Introduction to Modern Cryptography
Theresa, Celine, Prisca, Saibaba
November 15, 2022

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:

```
$\underline{Enc'(k,m)}:$
$IV \leftarrow \{0,1\}^\lambda$
$c_0 := IV$, if invoked for the first time
$c_0 := c_n^{last\_invoke\_from\_Enc'}$
$for\ i = 1, ..., l\ do$
    $c_i = H^s||(c_{i-1})Enc(k,m)$
$return\ (c_0, ..., c_n)$

    $\underline{Dec'(k,c)}:$
$IV := c_0$
```

Solution of Exercisesheet 4

```
$for\ i = 1, ..., l\ do$
    $m_i = c_{i-1} \oplus Dec(k, c_i)$
```

Proof, that Pi' remains EAV-mult secure:

Describe a successful adversary against the CPA security of Pi':
The adversary can choose the first message randomly. Then he knows that the recieved ciphertext is used as the IV for the next encryption. Because of this he can choose the next message adoptively. For example when he chooses the message like the recived cipehertext, he knows that the input to the encryption function is 0. So the adversary can influence every input to the encryption function