Sie dürfen Ihr Heft und alle Kopien, die ich ausgeteilt habe, benützen. Selbstverständlich sollen Sie auch Gebrauch machen von den eingebauten und den von uns zusätzlich programmierten Funktionen des Taschenrechners.

Der Lösungsweg muss immer ganz klar kommuniziert werden, Resultate ohne erkennbaren Lösungsweg geben keine Punkte.

1. Alice hat dummerweise zu kleine Primzahlen gewählt. Ihr öffentlicher Schlüssel besteht aus den Zahlen $n = 3551$ und $e = 257$. Bob verschlüsselt seine Nachricht b für Alice mit diesen Werten nach RSA und erhält die verschlüsselte Botschaft $c = 1292$, welche er via Mail an Alice sendet. Die böse Eve lauscht aber an der Leitung und gelangt so auch in den Besitz von c . Wegen dem kleinen Wert von n kann nun Eve c entschlüsseln.
   a) Wie geht Eve genau vor, um die Originalbotschaft b zu errechnen ?
   b) Welches ist diese Originalbotschaft b ? (Es handelt sich einfach um eine Zahl)

2. Die Gruppen D_3 , Z_9^* und Z_7^* haben alle 6 Elemente und könnten daher isomorph sein. Untersuchen Sie den Fall ! Ihre Antworten sind unwiderlegbar zu begründen.
   a) Sind D_3 und Z_9^* isomorph ?
   b) Sind D_3 und Z_7^* isomorph ?
   c) Sind Z_9^* und Z_7^* isomorph ?

3. Nochmals diese drei Gruppen D_3 , Z_9^* und Z_7^*.
   a) Wieviele Untergruppen hat D_3 ?
   b) Wieviele Untergruppen hat Z_9^* ?
   c) Wieviele Untergruppen hat Z_7^* ?

4. Was ist die Idee dahinter, einen Schlüssel s zuerst mit dem eigenen privaten und dann mit dem öffentlichen Schlüssel des Empfängers zu verschlüsseln und das Ergebnis dieser Operation einfach der mit s verschlüsselten Botschaft beizulegen und über einen öffentlichen, unsicheren Kanal zu übermitteln ? Wozu dieses doppelte Verschlüsseln von s ?

(1) a) Eve braucht den privaten Key d von Alice !

- n zerlegen in ein Produkt $p \cdot q$ 2
- $(p-1)\cdot(q-1) = m$ berechnen 2
- $d = e^{-1} \bmod m$! 2
- $c^d \bmod n$ ist die Originalbotschaft b ! 2

8/8

b) factor(3551) liefert $3551 = 53 \cdot 67$ 2

$52 \cdot 66 = m = 3432$ 2

euklidin(257, 3432) liefert $d = 641$ 2

$1292^{641} \bmod 3551$ ist die Originalbotschaft b. 6/6

12/12

$641 = 512 + 128 + 1$!

$2^9 \quad 2^7 \quad 2^0$

$1292^{641} \bmod n = 1292^1 \cdot 1292^{128} \cdot \left(1292^{128}\right)^4 \bmod n$

$= 1292 \cdot 3540 \cdot 437 \bmod n$

$= \underline{\underline{55}}$ (mein Jahrgang auf Velonummer ...)

20/20

(4) Zuerst mit

- dem privaten Key des Empfängers entschlüsseln

Dann mit:

- dem öffentlichen Key des Absenders entschlüsseln → s

Schritt 1 kann nur vom Empfänger gemacht werden, damit ist die Vertraulichkeit der Übermittlung garantiert 4

8/8

Schritt 2 findet nur vom richtigen Absender, wenn der Absender den privaten Key des Absenders kennt! Damit ist die Authentizität des Absenders noch gewährleistet! 4

(2) Die Gruppe D_3 haben wir als erstes Beispiel ausführlich behandelt (→ Theorieheft!).
Sie ist (im Gegensatz zu $\mathbb{Z}_9^*$ und $\mathbb{Z}_7^*$) nicht kommutativ!

⇒ a) nein 6/6 und b) nein 6/6 !! (oder: In D_3 ist 4x die 1 auf der Diagonalen!)

c) $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$

Die Quadrate in $\mathbb{Z}_7^*$: $\{1, 4, 2, 2, 4, 1\}$

" " in $\mathbb{Z}_9^*$: $\{1, 4, 7, 7, 4, 1\}$

Es wäre also gut möglich!

Vielfache von $a=2$ in $\mathbb{Z}_7^*$:

$a = 2,\ a^2 = 4,\ a^3 = 1$

Vielfache von 2 in $\mathbb{Z}_9^*$: $2, 4, 8, 7, 5, 1$

→ die ganze Gruppe!!

$= \mathbb{Z}_9^* = \{2, 2^2, 2^3, 2^4, 2^5, 2^6 = 1 = 2^0\}$

$\mathbb{Z}_9^*$ ist zyklisch 6/6

Gibt es auch so etwas in $\mathbb{Z}_7^*$??

$3,\ 3^2 = 2,\ 3^3 = 6,\ 3^4 = 18 = 4,\ 3^5 = 5,\ 3^6 = 1$

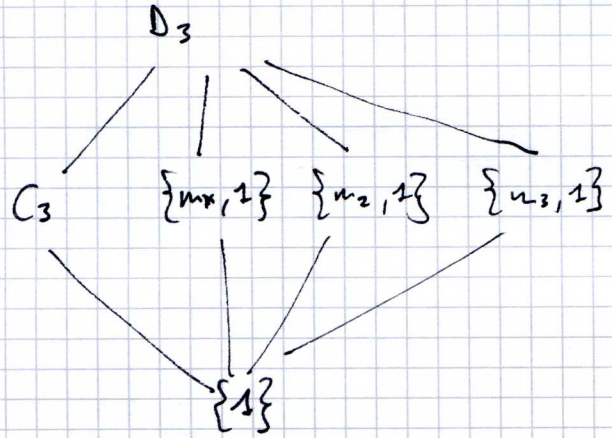
! also $\mathbb{Z}_7^* = \{3, 3^2, 3^3, 3^4, 3^5, 3^6 = 1\}$

Die Gruppen sind isomorph

$\mathbb{Z}_9^*$		$\mathbb{Z}_7^*$
1	↔	1
2	↔	3
$2^2 = 4$	↔	$2 = 3^2$
$2^3 = 8$	↔	$6 = 3^3$
$2^4 = 7$	↔	$4 = 3^4$
$2^5 = 5$	↔	$5 = 3^5$

18/18

(3) a)



total 6 UG.

6/6

b) & c) : gleiche Antworten wegen 2c), die Gruppen sind ja isomorph!

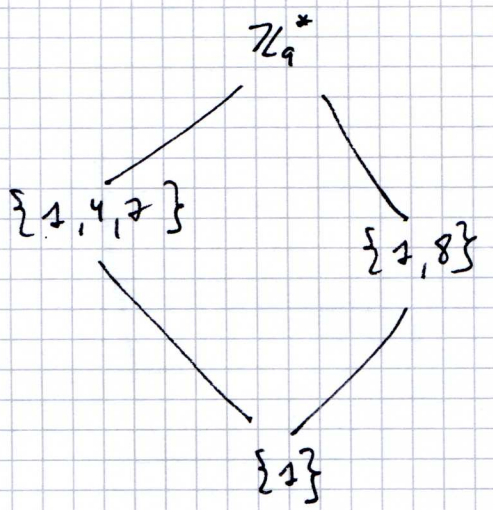
6/6

also in $\mathbb{Z}_9^*$ $\{1, 4, 7\}$ ist ein UG

$\{1, 8\}$ ist ein UG

2 und 5 dürfen nicht dabei sein, da sie mit ihren Vielfachen die ganze Gruppe ergeben.

(18/18)



6/6

$4 \cdot 8 = 32 \equiv 5$

die Vielfachen von 5 ergeben ganz $\mathbb{Z}_9^*$!

$\Rightarrow$ Antwort c) : 4

D: (8/8)!

$\rightarrow$ total 72 P.