Homework 1

Task 1 - Encryption Scheme (10 points)

(a)

procedure $\mathsf{Dec}(K = (d, \pi), C = (C[1], ..., C[4]))$:
$x_0 \leftarrow d$
for $i = 1$ to 4 **do**
    $x_i \leftarrow \pi(C[i])$
    $M[i] \leftarrow (x_i - x_{i-1} - 1 + i) \bmod 10$
return $M = (M[1], ..., M[4])$

(b)

Proof. Assume $M^* = C^* = (0, 0, 0, 0)$,

$$\begin{aligned}\Pr_{M \xleftarrow{\$} \mathbb{Z}_{10}^4}[M = M^*] &= \Pr_{M[1] \xleftarrow{\$} \mathbb{Z}_{10}}[M[1] = 0] \times \Pr_{M[2] \xleftarrow{\$} \mathbb{Z}_{10}}[M[2] = 0] \times \Pr_{M[3] \xleftarrow{\$} \mathbb{Z}_{10}}[M[3] = 0] \\ &\quad \times \Pr_{M[4] \xleftarrow{\$} \mathbb{Z}_{10}}[M[4] = 0] \\ &= \frac{1}{10} \times \frac{1}{10} \times \frac{1}{10} \times \frac{1}{10} = \frac{1}{10^4}\end{aligned}$$

Given $C^* = (0, 0, 0, 0)$ and $x_0 = d$, using the decryption algorithm, we can derive:
$x_1 = x_2 = x_3 = x_4 = \pi(0)$,
$M[1] = (\pi(0) - d - 1 + 1) \bmod 10 = (\pi(0) - d) \bmod 10$,
$M[2] = (\pi(0) - \pi(0) - 1 + 2) \bmod 10 = (1) \bmod 10 = 1$,
$M[3] = (\pi(0) - \pi(0) - 1 + 3) \bmod 10 = (2) \bmod 10 = 2$,
$M[4] = (\pi(0) - \pi(0) - 1 + 4) \bmod 10 = (3) \bmod 10 = 3$,
which give us: $M = (M[1], ..., M[4]) = ((\pi(0) - d) \bmod 10, 1, 2, 3) \neq (0, 0, 0, 0) = M^*$
Thus, we have:
$\Pr_{K \xleftarrow{\$} \mathsf{Kg}, M \xleftarrow{\$} \mathbb{Z}_{10}^4}[M = M^* \mid \mathsf{Enc}(K = (d, \pi), M = (M[1], ..., M[4])) = C^*] = 0 \neq \frac{1}{10^4} = \Pr_{M \xleftarrow{\$} \mathbb{Z}_{10}^4}[M = M^*]$, which is a violation of Shannon secrecy.
Therefore, this encryption scheme is not perfectly secret.

Task 2 - The Shuffle (19 points)

(a)

Since $\overline{M}$ is the bit-wise complement of M and M' is the concatenation of M and $\overline{M}$, we know M' satisfies the invariant that it has the same number of 0's and 1's.
Since π is a random permutation of $\{1, ..., 2n\}$ and $C[i] \leftarrow M'[\pi(i)]$, we know C is effectively a random permutation of M', which means C also satisfies the invariant that it has the same number of 0's and 1's.
Additionally, since we know the length of C is $2n$, C must contain exactly n 0's and n 1's.
Therefore, the ciphertext space can be described as:
$\mathcal{C} = \{C \in \{0,1\}^{2n}$: where C contains exactly n 0's and n 1's$\}$

(b)

procedure Dec'$(\pi, C = (C[1], ..., C[2n]))$:
for $i = 1$ to $2n$ **do**
    $M'[\pi(i)] \leftarrow C[i]$
for $j = 1$ to n **do**
    $M[j] \leftarrow M'[j]$
return $M = (M[1], ..., M[n])$

(c)

Since π is a random permutation of $\{1, ..., 2n\}$, each bit position in the ciphertext is equally likely to be any bit position in $M||\overline{M}$ which contains exactly n 0's and n 1's (as seen in part (a)). The encryption algorithm is effectively uniformly randomly shuffling $M||\overline{M}$.
Therefore, the distribution of Enc'(π, M) is uniform over the ciphertext space $\mathcal{C}$.
Assume we pick an arbitrary ciphertext C from the ciphertext space $\mathcal{C}$, the distribution of Enc'(π, M) for all ciphertext $C \in \mathcal{C}$ can be described as:

$$\begin{aligned}\Pr_{\pi \xleftarrow{\$} \text{Perms}(\{1,..,2n\}), M \xleftarrow{\$} \{0,1\}^n}[\text{Enc'}(\pi, M) = C] &= \Pr_{C^* \xleftarrow{\$} \mathcal{C}}[C = C^*] \\ &= \frac{1}{|\mathcal{C}|} \\ &= \frac{1}{\binom{2n}{n}} \\ &= \frac{(n!)^2}{(2n)!}\end{aligned}$$

(d)

Proof. For all $M \in \{0,1\}^n$ and $C \in \mathcal{C}$,

$$\Pr_{\pi \xleftarrow{\$} \mathsf{Kg}}[\text{Enc'}(\pi, M) = C] = \Pr_{\pi \xleftarrow{\$} \mathsf{Perms}(\{1,..,2n\})}[\text{Enc'}(\pi, M) = C]$$

$$= \Pr_{C^* \xleftarrow{\$} \mathcal{C}}[C = C^*]$$

(as explained in part(c), Enc' uniformly randomly shuffles $M||\overline{M}$)

$$= \frac{1}{|\mathcal{C}|}$$

$$= \frac{1}{\binom{2n}{n}}$$

$$= \frac{(n!)^2}{(2n)!}$$

Task 3 - Playing with AES (10 points)

(a)

AES(X, X) = 24 f3 dc 26 07 11 10 ad 52 58 a4 55 67 14 d0 1d

(b)

$C =$ AES(X, M) = 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 when
$M =$ fd e4 d4 2d 80 2d 9e 09 18 fd 5f ae 0c 6f a2 9c
I found M by running the InvertAES function with $K = X$ and $C =$ 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

(c)

$C =$ AES(K, X) = 37 d9 12 89 07 fa 24 b0 17 b1 04 b2 aa ee 5e 00 when
$K =$ 1c 0b bc 7f 17 0d bf d6 8d c6 8d 37 d5 6c 71 cf
I found K by brute forcing the key space (i.e. I wrote a while loop which generate a random 16-byte number as K for each iteration and return the first K whose AES(K, X) output has its last byte as 00).

Task 4 - Distinguishing Advantage (6 points)

(a)

Fact 1: $\Pr[D_1^{O_0} \Rightarrow 1] = \Pr_{b_1 \xleftarrow{\$} \{0,1\}}[b_1 = 1] = \frac{1}{2}$

Fact 2: $\Pr[D_1^{O_1} \Rightarrow 1] = \Pr_{b_1 \xleftarrow{\$} \{0,1\}}[b_1 = 1] = \frac{1}{2}$

$\mathbf{Adv}^{\mathsf{dist}}_{O_0,O_1}(D_1) = |\frac{1}{2} - \frac{1}{2}| = 0$

(b)

Fact 1:

$$\begin{aligned}
\Pr[D_2^{O_0} \Rightarrow 1] &= \Pr_{b_1 \xleftarrow{\$} \{0,1\}, b_2 \xleftarrow{\$} \{0,1\}}[b_1 \oplus b_2 = 1] \\
&= \Pr_{b_1 \xleftarrow{\$} \{0,1\}}[b_1 = 1] \times \Pr_{b_2 \xleftarrow{\$} \{0,1\}}[b_2 = 0] + \Pr_{b_1 \xleftarrow{\$} \{0,1\}}[b_1 = 0] \times \Pr_{b_2 \xleftarrow{\$} \{0,1\}}[b_2 = 1] \\
&= \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} \\
&= \frac{1}{2}
\end{aligned}$$

Fact 2:

$$\begin{aligned}
\Pr[D_2^{O_1} \Rightarrow 1] &= \Pr_{b_1 \xleftarrow{\$} \{0,1\}, b_2 \xleftarrow{b_1} \{0,1\}}[b_1 \oplus b_2 = 1] \\
&= \Pr_{b_1 \xleftarrow{\$} \{0,1\}}[b_1 = 1] \times \Pr_{b_2 \leftarrow 0}[b_2 = 0] + \Pr_{b_1 \xleftarrow{\$} \{0,1\}}[b_1 = 0] \times \Pr_{b_2 \xleftarrow{\$} \{0,1\}}[b_2 = 1] \\
&= \frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} \\
&= \frac{3}{4}
\end{aligned}$$

$\mathbf{Adv}^{\mathsf{dist}}_{O_0,O_1}(D_2) = |\frac{3}{4} - \frac{1}{2}| = \frac{1}{4}$