Aufgabenblatt Nr. 3

Aufgabe 1 V

Bei Merkle's Puzzle besteht der öffentliche Schlüssel aus einer Reihe von verschlüsselten Einträgen. Jeder Eintrag i enthält eine ID ID_i und einen symmetrischen Schlüssel k_i. Die Einträge sind mit schwachen Schlüsseln κ_i verschlüsselt.

Das Verfahren ist leider nicht effizient genug für den praktischen Einsatz. Bewerten Sie die folgenden Verbesserungsvorschläge aus Sicht der IT-Sicherheit.

Aufgabe 1.1

Anstelle der ID, die im Chiffrat den verwendeten Eintrag spezifiziert, enthält das Chiffrat die Nummer des Eintrags. Damit entfallen die ID_i und die Einträge (und damit der öffentliche Schlüssel) werden kleiner.

Aufgabe 1.2

Um den Aufwand für die Verschlüsselung zu verringern, werden alle Einträge mit dem gleichen Schlüssel κ verschlüsselt.

Aufgabe 1.3

Der Inhaber des öffentlichen Schlüssel markiert die Einträge seines öffentlichen Schlüssels, die in der Vergangenheit genutzt wurden, um eine mehrfache Nutzung gleicher Einträge zu vermeiden.

Aufgabe 2 V

Gegeben seien die Primzahlen $p = 17$ und $q = 19$, sowie $e = 19$ für den öffentlichen Schlüssel und $d = 91$ für den geheimen Schlüssel.

Aufgabe 2.1

Berechnen Sie $n = p \cdot q$ und prüfen Sie, dass $e \cdot d = 1 \bmod (p-1)(q-1)$.

Aufgabe 2.2

Alice möchte das ASCII-Zeichen 'A' verschlüsseln. Finden Sie die Binärdarstellung dieses Zeichens, interpretieren Sie diese als ganze Zahl, und verschlüsseln Sie diese Zahl.

Aufgabe 2.3

Entschlüsseln Sie Ihr Chiffrat mit dem geheimen Schlüssel.

Aufgabe 2.4

Wie groß darf die zu verschlüsselte Nachricht für die angegebenen Parameter höchstens sein? Wie viele Bit bzw. Byte lassen sich damit darstellen?

Aufgabe 3 V

Alice und Bob möchten einen Diffie-Hellman-Schlüsselaustausch durchführen. Sie nutzen dazu den Modulus $p = 23$ und den Generator $g = 5$.

Alice wählt ihren geheimen Exponenten $a = 14$, Bob wählt seinen geheimen Exponenten $b = 9$.

Bestimmen Sie die Nachrichten von Alice an Bob und von Bob an Alice sowie den gemeinsamen Schlüssel.