Problem Set 1

1. Let $E : \{0,1\}^2 \times \{0,1\}^3 \to \{0,1\}^3$ be the following family of maps:

$$\begin{array}{llll} E_{00} & = (001, 011, 010, 000, 110, 111, 101, 100) & E_{01} & = (001, 011, 010, 000, 110, 111, 101, 100) \\ E_{10} & = (001, 011, 010, 000, 110, 111, 101, 100) & E_{11} & = (001, 011, 010, 000, 110, 111, 101, 100) \end{array}$$

   Is E a block cipher? Explain your answer. Be specific and suitably detailed.

   E is a block cipher because for every key K, it is a valid permutation of the input. Therefore, for every messsage m in the message space $\{0,1\}^n$, $E_k(E_k^{-1}(m)) = m$ and $E_k^{-1}(E_k(m)) = m$. Although it isn't secure, it's syntactically a block cipher.

2. Let $E : \{0,1\}^3 \times \{0,1\}^3 \to \{0,1\}^3$ be the following family of maps:

$$\begin{array}{llll} E_{000} & = (011, 001, 000, 010, 101, 110, 100, 111) & E_{001} & = (000, 001, 010, 011, 100, 101, 110, 111) \\ E_{100} & = (001, 010, 110, 101, 000, 100, 111, 011) & E_{010} & = (011, 001, 010, 000, 111, 110, 100, 101) \end{array}$$

   Is E a block cipher? Explain your answer. Be specific and suitably detailed.

   This E is also a block cipher. Each key corresponds to a valid permutation, so a message can be recovered for any key message encrypted with E and key k by E^{-1} and the same k.

3. Let $E : \{0,1\}^3 \times \{0,1\}^3 \to \{0,1\}^3$ be the following family of maps:

$$\begin{array}{lllllllll} E_{000} = E_{101} = E_{010} = & (011, & 100, & 010, & 000, & 110, & 111, & 001, & 101) \\ E_{011} = E_{111} = E_{100} = & (001, & 110, & 011, & 000, & 100, & 111, & 010, & 101) \\ E_{110} = & (010, & 011, & 100, & 111, & 001, & 110, & 101, & 000) \\ E_{001} = & (001, & 000, & 100, & 111, & 011, & 101, & 110, & 010) \end{array}$$

   (a) Let $K = 111$ and $M = 110$. What is the value of the output $E_K(M)$?
   $E_{111}(110) = 010$

   (b) What is the value of $\mathsf{Cons}_E((110, 101))$? Explain your answer.
   $\{110\}$, because the only k for which $E_k(110) = 101$ is 110

   (c) What is the value of $\mathsf{Cons}_E((010, 100))$? Explain your answer.
   $\{110, 001\}$, because the set of keys k for which $E_k(010) = 100$ contains 110 and 001.

   (d) What is the value of $\mathsf{Cons}_E((010, 100), (100, 011))$? Explain your answer.
   $\{001\}$, because the set of keys k for which $E_k(010) = 100$ contains 110 and 001, but the only k for which $E_k(100) = 011$ is 011.

   (e) What is the value of $\mathsf{Cons}_E((100, 110))$? Explain your answer.
   $\{000, 101, 010\}$, because each of those three keys k, $E_k(100) = 110$

4. Let $E : \{0,1\}^{256} \times \{0,1\}^{256} \to \{0,1\}^{256}$ be the family of permutations defined as follows. For any key K and input $M = M[1]M[2]$ where $|M[1]| = |M[2]|$ and $\|$ denotes concatenation,

$$E_K(M[1]M[2]) = M[1] \oplus 1^{128} \parallel M[2] \oplus 0^{64}1^{64} .$$

(a) Explicitly specify $E^{-1} : \{0,1\}^{256} \times \{0,1\}^{256} \to \{0,1\}^{256}$
$E_K^{-1}(C[1]C[2]) = C[1] \oplus 1^{128} \parallel C[2] \oplus 0^{64}1^{64}$.

(b) Suppose the key K is $0^{150}10^{55}1^{50}$ and the plaintext is $0^{250}1^6$. What is the value of the ciphertext?
$1^{128}0^{64}1^{58}0^6$

(c) Suppose the key K is $1^{126}01^{129}$ and the ciphertext is $001^{127}0001^{124}$. What is the value of the plaintext?
$110^{126}10001^{60}0^{60}$

(d) Prove that E is not a secure PRF. The smaller the resource usage and the larger the advantage, the better your attack is. You need to write down all 4 parts of the proof, namely (1) the idea behind your attack, (2) the pseudocode of your attack, (3) the advantage analysis of your attacker, and (4) the attacker's resource usage.

1.

The idea behind the attack is that the adversary knows E, and therefore knows that E does not depend on a random key. Therefore, adversary A can guess if a given ciphertext corresponds to a message simply by encrypting the message with E. In the attack, the adversary simply feeds the string 0^{256} into the oracle and checks whether the resulting string is $1^{128}0^{64}1^{64}$.

2.

Adversary A^g:

$y \leftarrow g(0^{256})$

if y = $1^{128}0^{64}1^{64}$

    return 1

else

    return 0

3. First, we calculate the probability of the experiment returning $True$.

$$\begin{aligned} pr[Exp_E(A) \Rightarrow True] &= P[Exp_E(A) \Rightarrow T \wedge b = 0] * pr[b = 0] + P[Exp_E(A) \Rightarrow T \wedge b = 0] * p[b = 1] \\ &= P[Exp_E(A) \Rightarrow T \wedge b = 0] * 0.5 + P[Exp_E(A) \Rightarrow T \wedge b = 1] * 0.5 \\ &= (1 - 256^{-1}) * 0.5 + 0.5 \end{aligned}$$

Then, to get the advantage, we scale and shift the result.

$$\begin{aligned} Adv_E(A) &= 2 * Pr[Exp_E(A) \Rightarrow True] - 1 \\ &= 2 * ((1 - 256^{-1}) * 0.5 + 0.5) - 1 \\ &= 1 - 256^{-1} \end{aligned}$$

4. We only make one query to the adversary, which is of a constant size. Then we check one condition, which is also constant. The code size is also finite and constant

5. Let the message space be $\{0,1\}^3$, and let $\Pr[\, M = 000\,] = \Pr[\, M = 101\,] = \Pr[\, M = 110\,] = \Pr[\, M = 111\,] = 0.25$. Let the probability that M takes on a value other than $000, 101, 110$, and 111 be zero. Let $E : \{0,1\}^{64} \times \{0,1\}^3 \to \{0,1\}^3$ be the following block cipher.

$$E_{0^{64}} = E_{0^{63}1} = \ldots = E_{1^{64}} = (011, 110, 000, 100, 010, 001, 111, 101) .$$

We define an encryption scheme based on E as follows.

Key generation:	Return a bitstring uniform randomly drawn from $\{0,1\}^{64}$
Encryption of M with key K:	Return $E_K(M)$
Decryption of C with key K:	Return $E_K^{-1}(C)$

(a) What is the ciphertext expansion for this encryption scheme? (Specify your answer in bits.)
The ciphertext is always the same size as the plaintext (3 bits), so there are 0 bits of ciphertext expansion.

(b) $\Pr[\, M = 010 \,] =$? Explain your answer. Be clear and specific.
The probability that $M = 010$ is 0, because the probability of the message being anything other than $000, 101, 110$, or 111 is 0.

(c) $\Pr[\, C = 011 \,] =$? Explain your answer. Be clear and specific.
$\Pr[\, C = 011 \,] = 0.25$ Because only $M = 000$ would result in this ciphertext, and that has a 0.25 probability of occuring.

(d) $\Pr[\, M = 000 \mid C = 111 \,] =$? Explain your answer. Be clear and specific.
$\Pr[\, M = 000 \mid C = 111 \,] = 0$ because 000 will encrypt to a ciphertext 011, not 111.

(e) $\Pr[\, M = 110 \mid C = 111 \,] =$? Explain your answer. Be clear and specific. $\Pr[\, M = 110 \mid C = 111 \,] = 1$ because by the definition of E, 110 will always encrypt to 111.

(f) Does this encryption scheme provide perfect secrecy? Prove your answer.

For the scheme to provide perfect secrecy, it would need to meet the following definition:
For any $a, b \in \{0,1\}^n$, it is the case that $\Pr[\, M = a \mid C = b \,] = \Pr[\, M = a \,]$.
For contradiction, set $a = 110$ and $b = 111$.
We know that $\Pr[\, M = 110 \mid C = 111 \,] = 1$ and $\Pr[\, M = 110 \,] = 0.25$, so $\Pr[\, M = 110 \mid C = 111 \,] \neq \Pr[\, M = 110 \,]$

6. Let n be a positive integer, and let the message space be $\{0,1\}^n$. Let all possible messages in the message space be equally likely, and let the key space be

$$\{K \mid K \in \{0,1\}^n, \text{ and } K \text{ contains an even number of 1s.}\}$$

We define an encryption scheme $\mathcal{SE}$ as follows.

Key generation:	Return a bitstring uniform randomly drawn from $\{0,1\}^n$
Encryption of M with key K:	Return $M \oplus K$
Decryption of C with key K:	Return $C \oplus K$

Does $\mathcal{SE}$ provide perfect secrecy? Prove your answer.

No, $\mathcal{SE}$ does not provide perfect secrecy.

For $\mathcal{SE}$ to provide perfect secrecy, we would need that for any $a, b \in \{0,1\}^n$, $\Pr[\, M = a \mid C = b \,] = \Pr[\, M = a \,]$.

For contradiction, set $a = 0^n$, and $b = 0^{n-1}1$. Because we know that there are no keys k in the keyspace with an odd number of 1s and we would need $k = 0^{n-1}1$ to obtain that ciphertext, $\Pr\left[\, M = 0^n \mid C = 0^{n-1} \,\right] = 0$. However, 0^n is in the message space $0, 1^n$ so $\Pr[\, M = 0^n \,] = \frac{1}{2^n}$. Therefore, for $a = 0^n$ and $b = 0^{n-1}1$, $\Pr[\, M = a \mid C = b \,] \neq \Pr[\, M = a \,]$.