CS:6160 CRYPTOLOGY

TUTORIAL 2

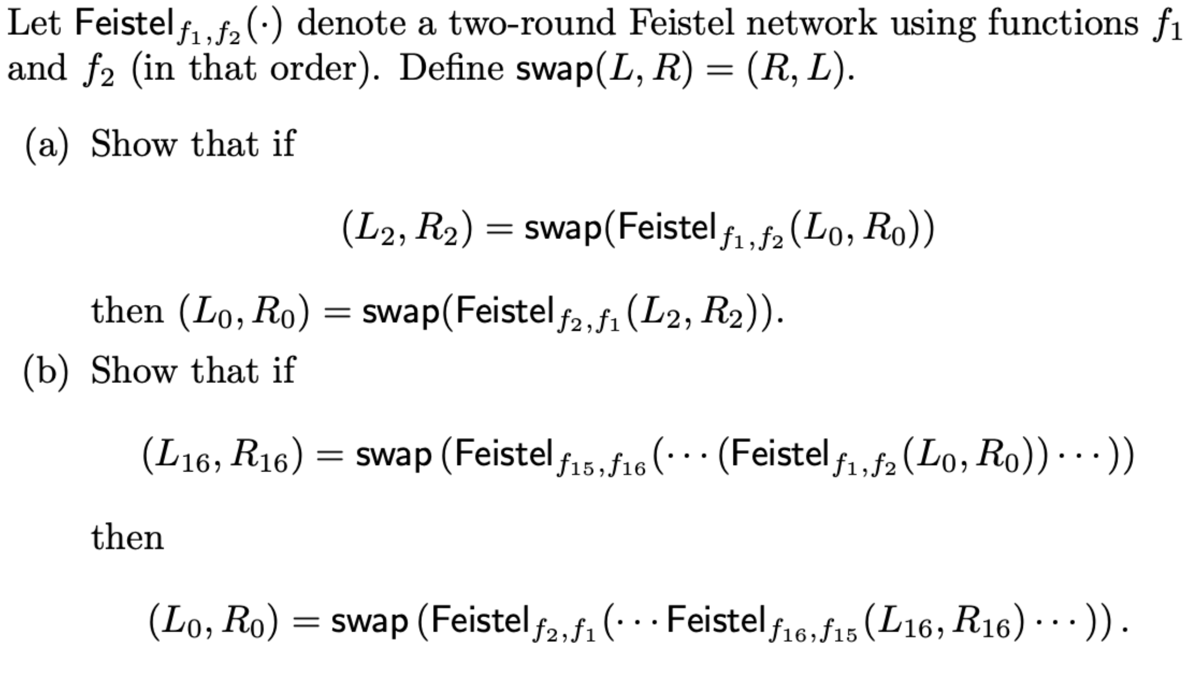
We will discuss these questions next week.

(1) Prove that if there exists a pseudorandom function that using a key of length n, maps n-bit inputs to single-bit outputs, then there exists a pseudorandom function that maps n-bit inputs to n-bit outputs.

(2) Fix a public, invertible permutation P and define the keyed function $F_k(x) := P(const||k||x)$. Show that F is not a PRF.

(3) What is the output of an r-round Feistel network when the input is (L_0, R_0) in each of the following two cases:
(a) Each round function outputs all 0s, regardless of the input.
(b) Each round function is the identity function.

(4) Note that from the below question it is clear that if we consider the output of DES as the swap of the output of the final round of the Feistel network (i.e. if the output of the Feistel network is (L_{16}, R_{16}) then the output of DES is (R_{16}, L_{16})), then **the only difference between the computation of DES_k and DES_k^{-1} is the order in which the sub-keys are used.**



Let $\mathsf{Feistel}_{f_1,f_2}(\cdot)$ denote a two-round Feistel network using functions f_1 and f_2 (in that order). Define $\mathsf{swap}(L, R) = (R, L)$.

(a) Show that if

$$(L_2, R_2) = \mathsf{swap}(\mathsf{Feistel}_{f_1,f_2}(L_0, R_0))$$

then $(L_0, R_0) = \mathsf{swap}(\mathsf{Feistel}_{f_2,f_1}(L_2, R_2))$.

(b) Show that if

$$(L_{16}, R_{16}) = \mathsf{swap}\left(\mathsf{Feistel}_{f_{15},f_{16}}(\cdots(\mathsf{Feistel}_{f_1,f_2}(L_0, R_0))\cdots)\right)$$

then

$$(L_0, R_0) = \mathsf{swap}\left(\mathsf{Feistel}_{f_2,f_1}(\cdots\mathsf{Feistel}_{f_{16},f_{15}}(L_{16}, R_{16})\cdots)\right).$$

(5) Show that DES has the property that $DES_k(x) = \overline{DES_{\bar{k}}(\bar{x})}$ for every key k and input x. Note that $\bar{x}$ denotes the bitwise complement of x. This is called the complementarity property of DES. Does this represent a serious vulnerability in the use of triple-DES as a pseudorandom permutation? Explain.

(6) Say the key schedule of DES is modified as follows: the left half of the master key is used to derive all the sub-keys in rounds $1 - 8$, while the right half of the master key is used to derive all the sub-keys in rounds $9 - 16$. Show an attack on this modified scheme that recovers the entire key in roughly 2^{28}.

(7) Let $f : \{0,1\}^m \times \{0,1\}^\ell \to \{0,1\}^\ell$ and $g : \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^\ell$ be block ciphers with $m > n$ and define $F_{k_1,k_2}(x) = f_{k_1}(g_{k_2}(x))$. Show a key-recovery attack on F using time $\mathcal{O}(n \cdot 2^m)$ and space $\mathcal{O}(\ell \cdot 2^n)$. *Hint: Meet-in-the-middle attack.*

(8) Define $DESY_{k,k'} = DES_K(x \oplus k^{'})$. The key length of DESY is 120 bits. Show a recovery attack on DESY taking time and space $\approx 2^{56}$.

SEPTEMBER 25, 2022 ; DEPT OF CSE, IIT HYDERABAD