5. Aufgabe: Shamirs ThreePass-Protokoll

Alice und Bob haben sich auf die Primzahl p=17 geeinigt. Zeigen Sie an einem Zahlenbeispiel, wie die Nachricht m=10 mit Shamirs ThreePass-Protokoll verschlüsselt von Alice zu Bob übertragen und am Ende entschlüsselt werden kann.

Wählen Sie passende Werte für e_A, e_B, d_A, d_B.

10=M verschlüsseln, p=17

eA ggT(eA,p-1)=1

ggT(eA, 16)=1

⇨ eA = 5

eA*dA=1 mod 16

5*dA =1mod 16

dA=1/5

eB ggT(eB, 16)=1

eB=1

6*dA=1mod 16

dB=1

Alice -> Bob

10^5 mod 17=6

Bob entschlüsselt

M=(((m^eA)^eB)^dA)^dB mod p

(((10^5)^1)^1/5)^1 mod 17= (100.000)^1/5)^1 mod 17= 100.000^1/5 mod 17=10 mod 17=M