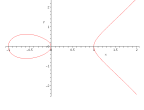
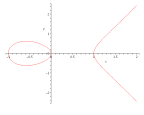
Kryptographie mit elliptischen Kurven

Gabor Wiese

Universität Regensburg



Problemstellung



Problemstellung

Caesar

Problemstellung

Caesar

General

Problemstellung

Caesar

Befehle

General

Problemstellung

Caesar

Befehle

General

Problemstellung

Caesar

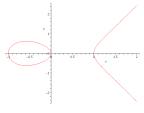
Befehle

Problem!!

General

Problemstellung

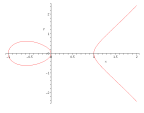
Caesar verschlüsselte seine Nachrichten durch Buchstabensubstitution:



Problemstellung

Caesar verschlüsselte seine Nachrichten durch Buchstabensubstitution:

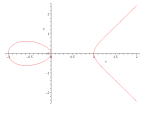
$A \mapsto D$,



Problemstellung

Caesar verschlüsselte seine Nachrichten durch Buchstabensubstitution:

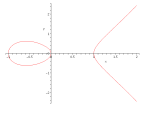
$A \mapsto D$, $B \mapsto E$,



Problemstellung

Caesar verschlüsselte seine Nachrichten durch Buchstabensubstitution:

$$A \mapsto D,\ \ B \mapsto E,\ \ C \mapsto F, \ldots, X \mapsto A, Y \mapsto B, Z \mapsto C.$$



Problemstellung

Caesar verschlüsselte seine Nachrichten durch Buchstabensubstitution:

$$A \mapsto D,\ \ B \mapsto E,\ \ C \mapsto F, \ldots, X \mapsto A,\ Y \mapsto B,\ Z \mapsto C.$$

Kein Problem für Miraculix!

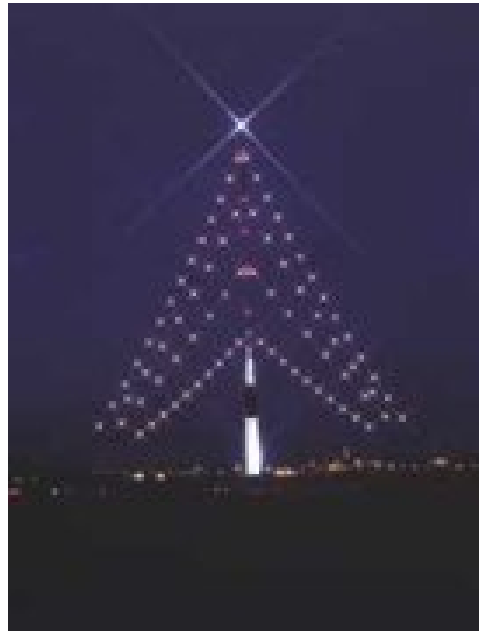
Problemstellung

Handy

Problemstellung

Handy

Sendemast



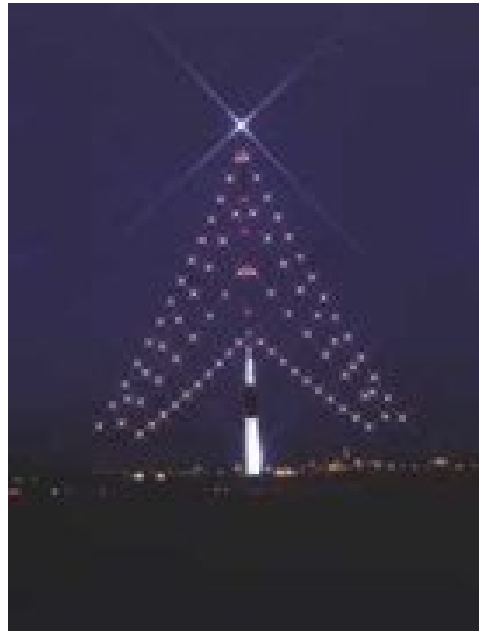
Problemstellung

Handy

Identifikation

Kommunikation

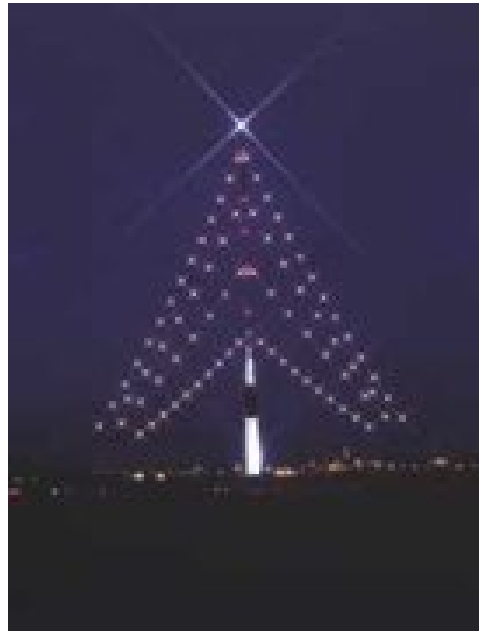
Sendemast



Problemstellung

Handy

Sendemast



Identifikation

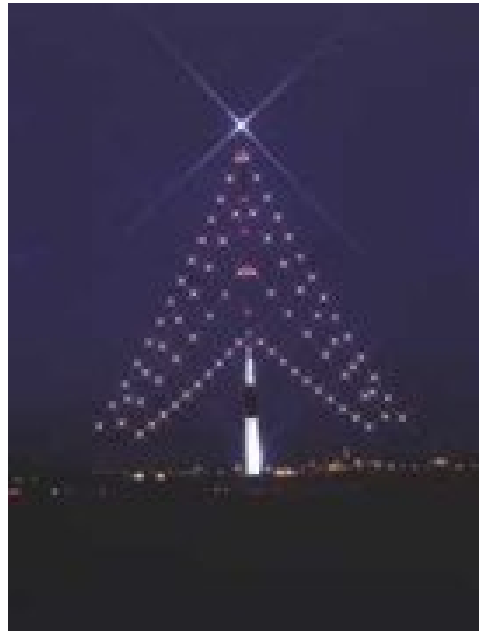
Kommunikation

Niemand soll auf meine Kosten telefonieren!

Problemstellung

Handy

Sendemast



Identifikation

Kommunikation

Niemand soll auf meine Kosten telefonieren!

(Es braucht nicht jeder alles zu wissen.)

Diffie-Hellman-Schlüsselaustausch


und sein

wollen einen gemeinsamen


zum Verschlüsseln und Entschlüsseln ihrer Nachrichten.

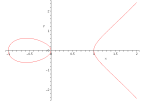
Diffie-Hellman-Schlüsselaustausch


und sein

wollen einen gemeinsamen


zum Verschlüsseln und Entschlüsseln ihrer Nachrichten.

Der Schlüssel soll nicht transportiert werden!



Diffie-Hellman-Schlüsselaustausch

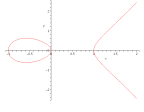

und sein

wollen einen gemeinsamen


zum Verschlüsseln und Entschlüsseln ihrer Nachrichten.

Der Schlüssel soll nicht transportiert werden!

Idee: Benutze asymmetrische Verfahren



Diffie-Hellman-Schlüsselaustausch

 und sein  wollen einen gemeinsamen 

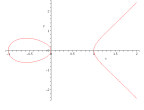
zum Verschlüsseln und Entschlüsseln ihrer Nachrichten.

Der Schlüssel soll nicht transportiert werden!

Idee: Benutze asymmetrische Verfahren

Beispiele:

- RSA
- diskrete Logarithmen (in endlichen Körpern)
- “Elliptische Kurven”

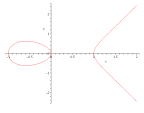


Elliptische Kurven

Eine elliptische Kurve ist eine Punktmenge in der x-y-Ebene der Form

$$y^2 = x^3 - ax - b$$

(ohne Selbstdurchschneidungen u. Ä.)



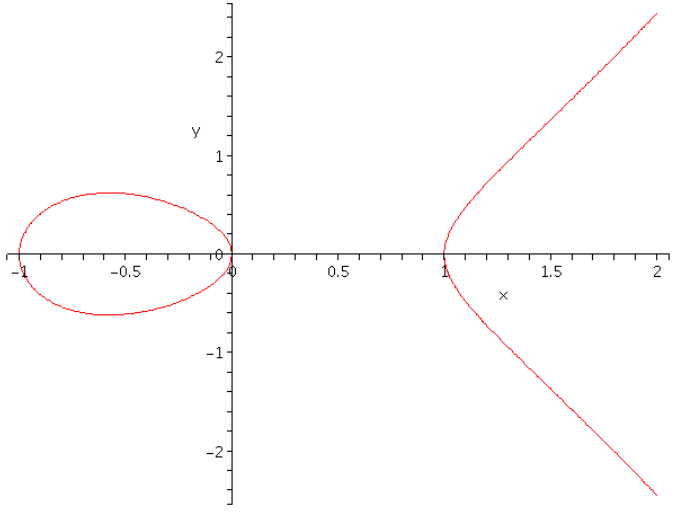
Elliptische Kurven

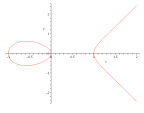
Eine elliptische Kurve ist eine Punktmenge in der x-y-Ebene der Form

$$y^2 = x^3 - ax - b$$

(ohne Selbstdurchschneidungen u. Ä.)

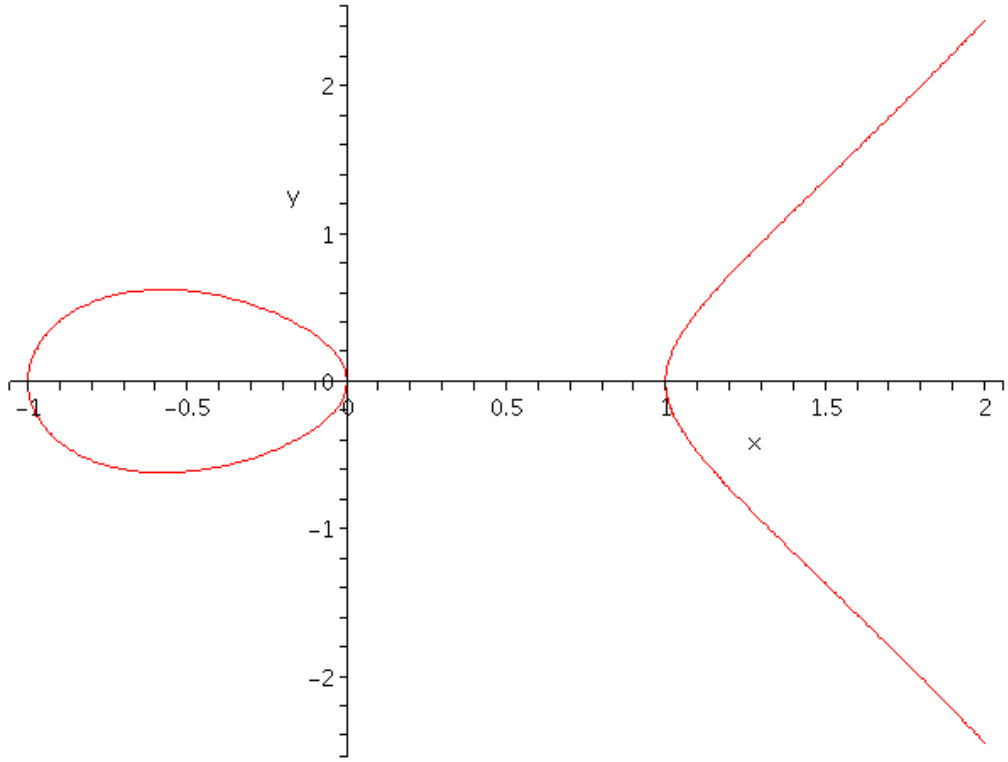
Beispiel: Die (reelle) elliptische Kurve $y^2 = x^3 - x$.

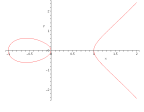




Elliptische Kurven - Addition

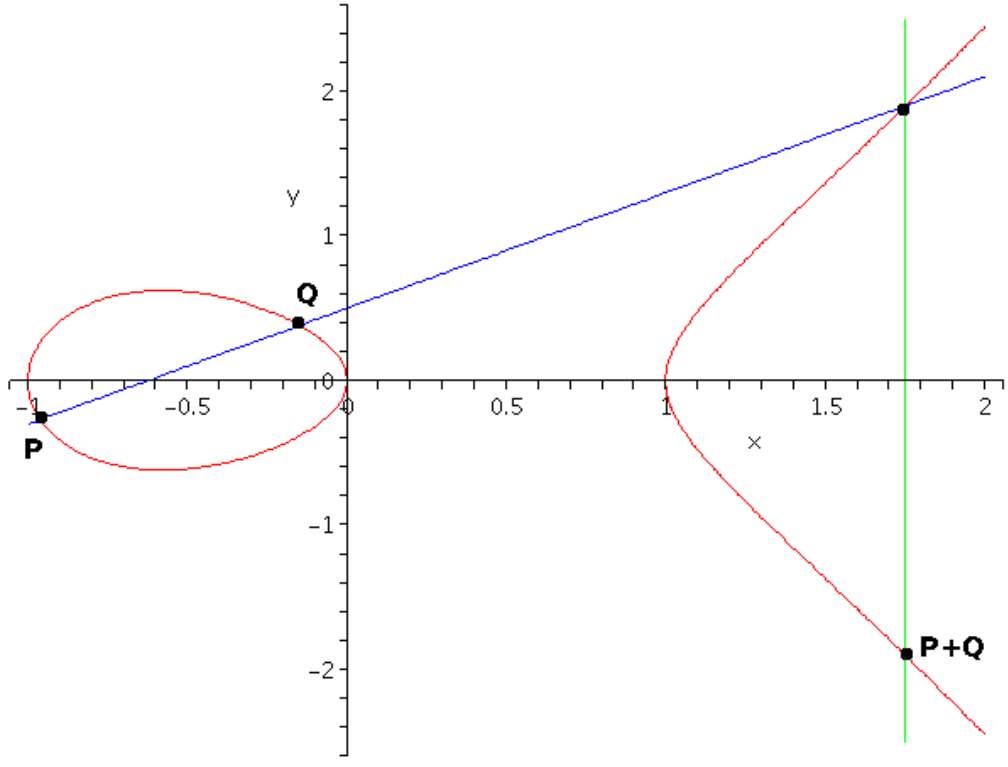
Elliptische Kurven haben etwas Besonderes: eine Addition!





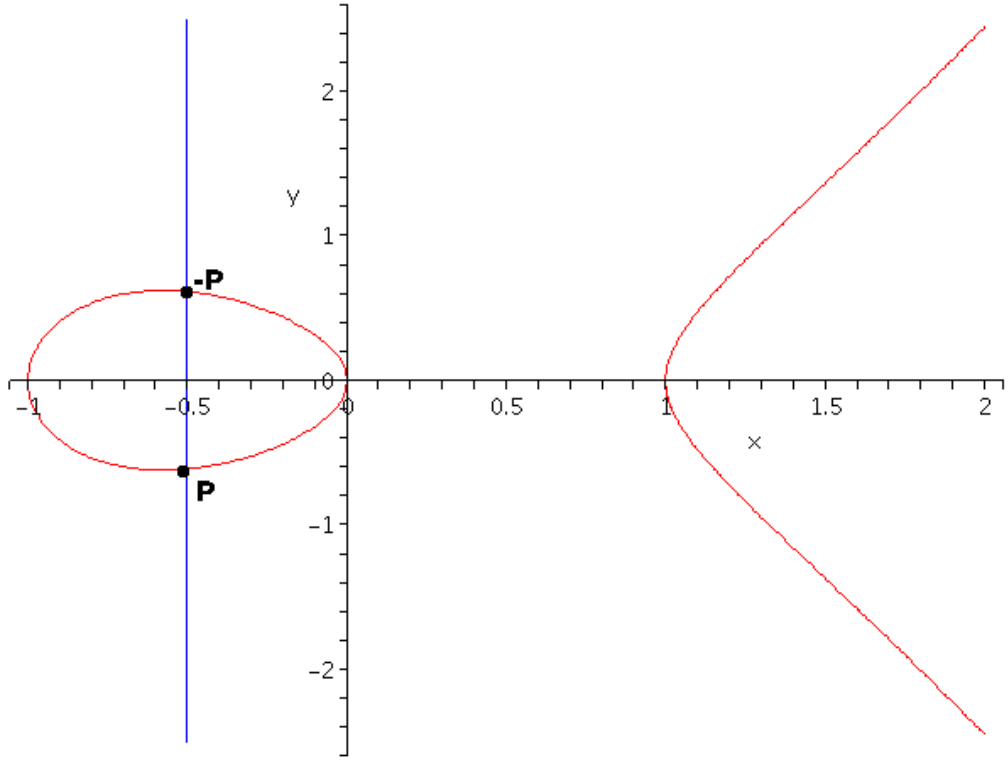
Elliptische Kurven - Addition

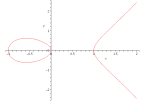
Elliptische Kurven haben etwas Besonderes: eine Addition!



Elliptische Kurven - Addition

Elliptische Kurven haben etwas Besonderes: eine Addition!

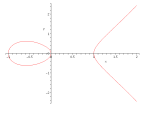




Elliptische Kurven sind Gruppen

Elliptische Kurven sind abelsche Gruppen!

D.h., die Addition ist genauso wie die Addition ganzer Zahlen

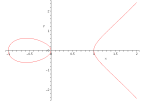


Elliptische Kurven sind Gruppen

Elliptische Kurven sind abelsche Gruppen!

D.h., die Addition ist genauso wie die Addition ganzer Zahlen

- assoziativ: $P + (Q + R) = (P + Q) + R$,
- kommutativ: $P + Q = Q + P$,
- es gibt ein neutrales Element 0, also $P + 0 = P$,
- man kann auch subtrahieren: $P + (-P) = 0$.



Elliptische Kurven sind Gruppen

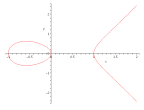
Elliptische Kurven sind abelsche Gruppen!

D.h., die Addition ist genauso wie die Addition ganzer Zahlen

- assoziativ: $P + (Q + R) = (P + Q) + R$,
- kommutativ: $P + Q = Q + P$,
- es gibt ein neutrales Element 0, also $P + 0 = P$,
- man kann auch subtrahieren: $P + (-P) = 0$.

Ist n eine natürliche Zahl, z. B. 213213973562353334595 1, dann schreibt man

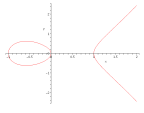
$$n \cdot P = \underbrace{P + P + \cdots + P}_{n-\text{mal}}.$$



Kinderleicht $\leftrightarrow$ Hammerhart

Sei P auf einer elliptischen Kurve vorgegeben.

Es ist kinderleicht, $n \cdot P$ auch für riesige (1000 Stellen) natürliche Zahlen n auszurechnen.

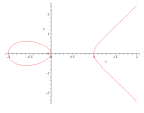


Kinderleicht $\leftrightarrow$ Hammerhart

Sei P auf einer elliptischen Kurve vorgegeben.

Es ist kinderleicht, $n \cdot P$ auch für riesige (1000 Stellen) natürliche Zahlen n auszurechnen.

Es erscheint hammerhart, aus der Kenntnis von P und $n \cdot P$ wieder n auszurechnen.



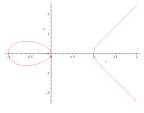
Kinderleicht $\leftrightarrow$ Hammerhart

Sei P auf einer elliptischen Kurve vorgegeben.

Es ist kinderleicht, $n \cdot P$ auch für riesige (1000 Stellen) natürliche Zahlen n auszurechnen.

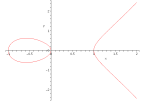
Es erscheint hammerhart, aus der Kenntnis von P und $n \cdot P$ wieder n auszurechnen.

Das ist die Asymmetrie, auf der der Diffie-Hellman-Schlüsselaustausch beruht.



Diffie-Hellman-Schlüsselaustausch

Allen bekannt: elliptische Kurve und ein Punkt P darauf.



Diffie-Hellman-Schlüsselaustausch

Allen bekannt: elliptische Kurve und ein Punkt P darauf.

Diffie-Hellman-Schlüsselaustausch

Allen bekannt: elliptische Kurve und ein Punkt P darauf.

1. Wählt $a \in \mathbb{N}$.

1. Wählt $b \in \mathbb{N}$.

Diffie-Hellman-Schlüsselaustausch

Allen bekannt: elliptische Kurve und ein Punkt P darauf.

1. Wählt $a \in \mathbb{N}$.
2. Berechnet $a \cdot P$.

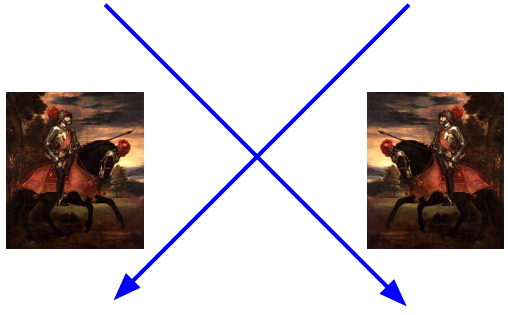
1. Wählt $b \in \mathbb{N}$.
2. Berechnet $b \cdot P$.

Diffie-Hellman-Schlüsselaustausch

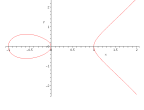
Allen bekannt: elliptische Kurve und ein Punkt P darauf.



1. Wählt $a \in \mathbb{N}$.
2. Berechnet $a \cdot P$.
3. Verschickt $a \cdot P$.
4. Empfängt $b \cdot P$.



1. Wählt $b \in \mathbb{N}$.
2. Berechnet $b \cdot P$.
3. Verschickt $b \cdot P$.
4. Empfängt $a \cdot P$.



Diffie-Hellman-Schlüsselaustausch

Allen bekannt: elliptische Kurve und ein Punkt P darauf.

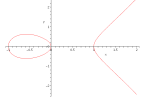


1. Wählt $a \in \mathbb{N}$.
2. Berechnet $a \cdot P$.
3. Verschickt $a \cdot P$.


4. Empfängt $b \cdot P$.
5. Berechnet $a \cdot (b \cdot P)$.

1. Wählt $b \in \mathbb{N}$.
2. Berechnet $b \cdot P$.
3. Verschickt $b \cdot P$.

4. Empfängt $a \cdot P$.
5. Berechnet $b \cdot (a \cdot P)$.



Diffie-Hellman-Schlüsselaustausch

Allen bekannt: elliptische Kurve und ein Punkt P darauf.

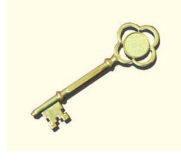


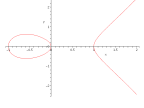
1. Wählt $a \in \mathbb{N}$.
2. Berechnet $a \cdot P$.
3. Verschickt $a \cdot P$.


4. Empfängt $b \cdot P$.
5. Berechnet $a \cdot (b \cdot P)$.

1. Wählt $b \in \mathbb{N}$.
2. Berechnet $b \cdot P$.
3. Verschickt $b \cdot P$.

4. Empfängt $a \cdot P$.
5. Berechnet $b \cdot (a \cdot P)$.

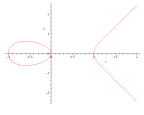
Gemeinsames Geheimnis:  $= (a \cdot b) \cdot P$.



Diffie-Hellman-Schlüsselaustausch

Transportiert werden $a \cdot P$ und $b \cdot P$.

Der Schlüssel $(a \cdot b) \cdot P$ wird nicht transportiert!



Diffie-Hellman-Schlüsselaustausch

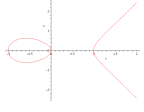
Transportiert werden $a \cdot P$ und $b \cdot P$.

Der Schlüssel $(a \cdot b) \cdot P$ wird nicht transportiert!

Das Berechnen von a, b bzw. $(a \cdot b) \cdot P$ aus $a \cdot P$ und $b \cdot P$ ist hammerhart (= praktisch unmöglich)!

Technische Details

- Man nimmt elliptische Kurven über einem endlichen Körper $\mathbb{F}_p$.
- Die Primzahl p sollte zumindest 100 Stellen haben.
- Nicht jede Kurve ist “sicher”.



Da hilft nur noch eins...