Dr. Dirk Frettlöh 24.4.2024

Übungen zur Vorlesung Kryptographie

Blatt 3

Aufgabe 9: (Euler-Fermat benutzen)
(a) Berechnen Sie $3^{1\,000\,003} \bmod 101$ von Hand, ohne Computerhilfe.

(b) Berechnen Sie die letzten beiden Dezimalziffern von $23^{1\,000\,005}$ von Hand, ohne Computerhilfe.

Aufgabe 10: (Quadratische Reste malen)
Finden Sie alle quadratischen Reste in Z_{15}, Z_{17} und Z_{19}. Visualisieren Sie die Quadrat-Wurzel-Beziehung jeweils in einem Graphen wie in Beispiel 2.4 der Vorlesung. (Überprüfen Sie für sich Ihr Ergebnis, ob es zu Aufgabe 11 bzw Satz 2.6 passt.)

(Für die Abgabe reicht der korrekte Graph. Die quadratischen Reste sind ja genau die, auf die ein Pfeil zeigt.)

Aufgabe 11:
(a) Zeigen Sie, dass in den Quadratische-Reste-Graphen wie in Aufgabe 10 oder Beispiel 2.4 im Skript nie ein Pfeil von einem Knoten $a \in Z_N \setminus Z_N^*$ zu einem Knoten $b \in Z_N^*$ geht, und umgekehrt auch nicht.

(b) Zeigen Sie: Ist p eine ungerade Primzahl, so hat ein quadratischer Rest $a \in Z_p^*$ genau zwei Quadratwurzeln.

Aufgabe 12: (Primitivwurzeln)
(a) Finden Sie alle Primitivwurzeln in Z_{10}^*. Zeigen Sie, dass das wirklich Primitivwurzeln sind.

(b) Finden Sie die kleinste Primitivwurzel in Z_{26}^*. Zeigen Sie, dass das wirklich eine Primitivwurzel ist.

(c) Finden Sie das kleinste $N \in \mathbb{N}$ $(N > 1)$, so dass es keine Primitivwurzel in Z_N^* gibt. Begründen Sie, warum dies wirklich das kleinste solche N ist.

(Diese Aufgabe lässt sich prima in `sagemath` *lösen.)*

Abgabe bis Dienstag 7.5.2024 bis 23:59 Uhr per Email an den Tutor.
Bitte die Abgaben so nennen: [techfakaccount]-bl$n$.pdf, also z.B. `dfrettloeh-bl2.pdf`, oder `dfrettloeh+mnebel-bl2.pdf`.

Jakob Niermann	Mi 16 Uhr in T2-233	janiermann+krypto@techfak.de
Enrico di Gaspero	Do 16 Uhr in U2-216	edigaspero+krypto@techfak.de
Lisa Henetmayr	Fr 10 Uhr in X-E0-205	lhenetmayr+krypto@techfak.de
Richard Freidhof	Fr 12 Uhr in T2-141	rfreidhof+krypto@techfak.de