应用密码学 第二次作业参考答案

1. 主观题

在 AES 算法中，构造有限域时使用的不可约多项式为 $x^8+x^4+x^3+x+1$，x 乘指用位运算实现 x 乘以一个普通的多项式：

$$b_7x^7+b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x^1+b_0x^0$$。

因此，有限域 GF(2^8)中，例如 16 进制“02”等价于多项式“x”，例如“05”等价于多项式“x^2+1”，使用 x 乘实现有限域 GF(2^8)上的字节运算方法计算：

16 进制的“0D”与“5||学号尾号”相乘的值。

解：以学号尾号为 7 为例，给出求解的详细过程如下：

0D= (0000 1101)

57= (0101 0111)　　#学号尾号为 7

$$\{57\}\cdot\{02\}=\{01010111\}\cdot\{00000010\}=\{10101110\}=\{AE\}$$

$$\begin{aligned}\{57\}\cdot\{04\}&=\{AE\}\cdot\{02\}=\{10101110\}\cdot\{00000010\}\\&=\{01011100\}\oplus\{00011011\}=\{01000111\}=\{47\}\end{aligned}$$

$$\{57\}\cdot\{08\}=\{47\}\cdot\{02\}=\{01000111\}\cdot\{00000010\}=\{10001110\}=\{8E\}$$

$$\begin{aligned}\{0D\}\cdot\{57\}&=(\{01\}\oplus\{04\}\oplus\{08\})\cdot\{57\}\\&=(\{01\}\cdot\{57\})\oplus(\{04\}\cdot\{57\})\oplus(\{08\}\cdot\{57\})\\&=\{01010111\}\oplus\{01000111\}\oplus\{10001110\}\\&=\{57\}\oplus\{47\}\oplus\{8E\}\\&=\{9E\}\end{aligned}$$

学号尾号为 0 算出来的最终结果为{BD}

学号尾号为 1　算出来的最终结果为{B0}

学号尾号为 2 算出来的最终结果为{A7}

学号尾号为 3 算出来的最终结果为{AA}

学号尾号为 4 算出来的最终结果为{89}

学号尾号为 5 算出来的最终结果为{84}

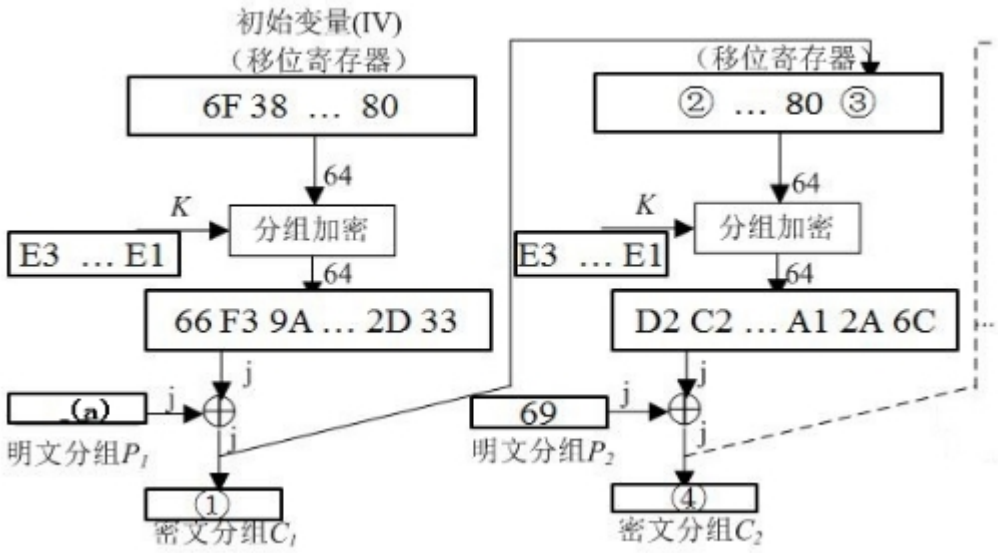
学号尾号为 6 算出来的最终结果为{93}

学号尾号为 8 算出来的最终结果为{D5}

学号尾号为 9 算出来的最终结果为{D8}

2.主观题

下图是某分组密码算法的 CFB 模式加密过程，图中所有数据为 16 进制。假设消息的长度超过 100 个分组，反馈长度为 j=8bits。其中(a)处为学号尾号的 16 进制。例如，‘0’的十进制为 48, 16 进制为 30H。



(1) 题目中的填空如下：

#学号尾号为 7，十进制为 55，16 进制为 37H

① $37 \oplus 66 = 51$

② 38

③ 51

④ $69 \oplus D2 = BB$

(2) 解密过程图