A. Phần 1

Tấn công như thế nào

Đầu tiên là chọn ra 2 plaintext P và P' và 2 cyphertext C và C' tương ứng.

Nếu C⊕C' = b, thì đây là một cặp hợp lệ. Với b là sự khác biệt giữa các cặp bản mã và bản rõ (vi sai).

Đặt K_R biểu thị chìa khóa liên quan đến vòng cuối cùng. Thông thường, chỉ cần một số bit của K_R để mở rộng đặc tính vi sai thành R vòng, tương ứng với các hộp S "hoạt động" của vòng R; chúng ta hãy biểu thị các bit này bằng k_R. Nếu chúng ta thực hiện vòng cuối cùng này cho mọi k_R có thể, và đếm số lần xuất hiện của đặc trưng khác biệt của chúng ta cho mỗi k_R, thì sau khi có đủ số lượng cặp văn bản rõ, cặp văn bản chính xác có thể được phân biệt.

Trong điều kiện gì

Để thực hiện tấn công người tấn công phải có được bản rõ đơn giản và bản mã của nó từ đó phân tích giá trị khác nhau của các cặp bản mã tương ứng. Cách Substitution Box hoạt động. Phải có một số cặp vi sai input và output với tỉ lệ cao.

Độ phức tạp

- $\frac{c}{p}$. Với c là số nhỏ và p là tỉ lệ của R – 1 round đầu tiên

No. of Round	Chosen Plaintexts	Known Plaintexts	Complexity
8	2^{14}	2^{38}	2^{9}
10	2^{24}	2^{43}	2^{15}
12	2^{31}	2^{47}	2^{21}
14	2^{39}	2^{51}	2^{29}
16	2^{47}	2^{55}	2^{37}

Định lý nào

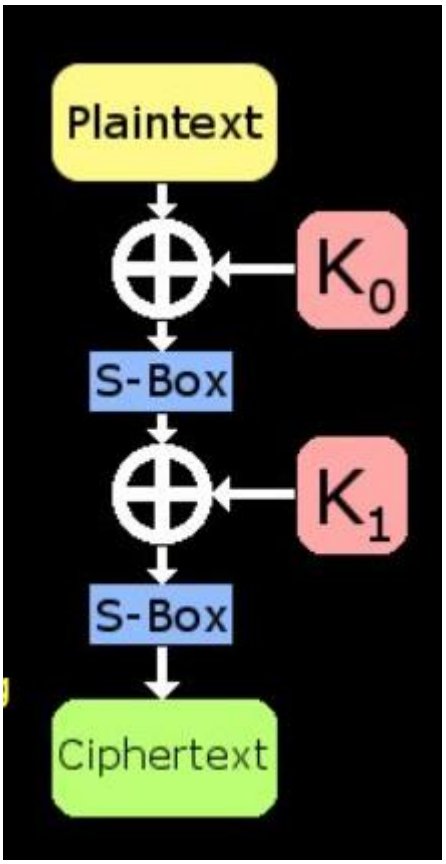
Giá trị của khóa không ảnh hưởng đến giá trị của vi sai

C Xor C' = P Xor K Xor P' Xor K

C Xor C' = P Xor P'

B. Phần 2

Ví dụ đơn giản với 2 round DES:



- K0 = 9, K1 = 3
- Sbox:

Input	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Output	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

- Bước 1, tính toán bảng phân phối vi sai của R – 1 round đầu tiên (ở đây 2 – 1 = 1 round).

```
Difference Distribution Table:
16 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 2 0 0 0 2 0 2 4 0 4 2 0 0
0 0 0 2 0 6 2 2 0 2 0 0 0 0 2 0
0 0 2 0 2 0 0 0 0 4 2 0 2 0 0 4
0 0 0 2 0 0 6 0 0 2 0 4 2 0 0 0
0 4 0 0 0 2 2 0 0 0 4 0 2 0 0 2
0 0 0 4 0 4 0 0 0 0 0 0 2 2 2 2
0 0 2 2 2 0 2 0 0 2 2 0 0 0 0 4
0 0 0 0 0 0 2 2 0 0 0 4 0 4 2 2
0 2 0 0 2 0 0 4 2 0 2 2 2 0 0 0
0 2 2 0 0 0 0 0 6 0 0 2 0 0 4 0
0 0 8 0 0 2 0 2 0 0 0 0 0 2 0 2
0 2 0 0 2 2 2 0 0 0 0 2 0 6 0 0
0 4 0 0 0 0 0 4 2 0 2 0 2 0 2 0
0 0 2 4 2 0 0 0 6 0 0 0 0 0 2 0
0 2 0 0 6 0 0 0 0 4 0 2 0 0 2 0
```

Từ bảng trên ta thấy được giá trị $\Delta X = B \rightarrow \Delta Y = 2$ là có tỉ lệ lớn nhất (8/16).

- Bước 2, từ các cặp plaintext và cyphertext thỏa mãn điều kiện: X1 = X, X2 = X Xor ΔX và Y1, Y2 tương ứng, ta tính toán được K1 tương ứng (đã biết Y1 Xor Y2 = ΔY và cách Substitution Box hoạt động). Từ các K1 tính toán được chọn ra K1 với tỉ lệ xuất hiện cao nhất.

```
Input Dif: 11
Output Dif: 2
Key 0: 9
Key 1: 3
K1 found: 3
```