Chapter 2: A Look into Cryptanalysis

2.1 Security Goals

In this informative age, there is a need to keep information about every aspect of our life. Information is extremely valuable like any other asset. Moreover, it is obvious, like other assets, information need to be secured from *attacks*. Until a few decades ago, the information collected by an organization was stored as physical files. The confidentiality of the file are taken care of by restricting the access among few authorized and trusted people within the organization.

With the advent of computers, information storage became electronic. Instead of being stored in the physical form, it is stored in computers and related devices. To make information secure, it should be protected and kept hidden from unauthorized access during both storage and transmission. To keep information secure, following three requirements need to be maintained:

Confidentiality: Confidentiality is the concealment of information or resources. During the last two decades, computer network created a revolution in the use of information. The need for keeping information secrecy arises from the use of computers in sensitive areas like government and corporate sectors etc.

Integrity: Integrity refers to the trustworthiness of data or resources and it usually deals with in terms of preventing unwanted and unauthorized changes. Integrity includes *content integrity* and *source integrity*. Working with integrity is absolutely different from working with confidentiality. With confidentiality, the data is either compromised or not, but integrity includes both the correctness and trustworthiness of data.

Availability: Availability is the ability to use the desired information or resource. It is an important aspect of reliability and system design. The aspect of availability that is relevant to security is that someone may deliberately arrange to deny access to some data or to a service by making it unavailable. Attempts to block availability are termed *denial of service attack* that can be most difficult to detect.

Cryptographic algorithms are designed to meet the above security goals.

2.2 Cryptanalysis

The goal of cryptanalysis is to find the weaknesses or insecurity in a cryptographic scheme, thus permitting its subversion or evasion. It is common misconception that every encryption method can be broken. In his *WWII* work at *Bell Labs, Claude Shannon* proved that one-time-pad cipher is unbreakable, provided the key material is

truly random, never reused, kept secret from all possible attackers and of equal or greater length than the message. *Cryptanalysis is the science of recovering the plaintext of a message without access to the key. Successful cryptanalysis may recover the plaintext or the key* **[1]**.

An attempt of cryptanalysis is called an *attack*. Attacks can be divided into two broad categories:

Cryptanalytic Attack: There are three general types of cryptanalytic attack **[41]**.

i. Ciphertext-only Attack: In this attack the attacker knows only the ciphertext to be decoded. The attacker will try to find the key or decrypt one or more pieces of ciphertext (only relatively weak algorithms fail to withstand a ciphertext-only attack).
ii. Known-plaintext Attack: The attacker has a collection of plaintext-ciphertext pairs and is trying to find the key or to decrypt some other ciphertext that has been encrypted with the same key.
iii. Chosen-plaintext Attack: This is a known plaintext attack in which the attacker can choose the plaintext to encrypted and read the corresponding ciphertext.

There are at least two other types of cryptanalytic attack.

i. Chosen-ciphertext Attack: The attacker has the able to select any ciphertext and study the plaintext produced by decrypting them.
ii. Chosen-key Attack: The attacker has the abilities required in the Chosen-plaintext and Chosen-ciphertext attacks.

An encryption scheme is *unconditionally secure* if the generated ciphertext does not contain enough information to determine uniquely the corresponding plaintext. Except onetime pad, no cipher is unconditionally secure.

The security of a *conditionally secure* algorithm depends on the difficulty in reversing the underlying cryptographic problem. Other than the one-time pad, all other ciphers fall into this category.

An encryption scheme is said to be *computationally secure* if:

a. The breaking of cipher is costly than the cost of the encrypted information.
b. The breaking of cipher is more time consuming than the useful lifetime of the information.

Non-cryptanalytic Attack: The non-cryptanalytic attacks do not exploit the mathematical weaknesses of the cryptographic algorithm. However, the goals of security can very much threatened by this class of attack. Figure 2.1 shows the taxonomy.

2.2.1 Differential Cryptanalysis

One of the most significant advances in cryptanalysis in recent years is differential cryptanalysis. Although this appears to have been discovered at least 30 years ago it was not reported in the open literature until 1990. The first published effort appears to have been the cryptanalysis of a block cipher called FEAL. This was followed by a number of papers by Biham and Shamir.

Differential cryptanalysis is the first popular attack that is capable of breaking DES in less than 2^{55} complexity.

Differential cryptanalysis exploits the high probability of certain occurrences of plaintext differences and differences into the last round of the cipher **[26]**. For example, consider a system with input $X = [X_1\, X_2 \ldots\ldots X_n]$ and output $Y = [Y_1\, Y_2 \ldots\ldots Y_n]$. The input difference is given by $\triangle X = X' \oplus X''$ where $\oplus$ represents a bit-wise exclusive-OR of $n - bit$ vectors. Hence, $\triangle X = [\triangle X_1\ \triangle X_2 \ldots.\triangle X_n]$. Similarly $\triangle Y = Y' \oplus Y''$ is the output difference and $\triangle Y = [\triangle Y_1\ \triangle Y_2 \ldots.\triangle Y_n]$. Differential cryptanalysis seeks to exploit a scenario where a particular $\triangle Y$ occurs given a particular input difference $\triangle X$ with a very high probability p_D. The pair $\triangle X$ & $\triangle Y$ is referred to as a differential cryptanalysis.

Differential cryptanalysis is a chosen plaintext attack, meaning that the attacker is able to select inputs and examine outputs in an attempt to derive the key.

2.2.2 Linear Cryptanalysis

Linear cryptanalysis tries to take advantage of high probability occurrences of linear expressions involving plaintext bits, ciphertext bits (actually bits from the 2nd last round output are used), and subkey bits. It is a known plaintext attack: that is, it is premised on the attacker having information on a set of plaintexts and the corresponding ciphertexts. However, the attacker has no way to select which plaintexts (and corresponding ciphertexts) are available. In many applications and scenarios, it is reasonable to assume that the attacker has knowledge of a random set of plaintexts and the corresponding ciphertexts. The basic idea is to approximate the operation of a portion of the cipher with an expression that is linear where the linearity refers to a mod-2 bit-wise operation (i.e., exclusive-OR denoted by "⊕"). Such an expression is of the form:

$$X_{i_1} \oplus X_{i_2} \oplus \ldots \oplus X_{i_u} \oplus Y_{j_1} \oplus Y_{j_2} \oplus \ldots \oplus Y_{j_v} = 0$$

where X_i represents the i^{th} bit of the input $X = [X_1, X_2, \ldots]$ and Y_j represent the j^{th} bit of the output $Y = [Y_1, Y_2, \ldots]$. This equation is representing the exclusive-OR "sum" of u

input bits and v output bits. The approach in linear cryptanalysis is to determine expressions of the form above which have a high or low probability of occurrence.

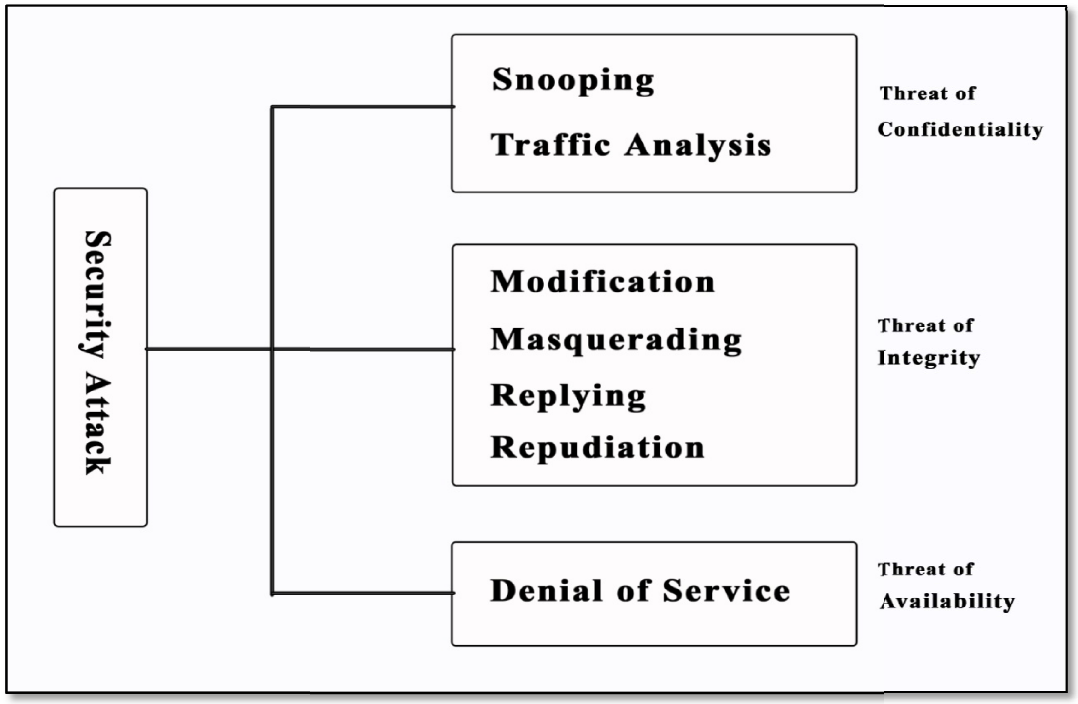

Figure 2.1: Taxonomy of Non-cryptanalytical Attack

2.3 More Attacks on Cryptosystem

Some more methods of attack on symmetric ciphers like DES and AES are discussed below:

2.3.1 Birthday Attack

The Birthday attack is a use of Linear Cryptanalysis, where it tries to attack cryptographic hash function by using Birthday paradox. The Birthday paradox can be stated as **[41]**:

What is the minimum value of k such that the probability is greater than 0.5 that at least two people in a group of k people have same birthday? The answer is 23 which quite a surprising result is. If there are 100 people $(i.e. k = 100)$ then the probability is $.9999997$ and the graph of the probabilities against the value of k is shown in Figure 2.2

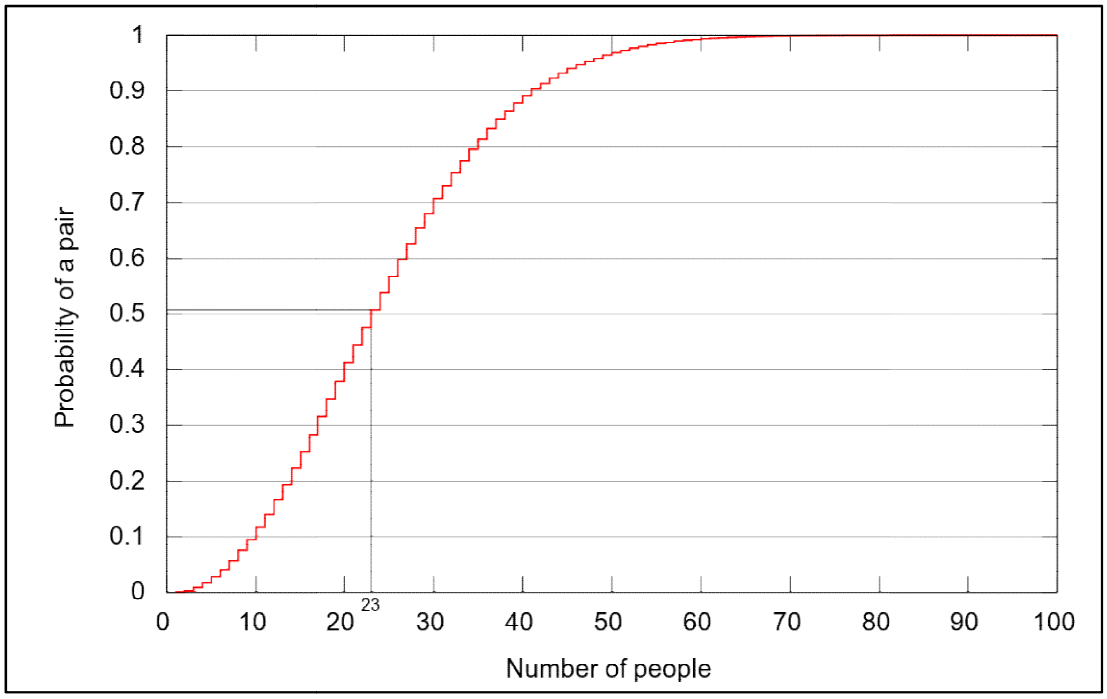

Figure 2.2: The Birthday Paradox

2.3.2 Implementation Attack

In comparison to others, the Implementation attack is a different approach to reveal the secret key. This method of attack searches the advantage of physical characteristics that occurs when a cryptographic algorithm is implemented in hardware. It never approaches the mathematical properties of the algorithm like as side channel attack. The approach of this attack deals with security requirements of cryptographic module like *Power Analysis*, *Timing Analysis*, *Fault Induction* and *TEMPEST*.

2.3.2.1 Power Analysis

The attack based on the analysis of power consumption can be divided into two types: Simple Power Analysis (SPA) and Differential Power Analysis (DPA). SPA involves direct analysis of electrical power consumption patterns whereas DPA has the same approach but utilizes advance statistical methods or other techniques to analyze the variations of electrical power consumption of a cryptographic module.

2.3.2.2 Timing Analysis

Measuring the time required by the cryptographic module to perform a mathematical operation of a cryptographic algorithm or process is the pathway of Timing analysis attack.

2.3.2.3 Fault Induction

Fault Induction attack utilizes external forces like microwaves, temperature, voltage to cause processing errors in the cryptographic module. Proper selection of physical security features may be used to reduce the risk of this attack.

2.3.1.4 TEMPEST

TEMPEST attack deals with detection and collection of electromagnetic signals emitted from a cryptographic module and associated equipment during processing.

2.3.3 Timing Attacks

A timing attack is analogous to a wild guessing the combination by observing how long it takes for someone to turn the dial from number to number. Timing attack is a serious threat and there are simple counter measures that can be used including the followings:

- Constant Exponentiation Time
- Random Delay
- Blinding

2.3.4 Boomerang Attack

Differential analysis has been used to break many published ciphers then that block cipher designers are thoughtful to ensure security against differential style attacks **[42]**. The algorithm designer obtains somehow an upper bound p on the probability of any differential characteristic for the cipher. Then the designer invokes an oft-repeated "folk theorem" to justify that any successful differential attack will require at least $1/p$ texts to break the cipher.

Unfortunately, according to David Wagner **[42]** this folk theorem is wrong and exhibits an attack which is Boomerang Attack.

The Boomerang attack is a differential attack that attempts to generate a quartet structure at an intermediate value half-way through the cipher. The attack considers four plaintexts P, P', Q, Q'along with their ciphertexts C, C', D, D'. Let E represents the encryption operation, and decompose the cipher into$E = E_1 \circ E_0$, where E_0 represents the first half of the cipher and E_1 represents the last half and the differential characteristics used call $\Delta \rightarrow \Delta^*$, for E_0 and $\nabla \rightarrow \nabla^*$ for E_1^{-1}. The graphical structure is shown in Figure 2.3 below.

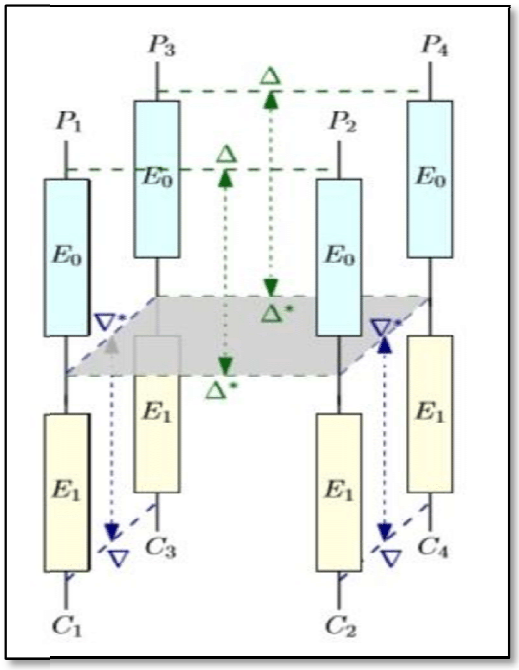

Figure 2.3: Boomerang Attack

2.4 Truncated Differential Analysis

The concept of truncated differential analysis was introduced by Lars R. Knudsen in **[49]**. Truncated differential is a type of differential where only a part of the difference in the ciphertexts can be predicted. The block ciphers which are secure against differential attack those are vulnerable against truncated differential or other higher order differentials. Traditional differentials used to predicts n bits of $2n$ bits block ciphers. So a differential that predict only a part of n bits value is called truncated differential.