

Homework 1

Task 1 - Encryption Scheme (10 points)

(a)

```

procedure Dec( $K = (d, \pi), C = (C[1], \dots, C[4])$ ) :
 $x_0 \leftarrow d$ 
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  $M = (M[1], \dots, M[4])$ 
    
```

(b)

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

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

Given $C^* = (0, 0, 0, 0)$ and $x_0 = d$, using the decryption algorithm, we can derive:

$$\begin{aligned}
 x_1 &= x_2 = x_3 = x_4 = \pi(0), \\
 M[1] &= (\pi(0) - d - 1 + 1) \bmod 10 = (\pi(0) - d) \bmod 10, \\
 M[2] &= (\pi(0) - \pi(0) - 1 + 2) \bmod 10 = (1) \bmod 10 = 1, \\
 M[3] &= (\pi(0) - \pi(0) - 1 + 3) \bmod 10 = (2) \bmod 10 = 2, \\
 M[4] &= (\pi(0) - \pi(0) - 1 + 4) \bmod 10 = (3) \bmod 10 = 3,
 \end{aligned}$$

which give us: $M = (M[1], \dots, M[4]) = ((\pi(0) - d) \bmod 10, 1, 2, 3) \neq (0, 0, 0, 0) = M^*$

Thus, we have:

$$\Pr_{K \leftarrow \text{Kg}, M \leftarrow \mathbb{Z}_{10}^4} [M = M^* \mid \text{Enc}(K = (d, \pi), M = (M[1], \dots, M[4])) = C^*] = 0 \neq \frac{1}{10^4} =$$

$\Pr_{M \leftarrow \mathbb{Z}_{10}^4} [M = M^*]$, 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 $\{1, \dots, 2n\}$ 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:

$$\mathcal{C} = \{C \in \{0, 1\}^{2n} : \text{where } C \text{ contains exactly } n \text{ 0's and } n \text{ 1's}\}$$

(b)

procedure $\text{Dec}'(\pi, C = (C[1], \dots, C[2n])) :$

for $i = 1$ to $2n$ **do**

$M'[\pi(i)] \leftarrow C[i]$

for $j = 1$ to n **do**

$M[j] \leftarrow M'[j]$

return $M = (M[1], \dots, M[n])$

(c)

Since π is a random permutation of $\{1, \dots, 2n\}$, 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 $\text{Enc}'(\pi, M)$ is uniform over the ciphertext space \mathcal{C} .

Assume we pick an arbitrary ciphertext C from the ciphertext space \mathcal{C} , the distribution of $\text{Enc}'(\pi, M)$ for all ciphertext $C \in \mathcal{C}$ can be described as:

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

(d)

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

$$\begin{aligned}\Pr_{\pi \leftarrow \text{Kg}} [\text{Enc}'(\pi, M) = C] &= \Pr_{\pi \leftarrow \text{Perms}(\{1, \dots, 2n\})} [\text{Enc}'(\pi, M) = C] \\ &= \Pr_{C^* \leftarrow \mathcal{C}} [C = C^*]\end{aligned}$$

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

$$\begin{aligned}&= \frac{1}{|\mathcal{C}|} \\ &= \frac{1}{\binom{2n}{n}} \\ &= \frac{(n!)^2}{(2n)!}\end{aligned}$$

Task 3 - Playing with AES (10 points)

(a)

(b)

(c)

Task 4 - Distinguishing Advantage (6 points)

(a)

(b)