Prof. Dr. A. Goerdt
Julian Pape-Lange

TU Chemnitz
Sommersemester 2023
04.06.2023

Datensicherheit und Kryptografie

9. Übung

Abgabe: Lösen Sie die Aufgabe **1**. Ihre Lösungen geben Sie bitte

- bis zum 09.06.2023 um 13:00 Uhr per Mail
  an `julian.pape-lange@informatik.tu-chemnitz.de`

ab.

1. Aufgabe: (3+2+3+2)P

(a) Zeigen Sie, dass aus $\text{ggT}(a, m) > 1$ folgt, dass $a^{m-1} \not\equiv 1 \pmod{m}$ gilt.

(b) Zeigen Sie, dass für gerade $m > 2$ die Ungleichung $(m-1)^{m-1} \not\equiv 1 \pmod{m}$ gilt.

(c) Zeigen Sie, dass für ungerade a die Äquivalenz $a^2 \equiv 1 \pmod{8}$ gilt.

(d) Sei $i \geq 0$ eine ganze Zahl. Finden Sie alle a, die die Äquivalenz $a^2 \equiv 1 \pmod{2^i}$ erfüllen.

2. Aufgabe:
Bei den bisherigen Signaturen war die Signatur oft in der selben Größenordnung wie die eigentliche Nachricht. Dies hat dazu geführt, dass wir (mindestens) etwa doppelt so viele Daten übertragen mussten, als es für die Nachricht alleine notwendig wäre.
Dies wollen wir vermeiden, indem wir die Nachricht erst mit einer so genannten Hash-Funktion verkürzen.

- Welche Probleme entstehen, wenn wir für die Hash-Funktion einfach die Einschränkung auf die ersten k Bits oder die reduktion auf einen kleinen Modul m verwenden?
- Welche Eigenschaften sollte eine Hash-Funktion idealerweise erfüllen?

3. Aufgabe:
Hash-Funktionen werden auch verwendet, um Passwörter sicher zu speichern. Anstelle des Passworts speichern seriöse Internetseiten nur den Hash des Passworts.

- Welche Vorteile ergeben sich daraus?
- Welche Nachteile ergeben sich daraus?
- Oft werden die gespeicherten Hashes noch mit Zusatzinformationen „gesalzen“. Wieso erhöht dies zusätzlich die Sicherheit des Passworts?

4. Aufgabe:
Wir können Texte durch Vertauschen der Zeichen verschlüsseln. Dafür ist eine Permutation, zum Beispiel $A = [3, 1, 2, 4]$ gegeben und ein Text $T =$ `abcd` wird durch vertauschen der Zeichen mit der Vorschrift $T'[i] = T[A[i]]$ verschlüsselt. In diesem Fall gilt also $T' =$ `cabd`.
Ich habe einen einfachen Text mit der Permutation

$$A = [1, 6, 11, 16, 2, 7, 12, 17, 3, 8, 13, 18, 4, 9, 14, 19, 5, 10, 15, 20]$$

verschlüsselt und

$$T' = \texttt{e\_a\_iectniheenexnfnt}$$

erhalten. Entschlüsseln Sie T'.