MODERN CRYPTOGRAPHY
University of Amsterdam, 2019

TEAM NAME: Your team name
STUDENT NAMES: Your names

Homework set 3

Contents

Group Project [7 pt]

Find concrete IND attackers for the proposed encryption systems from Week 1.

1. Find an attack or prove security of your scheme. You can deal with IND-EAV, IND-CPA, and IND-CCA security notions. [3 pts].
2. Find one other proposed system for which you can give a successful IND-EAV/IND-CPA/IND-CCA attacker [3pt]. State the name of the scheme you are attacking, describe the attacker and compute its success probability.
3. Find yet another proposed system for which you can give a successful IND-EAV/IND-CPA/IND-CCA attacker [1pt]. State the name of the scheme you are attacking, describe the attacker and compute its success probability.

Try to find as strong attacks as possible, where by strong we mean that an IND-EAV attack is stronger than an IND-CPA attack, which is stronger than an IND-CCA attack.

When you have completed any of the exercises above, please reply to to the posted encryption scheme with: "Team XXX has found an IND-YYY attack/has proved IND-YYY security on this scheme" (where XXX is your team name and YYY is the type of attack/proof you've found), without giving the actual details in order not to spoil the fun for the other teams. Once the homework deadline has passed, we will ask you to modify your answer to explain the actual attacks. Of course, you should include the attack details in your homework answers here.

Solution: □

Question 1 [1 pt]: PRF

Let F be a pseudorandom function with 128-bit key and 256-bit block length (output length). Which of the following functions G are pseudorandom generators? (Select all that apply.)

1. $G(x) := F_{0\cdots 0}(x) \| F_{1\cdots 1}(x)$, where x is a 256-bit input
2. $G(x) := F_x(0\cdots 0) \| F_x(0\cdots 0)$, where x is a 128-bit input
3. $G(x) := F_x(0\cdots 0)$, where x is a 128-bit input
4. $G(x) := F_x(0\cdots 0) \| F_x(1\cdots 1)$, where x is a 128-bit input

Solution: Your solution here. Answers have to be fully justified in order to get the full amount of points. □

Question 2 [2 pt]: not a PRF

Let F be a length-preserving pseudorandom function. For the following construction of a keyed function $F' : \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$,

$$F'_k(x) := F_k(0\|x)\|F_k(x\|1)\,,$$

give an attack to show that F' is not a pseudorandom function.

Solution: Your solution here □

Question 3 [6 pt]

Let F be a pseudorandom function and G be a pseudorandom generator with expansion factor $\ell(n) = n + 1$. For each of the following encryption schemes, state

- whether the scheme has indistinguishable encryptions in the presence of an eavesdropper (0.5pt) and
- whether it is CPA-secure (0.5pt).

In each case, the shared key is a uniform $k \in \{0,1\}^n$. Explain your answer (1pt) in one or two sentences.

1. To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.
2. To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$.
3. To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1 \| m_2$ with $|m_1| = |m_2|$, then choose uniform $r \in \{0,1\}^n$ and send $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$.

Solution: justify your answers □

Question 4 [4 pt]: Exercise 3.26 from [KL]

For any function $g : \{0,1\}^n \to \{0,1\}^n$, define $g^{\$}(\cdot)$ to be a probabilistic oracle that, on input 1^n, chooses uniform $r \in \{0,1\}^n$ and returns $\langle r, g(r)\rangle$. A keyed function F is a weak pseudorandom function if for all PPT algorithms D, there exists a negligible function negl such that:

$$\left|\Pr[D^{F_k^{\$}(\cdot)}(1^n) = 1] - \Pr[D^{f^{\$}(\cdot)}(1^n) = 1]\right| \leq \mathsf{negl}(n)$$

where $k \in \{0,1\}^n$ and $f \in \mathsf{Func}_n$ are chosen uniformly.

1. Prove that if F is pseudorandom then it is weakly pseudorandom.

2. Let F' be a pseudorandom function, and define

   $$F_k(x) := \begin{cases} F'_k(x) & \text{if } x \text{ is even} \\ F'_k(x+1) & \text{if } x \text{ is odd.} \end{cases}$$

   Prove that F is weakly pseudorandom, but *not* pseudorandom.

3. Is CTR-mode encryption using a weak pseudorandom function necessarily CPA-secure? Does it necessarily have indistinguishable en- cryptions in the presence of an eavesdropper? Prove your answers.

4. Prove that Construction 3.30 (on page 83 in [KL]) is CPA-secure if F is a weak pseudo-random function.

Solution: □

Question 5 [2 pt]: Exercise 3.14 from KL

Argue that if F is a length-preserving pseudorandom function, then $G(s) := F_s(1) \| F_s(2) \| \cdots \| F_s(\ell)$ is a pseudorandom generator with expansion factor $\ell \cdot n$.

Solution: □

Programming Question 6 [8 pt]

Solve programming assignment 3. Describe the solution and how you proceeded in your pdf answer to this Homework. Please include the final answer as well. You may use any programming language you like to solve the problem, and you may include a link to your code in the submission.

Solution: □