**Cryptanalysis**

Cryptanalysis is the study of cryptosystems with the objective of attacking them and decrypting codes and ciphers. The field includes rigorous mathematical investigation of encryption and decryption algorithms as well as side-channel attacks whereby flaws in implementation are exploited rather than a mathematical flaw in the algorithm itself.

Cryptanalysis generally falls into one of several categories which can be broadly considered to be ciphertext only (where only the encrypted output is known), known plaintext (where the plaintext corresponding to some given ciphertext is known), chosen plaintext (where the cryptanalyst may choose plaintext and receive the related ciphertext) and chosen ciphertext attacks (where the cryptanalyst may choose some ciphertext and receive the corresponding plaintext).

**Linear & Differential Cryptanalysis**

These are both instances of known plaintext attacks where to be effective a certain amount of plaintext and its corresponding ciphertext must be known. The approaches were initially designed to aid in breaking the Data Encryption Standard (DES). In this case the fact that the algorithm was known (although the key in each case was not) enabled plaintext to be encrypted by the cryptanalyst to see the related ciphertext.

Linear cryptanalysis is an approach where we aim to find affine approximations to the action of a cipher. Letter frequency analysis is one of the simplest forms of linear cryptanalysis. Differential cryptanalysis is an approach to cryptanalysis whereby differences in inputs are mapped to differences in outputs and patterns in the mappings of plaintext edits to ciphertext variation are used to reverse engineer a key.

Linear and differential cryptanalysis are most often applied to block ciphers (encryption functions operating on messages that are split into blocks). They are symmetric key algorithms.

**Linear Cryptanalysis**

The paradigm of linear cryptanalysis was originally designed in 1993 as a theoretical attack on DES. It is now used widely on block ciphers across the field of cryptanalysis and is an effective starting point for developing more complex attacks. Linear cryptanalysis posits a linear relationship between the elements (characters or individual bits) of plaintext, the ciphertext, and the key. It therefore tries to find a linear approximation to the action of a cipher, i.e. if "ciphertext = f(plaintext, key)", then we are trying to find a linear approximation of f. Any linear relation between the plaintext bits and ciphertext bits can be written as a chain of exclusive-or operations of the following form:

Xi1⊕Xi2⊕⋯⊕Xiu⊕Yj1⊕Yj2⊕⋯⊕Yjv

=Kk1⊕Kk2⊕⋯⊕Kk

where ⊕ denotes the binary operation XOR (exclusive-OR), Xi denotes the ith bit of the input X = [X1, X2, …], Yj denotes the jth bit of the output Y = [Y1, Y2, …] and Kk denotes the kth bit of the key K = [K1, K2, …]. The sum therefore denotes the XOR ‘sum’ of u input and v output bits vs w private key bits.

**Steps to perform Linear Cryptanalysis**

In the most common use case, we assume that everything about the encryption algorithm is known apart from the private key. Performing linear cryptanalysis on a block cipher usually consists of three steps.

1. Find linear approximations of the non-linear parts of the encryption algorithm (usually only the substitution boxes, known as S-boxes).
2. Combine linear approximations of S-boxes with the rest of the (linear) operations done in the encryption algorithm, to obtain a linear approximation of the entire encryption algorithm. This linear approximation is a function which relates the plaintext bits, the ciphertext bits, and the bits of the private key.
3. Use the linear approximation as a guide for which keys to try first. This leads to substantial computational savings over trying all possible values of the key. Multiple linear approximations may be used to further cut down the number of keys that need to be tried.

**Differential cryptanalysis** preceded linear cryptanalysis having initially been designed in 1990 as an attack on DES. Differential cryptanalysis is similar to linear cryptanalysis; differential cryptanalysis aims to map bitwise differences in inputs to differences in the output in order to reverse engineer the action of the encryption algorithm. It is again aiming to approximate the encryption algorithm looking to find a maximum likelihood estimator of the true encryption action by altering plaintexts or (looking at different plaintexts) and analysing the impact of changes to the plaintext to the resulting ciphertext. Differential cryptanalysis is therefore a chosen plaintext attack.