Institut für Informatik, Universität Bern
Einführung in die Informatik, HS 2021

Prof. Christian Cachin

Kryptographie – Übungen

1. Eine Hashfunktion?

Gegeben sei eine grosse Primzahl p und eine Zahl $g \in \mathbb{Z}_p^*$, so dass das Problem des diskreten Logarithmus modulo p zur Basis g schwierig ist. Dies bedeutet, kein effizienter Algorithmus findet für ein gegebenes, zufälliges $y \in \mathbb{Z}_p^*$ ein x für welches $g^x = y$ **mod** p gilt.

Die Funktion $H : \mathbb{Z} \to \mathbb{Z}_p^*$ sei definiert durch $H(a) = g^a$ **mod** p. Beachte, dass H Argumente erlaubt, welche viel grösser sein können als ihre Ausgabe (d.h., $a \gg p$). Ist H eine kryptographisch sichere Hashfunktion? Begründen Sie die Antwort.

2. Modulare Exponentiation

In der Vorlesung die Exponentiation modulo eine Primzahl gezeigt für die Rechnung 7^8 **mod** 11. Da $8 = 2^3$ funktionierte dies durch wiederholtes Quadrieren modulo 11 und zwar so, dass kein Zwischenresultat grösser wurde als $121 = 11^2$.

Wie kann man effizient eine modulare Exponentiation a^b **mod** m berechnen, wenn der Exponent b und der Modulus m beliebige, grosse Zahlen sind? Dabei sollte kein Zwischenresultat grösser werden als m^2. Repräsentieren Sie dazu den Exponenten im Binärsystem als $b = (b_k b_{k-1} \ldots b_1 b_0)_2$.

a) Beschreiben Sie einen Algorithmus dafür in Pseudocode oder in einer Programmiersprache Ihrer Wahl.

b) Berechnen Sie nach dieser Methode $x = 7^{151}$ **mod** 15. Zeigen Sie alle Zwischenergebnisse, indem Sie entweder von Hand rechnen oder die Zwischenschritte durch Ihr Programm ausgeben lassen.