Cryptography and Networked Systems Security

Prof. Dr.-Ing. Volker Roth
Freie Universität Berlin

Homework 3

Academic Integrity

Hereby I certify that I have neither received nor given help in answering the questions in this homework assignment.

_____

Date, signature, name in block letters

Question 1 (10 pts.)

Prove that if a private-key cipher Π can encrypt messages of arbitrary length and the adversary is not restricted to output messages of equal length then Π cannot have indistinguishable encryptions in the presence of an eavesdropper.

Hint: The answer is not as trivial as you may think at first glimpse. Note that Π does not necessarily have to encrypt a message of length ℓ into a ciphertext of equal length ℓ. Consider a polynomial upper bound $p(\cdot)$ on the length of the ciphertext when Π is used to encrypt a single bit and use that as a starting point.

Question 2 (10 pts.)

Let G be a pseudorandom generator where $|G(s)| > 2|s|$.

1. Is $G'(s) = G(s0^{|s|})$ necessarily a pseudorandom generator?

2. Is $G'(s) := G(s_1 \cdots s_{n/2})$, where $s = s_1 \cdots s_n$, necessarily a pseudorandom generator?

Question 3 (10 pts.)

Present formulas for encryption/decryption of all the different modes of encryption we have seen. For which modes can decryption be parallelized?

Question 4 (10 pts.)

Let $\Pi_i = (\mathrm{Gen}_i, \mathrm{Enc}_i, \mathrm{Dec}_i)$ for $i = 1, \ldots, r$ and $2 \leq r \in \mathbb{N}$. One of the Π_i is CPA-Secure. Construct a CPA-secure encryption scheme Π, which uses $\Pi_1, \ldots, \Pi_r$, while not knowing which of the Π_i is CPA-Secure. Prove that your Π is CPA-Secure.

Question 5 (10 pts.)

1. Show that the CBC, OFB and CTR-Mode are not CCA-secure encryption schemes (for every F).
2. Do the operation modes presented in the lecture protect the integrity of the data? Discuss!