A Comphrehensive Study on Known Plaintext Attack, Chosen Plaintext Attack and Ciphertext Only Attack.

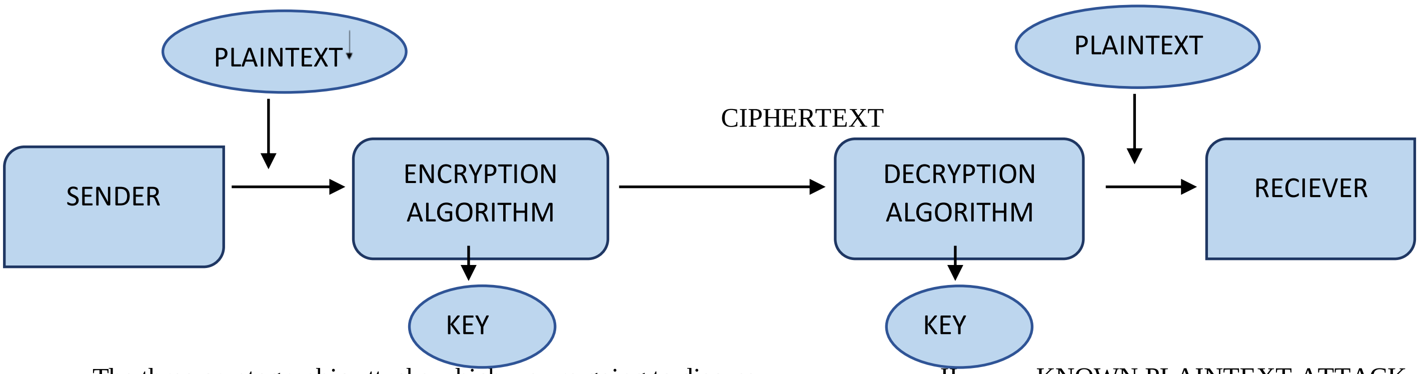
Kanika Kapoor[1], Siddharth Nanda[2], Rajeshwari Gundla[3]
[1]*U.G. Student, SOE, ADYPU, Lohegaon, Pune, Maharashtra, India*
[2]*Faculty - IT, iNurture, Bengaluru, India*
[3]*Senior Faculty - IT, iNurture, Bengaluru, India*

Abstract- Cryptographic attacks are the attacks which tries to break the cryptosystem using various cryptographic techniques are algorithms. This paper mainly focuses on three types of cryptographic attack those are known plaintext attack , ciphertext only attack and chosen plaintext attack. It covers heir descriptions with functionalities and also their application. It also gives thorough comparison between those three types of cryptographic attacks and also tells us about the security measures to be taken and the threat perception about cryptographic attacks.

Keywords- Known Plaintext Attack , Ciphertext Only Attack , Chosen Plaintext Attack.

I. INTRODUCTION

Cryptology is a science which is related with securely storing and communication of data which is usually in a secret form. It consist of two crucial fields : cryptography and cryptanalysis.[4] Converting data to make them more protected and resistant is basically cryptography and cryptanalysis is associated with breaking of codes. In cryptography, provision of information security services by making use of cryptographic techniques is referred as cryptosystem. Cryptosystem is also acknowledged as cipher system . The below diagram illustrates the basic cryptosystem model which is providing confidentiality to the data being transferred from receiver to sender. The below model describes the cryptosystem. In cryptosystem, sender wish to send the message to receiver but confidentiality of the information should be maintained so the plaintext is covered into ciphertext by using encryption algorithm which consist of key and then the ciphertext is transformed into plaintext again to make it readable for the receiver by using decryption algorithm.



The three cryptographic attacks which we are going to discuss:

Known plaintext attack: In this , invader has the access to ciphertext i.e the encrypted text as well as plaintext and through this invader can gain information easily and also can acknowledge the secret keys used.[5]

Chosen plaintext attack: In this, invader can access the ciphertext of corresponding plaintext. In this attack the surveillance of the cryptosystem is reduced and due to which the data which is transferred can be easily crack by the invader.[6]

Ciphertext only attack : In this, invader has availabilityof only the ciphertext and does not access to any of the plaintext , the task of the invader is to discover about the key used or develop some algorithm to get the plaintext out of that ciphertext.[7]

II. KNOWN PLAINTEXT ATTACK

For cryptographers and cryptanalyst known plaintext attack has been topic of major interest.[1]It is very easy for the invader to gain dataregarding the encryption key.In this attack, as the invader know the ciphertext of the comparable plaintext and through manipulating the information invader can get access to key.[8] Adopting this attack against easy and simple cipher is the way of getting more success more rapidly. Known plaintext attack was utilized in the second world war. British attacking the enigma cipher of the german is most commonly known example of this attack at the time of second world war. Simple XOR cipher was initially used in operating system like MS-DOS and machintosh and was quite known. The simple XOR cipher can be get easily targeted by this attack. However now-a-days it is difficult to attack modern ciphers using known plaintext attack.

III. CHOSEN PLAINTEXT ATTACK

An arbitrary plaintext is chosen in this attack and that arbitrary plaintext is later encrypted by the invader and then he gains the analogous ciphertext. Invader later tries to get the knowledge about the secret key or he can find any algorithm as an alternative to decrypt the ciphertext.[9]this attack is more convenient for intruder as intruder gets chance to chose any text , intruder can obtain more dataregarding the system which will be beneficial for intruder. Complexity of exhaustive search applying related key is reduced through adapting chosen plaintext attack technique.[2] Like known plaintext attack similarly chosen plaintext attack was also used in second world war. Within this attack we also have adaptive chosen plaintext attack in which the intruder or attacker goes for the small block of text instead of big block of text which is being encrypted , adapting this technique allows attacker to investigate the system in more detailed manner.

IV. CIPHERTEXT ONLY ATTACK

Only ciphertext is accessible by the attacker in this attack. The attack in which ciphertexts are only thing that are being seen by the adversary is referred as ciphertext only attack.[3] Attacker does not have any access to plaintext. Through the given ciphertext attacker has to discover a secret key or develop an algorithm that can be used to recover the plaintext. Recovering more plaintext is the target of the attacker. Ciphertext only attacks are the attacks which are tried by maximum number of the hackers. So while designing any system and algorithm providing security to them from this attack should be our primary motive. Modern cryptosystems are resistant to this attack.[10]

TABLE OF COMPARISON

ATTACKS	LEVEL OF EASE	LEVEL OF THREAT
Known Plaintext Attack	Easy	Most threatful
Chosen Plaintext Attack	Easy	Optimum threatful
Ciphertext Only Attack	Difficult	Least threatful

V. IMPORTANCE OF OUR RESEARCH

a. THREAT PERCEPTION

Now-a-days with development of technology world is getting habitual to the on-click applications, obviously using this will generate digital data and transportation of information through digital medium is increasing day-by-day. But the data which is being transmitted is very sensitive it may contain someone's address, someone's credit card number. So, to overcome with this security threat encryption technology came up, it will encrypt the data which will make it secure but even after use of encryption various menace to confidentiality are still there. And menace to confidentiality includes cryptographic attack ,they are the method to break the surveillance of the cryptosystem by manipulating and finding a weak point in cipher, code, key etc.

b. STEPS FOR SECURITY

As we know cryptographic attacks are being one of the way to broke the encryption, we can tackle cryptographic attack if we use cryptographic technique properly and in an efficient way to make our cryptosystem strong which also includes managing and utilizing our set of keys in a proper manner. And to achieve this we can follow few simple steps so that we could make our cryptosystem strong and prevent cryptographic attack, for making cryptosystem work perfectly the intended individual should have knowledge about the keys applied to encrypt or decrypt. Various identification and access management tools should be in use in any organization for protecting data. We should have the knowledge about the hierarchy of data ,which is most important and should know which data to be encrypt and which to be not. Providing data security in all of its states should be the main motive because data could be in motion, in rest or in use so it should be protected everytime regardless of in which state it is. While developing your encryption process your should strategize your process and should look out for various things such as key management, classification of data, lifecycle of encryption, access control etc.[11]

VI. FUTURE SCOPE AND DISCUSSION

Cryptography as a whole is developing ,elliptic curve cryptography, quantum computation are few of the technology which will be followed in cryptography. In elliptic curve cryptography the encryption technique uses the behaviour of elliptic curve in finite fields which we know is complex and in quantum computation, this technique is performed in quantum computer or processor. But in future invasions on such techniques are also possible , you can never say that they are fully secured. Somewhere the vulnerabilities are found and utilized against the system that is very harmful for our cryptosystem.[12]

VII. CONCLUSION

Cryptographic encryption technique is being adapted by most of the people. It is secured but still exposed to cryptographic attacks so it is necessary to make your systems secure from such invasion. Known plaintext attack , chosen plaintext attack and ciphertext only attack were the type of attacks that we saw in this paper and also their comparisons and security measures.

VIII. REFERRENCES

[1]. Li Gong, Mark A. Lomas, Roger M. Needham, Jerome H. Saltzer "Protecting Poorly Chosen Secrets From Guessing Attack" IEEE Journal on Selected Areas in Communication, Vol. 11,no.5,June 1993.

[2]. Eli Biham "New Types Of Cryptanalytic Attacks Using Related Keys" Journal of Cryptology.

[3]. Moni Naor, Moti Yung "Public-Key Cryptosystems Provably Secure Against Chosen Ciphertext Attacks.

[4]. Ashish Kumar Kendhe, Himani Agarwal "A Survey Report On Various Cryptanalysis Techniques" International Journal Of Soft Computing And Engineering , Volume-3, Issue-2,May 2013.

[5]. https://en.wikipedia.org/wiki/Known-plaintext_attack accessed on 7th April 2019.

[6]. https://en.wikipedia.org/wiki/Chosen-plaintext_attack accessed on 7th April 2019.

[7]. https://en.wikipedia.org/wiki/Ciphertext-only_attack accessed on 7th April 2019.

[8]. http://www.crypto-it.net/eng/attacks/known-plaintext.html accessed on 7th April 2019.

[9]. http://www.crypto-it.net/eng/attacks/chosen-plaintext.html accessed on 7th April 2019.

[10]. http://www.crypto-it.net/eng/attacks/known-ciphertext.html accessed on 7th April 2019.

[11]. http://edge.siriuscom.com/security/7-key-elements-of-a-successful-encryption-strategyaccessed on 8th April 2019.

[12]. Nicholas G. Mcdonald "Past,Present, And Future Methods Of Cryptography And Data Encryption.