

Grundlagen der Informationssicherheit WS 2017/2018:

Übungsblatt #2

Due on Dienstag, November 21, 2017

Gruppenabgabe

Lukas Baur, Felix Bühler, Marco Hildenbrand

Aufgabe 1

Getting the code (a, b)

Als erstes sendet der Angreifer eine Anfrage zum Verschlüsseln von 0 (also $E(0, (a, b))$). Zurückgegeben wird demnach: $E(x, (a, b)) = E(x, (a, b)) = (0 * a) +_n b = b$.

Im Anschluss sendet der Angreifer eine Anfrage zum Verschlüsseln von 1. Es gilt offensichtlich:

$E(x, (a, b)) = E(1, (a, b)) = (1 * a) +_n b = a +_n b$ Nun kann a leicht bestimmt werden, da $E(1, (a, b))$ sowie b bekannt ist. (a berechnet sich aus $E(1, (a, b)) - b$ bzw. $n + (E(1, (a, b)) - b)$ falls $E(1, (a, b)) - b$ negativ ist.)

Win the game with advantage = 1

Da der Schlüssel (a, b) nun bekannt ist, kann trivialerweise jeder Cifer-Text damit entschlüsselt werden.

Dass der advantage demzufolge bei 1 liegt, dürfte offensichtlich sein.

Da der Angreifer den Code nun dechiffrieren kann, kann er das Tupel (z_0, z_1) senden und erhält $z_i =: c$.

Er verschlüsselt nun (ggf. eigenständig) z_0 und z_1 . Nun kann er vergleichen ob $E(z_0, (a, b)) = c$ gilt. Falls ja, so war $i = 0$, sonst $i = 1$.

Alternativ entschlüsselt er c mit (a, b) und erhält z_0 oder z_1 und entscheidet entsprechend.

Aufgabe 2

Aufgabe 2.1

s

Aufgabe 3

Wir schreiben um:

$a = p_1 + r_1$ mit $0 \leq r_1 < n$ und $p_1 = k * n, k \in \mathbb{N}$ und demnach offensichtlich $r_1 = a \bmod n$

$b = p_2 + r_2$ mit $0 \leq r_2 < n$ und $p_2 = \tilde{k} * n, \tilde{k} \in \mathbb{N}$ und demnach offensichtlich $r_2 = b \bmod n$

$$\begin{aligned} &\text{Dann gilt: } (a * b) \bmod n \\ &= (p_1 + r_1) * (p_2 + r_2) \bmod n \\ &= (p_1 p_2 + r_1 p_2 + p_1 r_2 + r_1 r_2) \bmod n \\ &= p_1 p_2 \bmod n + r_1 p_2 \bmod n + p_1 r_2 \bmod n + r_1 r_2 \bmod n \\ &= kn\tilde{k}n \bmod n + r_1 n\tilde{k} \bmod n + knr_2 \bmod n + r_1 r_2 \bmod n \\ &= 0 + 0 + 0 + r_1 r_2 \bmod n \\ &= r_1 r_2 \bmod n \\ &= (a \bmod n)(b \bmod n) \bmod n \text{ (nach Definition)} \\ &\square \end{aligned}$$

Aufgabe 4

Da $(R, +, *)$ ein kommutativer Ring ist, gilt:

$(R, +, *)$ ist assoziativ

in $(R, +, *)$ existiert ein neutrales Element e bzgl. der Multiplikation

$(R, +, *)$ ist distributiv

$(R, +, *)$ ist kommutativ bezüglich $*$.

R^* ist nun definiert als die Menge aller invertierbaren Elemente aus $(R, +, *)$.

\mathbb{Z} :

$$1. (x * y) * z = x * (y * z) \forall x, y, z \in R^*$$

$$2. \exists x^{-1} \in R^* : x * x^{-1} = x^{-1} * x = e, \forall x \in R^*$$

$$3. \exists e \in R^* : x * e = e * x = x, \forall x \in R^*.$$

1. Da $R^* \subseteq R$ ist, gilt (1) offensichtlich immer noch.

2. Nach Voraussetzung besteht R^* nur aus invertierbaren Elementen, also existiert auch ein Inverses e in R^* :

Sei x invertierbar in R^* , dann existiert ein $x^{-1} \in R^*$, das dessen Inverse bildet (nach Definition von R^*). Da $e * e^{-1} = e^{-1} * e = 1 \Leftrightarrow e^{-1} = e$. Da $e \in R$ war, und offensichtlich invertierbar ist, so ist es auch $\in R^*$

3. Da $(R, +, *)$ ist kommutativ bezüglich $*$ war, und für jedes $y \in R$ ein neutrales Element existiert, so gilt auch $x * e = e * x = x, \forall x \in R^*$ sofern, dieses e auch in R^* vorhanden ist. Dies ist gemäß (2) erfüllt.

Also erfüllt $(R^*, *)$ alle Gruppenaxiome. \square

Aufgabe 5

Aufgabe 6

ExtendedEuclid(32,51):

a'	b'	x_0	y_0	x_1	y_1	q	r
32	51	1	0	0	1	0	32
51	32	0	1	1	0	1	19
32	19	1	0	-1	1	1	13
19	13	-1	1	2	-1	1	6
13	6	2	-1	-3	2	2	1
6	1	-3	2	8	-5	6	0
1	0	8	-5	-51	32		

$$1 = 8 * 32 + (-5) * 51$$

$$32^{-1} =_{51} 8$$

$$32^{-1} * 32 \bmod 51 = 8 * 32 \bmod 51 = 256 \bmod 51 = 1 \quad \square$$