

Tutorial on Differential Cryptanalysis

An Example of a 0R-Attack on 5-Round DES

Here is a right pair:

$$P = D8\ A5\ 3E\ ED\ F2\ 28\ A6\ 3B$$

$$P^* = 98\ F9\ 3E\ ED\ F6\ 28\ A6\ 3B$$

$$T = A5\ 31\ 95\ F7\ B4\ 6B\ 7D\ DC$$

$$T^* = E5\ 6D\ 95\ F7\ B0\ 6B\ 7D\ DC$$

$$T' = 40\ 5C\ 00\ 00\ 04\ 00\ 00\ 00$$

$$P^{-1}(40\ 08\ 00\ 00) = 0A\ 00\ 00\ 00$$

$$E(T'_R) = E(04\ 00\ 00\ 00) = 00_x\ 08_x\ 00_x\ 00_x\ 00_x\ 00_x\ 00_x\ 00_x$$

When we look at the D.D.T. of $S2$ in the entry $08 \rightarrow A$ we see that there are 16 pairs of input with difference 08 that can create an output difference of A in $S2$, they are:

$(02,0A)$, $(06,0E)$, $(0A,02)$, $(0E,06)$, $(11,19)$, $(15,1D)$, $(19,11)$, $(1D,15)$, $(20,28)$, $(22,2A)$, $(24,2C)$, $(26,2E)$, $(28,20)$, $(2A,22)$, $(2C,24)$, $(2E,26)$.

$$E(T_R) = E(B4\ 6B\ 7D\ DC) = 16_x\ 28_x\ 0D_x\ 16_x\ 2F_x\ 3B_x\ 3B_x\ 39_x$$

Therefore, the possible subkey values for $S2$ in the fourth round is the list $\oplus 28_x$:

$2A$, $2E$, 22 , 26 , 39 , $3D$, 31 , 35 , 08 , $0A$, $0C$, $0E$, 00 , 02 , 04 , 06 .

Note that the same list is produced by considering T^* . Thus exhaustive search is reduced by a factor 4, since we have 16 values to 6 bits (i.e., we found two bits of information).

An Example of a 0R-Attack on 5-Round DES (cont.)

Using another right pair whose:

$$T = 33 \ F2 \ 30 \ 55 \ C7 \ 44 \ 49 \ 75$$

$$E[T_R] = E[C7 \ 44 \ 49 \ 75] = 38_x \ 0E_x \ 28_x \ 08_x \ 09_x \ 12_x \ 2E_x \ 2B_x$$

Therefore, the possible subkey values for $S2$ in the fourth round is the list $\oplus 0E_x$:

0C, 08, 04, 00, 1F, 1B, 17, 13, 2E, 2C, 2A, 28, 26, 24, 22, 20

The correct subkey must appear in both suggestions, therefore in their intersection, which is:

0C, 04, 2A, 2E, 26, 22, 00, 08.

By intersecting with another pair whose:

$$T = A4 \ 9C \ AD \ EE \ 0E \ EE \ 40 \ 01$$

$$E[T_R] = E[0E \ EE \ 40 \ 01] = 21_x \ 1D_x \ 1D_x \ 1C_x \ 08_x \ 00_x \ 00_x \ 02_x$$

Therefore, the possible subkey values for $S2$ in the fourth round is the list $\oplus 1D_x$:

1F, 1B, 17, 13, 0C, 08, 04, 00, 3D, 3F, 39, 3B, 35, 37, 31, 33

The correct subkey must appear in both suggestions, therefore in their intersection, which is:

0C, 04, 00, 08.

Note that $0C \oplus 04 = 08$, $00 \oplus 08 = 08$, which actually forced by the characteristics.

Remark: The key that was used was $0A \ 0A \ 0A \ 0A \ 0A \ 0A \ 0A \ 0A$, which means that the subkey entering $S2$ of round five is: 000000_b