CRYPTANALYSIS AND CRYPTANALYTIC ATTACKS

Cryptanalysis is a study of various methods used to understand or decode encrypted information with no access to the confidential information usually required to do so. It is also referred to as code-breaking or code-cracking.

Types of Cryptanalysis Attacks:

- **Known-Plaintext Analysis or KPA –** In this, the attacker is aware of plaintext-ciphertext pairs. For finding the encryption key, all an attacker has to do is map those pairs. This attack is relatively easy as there is already plenty of information readily available with the attacker.

- **Chosen-Plaintext Analysis or CPA –** This attack is conducted by choosing random plaintexts and then obtaining the corresponding ciphertexts. The attacker must find the encryption key. Though it is pretty similar to KPA and relatively simple to implement, the success rate is not high.

- **Ciphertext-Only Analysis or COA –** An attack of this kind is possible when the attacker knows only some ciphertext and is trying to find the corresponding encryption key and plaintext. Though this kind of attack is the hardest of all, the success rate is relatively high as only the ciphertext is needed.

- **Man-In-The-Middle or MITM attack –** This attack successfully intercepts the message between two communicators sent through a secured channel.

- **Adaptive Chosen-Plaintext Analysis or ACPA –** Though it is similar to CPA, it involves attackers requesting ciphertexts of additional plaintexts.

Tools Used in Cryptanalysis:

- **CrypTool**: Launched in 1998, it is an online learning tool that explains cryptanalysis and cryptography. It aims to explain the concept of network security threats and cryptology. It contains asymmetric ciphers like RSA and elliptic curve cryptography.

- **EverCrack**: It is a GPL open-source software that mainly deals with monoalphabetic substitution and transposition ciphers. It is a cryptanalysis engine that supports multiple languages, including English, French, German, Italian, Spanish, Swedish, etc. It was initially developed in the C language and currently focuses on online web-based applications. Its programming is kernel-based, which means that it deciphers complex ciphers for the kernel.

- **Cryptol**: Developed by software development firm Galois Inc., this learning tool analyzes algorithms and implementations. It was initially designed for NSA; this tool is also widely used by private firms. The programming language is used for developing and using cryptography, such as the implementation and design of new ciphers and verifying cryptographic algorithms.

Attack on DES:

- **brute-force attack:**

Brute Force is the most simple and practical way to break a cipher. It consists in trying every key combination possible until the right one is found. Having the right key you can then break the cipher and read what was ciphered. The number of possibilities is determined by the keys size in bits, since DES only has a 64 bit key, the number of combinations is rather small and a personal computer can break it in a few days. This was the main reason why DES lost its credibility and began not to be used.

*(Note: **Attacks faster than Brute Force Attack***

None of this kind of attacks are feasible to use in practice, but they show that in theory the algorithm has some glitches that by now they might not be a problem, but on the future with the increasing power of the machines they might become a serious concern.)

- **Differential Cryptanalysis :**

Rediscovered by Adi Shamir and Eli Biham back in the 80's, that claimed that in order to break all the 16 rounds of the DES there were required 2^49 chosen texts. Since DES was designed to be DC resistant this was for sure a glitch that could make a faster attack, because the possibilities are not infinite like in brute force, but still it might be as bad, because the attacker needs to be lucky to find a suitable text not beyond the 2^49 attempt.

- **Linear Cryptanalysis:**

In 1993 Mitsuru Matsui discovered that using his method there were "only" needed 2^43 Known plaintexts. This was the first reported experimental LC to DES, and although it's only theoretical it shows once again that DES is breakable specially taking into account that DES was not designed to deal with this kind of attack. Still, there are a lot of texts to test, might not be as practical as brute force.

(NOTE: **DIFFERENCE BETWEEN CRYPTOGRAPHY AND CRYPTANALYSIS)**

Cryptography is used to hide information, especially over an unsecured channel or transmission mode. Today, most of the messages are communicated over the internet, including bank interactions and email communication. Therefore, it becomes imperative to secure messages. This technique converts a plaintext (message to be communicated) to a ciphertext message by employing encryption techniques. The process of obtaining a ciphertext from a plaintext is called decryption.

Cryptanalysis is used as a method of decrypting a ciphertext into plaintext. An unauthorized person tries to decrypt the message by eavesdropping on the unsecured channel. It is also known as **code-breaking**. This person is not bound by any rules. He may use any method to acquire the plaintext.