Einführung zu RSA

Andreas Zweili, Ismail Cadaroski, Ivan Höhler, Michael Stratighiou

17. Dezember 2016

Inhaltsverzeichnis

1 Biographie

Hallo Dies ist ein Test

2 Verschlüsseln

TODO: Sind das wirklich alles Sections? Ich habe sie jetzt mal in Subsections geändert. Ist evtl. eher Fett gemeint?

2.1 Schlüsselkontruktion

N = Privatschlüssel p= primzahl q = primzahl

Gleichung erstellen nach :

$$\begin{aligned}\varphi(N) &= \varphi(p * q) \\ &= \varphi(p) * \varphi(q) \\ &= (p - 1) * (q - 1)\end{aligned}$$

2.2 Wählen der Variablen

$$\begin{aligned}p &= 7 \\ q &= 11 \\ \varphi(N) &= \varphi(11 * 7)\end{aligned}$$

2.3 Privatschlüssel

2.4 Öffentlicher Schlüssel

3 Verschlüsselung

Hallo Dies ist ein Test

4 Verteilung/Übertragung

Hallo Dies ist ein Test

5 Entschlüsselung

Hallo Dies ist ein Test

6 Schwachstellen

Hallo Dies ist ein Test

7 Referenzen