13.36 Aufgabe: RSA-Signatur

Gegeben sind der öffentliche Schlüssel (e=3, n=55) von Alice:

a) Sie erhalten eine Nachricht mit der Zahl „2“ die zusätzlich mit der digitalen Signatur von Alice ausgestattet wurde. Die Signatur lautet „18“. Prüfen Sie die Signatur.
b) Sie erhalten eine weitere Nachricht von Alice mit der Zahl „4“ und der Signatur „47“. Wie sieht es in diesem Fall mit der Authentizität des Absenders aus?
c) Sie wollen die Signatur von Alice unter der Nachricht „7“ fälschen. Berechnen Sie die Signatur und prüfen Sie diese im Anschluss.

a)

18^3 mod 55= 2

2 mod 55=2

Stimmt

b)

47^3 mod 55= 38

47 mod 55= 47

falsch

c)

x^3 mod 55 = 7

55n +28=x, n Element von N

55*1+28=83

83^3 mod 55 = 7