Sample Solutions for 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.

   Solution: Yes. A block cipher is a family of permutations that can be indexed by bitstrings representing the keys. E is a family of one permutation in this case. Every possible key corresponds to a particular permutation on $\{0,1\}^3$.

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.

   Solution: No. A block cipher is a family of permutations that can be indexed by bitstrings representing the keys. However, in this case, four of the eight possible keys do not correspond to any permutation on $\{0,1\}^3$.

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 $E_K(M)$?

   Solution: From the second row, $E_{111}(110) = 010$.

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

   Solution: From the third row, $E_{110}(110) = 101$. Since this is the only key that maps 110 to 101, we have that
$$\mathsf{Cons}_E((110, 101)) = \{110\} .$$

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

Solution: From the third and fourth rows, $E_{110}(010) = 100$ and $E_{001}(010) = 100$, respectively. Since these two keys are the only keys that map 010 to 100, we have that

$$\mathsf{Cons}_E((010, 100)) = \{110, 001\} \; .$$

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

Solution: From the fourth row, $E_{001}(010) = 100$ and $E_{001}(100) = 011$. Since this is the only key that maps 010 to 100 and 100 to 011, we have that

$$\mathsf{Cons}_E((010, 100), (100, 011)) = \{001\} \; .$$

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

Solution: From the first row, $E_{000}(100) = E_{101}(100) = E_{010}(100) = 110$. Since these are the only keys that map 100 to 110, we have that

$$\mathsf{Cons}_E((100, 110)) = \{000, 101, 010\} \; .$$

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 $E^{-1} : \{0,1\}^{256} \times \{0,1\}^{256} \to \{0,1\}^{256}$

Solution: For any key K and input $C = C[1]C[2]$ where $|C[1]| = |C[2]|$,

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

(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?

Solution: From the description of E, we have

$$\begin{aligned} E_K(0^{250}1^6) &= E_K(0^{128} \parallel 0^{122}1^6) \\ &= 0^{128} \oplus 1^{128} \parallel 0^{122}1^6 \oplus 0^{64}1^{64} \\ &= 1^{128} \parallel 0^{64}0^{58}1^6 \oplus 0^{64}1^{64} \\ &= 1^{128} \parallel 0^{64}1^{58}0^6 \\ &= 1^{128}0^{64}1^{58}0^6 \; . \end{aligned}$$

(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?

Solution: From the description of E, we have

$$\begin{aligned} E_K(001^{127}0001^{124}) &= E_K(001^{126} \parallel 10001^{124}) \\ &= 001^{126} \oplus 1^{128} \parallel 10001^{124} \oplus 0^{64}1^{64} \\ &= 110^{126} \parallel 10001^{60}1^{64} \oplus 0^{64}1^{64} \\ &= 110^{126} \parallel 10001^{60}0^{64} \\ &= 110^{126}10001^{60}0^{64} . \end{aligned}$$

(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.

Solution:

(1) Idea. For any input message, we know exactly what E will output as the ciphertext regardless of the value of the key. Thus, as an adversary, we can tell whether our oracle g is a real or a random one by giving an input message and checking whether the output ciphertext is what we expect. If it is, we declare that g must be a real permutation chosen from E. Otherwise, we bet that g is a function chosen at random from the set of all possible functions mapping 256 bits to 256 bits.

(2) Pseudocode of the attack. We define an adversary A playing a PRF game against E as follows.

Adversary A^g
  $C \leftarrow g(0^{256})$
  If $C = 1^{128}0^{64}1^{64}$ then return 1 else return 0

(3) Analysis. We analyze the advantage of A in the PRF game here. First, we focus on the probability that A guesses correctly in the PRF game, namely $\Pr\left[\mathbf{Exp}_E^{\mathrm{prf}}(A) \Rightarrow \mathbf{T}\right]$. Let b be the bit that the challenger chooses in the beginning of the PRF game, and let d be the bit output by A.

$$\Pr\left[\mathbf{Exp}_E^{\mathrm{prf}}(A) \Rightarrow \mathbf{T}\right] = \Pr\left[\mathbf{Exp}_E^{\mathrm{prf}}(A) \Rightarrow \mathbf{T} \mid b=1\right] \cdot \Pr[b=1] + \Pr\left[\mathbf{Exp}_E^{\mathrm{prf}}(A) \Rightarrow \mathbf{T} \mid b=0\right] \cdot \Pr[b=0] \tag{1}$$

We analyze each of the conditional probability terms above in turn.

Case 1: Suppose $b = 1$. Thus, $g = E_K$ for a key K chosen uniformly at random from the set of all possible keys by the challenger. Let C be as defined in the first line of the pseudocode of A. From the definition of E, we know that

$$C = E_K(0^{256}) = 0^{256} \oplus 1^{128}0^{64}1^{64} = 1^{128}0^{64}1^{64} .$$

Therefore, from the second line in the pseudocode of A, we have that A returns 1. Thus,

$$\Pr\left[\mathbf{Exp}_E^{\mathrm{prf}}(A) \Rightarrow \mathbf{T} \mid b=1\right] = 1 . \tag{2}$$

Case 2: Suppose $b = 0$. Thus, g is chosen, by the challenger, uniformly at random from the set of all functions mapping 256 bits to 256 bits. Thus, upon the only query, g returns a bitstring chosen at random from $\{0,1\}^{256}$. Consider the following derivation:

$$\begin{aligned}
\Pr\left[\,\mathbf{Exp}_E^{\mathrm{prf}}(A) \Rightarrow \mathbf{T} \;\middle|\; b=0\,\right] &= 1 - \Pr\left[\,\mathbf{Exp}_E^{\mathrm{prf}}(A) \Rightarrow \mathbf{F} \;\middle|\; b=0\,\right] \\
&= 1 - \Pr\left[\, d=1 \mid b=0 \,\right] \\
&= 1 - \frac{1}{2^{256}}\,. \qquad (3)
\end{aligned}$$

The last line follows from the fact that a uniform-randomly chosen bitstring of length 256 bits equals a particular bitstring, namely $1^{128}0^{64}1^{64}$, with the probability $\frac{1}{2^{256}}$.

Substituting Equations (2) and (3) into Equation (1), we have

$$\begin{aligned}
\Pr\left[\,\mathbf{Exp}_E^{\mathrm{prf}}(A) \Rightarrow \mathbf{T}\,\right] &= \Pr\left[\,\mathbf{Exp}_E^{\mathrm{prf}}(A) \Rightarrow \mathbf{T} \;\middle|\; b=1\,\right]\cdot \Pr[\,b=1\,] + \Pr\left[\,\mathbf{Exp}_E^{\mathrm{prf}}(A) \Rightarrow \mathbf{T} \;\middle|\; b=0\,\right]\cdot \Pr[\,b=0\,] \\
&= 1\cdot \Pr[\,b=1\,] + \left(1 - \frac{1}{2^{256}}\right)\cdot \Pr[\,b=0\,] \\
&= 1\cdot \frac{1}{2} + \left(1 - \frac{1}{2^{256}}\right)\cdot \frac{1}{2} \\
&= \frac{1}{2} + \frac{1}{2} - \frac{1}{2^{257}}
\end{aligned}$$

Thus,

$$\begin{aligned}
\mathbf{Adv}_E^{\mathrm{prf}}(A) &= 2\cdot \Pr\left[\,\mathbf{Exp}_E^{\mathrm{prf}}(A) \Rightarrow \mathbf{T}\,\right] - 1 \\
&= 2\cdot\left(\frac{1}{2} + \frac{1}{2} - \frac{1}{2^{257}}\right) - 1 \\
&= 1 + 1 - \frac{1}{2^{256}} - 1 \\
&= 1 - \frac{1}{2^{256}}\,.
\end{aligned}$$

(4) Resource usage. The adversary A submits 1 query of total length 256 bits. The running time of A is $O(1)$ plus the time it takes for 1 oracle call.

Since A has a high advantage value (very close to 1) and uses a small amount of resources, we can conclude that E is an insecure block cipher under the PRF game.

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.)

Solution: Since $|M| = |C| = 3$, the ciphertext expansion is 0.

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

> **Solution:** From the problem description, 010 is not among the four possible messages. Thus, $\Pr[M = 010] = 0$.

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

> **Solution:** For any key $K \in \{0,1\}^{64}$, we know that $E_K(000) = 011$. Thus,
>
> $$\Pr[C = 011] = \Pr[M = 000] = 0.25 .$$

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

> **Solution:** For any key $K \in \{0,1\}^{64}$, we know that $E_K(110) = 111$. Thus, if we know that $C = 111$, then we know that $M = 110 \neq 000$. Thus,
>
> $$\Pr[M = 000 \mid C = 111] = 0 .$$

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

> **Solution:** For any key $K \in \{0,1\}^{64}$, we know that $E_K(110) = 111$. Thus, if we know that $C = 111$, then we know that $M = 110$. Thus,
>
> $$\Pr[M = 110 \mid C = 111] = 1 .$$

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

> **Solution:** No, it does not. We show that there exists $a, b \in \{0,1\}^3$ such that
>
> $$\Pr[M = a \mid C = b] \neq \Pr[M = a] .$$
>
> Let $a = 000$ and $b = 111$. Then, we have that
>
> $$\Pr[M = a \mid C = b] = 0$$
>
> from the answer for part (d) while $\Pr[M = a] = 0.25$ from the problem description.

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.

Solution: No, it does not. We show that there exists $a, b \in \{0,1\}^n$ such that

$$\Pr[\, M = a \mid C = b \,] \neq \Pr[\, M = a \,] \ .$$

Let $a = 0^n$ and $b = 0^{n-1}1$. Then, we have that

$$\Pr[\, M = a \mid C = b \,] = 0 \qquad \text{while} \tag{4}$$

$$\Pr[\, M = a \,] = \frac{1}{2^n} \ . \tag{5}$$

To see why Equation (4) holds, notice that, since $C = M \oplus K$, it impossible that $M = 0^n$ and $C = 0^{n-1}1$ simultaneously. The reason is that no key K with even number of 1s could make this happen. Equation (5) holds since all possible messages in $\{0,1\}^n$ are equally likely.