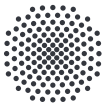

University of Stuttgart
Institute of
Information Security

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

Homework 1
Submission in the lecture on November 7, 2017

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: Encryption Schemes (5 points)

Let $X = \{a, b, c\}$ be a set of plaintexts, $Y = \{A, B, C\}$ a set of ciphertexts, and $K = \{k_1, k_2, k_3\}$ a set of keys.[2] The tables below define three different encryption functions $E : X \times K \to Y$. For which cases does there exist a D such that (X, K, E, D) is an encryption scheme? Explain your answers and (if applicable) define D.

(a)

	a	b	c
k_1	A	B	C
k_2	B	C	A
k_3	C	A	B

(b)

	a	b	c
k_1	A	B	C
k_2	B	A	C
k_3	A	B	C

(c)

	a	b	c
k_1	A	B	A
k_2	B	C	B
k_3	C	B	C

Problem 2: Vernam (5 points)

Let $M = \{0, 1\}^{80}$ be the set of bit strings of length 80.

Let

$$y = \texttt{96 c4 ca 8c 4b 2a 7e 79 c5 8c} \quad \text{and}$$
$$k = \texttt{de ad be ef 23 42 17 12 a0 fe}$$

words in M (given in hexadecimal notation). A word x has been encrypted to y using the key k with the Vernam encryption scheme. What is x? Explain how you calculated x.

Note: The plaintext contains a human readable word encoded with the ASCII format. You can use an ASCII table to decode the bytes into human readable characters.

[1] SHOULD, MUST, and MUST NOT are used as defined in RFC2119.
[2] The sets X, Y, and K contain pairwise distinct bit strings ($\in \{0, 1\}^*$) each, which are represented by the given symbols for readability.

Problem 3: Insecurity of an Encryption Scheme

Let $l > 0$. Let $\mathcal{S} = (X, K, E, D)$ be a tuple with

- $X = \{0,1\}^l$
- $K = \{0,1\}^l$
- E defined as follows:

  1: **function** $E(x \in X,\ k \in K)$
  2: Randomly choose $r \in \{0,1\}^l$;
  3: Let $z := x \oplus 1^l$;
  4: Let $r' := r \oplus k$;
  5: Let $y := r' || z$;
  6: **return** y;
  7: **end function**

  with 1^l being a bit string of length l consisting only of bits with value 1 and with $||$ denoting concatenation of bit strings.

(a) Define D such that $\mathcal{S}$ is an encryption scheme. (5 points)

(b) Show that $\mathcal{S}$ is insecure, i.e., provide an algorithm (attacker) that wins the security game with advantage 1. (5 points)