Solution of Exercisesheet 4

Exercise 4-1

Let G be a pseudorandom number generator with output of length 2n. We split the output in two parts as

$$G(x) := G^0(x)||G^1(x) \quad with \quad G^b(x) \in \{0,1\}^n$$

So $|G(s)| = 2n$.

Given the construction $G_n(s)$, denoted as the n-bit prefix of $G(s)$, i.e.,

$$G_n(s) = G^0(x)||0^n$$

And given the keyed function

$$F_k(x) = G_n(k) \oplus x$$

so

$$F_k(x) = G^0(x)||0^n \oplus x$$

This shows us that last n bits in this case is same as the input x. Hence this function is not a PRF as this function can be distinguished from a uniformly selected function f by checking if the last n bits of the output is same as the input x.

Exercise 4-2

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
    $return\ r, k, c$
$else$:
    $return\ r, 0, c$

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

Solution of Exercisesheet 4

$return$

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'.
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.