§0: Motivation

Stichworte:

Verschlüsselungsprobleme

A/Symmetrische Verschlüsselung von Nachrichten

Anwendungen: per Internet einkaufen, Online-Banking, persönliche Daten geheimhalten... → Kommunikation über öff. Kanäle

Lösung folgender Probleme erforderlich:

- Schlüsselaustausch über öffentliche Kanäle
- Verschlüsselung ohne vorherigen Schlüsselaustausch
- Digitale Signaturen

Lösung mit elementarer Zahlentheorie, insb. RSA-Verfahren

⇝ heute: Verfahren mit elliptischen Kurven praktisch

Elliptische Kurven

▷ typische Beispiele

▷ Gruppenoperation auf elliptischen Kurven kryptographisch interessant

▷ Die Sicherheit der ECC ("elliptic curve cryptography") beruht auf dem Problem des diskreten Logarithmus auf ellipt. Kurven

---

Kryptologie

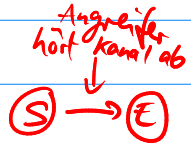
Die Kryptologie besteht aus den folgenden beiden Gebieten:

Kryptographie: Studium mathematischer Techniken zur Verschlüsselung von Informationen oder geheimen Nachrichten und dem Schutz von Daten.

Kryptoloanalyse: Beschreibung der Rückgewinnung von Informationen aus verschlüsselten Texten, der Entschlüsselung.

Oft meint man mit "Kryptographie" die Kryptologie.

Früher wurde die Kryptographie vor allem im militärischen oder diplomatischen Sektor verwendet, heutzutage steht in unserer vernetzten Welt vor allem auch der praktische Nutzen im Alltag im Vordergrund: im Internet einkaufen, online-Banking, persönliche Daten geheimhalten bzw. Datenschutz, Nachrichten und Dokumente digital unterschreiben etc.
Das Internet liefert schnelle Informationswege über öffentliche Kanäle, die leicht abgehört werden können, so dass die Verschlüsselung schützenswerter Daten unumgänglich wird. Auch die Möglichkeit zur Signierung wird nötig, weil sehr leicht Absenderangaben gefälscht werden können.
Eventuell nicht abhörsichere Kanäle können außer dem Internet aber auch Briefe, Radio, Boten, etc. sein.



Bei der symmetrischen Verschlüsselung von Daten gibt es einen Sender S und einen Empfänger E, die sich beide auf einen gemeinsamen Schlüssel geeinigt haben, der zum Ver- und Entschlüsseln dient. Beim Caesar-Code z.B. ist dies die Vereinbarung, jeden Buchstaben durch den 3. nachfolgenden im Alphabet zu ersetzen, also $A \mapsto D$, $B \mapsto E$, $C \mapsto F$, $D \mapsto G$, usw., die Entschlüsselung ist klar. Derartige monoalphabetische Chiffrierungen, bei der jeder Buchstabe des Alphabets stets durch denselben Geheimtextbuchstaben chiffriert wird, sind durch Häufigkeitsanalysen durch einen Angreifer, der die verschlüsselten Nachrichten abhört, sehr leicht zu entschlüsseln (übrigens gibt es auch heutzutage pdf-Verschlüsselungsprogramme, die so arbeiten!).

In dieser Vorlesung behandeln wir die heutzutage gängigen modernen Methoden, die als sicher gelten. Worauf diese starke Sicherheit beruht, hat mathematische Gründe, die wir besprechen möchten. Vor allem interessiert uns, wie und welche Mathematik in die Kryptologie kommt, so dass wir deren Verfahren verstehen können.

Die Anwendungen erfordern die Lösung folgender Probleme bei symmetrischen Verschlüsselungsverfahren:

- Schlüsselaustausch über öffentliche Kanäle ("öffentliche Schlüssel")
- Verschlüsselung ohne vorherigen Schlüsselaustausch (mit "geheimen Schlüsseln", die nicht versendet werden)
- digitale Signierung / Authentifizierung

Dies können asymmetrische Verfahren leisten (auch "Public-Key-Kryptographie" genannt) und gehen zurück auf Ideen von Diffie und Hellman aus den 70er Jahren:
Jeder Nutzer eines Kommunikationskanals hat einen privaten Schlüssel, den er geheim hält und niemand sonst kennt, sowie einen öffentlichen Schlüssel, den jeder einsehen kann. Eine Nachricht wird dann unter Ansatzen einer Funktion $x \mapsto f(x)$ verschlüsselt, die zwar leicht zu berechnen, aber praktisch nur mit Kenntnis des privaten Schlüssels des rechtmäßigen Empfängers entschlüsselt werden kann. Der Sender der Nachricht wird dafür den öffentlichen Schlüssel des Empfängers zur Verschlüsselung benutzen.
Eine derartige Funktion heißt Einwegfunktion.

- Beim RSA-Verfahren, das wir kennen lernen werden, ist diese Fkt. die Multiplikation zweier Primzahlen $(p,q) \mapsto p \cdot q$.
- Beim ECC-Verfahren ist dies die Fkt. $x \mapsto m \cdot x$ in einer abelschen Gruppe, nämlich die Gruppe auf einer elliptischen Kurve.

In einem ersten Teil der Vorlesung stellen wir gängige Verfahren dar, die leicht mit dem Zahlring $\mathbb{Z}$ und Strukturen darin realisiert werden können, dabei werden wir nur einige Hilfsmittel der elementaren Zahlentheorie entwickeln und dafür heranziehen. In einem zweiten Teil studieren wir die Eigenschaften elliptischer Kurven als interessante geometrische

und arithmetische Objekte, die sich in der Praxis der Kryptographie als nützlich erwiesen haben. Wir besprechen dann auch die Sicherheit und Implementierung dieser Verfahren und vergleichen sie miteinander.

Elliptische Kurven

Was sind elliptische Kurven? Jedenfalls sind elliptische Kurven keine Ellipsen. Ellipsen lassen sich durch Gleichungen der Form

$$\left(\frac{x}{a}\right)^2 + \left(\frac{y}{b}\right)^2 = 1 \quad \text{mit } a,b \in \mathbb{R}\setminus\{0\}$$ beschreiben.

Durch die Parametrisierung $x(t) = a\cos t$, $y(t) = b\sin t$ ergibt sich für die Bogenlänge der Ellipse ein elliptisches Integral (zweiter Art), nämlich

$$\int_0^{2\pi} \sqrt{\left(\frac{dx(t)}{dt}\right)^2 + \left(\frac{dy(t)}{dt}\right)^2}\, dt = 4\int_0^{2\pi} \sqrt{a^2\cos^2 t + b^2 \sin^2 t}\, dt.$$

I.a. lässt sich dies nicht elementar integrieren (außer natürlich falls $a=b$, d.h. ein Kreis vorliegt). Mit Hilfe von elliptischen Kurven findet man jedoch nicht-elementare Stammfunktionen für diese Integrale (↝ s. Funktionentheorie). Aufgrund dieses Zusammenhangs haben elliptische Kurven ihren Namen, sie haben ansonsten nichts mit Ellipsen zu tun.

Was sind nun elliptische Kurven? Es sind "abelsche Varietäten der Dim. 1". Elliptische Kurven sind spezielle algebraische Kurven über einem Körper k. Es handelt sich dabei um glatte kubische Kurven, deren definierende algebraische Gleichung sich meist in die Form

$$E:\ y^2 = x^3 + ax + b, \qquad a,b \in k,$$ bringen lässt.

Als Punktemenge haben wir dafür

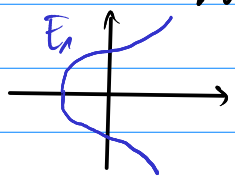
$$E(k) := \{(x,y) \in k^2 :\ y^2 = x^3 + ax + b\} \cup \{O\},$$

die Kurve hängt nur von a, b ab.

Die Rolle des zusätzlichen sog. "unendlich fernen Punkts" O werden wir dabei noch näher beleuchten.

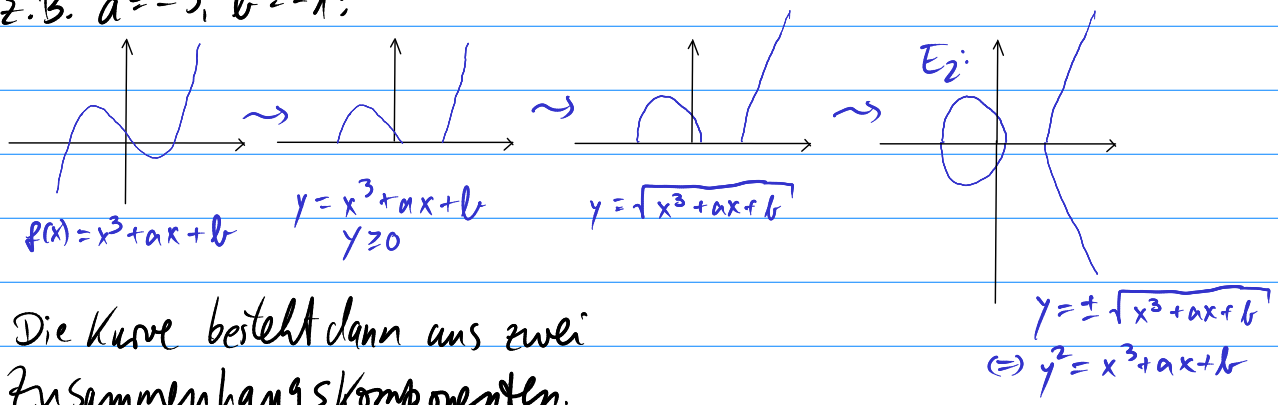
Zwei typische Beispiele für elliptische Kurven:

1.) $E_1: y^2 = x^3 + 17$, hier liegen sogar Punkte mit ganzzahligen Koordinaten auf E_1, nämlich $(-2,3)$, $(-1,4)$, $(2,5)$



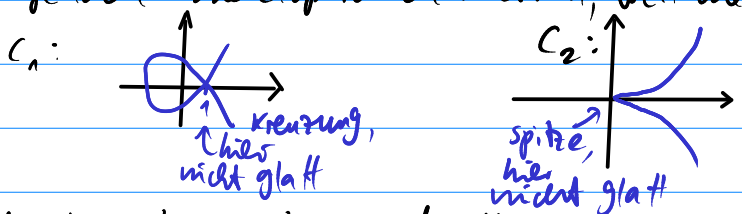
Die Kurve besteht hier aus einer Zusammenhangskomponente.

2.) $E_2: y^2 = x^3 + ax + b$, wenn $f(x) = x^3 + ax + b$ drei verschiedene Nst. hat, z.B. $a = -3$, $b = -1$:



Die Kurve besteht dann aus zwei Zusammenhangskomponenten.

Bem: Die kubischen Kurven $C_1: y^2 = x^3 - 3x + 2$ und $C_2: y^2 = x^3$ z.B. sind jedoch keine elliptischen Kurven, weil diese nicht glatt sind:



Für die Kryptographie sind ellipt. Kurven interessant, weil sich eine Verknüpfung auf ihrer Punktemenge definieren lässt, mit der diese zu einer Gruppe wird. Dabei gerade auch endliche Körper zuzulassen, macht diese Verknüpfung auf Rechenmaschinen realisierbar. Die Sicherheit der darauf beruhenden "ECC" (elliptic curve cryptography) beruht darauf, dass das Problem des diskreten Logarithmus auf einer elliptischen Kurve E, nämlich die Umkehrung der Abb. $P \mapsto m \cdot P$ für $m \in \mathbb{N}$ fest, nach heutigem Wissensstand rechnerisch i.a. extrem schwer realisierbar ist. (Bem.: $m \cdot P := \underbrace{P + \ldots + P}_{m\text{-mal}}$, wobei "+" die Gruppenverknüpfung auf der elliptischen Kurve bezeichnet.)