

# Course Designs for Mathematical Foundations of Cyberspace Security

Organized by c0ver

January 2021

## 1

- (1) 求学号反序组成的数字内最大的 2 个素数;
- (2) 求学号正序和反序组成的两个数字的最大公因数和最小公倍数。

## 2 RSA 加密与解密:

1. 使用学号反序组成的数字内最大的 2 个素数对学号进行 RSA 加密和解密运算;
2. 使用中国剩余定理对解密运算进行加速。

## 3 现有一个花色的扑克牌，将扑克牌记作:

$$G \left( A \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 10 \ J \ Q \ K \right)$$

1. 按照置换群  $G_1, G_2, G_3$  各洗  $r_1, r_2, r_3$  次，输出结果;
2. 如果要求再洗若干次要求复原  $G$ ，如何操作? ( $r_1, r_2, r_3$  分别是学号的最后 3 位:2、0、3)

$$G_1 \left( \begin{array}{cccccccccccc} A & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & J & Q & K \\ 10 & Q & A & 5 & 2 & 6 & K & 3 & 8 & 9 & 7 & J & 4 \end{array} \right)$$

$$\mathbf{G}_2 \left( \begin{array}{cccccccccccccccc} A & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & J & Q & K \\ 3 & 6 & 7 & A & 10 & K & 4 & 2 & J & Q & 9 & 5 & 8 \end{array} \right)$$

$$\mathbf{G}_3 \left( \begin{array}{cccccccccccccccc} A & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & J & Q & K \\ 4 & A & 3 & K & J & 10 & 6 & Q & 8 & 9 & 5 & 7 & 2 \end{array} \right)$$