PS Einführung Kryptographie und IT-Sicherheit

Salzburg, T01, 14:45 *29.04.2024*

19.) Diskutieren sie die beiden im PS zur Frage "Wie viele Menschen müssen in einem Raum sein, damit die Wahrscheinlichkeit grösser als 0.5 ist, dass eine der Personen an einem vorgegebenen Tag Geburtstag hat?" besprochenen Lösungen, und insbesondere, welche der beiden unter welchen Umständen korrekt ist.

20.) Beweisen sie **auf nachvollziehbare Weise**: Eine Hash Funktion produziert einen m-Bit Output. Um eine Nachricht zu finden, die auf einen gegebenen Wert abgebildet wird, müssen 2^m Nachrichten generiert und gehashed werden. Um zwei Nachrichten zu finden, die den selben Hash-Wert liefern, müssen nur $2^{m/2}$ Nachrichten produziert werden.

21.) In der Protokollattacke gegen digitale Empfangsbestätigungen spielen die Vorraussetzungen $V_x = E_x$ und $S_x = D_x$ eine wesentliche Rolle. Führen sie Schritt für Schritt die beschriebene Attacke (Slides S.91 und 92) mit und ohne die beiden Vorraussetzungen durch und erklären sie genau, bei welchen Schritten (und warum) die Attacke ohne die Vorraussetzungen nicht funktioniert.

22.) Erklären sie, warum die Verwendung von Hashfunktionen im Kontext mit digitalen Signaturen die Protokollattacke gegen digitale Empfangsbestätigungen verunmöglicht. Bedenken sie dabei insbesondere, dass in diesem Fall NachrichtenHash und Nachricht übermittelt werden.

23.) Führen sie eine Geburtstagsattacke (beschrieben auf S. 87 der VO-Slides) durch: Erstellen sie **zwei** semantisch unterschiedliche Dokumente (wie im besprochenen Beispiel die beiden unterschiedlichen Mietverträge) im Format ihrer Wahl (Word, Postscript, etc.), und modifizieren sie **beide Varianten** Semantik-erhaltend automatisiert (beschreiben sie das detailliert, wie sie dabei vorgehen), bis sie auf zwei Varianten mit dem gleichen hash-Wert treffen (verwenden sie als Hash-Wert einen Teil des Outputs der eigentlich obsoleten Hashfuntion MD-5).

VIEL ERFOLG !!