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: