technische universität
dortmund

Sicherheit: Fragen und Lösungsansätze

Thomas Ruhroth

Übung 4

- HA2
- HA3
- Start in Prüfungen

HA 1.1

Key				Round 1				Round 2			
f4	5d	51	18	b3	ee	bf	a7	f7	19	a6	01
b4	9e	f4	98	6a	f4	00	98	E5	11	11	89
58	cd	5e	9c	7c	b1	ef	73	38	89	66	15
ea	a8	cf	a6	47	ef	20	86	1b	f4	d4	52

HA1.2(Key: Schlüssel)

Zustandsmatrix 1			
c1	dc	73	73
d2	e8	4f	e6
f7	9b	60	fc
d4	f8	7e	ee

Zustandsmatrix 2			
78	86	8f	8f
b5	9b	84	8e
68	14	d0	b0
48	41	f3	28

Zustandsmatrix 3			
78	86	8f	8f
9b	84	8e	b5
d0	b0	68	14
28	48	41	F3

Zustandsmatrix 4			
be	78	a5	26
16	16	71	31
20	a1	12	1c
93	35	ee	d6

HA 1.6 und 1.7

Zustandsmatrix 5 (Key: Round 1)			
0d	96	1a	81
7c	e2	71	a9
5c	10	fd	6f
d4	da	ce	50

Zustandsmatrix 6 (Key: Round 2)			
20	89	04	0d
7d	b2	c2	99
6c	21	2c	df
48	bc	83	da

Aufgabe 2 - Bemerkungen

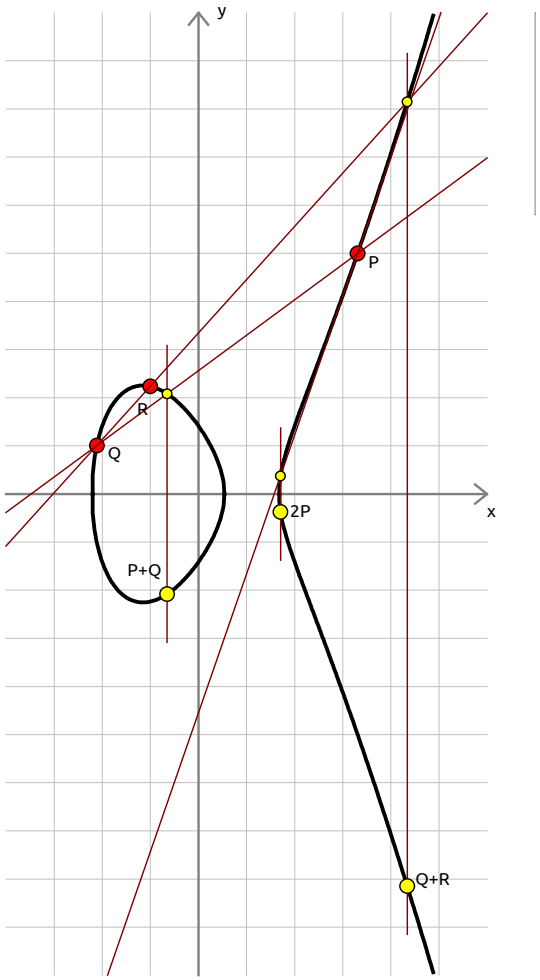
- Fehlerabschätzungen?
- Rechenweg angeben, dann kann man Teilpunkte geben
- 2P wird anders als P+Q bzw Q+R berechnet

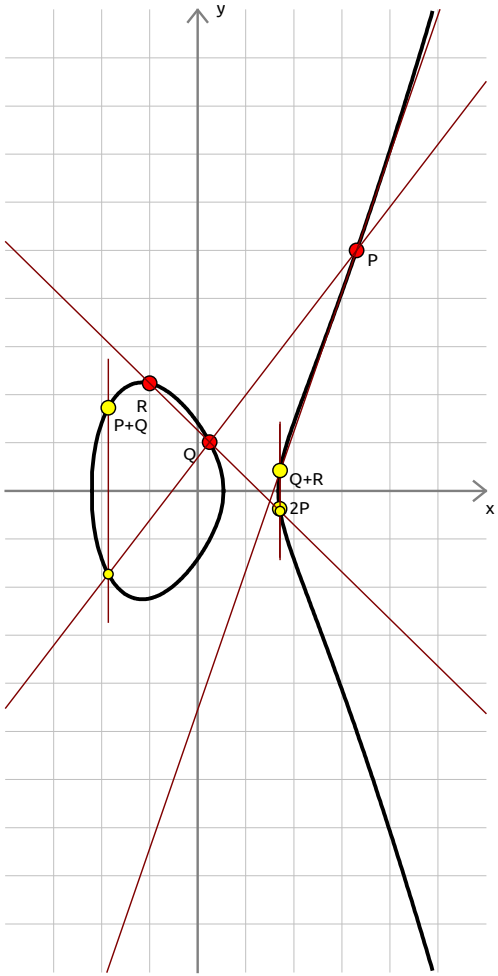
Aufgabe 2

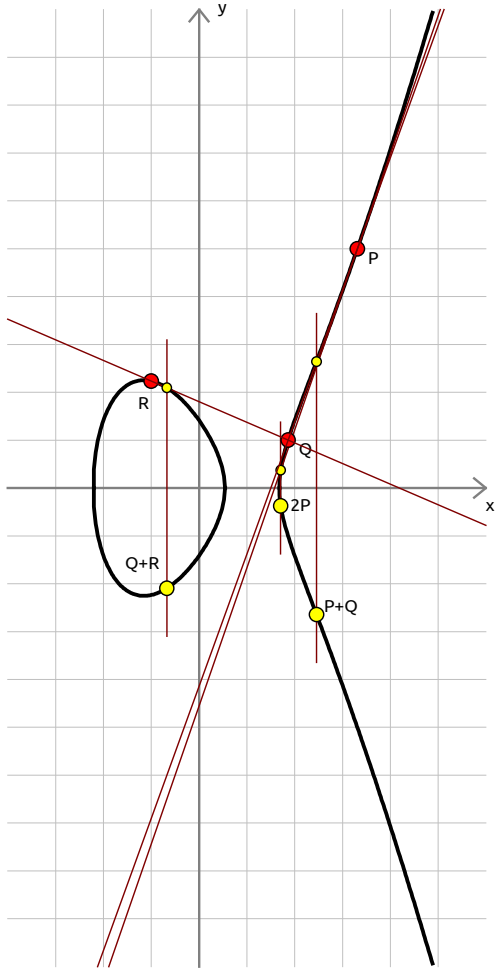
- $y^2 = x^3 - 4x + 2$
- P = (?,5)
  - $5^2 = x^3 - 4x + 2$
  - $23 = x^3 - 4x$
  - x ca 3.31
- Q = (?,1)
  - $1^2 = x^3 - 4x + 2$
  - $-1 = x^3 - 4x$
  - Ca 0.25 oder 1.82 oder -2 (genau)
- R = (-1, ?)
  - $y^2 = -1^3 - 4(-1) + 2$
  - $y^2 = -1 + 4 + 2$
  - $y^2 = 5$
  - ca. 2.23 oder -2.23

Aufgabe 2

- P = (3.31,5) ± 0.02
- Q_1 = (0.25,1) ± 0.01 Q_2 = (1.86,1) ± 0.1 Q_3 = (-2.11,1) ± 0.15
- R_1 = (-1, 2.24) ± 0.01 R_2 = (-1, -2.24) ± 0.01
- -P = (3.31,-5)
- 2P = (1.71,-0.38) $\pm(0.05,0.07)$
- P + Q
  - P + Q_1 = (-1.85,1.75) $\pm(0.05,0.10)$
  - P + Q_2 = (2.46,-2.64) $\pm(0.1,0.1)$
  - P + Q_3 = (-0.65,-2.08) $\pm(0.20,0.05)$
- Q + R
  - Q_1 + R_1 = (1.72,0.43) $\pm(0.05,0.10)$
  - Q_2 + R_1 = (-0.67,-2.1) $\pm(0.1,0.01)$
  - Q_3 + R_1 = (4.34,-8.15) $\pm(0.20,1)$
  - Q_1 + R_2 = (0.42,0.63) $\pm(0.05,0.10)$
  - Q_2 + R_2 = (7.4,-19.45) $\pm(0.1,0.75)$
  - Q_3 + R_2 = (11.54,38,63.15) $\pm(0.20,1.5)$


y
x
P
R
Q
2P
P+Q
Q+R


y
x
P
R
P+Q
Q
Q+R
2P


y
x
P
R
Q
2P
Q+R
P+Q

HA3

RSA Schlüsselpaare: Berechnung

- wähle 2 große Primzahlen p , q
  - *Vorgegeben: $p = 13$, $q = 17$*
- Berechne RSA-Modul $n = pq$
  - *Berechne $n = 13 * 17 = 221$*
- Berechne $\varphi(n) = (p-1)(q-1)$
  - *Berechne $\varphi(n) = 12*16 = 192$*
- Wähle öffentlichen Exponent e $\in$ *{1, 2, …, $\varphi(n)$-1}* so, dass $ggT(\varphi(n), e) = 1$
  - *Vorgegeben: $e = 5$*

1. Berechne privaten Exponenten d, so dass

   $ed \bmod \varphi(n) = 1 \bmod \varphi(n)$, da e so gewählt ist, dass $ggT(\varphi(n), e) = 1$, ist gewährleistet, dass es immer ein Inverses zu e modulo φ(n) gibt, d.h. dass es einen zugehörigen privaten Schlüssel d zu e gibt

   - D = 77

Verschlüsseln:

- $5^5 \bmod 221 = 31$
- Endschlüsseln
- $31^{77} \bmod 221 = 5$
-

Klassen

- RSA und DES
  - Chiper: Fassadenklasse für Ver- bzw- Entschlüsselung
  - ChiperInputStream
  - ChiperOutoutStream
- RSA
  - KeyPairGenerator: Schlüsselpaarerzeugung
  - KeyPar: Schlüsselpar
- DES
  - SecretKeyfactory: Schlüsselerzeugung
  - SecretKey: schlüssel

“algorithm/mode/padding”

- Algorithm
  - Verschlüsselungsmechanismus
    - z.B. RSA, DES
- Mode
  - Angabe des genutzen Blockmodes
    - CBC, CBC8
- Padding
  - Angabe des genutzten Padding-Algorithmus

Programm (interessante Zeilen)

```
KeyPair keyPair;
KeyPairGenerator keyGen = KeyPairGenerator.getInstance("RSA");
keyGen.initialize(512);
keyPair = keyGen.generateKeyPair();
Cipher cipher = Cipher.getInstance("RSA");
byte[] aMessage = "Sicherheit: Fragen und Lösungsansätze".getBytes();
cipher.init(Cipher.ENCRYPT_MODE, keyPair.getPublic());
byte[] ciphertext = cipher.doFinal(aMessage);

cipher.init(Cipher.DECRYPT_MODE, keyPair.getPrivate());
byte[] bMessage= cipher.doFinal(ciphertext);

….
System.out.println("Massage: " + new String(bMessage));
```

Simulation

- 3 Personen
  - Prüfer
  - Protokollant
  - Prüfling

- Prüfer
  - Fragen sind Startfragen!
- Protokollant
  - Beobachtung des Prüflings
  - Beantwortet er die Fragen
    - Richtig
    - Zügig/Spontan
    - Präzise
  - Soll in einer Rückmelderunde Feedback geben können

Rückmelderunde

Runde A

- Was war der Inhalt des Kurses?
  - Hinweis: Bei 2-3 Themen, die nur kurz genannt werden, einhaken und nach Details fragen.
  - Ca. 2-3 Minuten reden lassen
- In welchem Bereich nutzt man das Basic Access Protokoll?
- Was ist das? Wie funktioniert es?
- Was macht eine One-Way-Funktion aus?

Runde B

- Welche Bereiche haben wir in SFL behandelt?
  - Hinweis: Bei 2-3 Themen, die nur kurz genannt werden, einhaken und nach Details fragen.
  - Ca. 2-3 Minuten reden lassen
- Was ist Kollisionsresistenz?
- Wie funktioniert das Kerberos-Protokoll?
- Welche Besonderheiten besitzt es?

Runde C

- Was waren ihre Lieblingsthemen in SFL?
  - Hinweis: Bei 2-3 Themen, die nur kurz genannt werden, einhaken und nach Details fragen.
  - Ca. 2-3 Minuten reden lassen
- Was ist ein Zero-Knowledge-Verfahren?
- Wie funktioniert ein Zero-Knowledge-Verfahren?
- Warum sind Schlüsselvereinbarungsverfahren wichtig?