Computersystemsicherheit - Übungsblatt 1

Lehrstuhl für Angewandte Kryptographie

Wird in den Übungsgruppen vom 30. Oktober bis 03. November behandelt.

Aufgabe 1: Grundlegende Begriffe

(a) Was ist der Unterschied zwischen *Safety* und *Security*?

(b) Was bedeutet *Defense in Depth*? Geben Sie ein Beispiel aus der Realität.

(c) Erklären Sie den Begriff *Fail-safe-Standards* und geben Sie Beispiele an, die **nicht** in der Vorlesung erwähnt wurden.

Aufgabe 2: Kryptographie

(a) Was sind *drei* wesentlichen Schutzziele der Kryptographie?

(b) Was sind die Unterschiede zwischen symmetrischen und asymmetrischen Kryptoverfahren? Geben Sie jeweils ein Kryptoverfahren als Beispiel an.

Aufgabe 3: Abgewandelte Definiton des OTP

Betrachten Sie die folgende Definition des leicht abgewandelten One-Time-Pad (OTP) Verschlüsselungsverfahren, bei dem der Schlüssel als ein Paar (k_1, k_2) aus zwei n-bit Schlüsseln definiert ist.
Formell:

$$
\begin{aligned}
&Gen: \text{ Ausgabe eines zufälligen Schlüsselpaars } (k_1, k_2) \xleftarrow{\$} \{0,1\}^{2n} \\
&Enc: c = m \oplus k_1 \oplus k_2 \\
&Dec: m = c \oplus k_1 \oplus k_2
\end{aligned}
$$

Analysieren Sie die Eigenschaften dieses abgewandelten OTP-Verfahrens:

(a) Zeigen Sie, dass die oben beschriebene Verschlüsselung und Entschlüsselung korrekt ist und die ursprüngliche Nachricht m wiederhergestellt werden kann.

(b) Ist es sicher, einen Teil des Schlüssels (z.B. k_1 oder k_2) für verschiedene Nachrichten zu wiederverwenden?
Begründen Sie Ihre Antwort.

Aufgabe 4: Sicherheit gegenüber Chosen-Ciphertext-Attacks (Recherche)

In der Vorlesung haben Sie den Sicherheitsbegriff *indistinguishability against chosen-plaintext attacks (IND-CPA)* kennengelernt. In dieser Aufgabe beschäftigen wir uns mit der stärkeren Sicherheitsdefinition von *indistinguishability against chosen-ciphertext attacks (IND-CCA)*.

(a) Finden Sie heraus, was Chosen-Ciphertext-Attacks (CCA) in der Kryptographie bedeuten. Analysieren Sie insbesondere welche zusätzlichen Möglichkeiten ein Angreifer im Vergleich zu IND-CPA hat.

(b) Skizzieren Sie das Sicherheitsspiel für IND-CCA ähnlich wie das Sicherheitspiel für IND-CPA, das Sie in der Vorlesung gesehen haben.
Beschreiben Sie, wie das Spiel abläuft und was das Ziel des Angreifers ist.