1. 若明文是 $\{00010203040506070809 0A0B0C0D0E0F\}$,
密钥是 $\{01010101010101010101010101010101\}$，考虑 AES 加密算法的运算：

(a) 用 4×4 的矩阵表示最初的状态数组；

(b) 给出初始化轮密钥加后的状态数组；

(c) 给出字节代替后的状态数组；

(d) 给出行移位后的状态数组；

(e) 给出列混淆后的状态数组。

2. 教材 81 页第 3 题。

2025 年 3 月 12 日