实验 1: DES 加密算法实现

1. 实现 16 轮 DES 加密算法.
2. DES 算法正确性检验：请依据下面的实验结果检验程序的正确性.
   - **设16进制明文X为：**
     0123456789ABCDEF
   - **密钥K为：123456789ABCDEF0**
   - **加密后的密文为：**

     85E813540F0AB405
3. 随机生成 64 比特明文 x，随机生成 64 比特密钥 k，

i. 随机改变明文 x 的一个比特位，即 1 变 0, 0 变 1，得到 x'.

测试 $y = \mathrm{DES}_{\mathrm{k}}(x)$和 $y' = \mathrm{DES}_{\mathrm{k}}(x')$中有多少位不同，即

$$y \oplus y'$$

中“1”的个数.

ii. 设 $\mathrm{DES}_{\mathrm{k}}^{i}(x)$ 是 DES 经过 i 轮加密后的结果，其中 $1 \le i \le 16$.

对 $i = 1, \ldots, 16$ 分别测试 $z = \mathrm{DES}_{\mathrm{k}}^{i}(x)$ 与 $z' = \mathrm{DES}_{\mathrm{k}}^{i}(x')$ 有多少位不同. 找到最小的 i 值，使得 $z \oplus z'$ 中“1”的个数约等于 32.

iii. 对明文 x 的 64 个不同的位置分别进行试验 ii.

假设 x'是 x 第 j 个位置取反后的结果，即 1 变 0, 0 变 1.

对固定的 i，记 $z = \mathrm{DES}_{\mathrm{k}}^{i}(x)$，$z' = \mathrm{DES}_{\mathrm{k}}^{i}(x')$.

我们记 $z \oplus z'$ 中“1”的个数为 $e(i, j)$.

计算

$$e_i = \frac{1}{64}\sum_{j=1}^{64} e(i, j), \quad i = 1,2, \ldots, 16.$$

找到最小的 i 值，使得$e_i \approx 32$.