$$= \alpha(x+y) = \alpha x + \alpha y$$

$$f(x+y) = f(x) + f(y)$$

$$f(x) = \alpha x$$

$$f(x \oplus y) = f(x) \oplus f(y)$$

$k?$ $E_k(x) = y$ $2^{56} \to 2^{55}$

$E_k(\bar{x}) = y'$

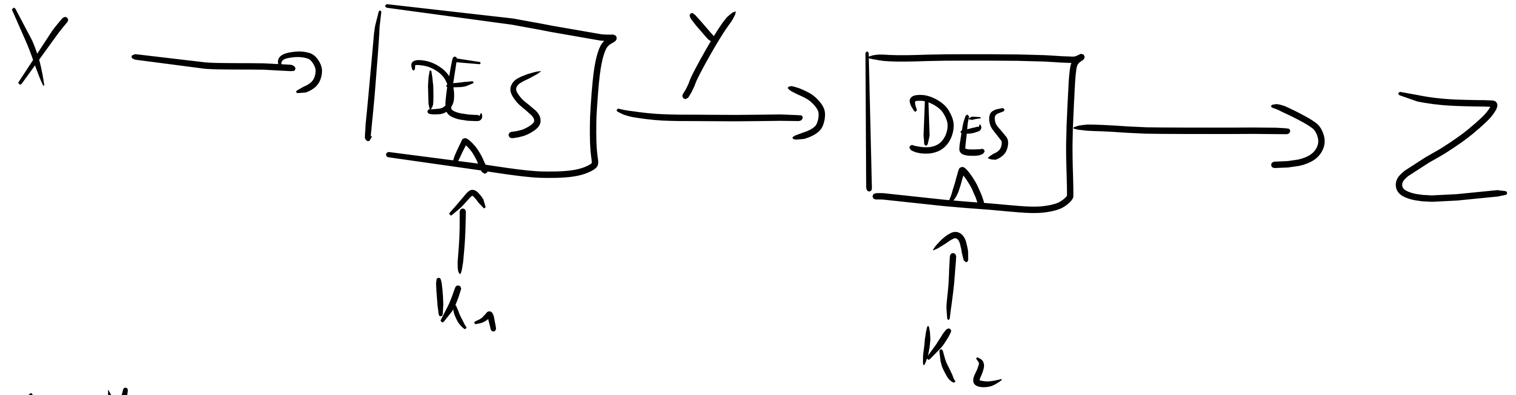
For each k^* s.t. first bit is zero

$$E_{k^*}(x) \overset{?}{=} y$$

$$E_{k^*}(x) \overset{?}{=} \overline{y'} \to E_{\overline{k^*}}(\bar{x}) = y'$$

$$DES_{K_2}(DES_{K_1}(X)) = Z$$

X' Z'



K_1^* K_2^*

$$Y = DES_{K_1^*}(X)$$

$$Y = DES^{-1}_{K_2^*}(Z)$$

```
$2^{56}$ [ Loop over $K_1^*$
             $(K_1^*, DES_{K_1^*}(X))$          ↙ y
             store in a table
                          $2^{56}$ entries
+
$2^{56}$ [ Loop over $K_2^*$
             $Y = DES^{-1}_{K_2^*}(Z)$
             look up $(K_1^*, Y)$
=            $DES_{K_1^*}(DES_{K_2^*}(X')) = Z'$
time: $2^{57}$
```