University of Stuttgart
Institute of
Information Security

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

Homework 3

Submission into the *green SEC mailbox* in front of Room 2.041 until December 5, 2017, 17:30.

(No submission in the lecture anymore!)

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.
- If you do not adhere to these rules, you risk loosing points.

Problem 1: RSA Encryption and Fast Exponentiation (5 points)

Let $(n, e) = (77, 11)$ be a public RSA key. Use this key to encrypt the plaintext 9 by executing the algorithm FastExponentiation (see Slide Set 2, Slide 43). Show your calculations in the table as presented in the lecture and write down your result separately.

Problem 2: Hash Functions and Collision Resistance

In this problem, we consider hash functions that only take inputs up to a certain length (contrary to our definition in the lecture). We use $\{0,1\}^{<n}$ (with some $n \in \mathbb{N}$) to denote the set of all bit strings up to (but not including) length n.

Let $L > l > 0$.

(a) Is the function h below a collision resistant hash function? Prove your answer. (2 points)

Let $h : \{0,1\}^{<2^l} \to \{0,1\}^l$ with $h(x) = |x|_1$, where $|x|_1$ encodes the number of ones in x (as a bit string of length l).

(b) Let $h : \{0,1\}^{<L} \to \{0,1\}^l$ a collision resistant hash function. Is the function H below a collision resistant hash function? Prove your answer. (3 points)

Let $H : \{0,1\}^{<2L-1} \to \{0,1\}^l$ with

- $H(x) = h(x)$ if $x \in \{0,1\}^{<L}$ and
- $H(x) = h(x_1) \oplus h(x_2)$ if $x = x_1||x_2 \in \{0,1\}^{<2L-1}$ for $x_1 \in \{0,1\}^{L-1}$ and $x_2 \in \{0,1\}^{<L}$ (recall that $||$ denotes the concatenation of two bit strings).

Problem 3: Collision Resistance and Confidentiality (5 points)

In this problem, we analyze whether a hash function that discloses parts of its input can be collision resistant.

Let h be a hash function with output length l. Furthermore, let h' be a hash function with output length $(l+1)$ where $h'(x) = x(0)||h(x)$ (for all $x \in \{0,1\}^*$; for the empty word $x = \epsilon$, we define $x(0) = 1$ for the purpose of this task).

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

Prove that the collision resistance of h implies the collision resistance of h', i.e., if you have a collision for h', you can construct a collision for h.

Problem 4: Insecurity of CBC-MAC with Variable Length (5 points)

Prove that the CBC-MAC is insecure if it is used on messages of different lengths, i.e., if it is used (with the same key) on several messages with different numbers of blocks.

Note that this requires you to define an attacker on the security game (see Slide Set 3, Slide 36) and to show that his advantage is large. To be more specific, your attacker should be able to get an advantage of 1.

Problem 5: Insecurity of PKCS#1 with Insecure Hash (5 points)

Prove that the PKCS#1 signature scheme is insecure if the underlying hash function is not collision resistant. That is, you can assume that an attacker on PKCS#1 knows a collision for the hash function.

Note that, similar to above, this requires you to define an attacker on the security game (see Slide Set 4, Slide 8) and to show that his advantage is large. To be more specific, your attacker should be able to get an advantage of 1.