H(x,y)=AES(x,x) xor y
Возьмём x_1 любое
Возьмём y_1=AES(z,z), где z — любое
Тогда следует взять x_2=z и y_2=AES(x_1,x_1)
Получили пары, на которых данная хэш-функция даёт коллизии