ComSysSec Übung 3

Thiemo Ganesha Welsch, Quang Duy Nguyen, Egemen Ulutürk, Leonard Bongard

2)

a) RSA-Signatur

s = (Enc(H(m))^d ) mod N

* uns fehlt d: d = mul. Inverse von e
* wir rechnen den erw. ekl. Algo: ggT(e, phi(n)) uns fehlt noch phi(n)
* Primfaktoren von n = p \* q = 7 \* 11 = 77
* Also phi(n) = (11-1) \* (7-1)= 60
* Also nun ggT(43,60) = 1 erw. ekl. Algo. : d = 7, l = -5
* Also ist d = 7
* Also s = (Enc(17)^7 )mod 77 = 17

b) RSA-Verifikation

s^e mod N = Enc(H(m)) mod N

62^23 mod N = Enc(3) mod N

62^23 mod N = 3^23 mod 91

69 != 61 🡨 Keine gültige Signatur

3)

a)