Problem Set 1

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

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

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

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

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

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

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

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

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

   (b) What is the value of $\mathsf{Cons}_E((110, 101))$? Explain your answer.

   (c) What is the value of $\mathsf{Cons}_E((010, 100))$? Explain your answer.

   (d) What is the value of $\mathsf{Cons}_E((010, 100), (100, 011))$? Explain your answer.

   (e) What is the value of $\mathsf{Cons}_E((100, 110))$? Explain your answer

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,

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

   (a) Explicitly specify $E^{-1} : \{0,1\}^{256} \times \{0,1\}^{256} \to \{0,1\}^{256}$

   (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?

   (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?

   (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.

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.)

(b) $\Pr[\,M = 010\,] =$? Explain your answer. Be clear and specific.

(c) $\Pr[\,C = 011\,] =$? Explain your answer. Be clear and specific.

(d) $\Pr[\,M = 000 \mid C = 111\,] =$? Explain your answer. Be clear and specific.

(e) $\Pr[\,M = 110 \mid C = 111\,] =$? Explain your answer. Be clear and specific.

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

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.