CS5760: Topics in Cryptanalysis **2025**

Lecture 4: 27 January 2025

Instructors: Maria Francis and M. V. Panduranga Rao *Scribe: Gautam Singh*

4.1 Attack on DES

The iterative characteristic by itself is not enough to break 16-round DES due to its low probability. However, it was enough for DES reduced to 15 rounds. To retain this probability, we use a new round 1. This new round 1 will generate plaintexts with XOR $(\psi, 0)$ which can then be fed into the characteristic.

Suppose P is a 64-bit plaintext and let v_i be a 32-bit constant with the first 12 bits equal to the possible outputs of S1, S2, S3 after the first round and 0 elsewhere for $0 \leq i < 2^{12}$. Define for $0 \leq i < 2^{12}$

$$P_i = P \oplus (v_i, 0) \quad \bar{P}_i = P_i \oplus (0, \psi) \tag{4.1}$$

$$T_i = \mathrm{DES}(P_i, K) \quad \bar{T}_i = \mathrm{DES}(\bar{P}_i, K). \tag{4.2}$$

Then, $P_i \oplus P_j = (v_k, \psi)$. Out of the 2^{24} possibilities of (i, j), each v_k occurs exactly 2^{12} times. Now, an XOR of ψ is fed into the first round, but we do not know which v_k is to be chosen initially to cancel the output of the F function and give us the desired $(\psi, 0)$ input to the second round. Trying all 2^{24} possibilities is slow. To find the right v_k, we exploit the cross-product structure of P_i and $\bar{P}_j$. Notice that a right pair will have zero outputs at S4, ..., S8 at the last round. Thus, we can feed in the plaintexts P_i and $\bar{P}_j$ to get outputs T_i and $\bar{T}_j$. These 2^{13} outputs can then be hashed by these 20 positions.