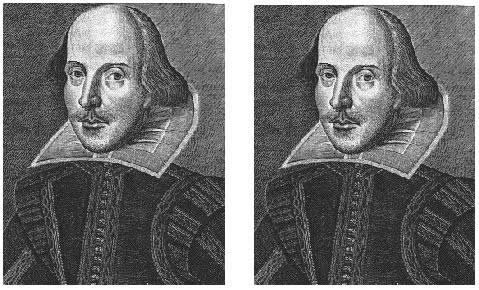
* Security through Inconspicuous:

Steganography is a form of cryptography that stores the data into form which is not noticeable by any other person. Instead of using encryption, the medium which is used, steganography uses human recognizable objects like picture, audio and video files. Steganography mediums are web pages, communication protocols, data streams, etc. One of the simple executions of steganography is using invisible ink between the lines of message in any paper or document.

Major stenographic is used with computers which uses numbers that can’t be determined by humans. Consider the following example: An audio .wav files has 16 bit number ranging from 65535. Any individual can split up the message and include them one at a time, in every audio sample. Finally, change the amplitude by one in sample. So this means an audio file sample representing 65656 any random number, could be changed by one. By doing this a human ear can hear this, this is the way in which secret message is encrypted in an audio file, without making any pragmatic change or altering files. Any person cannot be able to tell what message was secured. This is where security through obscurity comes into existence. Any secured message can easily be decrypted, by a cryptographer. A message secured in a picture, by audio or video files can pass through without being noticed.

Everyone says that terrorist attack of September 11, 2001 was made using steganography, cryptography and internet. Prior to attack a US student newspaper revealed “Lately, al-Qaeda

operatives has been sending hundreds of encrypted messages that have been hidden in files on digital photographs on the auction site eBay.com”. This is an assertion if it is true then it is a very effective way to secure information, without any advancement. Al-Qaeda might have known that US could break any time of encryption. So this steganography approach is very intelligent approach.

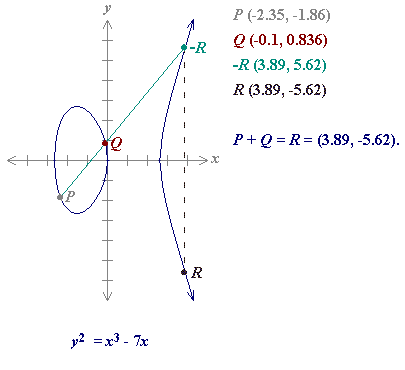


The above figure has secured data which is hidden in the image, on the right. Both the images look similar, and any person cannot differentiate between the secured and original. Secured image can only be known, by knowing binary codes of two pictures. Here the core point is that it is difficult to differentiate, between two pictures until you are an expert in steganography.

**FUTURE METHODS OF ENCRYPTIONS**

**Elliptic Curve Cryptography:**

Although elliptic curve cryptography has been found, the author considers it as future cryptography technique. It is due to the fact that their advantages and disadvantages are not known. Elliptic curve cryptography uses complex elliptic curve in a finite field. The algorithm used for elliptic curve cryptography is same a Diffie Hellman key exchange and RSA encryption. Here the number chosen from a finite field are always within an elliptic curve.

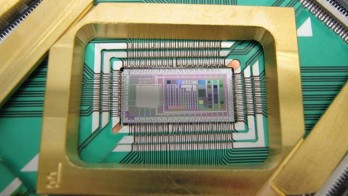


The above figure of elliptic curve cryptography could be used with RSA algorithm where P and Q are two primes. When these primes are chosen, in a finite field of elliptic curve, the size of the key will be small, but it gives the same security. The time taken for encryption and decryption will significantly reduce. So, these helps huge amount of data transfer with security. Just like any other type of encryption like RSA, Diffie Hellman, etc. even elliptic curve cryptography must be extensively tested before it is deployed to any commercial, private and government use.

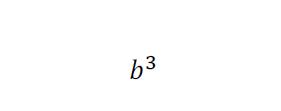
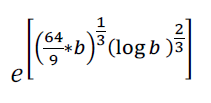
**Quantum Computation:**

Quantum Computation is used in Quantum Computer or processor. A Quantum processor used Quantum mechanical principle like Quantum Superposition, Quantum entanglement. These modern computer store data as binary called as bits which are zeros and ones.

The calculation in modern computers mainly works bit by bit. Quantum computer stores the data by using quantum superposition of many states, where these states are stored in quantum bits or qbits. Depending upon the design of the quantum, each q bit can store numbers from instantly. These computation uses magnitude rather than transistors.



The above figure shows that world’s first commercial processor in quantum computation. The capacity is 1000 times less than that of modern transistor processor. Quantum computing is still not effectively used. Quantum processors which are manufactured today are very small, and they do not have computational size as if transistor processors. Some people scare that a pragmatic quantum computer, which is successful, will kill the world financial system, by breaking every security system. Public key cryptography depends more on discrete logarithm and prime factorization where computer are slow to perform this.



The above equation (left) shows the time taken to run GNFS algorithm for computing a prime number factor using a binary processor. Whereas equation on right, shows algorithm discovered by Peter Shor. These calculate prime factor on a quantum computer, in both equation b represents the number of bytes in a number. Shor’s algorithm runs fast compared to GNFS algorithm runtime. To add up the power of theoretical quantum computer, let us assume RSA numbers such as RSA-640, a number with 193 digits was factor by 80 by 2.2 GHz computer over the span of five months. If this same number was applied to one of the quantum computer of equal size, Shor’s algorithm would have factored it within 17 seconds. Numbers which take billions of years will only take hours or minutes by using quantum computers.