INTRODUCTION

Cryptography

The word cryptography comes from Greek meaning hidden writing and some of the earliest forms of secret writing comes from ancient Greece as well.

Need of Cryptography

To communicate securely or to ensure confidentiality, integrity, and authentication of data.

STEGANOGRAPHY

Definition

The word steganography means covered writing. It is the practice of concealing information such that the existence of apparent message is not visible to the observer.

Earliest use

Herodotus known as the father of history described a method of secret writing. He used a wooden board to write a message and covered it with wax. This technique was used to send military correspondence During Greece's war with Persia in 5th century BC. This sort of concealment is known steganography.

Draw Backs

The main issue was that if the message was discovered its contents were revealed easily. This dilemma gave rise to cryptography.

TYPES OF CRYPTOGRAPHY

Transposition

Transposition is when a document is rearranged creating an anagram and it is the earliest form

Of cryptography.

Substitution

In substitution elements are replaced by some other elements and it is a more modern form of cryptography then transposition.

TRANSPOSITION

Transposition cipher

Transposition cipher is a cryptographic method in which the positions of characters in the plain text are rearranged according to a specific algorithm. Basically some sort of permutation is applied to replace them. Since the position of characters is changed that's why it is referred as transposition.

Example

.Rail Fence Transposition

.Row Column Transposition

RAIL FENCE TRANSPOSITION

Definition

Rail Fence Transposition is the simplest form of transposition. In this technique plain text is written down as sequence of diagonals and read off as sequence of rows. This technique mainly depends upon the depth value.

Key

Depth value is actually the number of rows chosen to convert this in cipher text. This is actually like a key which is already decided between sender and receiver.

Example

Let's say I want to send a message **ITU UNIVERSITY** by using depth value 2. Now you have 2 rows start writing first word in first row and second word in second column continue until the full message is written. Now read it row by row and you got yourself a cipher text **IUNVRIEST.**

ROW COLUMN TRANSPOSITION

Definition

This transposition technique is a bit more complex than the previous one. In this scheme we take a rectangle the number of rows and columns of the rectangle are already decided between the sender and the receiver. The plain text is written row by row and the cipher text is read off column by column but here comes a very important thing. The key.

Key

There is a certain pattern or order in which the columns are read and the cipher text is generated Again this key is already decided between the sender and the receiver which helps the receiver to decrypt the message.

Example

Now let's take a sentence **KILL CORONA VIRUS AT TWELVE AM TOMOROOW.** Now take a rectangle of 6 rows and 5 columns write the message row by row and according to the key let's say **4312567**. Please not that this key is actually written in this order on the rows and we read these rows according to this key not by row number and after that we get our cipher text which in this case is **LATARLVTMOINAERKOSVOCIWTWOREOYRULEMZ.** You can repeat this process again to create a more complex cipher text.

SUBSTITUTION

Substitution is a technique in which letters are replaced by some other letters. There is no specific method or rule for this you can substitute it however you want. Basically you are the one here to make rule according to you or however you like.

Earliest Use

Substitution has existed since the times of Greece and it is in fact more complex or much more efficient and reliable method of cryptography than substitution as complex encryption in transposition also created issues for the receiver. Some of the earliest substitution method was CEASER CIPHER which again was used in times of Greece. Interesting thing about cryptography is the actual need of it raised because of war as military messages play a key role in these crucial times.

CEASER CIPHER

CEASER cipher was the most popular cipher in the earliest time. It traditionally used shift of three letters from the alphabetical order. This is not some kind of restriction in substitution it was just how CEASER used it. Here the shift of three was a key which was already decided between the sender and the receiver.

More generically it can also be written as **(l + k) mod 26.** Here **l** is the letter **K** is the key and **mod 26** basically keeps you in a loop of these letters. You will understand when you have to shift **Y**.

Draw Backs

So there are total of 26 variations of CEASER CIPHER and if someone knows that CEASER CIPHER was used to encrypt this message it will take no time to decrypt because of only 26 variation. By 26 variations I mean 26 types of shift as there are only 26 letters in alphabet.

Solution

A better solution to this to this is to replace them randomly as it will create 400 followed by 24 zeroes of permutation. That's a lot of combination. But this can also sometimes create difficulties for the receiver as it will also be hard for him to decrypt.

KEYWORD CIPHER

A much better method of substitution is keyword substitution as it is more complex hard to decrypt and easier for the receiver to decrypt.

EXAMPLE

In keyword cipher the sender and the receiver agree upon a key which is basically a word so in the case let's take a key for example **LOOP** now we remove the repeating letters and it becomes **LOP** now by writing this first just write the rest of the alphabets excluding these. Let's say I want to encrypt the word **HEELO** we simply write normal 26 alphabets and replace them with the previous one and you got yourself a cipher text.

HISTORICAL EVOLUTION of CRYPTOGRAPHY

Substitution was such a powerful method of encryption that it lasted centuries like it had been used by every empire that had existed. It was successfully used in 50ad, 100ad, 250ad, 500ad, 600ad, 700ad, it lasted until 8th century. I mean something that had been a part of our history and important part of every greatest empire that existed and we knew nothing about it. Well it lasted until 8th century. We all know about the golden period of ISLAMIC world. How BAGHDAD had become center of the knowledge for the whole world. These times brought up a man named **ABU YUSUF**. The man who finally decrypted these substitution ciphers particularly keyword cipher. The method introduced by him is known as frequency analysis.

Frequency Analysis

This method is really simple. I will try to make it as simple as possible for better understanding. Just take the plain text cipher and count the frequency of every word and write them in order of their frequency like the word with higher frequency at top and vice versa. Then take a text a full page long text and again count the frequency and write them in same order. Now replace the cipher text letter with the highest frequency letter taken from text and we do it in order just like that you have successfully decoded a substitution cipher that had been used for centuries by greatest empires of our world.

CORE CONCEPTS

Symmetric Encryption

In simple words in symmetric encryption sender sends a message to receiver by encrypting the message with a key now receiver can decrypt this message only with the same key. The biggest challenge here is key exchange, how they can safely exchange keys. Well if the key is sent with the message then encrypting this makes no sense.

Asymmetric Encryption

Asymmetric encryption is a more reliable or safe method of communication. In asymmetric encryption each sender and receiver has two keys. One public key and the other one is Private Key. Now let's say A wants to send a message to B. Now their public key is known by everyone but thing about private key is that no one knows about it except the owner. Perfectly solving the issue of key exchanging. Here A will encrypt the message with the public key of B and this message will be encrypted with the private key of B. If the message is encrypted with someone's public key it can only be encrypted with his private key.

MODERN CONCEPTS

.DNA Cryptography

.Quantum Cryptography

DNA CRYPTOGRAPHY

Introduction to DNA Cryptography

We all know DNA already stores information about our body from eye color to skin tone. It programs our entire body. DNA is made up of four bases ADENINE, GUANINE, CYTOSINE, and THYMINE or AGCT. The specific groups of these three are known as codons.

Example

In 1999 in NEW YORK scientists substituted all 64 possible codons with letters, numbers and grammar symbols. Then they arranged these codons in specific order to form a message which was then hidden on a letter under a smudge. This letter was then mailed back to them, upon receiving they took the DNA sample decoded and that's how they received the message secretly. A beautiful example of cryptography.

It soon became obvious that DNA cryptography can code much more then text. By translating binary codes in DNA codons digital data can be programmed into synthetic data and then it can be translated back to 0 and 1.

Benefits

Hypothetically it is considered that 400 followed by 6 zeros GB data can be stored on a fingertip. U can literally store all the movies in HD in a small tube literally the size of baby finger.

We all know that digital devices wore out after few decades resulting in the loss of information well DNA has a half-life of 500 years meaning half of its bonds will break after 500 years and if left in a dark cold place their half can increase up to 200,000 years.

QUANTUM CRPYTOGRAPHY

Introduction to Quantum Cryptography

So quantum cryptography is different from rest as it is defendant on the laws of physics which makes it impossible for eve dropper to know the exact key. It specifically depends on Heisenberg's uncertainty principle and on no-cloning theory.

Key

So let me explain u this by using the simplest key exchanging method which is BB84. So first understand this that here photons are used to make a key. Here comes the Heisenberg's uncertainty principle which tells us that one cannot know everything about the quantum state of a particle. So photons are always in spin motion. This motion can be changed by using filters like horizontal, vertical, forward slash, back slash shape like filters. Now vertical and backslash shape filter is known as 1 and horizontal and forward slash 0. Now there are particularly two basis rectilinear base and diagonal base.

Now let's say sends photons to B using random filters and same way B will also use random filters to receive them. They now share the basis used publically and will make the key of the bits in which same filters were used. Now the share the subset of the key. Here comes the major part of the subset key is

not same they will instantly know there an eve dropper. Let me explain for sue the eve dropper will one time use the wrong filter altering the spin direction of bit which will also change the bit thus forcing them to abandon they key.

No-Cloning Theory

Well one can imagine what if clone these photons well there is a theory called no-cloning theory which prevents one from cloning these photons so basically there is no method as it is based on laws of physics. And there can only be one state of photon which mathematical form is known as discrete thus giving it a name quantum.

POST QUANTUM CRYPTOGRAPHY

Post quantum cryptography is being developed as quantum computers will be able to break al classical cryptography methods mentioned above. Question here is will it be able really safe as it is the purpose.

Challenges

Can post quantum algorithms keep up with pace of quantum computers.

If quantum cryptography only becomes accessible to powerful governments how will it affect the data privacy system around the world.