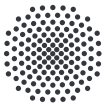

University of Stuttgart
Institute of
Information Security

Grundlagen der Informationssicherheit
Winter Term 2017/18
Prof. Dr. Ralf Küsters

Homework 2
Submission in the lecture on November 21, 2017

Note: This is an updated version. Updates are marked in red.

General Notes

- If you encounter difficulties, you SHOULD[1] ask the teaching assistants in the tutorial sessions.
- 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.
- You MUST hand in your submission *before/at the start of the lecture*! You SHOULD insert your submission into the green mailbox in front of room 2.041. For this sheet, you MAY still hand in your submission at the beginning of the lecture in the lecture room.
- If you do not adhere to these rules, you risk loosing points.

Problem 1: Affine Encryption Scheme (5 points)

The affine encryption scheme with parameter $n > 1$ is $(\mathbb{Z}_n, \mathbb{Z}_n^* \times \mathbb{Z}_n, E, D)$ with E and D defined as follows:

$$E(x \in \mathbb{Z}_n, (a,b) \in \mathbb{Z}_n^* \times \mathbb{Z}_n) = (a \cdot_n x) +_n b$$
$$D(y \in \mathbb{Z}_n, (a,b) \in \mathbb{Z}_n^* \times \mathbb{Z}_n) = a^{-1} \cdot_n (y -_n b)$$

Note that "$-_n$" is defined as $c -_n d := (c - d) \bmod n$ for $c, d \in \mathbb{Z}$.

Construct an attacker that derives the key (a, b) and uses this key to (always) win the security game. Show that your attacker always wins the security game.

Problem 2: Insecurity of R-CTR-Vernam (5 points)

Show that the R-CTR mode is insecure (i.e., it does not fulfil the security definition in Slide Set 1 on Slide 31f.) if the Vernam encryption scheme is used in place of the block cipher. Show that your attacker always wins the security game. You can assume that R-CTR-Vernam works with blocks of the length 128 and keys of the same length.

Hint: For the attack, it is sufficient to use plaintexts with only very few blocks.

Problem 3: Calculation Rule in $\mathbb{Z}_n$ (5 points)

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}, n \geq 1$. Show that $(a \cdot b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$.

Problem 4: Group of Units of a Commutative Ring (5 points)

Let R^* be the set of units of a commutative ring $(R, +, \cdot)$. Show that $(R^*, \cdot)$ is a group.

Problem 5: Greatest Common Divisor Property (5 points)

Let $a, b \in \mathbb{Z}$. Show that $\gcd(a, b) = \gcd(b, a \bmod b)$.

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

Problem 6: Extended Euclidian Algorithm (5 points)

Use the extended Euclidian algorithm to calculate the inverse of 32 in $\mathbb{Z}_{51}$. Show your calculations in the table as presented in the lecture (see Slide Set 2, Slide 31) and write down the value of 32^{-1} separately.

Note: You might already know a slightly different presentation of the extended Euclidian algorithm. You MUST, however, use the table exactly as presented in the lecture.