UEE4611 Assignment #3 Solution

1. For any block cipher, the fact that it is a nonlinear function is crucial to its security. To see this, suppose that we have a linear block cipher EL that encrypts 256-bit blocks of plaintext into 256-bit blocks of ciphertext. Let $EL(k, m)$ denote the encryption of a 256-bit message m under a key k (the actual bit length of k is irrelevant). Thus,

$$EL(k, [m_1 \oplus m_2]) = EL(k, m_1) \oplus EL(k, m_2)$$

for all 256-bit patterns m_1, m_2.
(a) What is the ciphertext of 0, the all-zero string?
(b) A "chosen ciphertext" means that an adversary has the ability to choose a ciphertext and then obtain its decryption. At least how many plaintext/ciphertext pairs does an adversary need to decrypt any ciphertext without knowledge of the secret key? And how?

(a)

$$\begin{aligned} EL(k, 0) &= EL(k, [0 \oplus 0]) \\ &= EL(k, 0) \oplus EL(k, 0) \\ &\Rightarrow EL(k, [0]) = 0 \end{aligned}$$

(b) The least number of plaintext/ciphertext pairs an adversary need to decrypt any ciphertext without knowledge of the secret key is 256.
This is because any 256-bit ciphertext can be expressed as a linear combination of a basis of the 256-bit vector space, which is of dimension 256.
So if you have 256 plaintext/ciphertext pairs, you can find out all coefficients of the linear combination.

2.Consider the encryption of DES. (For simplicity, assume the initial permutation is the identity permutation.) Suppose we have a plaintext $A||B$, where $A, B \in \{0,1\}^{32}$
(a) Suppose the DES F function mapped every 32-bit input R, regardless of the value of the input K, to 32-bit string of zero. What is the ciphertext of $A||B$ under this DES?
(b) Now suppose F is the identity function, i.e., $F(M) = M$ for all $M \in \{0,1\}^{32}$. What is the ciphertext of $A||B$ under this DES?

(a)

$$
\begin{aligned}
A_1 &= B_0 \\
B_1 &= A_0 \oplus (F(k_1, B_0)) \\
&= A_0 \oplus 0 \\
&= A_0 \\
A_2 &= B_1 = A_0 = A \\
B_2 &= A_1 = B_0 = B \\
&\vdots \\
A_{16} &= A_2 = A \\
B_{16} &= B_2 = B
\end{aligned}
$$

$$\Rightarrow \textbf{ciphertext} = (B||A)$$

(b)

$$
\begin{aligned}
A_1 &= B_0 \\
B_1 &= A_0 \oplus (F(k_1, B_0)) \\
&= A_0 \oplus B_0 \\
A_2 &= B_1 = A_0 = A \\
B_2 &= A_1 \oplus B_1 \\
&= B_0 \oplus (A_0 \oplus B_0) \\
&= B_0 \oplus (B_0 \oplus A_0) \\
&= (B_0 \oplus B_0) \oplus A_0 \\
&= A_0 \\
A_3 &= B_2 = A_0 \\
B_3 &= A_2 \oplus B_2 \\
&= A_0 \oplus B_0 \oplus A_0 \\
&= B_0 \\
&\vdots \\
A_{16} &= A_1 = B_0 = B \\
B_{16} &= B_1 \\
&= A_0 \oplus B_0 \\
&= A \oplus B
\end{aligned}
$$

$$\Rightarrow \textbf{ciphertext} = A \oplus B || B$$

3. The 32-bit swap after the sixteenth iteration of the DES algorithm is needed to make the encryption process invertible by simply running the ciphertext back through the algorithm with the key order reversed. However, it still may not be entirely clear why the 32-bit swap is needed. To demonstrate why, solve the following exercises. First, some notation:

$A||B$ **= the concatenation of the bit strings** A **and** B
$T_i(R||L)$ **= the transformation defined by the** i**th iteration of the encryption algorithm for** $1 \leq I \leq 16$
$TD_i(R||L)$ **= the transformation defined by the** i**th iteration of the encryption algorithm for** $1 \leq I \leq 16$
$T_{17} = L||R$**, where this transformation occurs after the sixteenth iteration of the encryption algorithm**

(a) Show that the composition $TD_1(IP(IP^{-1}(T_{17}(T_{16}(L_{15}||R_{15})))))$ **is equivalent to the transformation that interchanges the 32-bit halves,** L_{15} **and** R_{15}**. That is, show that**

$$TD_1(IP(IP^{-1}(T_{17}(T_{16}(L_{15}||R_{15}))))) = R_{15}||L_{15}$$

(b) Now suppose that we did away with the final 32-bit swap in the encryption algorithm. Then we would want the following equality to hold:

$$TD_1(IP(IP^{-1}(T_{16}(L_{15}||R_{15})))) = L_{15}||R_{15}$$

Prove it or disprove it.

(a)

$$\begin{aligned} & TD_1(IP(IP^{-1}(T_{17}(T_{16}(L_{15}||R_{15}))))) \\ & \quad = TD_1(IP(IP^{-1}(T_{17}((L_{16}||R_{16}))))) \\ & \quad = TD_1(IP(IP^{-1}((R_{16}||L_{16}))) \\ & \quad = TD_1(R_{16}||L_{16}) \\ & \quad = R_{15}||L_{15} \end{aligned}$$

(b)

$$\begin{aligned} & TD_1(IP(IP^{-1}(T_{16}(L_{15}||R_{15})))) \\ & \quad = TD_1(IP(IP^{-1}(L_{16}||R_{16}))) \\ & \quad = TD_1(L_{16}||R_{16}) \\ & \quad = R_{16}||L_{16} \oplus F(R_{16}, k) \\ & \quad = L_{15} \oplus F(R_{15}, k)||L_{16} \oplus F(R_{16}, k) \\ & \quad \neq L_{15}||R_{15} \end{aligned}$$