EI Assignment 09

Vithusan Ramalingam (21-105-515)

Jan Ellenberger (21-103-643)

Aufgabe 1.)

H ist eine kryptografisch sichere Hashfunktion, da die Eigenschaften erfüllt sind.

a) H ist eine One-Way-Funktion von da her schwierig zu invertieren. ✓

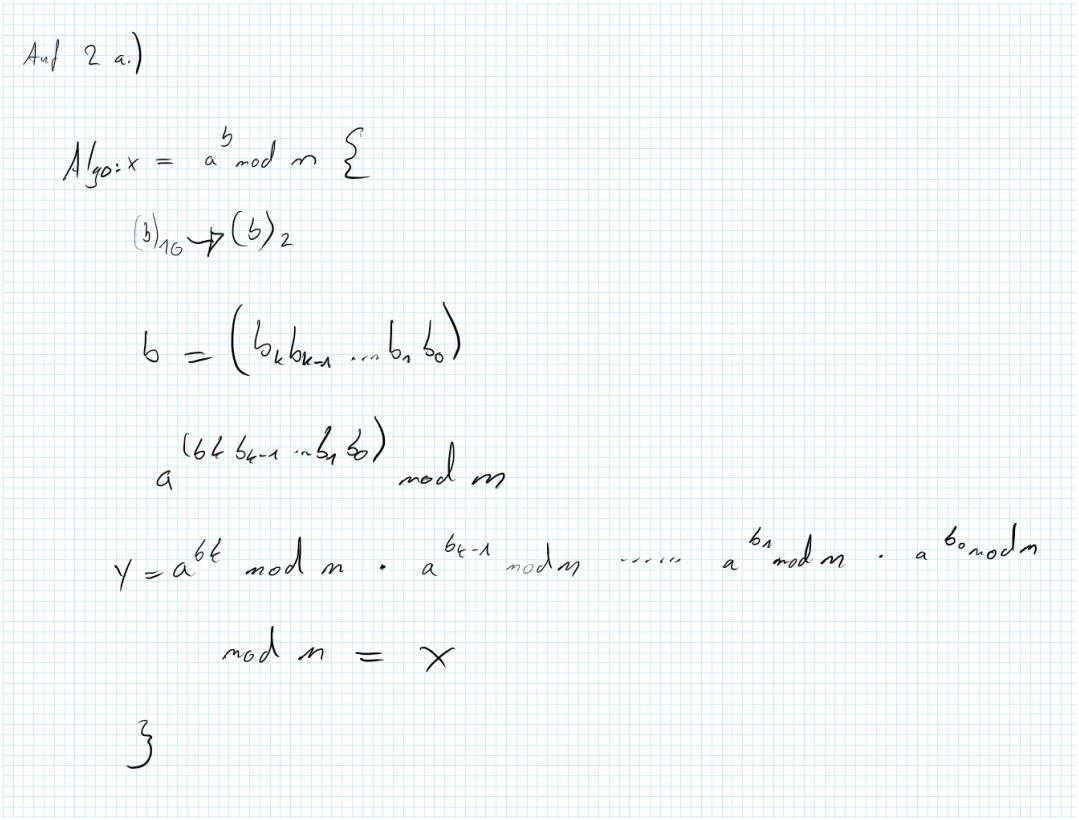
   Mithilfe des gewählten Formates verhindert man dass die Funktion einfach invertiert werden kann. Die Funktion kann sehr grosse Werte generieren, alleine das macht es schwierig, H(a) herzuleiten.

b) H ist collision-free, es ist praktisch nicht möglich zwei unterschiedliche Werte zu finden, (x_1 nichtgleich x_2) sodass H(x1) = H(x2). ✓
   Eine Kollision ist nicht unmöglich, jedoch ist die Wahrscheinlichkeit sehr gering. Da p eine Primzahl ist. (Kleiner Fermat Satz)
   Ausserdem kann g kein Vielfaches von p sein, da ansonsten H(a) = 0 ist. Unabhängig davon wie gross a ist. Was es zusätzlich schwieriger macht die Funktion zu rekonstruieren.

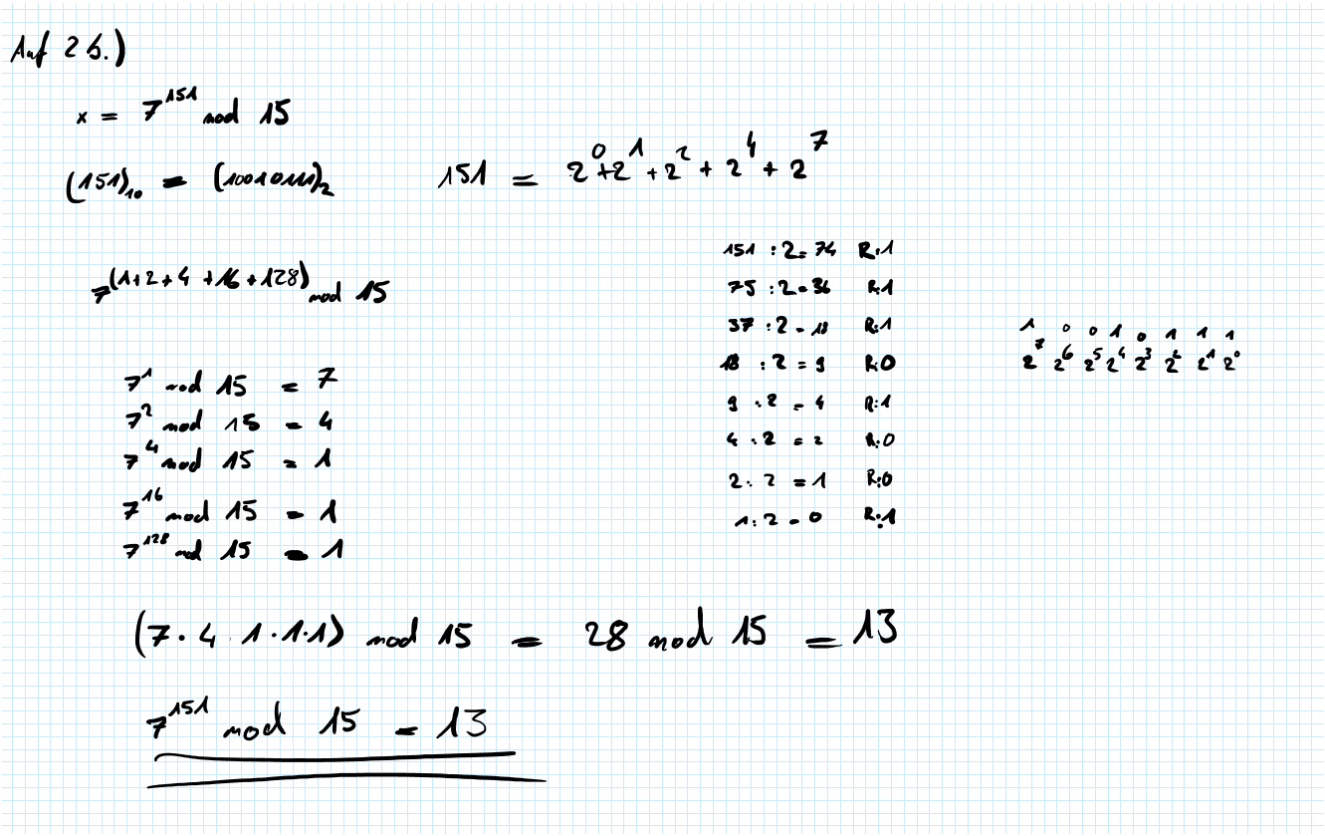
c) Die herausgegebenen Werte von H sehen zufällig aus. (obwohl H deterministisch ist).✓

   Die herausgegebenen Werte sehen willkürlich aus

Augabe 2. a)



Aufgabe 2.b)


Auf 2 b.)
x = 7^151 mod 15
(151)_10 = (10010111)_2
151 = 2^0 + 2^1 + 2^2 + 2^4 + 2^7
7^(1+2+4+16+128) mod 15
7^1 mod 15 = 7
7^2 mod 15 = 4
7^4 mod 15 = 1
7^16 mod 15 = 1
7^128 mod 15 = 1
151 : 2 = 75 R:1
75 : 2 = 37 R:1
37 : 2 = 18 R:1
18 : 2 = 9 R:0
9 : 2 = 4 R:1
4 : 2 = 2 R:0
2 : 2 = 1 R:0
1 : 2 = 0 R:1
1 0 0 1 0 1 1 1
2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0
(7 . 4 1 . 1 . 1) mod 15 = 28 mod 15 = 13
7^151 mod 15 = 13