# Linear attacks

$$\Pr\left[\, m[i_1]\oplus\cdots\oplus m[i_r] \;\oplus\; c[j_1]\oplus\cdots\oplus c[j_v] \;=\; k[l_1]\oplus\cdots\oplus k[l_u] \,\right] = \tfrac{1}{2} + \varepsilon$$

Thm: given $1/\varepsilon^2$ random $(m, c=DES(k, m))$ pairs then

$$k[l_1,\ldots,l_u] \;=\; \text{MAJ}\left[\; m[i_1,\ldots,i_r] \;\oplus\; c[j_1,\ldots,j_v] \;\right]$$

with prob. ≥ 97.7%

$\Rightarrow$ with $1/\varepsilon^2$ inp/out pairs can find $k[l_1,\ldots,l_u]$ in time $\approx 1/\varepsilon^2$ .