University of Stuttgart
Institute of
Information Security

Security and Privacy
Summer Term 2018
Prof. Dr. Ralf Küsters

Homework 2

Submission into the *red SEC mailbox* in front of Room 2.041 until June 5, 2018, 14:00.

General Notes

- If you encounter difficulties, you SHOULD[1] ask the teaching assistants (see ILIAS for contact information).
- To solve the homework, you SHOULD form teams of 3 people.
- Your team size MUST NOT exceed 3 people.
- You MUST submit your homework on paper (one submission per team).
- You are free to choose whether you write your solutions in German or in English.
- If your submission contains multiple sheets, you MUST staple them.
- Each sheet of your submission MUST include all team member's names and matriculation numbers.
- If you do not adhere to these rules, you risk losing points.

Problem 1: Matching Algorithm (4 points)

Develop an algorithm $\mathtt{match}(m, t)$ that, given a message $m \in \mathcal{M}$ and a term $t \in \mathcal{T}$, decides whether m matches t and, if it does, computes a matcher σ of m and t.

What is the time and space complexity of your algorithm?

Problem 2: Basics - Probability Theory

Solve the following tasks about probability theory:

(a) Prove the following Lemma from Slide Set 02, Slide 24: (2 points)

Let $E_1 \subseteq \Omega_1$ and $E_2', E_2 \subseteq \Omega_2$ such that $P_2(E_2) > 0$ and $E_2 \subseteq E_2'$. Then the following holds true:

$$P(E_1 \times E_2' \mid \Omega_1 \times E_2) = P_1(E_1)$$

(b) Prove the following Lemma from Slide Set 02, Slide 25: (2 points)

Let $(\Omega, 2^\Omega, P)$ be a probability space , $\mathcal{X}$ a finite set, $X : \Omega \to \mathcal{X}$ a random variable, and $P^X : 2^\mathcal{X} \to [0, 1]$ with

$$P^X(A) = P(X \in A) \quad [= P(X^{-1}(A))]$$

Then $(\mathcal{X}, 2^\mathcal{X}, P^X)$ is a probability space.

[1] SHOULD, MUST, and MUST NOT are used as defined in RFC2119.

SEC

Problem 3: Basics - Algorithms (4 points)

Let $R(\cdot)$ be some probabilistic algorithm with runtime upper bounded by a constant $t \in \mathbb{N}$ (for all possible inputs). Let $M := \mathbb{Z}_{15}$ be a set of numbers. Consider the following algorithm:

function $A(z)$
  $a, b = 1$
  $c \xleftarrow{\$} \{0,1\}$
  if $c = 1$ **then**
    $a \xleftarrow{\$} M$
    if $a < 12$ **then**
      $d \xleftarrow{\$} R(z)$ ▷ Denotes the execution of a probabilistic algorithm, see Slide Set 02, Slide 47
    else
      $b \xleftarrow{\$} \{0,1\}^2$
    end if
  end if
  out $= a \cdot b \cdot c$ ▷ Regular multiplication of three natural numbers. Binary strings are interpreted as numbers as usual.
  return *out*
end function

Let $z \in \{0,1\}^*$:

(a) Define the probability space of $A(z)$ via a product space as presented in the lecture.

(b) Compute $\Pr[A(z) = 1]$.

(c) Compute $\Pr[d \neq \perp]$ (see Slide Set 02, Slide 37 for this notation).

(d) Compute $\Pr[A(z) \leq 24 \mid b = 2]$

Problem 4: Basics - Group Theory

Solve the following tasks about group theory:

(a) Decide for each of the following groups whether they are cyclic. Prove your statement. (2 points)

- $(\mathbb{Z}_8^*, \cdot_8)$
- $(\mathbb{Z}_{10}^*, \cdot_{10})$

(b) Prove the following Lemma from SlideSet 02, Slide 61: (2 points)

Let $n \geq 1$. Then $(\mathbb{Z}_n^*, \cdot_n)$ is an abelian group.