DIFFERENTIAL LINEAR ATTACK

Differential-Linear Attack is a hybrid cryptanalysis technique that combines differential cryptanalysis and linear cryptanalysis to attack symmetric-key block ciphers. The differential-linear attack uses a differential characteristic on the first rounds and a linear approximation on the last rounds to exploit weaknesses more efficiently than either method alone. By filtering plaintext-ciphertext pairs that follow the differential characteristic, the attacker applies the linear approximation to the filtered set. To find the good differential linear characteristic, a Differential Linear Connectivity Table (DLCT) is needed. The DLCT shows how strongly input differences and linear masks are connected through an S-Box. or a vectorial Boolean function S : $\{0, 1\}^n \rightarrow \{0, 1\}^m$ (e.g., an n-to-m bit S-box in a block cipher), the DLCT of S is an $2^n \times 2^m$ table whose rows correspond to input differences to S and whose columns correspond to bit masks of outputs of S. The value in the cell (Δ, λ), where Δ is a difference and λ is a mask is given as

$$DLCT_S(\Delta, \lambda) \triangleq \left| \left\{ x \middle| \lambda \cdot S(x) = \lambda \cdot S(x \oplus \Delta) \right\} \right| \cdot$$

This Project presents construction of DLCT table for the S-boxes of DES, Midori Cipher and PRESENT Cipher.

*The input S-Boxes are given as apart of the program and the DLCT for the corresponding S-boxes are stoed in .txt files.

DES/ main.py:

This program contains two functions: extractbits() and computedlct(). Extratbits() takes any six bit input and return the row index and column index. Computedlct() generate the 64*16 DLCTfor all the 8 s-boxes and store it in the dlct_tables.txt.
DES/ DES_S_Boxes.py contains the 8 s-boxes of DES.

midori/main.py: Midori is a block cipher and it contains 2 sboxes. It generates the DLCT for the two s-boxes and the result in stored in midori_dlct_table.txt.

Input: Midori S-box
Output: DLCT for the midori S-box

Present/main.py: PRESENT is a lightweight block cipher and it contains one s-box. This code generates the DLCT for the PRESENT S-box and result is stored in present_dlct_table.txt

Input: PRESENT S-box
Output: DLCT for the PRESENT S-box

By analyzing the DLCT of the DES S-boxes, the DL attack can be performed on reduced round DES. DL Attack can be performed on ASCON encryption algorithm. (ref: https://eprint.iacr.org/2019/256.pdf)