13.27 Aufgabe: Hybride Verschlüsselung mit RSA und Verschiebechiffre

Gegeben Sie ein hybrides Verschlüsselungsverfahren nach der Abbildung in Kapitel 6.2, bei dem RSA asymmetrisch und die Verschiebechiffre (vgl. Aufgabe 13.2, 26 Buchstaben im A-Z im Alphabet) als symmetrisches Verfahren eingesetzt werden.

Bob hat den öffentlichen RSA-Schlüssel e=7, n=55. Alice schickt in einer ersten Nachricht die Zahl 9 an Bob. Dies entspricht dem verschlüsselten symmetrischen Schlüssel. Danach folgt in der zweiten Nachricht der Ciphertext YOFZAOFLXOVF.

a) Bestimmen Sie den geheimen RSA-Schlüssel d und den verwendeten symmetrischen Schlüssel K.
b) Welche Nachricht hat Alice an Bob übertragen?

a)

n=55

sigma(55)=40

e*d mod n

ggT	Inverse^berechnen (Von unten nach oben lesen)
40=5*7 +5	=>1=3*(40-5*7)-2*7= 3*40-17 *7
7=1*5 +2	=>1=3*5-2*7
5=2*2+1	=>1=5-2*(7-1*5)=3*5-2*7
2=2*2+0	

Es folgt

1=3*40-17*7 mod 40

1=0-17*7 mod 40

d=-17+40=23

9^23 mod 55

9^1=9*1*1= 9 mod 55

9^10= 9*9 =81 mod 55=26 mod 55

9^101=26*26*9=6084 mod 55 = 26 mod 55

9^1011=34*34*9=10404 mod 55=9 mod 55

9^10111=9*9*9=729 mod 55= 14 mod 55

⇨ K =14

b)
Y-14=K
O-14=A
F-14=R
Z-14=L
A-14=M
O-14=A
F-14=R
L-14=X
X-14=J
O-14=A
V-14=H
F-14=R

Entschlüsselt: KARLMARXJAHR | Karl Marx Jahr