Solution of Exercisesheet 4

Exercise 4-1

Let adversary A can choose can choose messages x_1 and x_2. Then corresponding keyed functions

$$F_k(x_1) := G_n(k) \oplus x_1$$
$$F_k(x_2) := G_n(k) \oplus x_2$$

A can compute $F_k(x_1) \oplus F_k(x_2) = x_1 \oplus x_2$

With this adversary can easily distingush from a uniformly selected function f by checking

$$(F_k(x_1) \oplus F_k(x_2)) \oplus x_1 => x_1 \oplus x_2 \oplus x_1 = x_2$$

or

$$(F_k(x_1) \oplus F_k(x_2)) \oplus x_2 => x_1 \oplus x_2 \oplus x_2 = x_1$$

Hence this will not be a PRF as this keyed function can be distinguished from a uniformaly selected function.

Exercise 4-2

(a) F_k'(x) = F_k(x $\oplus 1^n$)
Assume F_k'(x) is not a secure PRF and an adversary $\mathcal{A}$ can distinguish F_k'(x) and a random function f(x).
We construct $\mathcal{B}$, an adversary for F_k(x) that runs $\mathcal{A}$ as a subroutine.
$\mathcal{B}$ queries $\mathcal{A}$ with x $\oplus 1^n$ and outputs what x $\oplus 1^n$ outputs.
$\mathcal{B}$ is an efficient adversary to F_k(x).
But F_k(x) is secure and $\mathcal{B}$ can't exist.
$\Rightarrow$ F_k'(x) is a secure PRF

(b) F_k'(x) = F_k(x) || F_k(x $\oplus 1^n$)
$\Rightarrow$ F_k'(x) is not a secure PRF.
Adversary $\mathcal{A}$ can make two queries $x_1 = 000$, $x_2 = 111$
F_k'(x_1) = F_k(000) || F_k(111) = F_k(x_1) || F_k(x_2)
F_k'(x_2) = F_k(111) || F_k(000) = F_k(x_2) || F_k(x_1)
The left and right halves of the results correspond to each other and vice versa and produce not uniformly random results.
The adversary can therefor distinguish F_k'(x) from a true random function.

(c) F_k'($x_1||x_2$) = F_k(x_1) || F_k(x_2)
$\Rightarrow$ F_k'(x) is not a secure PRF.
Adversary $\mathcal{A}$ can make the query $x_1 = 00$
F_k'(x_1) = F_k(0) || F_k(0)
The left and right halves of the results correspond to each other and vice versa and produce

Solution of Exercisesheet 4

not uniformly random results.
The adversary can therefor distinguish F_k'(x) from a true random function.

(d) F_k'(x) = F_k(0||x) || F_k(1||x)
Constructing a distinguisher $\mathcal{D}$ for F_k from a distinguisher $\mathcal{D}$' for F_k'. $\mathcal{D}$ runs $\mathcal{D}$'. When $\mathcal{D}$' asks to call its oracle on a string x, $\mathcal{D}$ calls its oracle on the strings 0||x and 1||x, concatenates the answers, and gives the resulting string to $\mathcal{D}$' as its answer. Finally $\mathcal{D}$ outputs what $\mathcal{D}$' outputs.
It is clear that

- $\mathcal{D}$ runs in poly time if $\mathcal{D}$' does;
- if $\mathcal{D}$'s oracle implements F_k, its success probablility is the same as that of $\mathcal{D}$' when its oracle implements F_k'; and
- if $\mathcal{D}$'s oracle implements a random function, its success probability is the same as that of $\mathcal{D}$' when its oracle does likewise.

(e) F_k'(x) = *truncate last m bits of* F_k(x), m < |F_k(x)|
F_k'(x) has the form $\{0,1\}^n \times \{0,1\}^n \Rightarrow \{0,1\}^{n-m}$, |x| = n
Assume F_k'(x) is not a secure PRF and an adversary $\mathcal{A}$ can distinguish F_k'(x) and a random function f(x) $\in \{0,1\}^{n-m}$.
We construct $\mathcal{B}$, an adversary for F_k(x) that runs $\mathcal{A}$ as a subroutine.
$\mathcal{B}$ queries $\mathcal{A}$ with x and outputs x truncated by the last m bits.
$\mathcal{B}$ is an efficient adversary to F_k(x) but shortened by m bits.
Since the results of F_k(x) are uniformly distributed, a shortened result of F_k(x) is uniformly distributed as well.
Therefore $\mathcal{B}$ can't exist.
$\Rightarrow$ F_k'(x) is a secure PRF

Exercise 4-3

Task: Prove that indistinguishability of multiple encryptions in the presence of an eavesdropper does not imply indistinguishability of encryptions under a chosen plaintext attack.

We show this by a proof by contradiction. Let's assume that an arbitrary encryption scheme $\Pi = (Gen, Enc, Dec)$ exists, that is EAV-Mult secure.
$\Pi' = (Gen', Enc', Dec')$ is constructed as follows:
$Gen' = Gen$
Enc' and Dec' are constructed similar to the Chained Cipher Block Chaining:
$\underline{Enc'(k,m)}:$
$c \leftarrow Enc(k,m)$
$if\ m = r$:, r is choosen uniformly at random, but is fixed for all encryptions
$\quad return\ r, k, c$
$else:$

Solution of Exercisesheet 4

$return\ r, 0, c$

$\underline{Dec'(k,c)}:$
$parse(\bot, \bot, c)$
$m \leftarrow Dec(k,c)$
$return$

Proof, that Π' remains EAV-mult secure:
Proof by contradiction: We assume there is an adversary $\mathcal{A}$ who can break Π'. We then construct an adversary $\mathcal{B}$ against Π as follows: The adversary $\mathcal{B}$ has access to the encryption function Enc'. To use the adversary $\mathcal{A}$ against the security of Π', $\mathcal{B}$ has to provide the interface for $\mathcal{A}$. He does this by simulating the encryption for $\mathcal{A}$. $\mathcal{A}$ outputs two message vector $(m_0^1, m_0^2, ..., m_0^t)$ and $(m_1^1, m_1^2, ..., m_1^t)$ with $|m_0^i| = |m_1^i| \forall i$. The adversary $\mathcal{B}$ than samples a bit $b \leftarrow \$\{0,1\}$ and invokes his own encryption function $Enc(k,m)$ to compute $tup^i = \begin{cases} (r, k, Enc(k, m_b^i)) & if\ m_b^i = r \\ (r, 0, Enc(k, m_b^i)) & else \end{cases}$
Then he forwards $(tup^1, tup^2, ...tup^t)$ to $\mathcal{A}$. Eventually $\mathcal{A}$ outputs a bit b'. The adversary $\mathcal{B}$ outputs the same bit b'.
We see, $\mathcal{B}$ is efficient, if $\mathcal{A}$ is.
To analyse the success,

Describe a successful adversary against the CPA security of Π':
For the first call to the enncryption oracle, the adversary can choose the message randomly. It is very unlikly that he guesses the message so that $m = r$. In this case, he would learn k immediatly. If the adversary doesn't guess the correct message he learns r. With this information he can choose the next message correct with $m = r$ and then learn k.
Because he knows all about the encryption except k yet, he now knows the complete encryption scheme and can distinguish for any two messages sent to the challenger, from which message he recieves the ciphertext. So the adversary can win the game with a probability of 1 which is greater than a negligible function.