Cryptography: Homework 9

(Deadline: 10am, 2022/11/25)

1. (30 points) Suppose that the current state in an AES encryption is

$$s = \begin{pmatrix} 33 & D2 & 04 & 96 \\ F1 & C4 & D0 & 0C \\ 8C & E7 & DE & 48 \\ D3 & A4 & 2C & B5 \end{pmatrix}.$$

   Calculate **MixColumns**(s).

2. (20 points) Consider the following key-exchange protocol:

   - Alice chooses $k, r_1 \in \{0,1\}^n$ uniformly, and sends $s_1 = k \oplus r_1$ to Bob.
   - Bob chooses $r_2 \in \{0,1\}^n$ uniformly, and sends $s_2 = s_1 \oplus r_2$ to Alice.
   - Alice chooses $r_3 \in \{0,1\}^n$ uniformly, and sends $s_3 = s_2 \oplus r_3$ to Bob.
   - Bob chooses $r_4 \in \{0,1\}^n$ uniformly, and sends $s_4 = s_3 \oplus r_4$ to Alice.
   - Alice computes $s_5 = k \oplus s_3 \oplus s_4$ and sends s_5 to Bob.
   - Alice outputs k and Bob outputs $s_5 \oplus r_4$.

   Is the protocol correct? Is the protocol secure? Prove your answers.