WiSe'21/'22, hhu
K. Halupczok

Vorlesung Einführung in die Zahlentheorie

EZ 12: Algorithmische Zahlentheorie

Stichworte: Faktorisierungsproblem, RSA, Münzwurf am Telefon, DL-Problem, Diffie-Hellman, DH-Problem, ElGamal, Primzahltestproblem, Carmichaelzahl, Korselt-Kriterium, Miller-Rabin-Test

---

12.1. Einleitung: Wir beschreiben Anwendungen der Zahlentheorie in der Kryptographie/Algorithmik. Bestimmte Anwendungen nutzen die Schwierigkeit bestimmter zahlentheoretischer Probleme aus, insbesondere das

12.2. Faktorisierungsproblem: Sei N eine beliebige, große zusammengesetzte nat. Zahl. Man zerlege N in die Primfaktoren, d.h. gib die PFZ an.

Dafür genügt es, ein Verfahren zur Auffindung eines nichttrivialen Teilers t von N anzugeben ($1 \neq t \neq N$); dieses wird wiederholt auf $\frac{N}{t}, \frac{N}{t,t_1}, \ldots, \frac{N}{t,t_1,t_2,\ldots}$ angewendet bis alle Primfaktoren ermittelt sind. (Eine nat. Zahl hat wenig genug Primfaktoren...)

Dieses Problem 12.2 ist bis heute ein rechnerisch sehr aufwändiges Problem. Man sollte vorher bereits sichergestellt haben, dass N nicht prim = zusgesetzt ist:

12.3. Primzahltestproblem: Sei N eine beliebige, große nat. Zahl. Entscheide, ob N eine Primzahl oder zusammengesetzt ist.

Wir gehen im Moment davon aus, dass das PZtestproblem leicht zu lösen ist (was es in der Praxis ist, dazu später ab 12.23).

Heute ist für das Faktorisierungsproblem nach wie vor das Zahlkörpersieb (um 1990) am schnellsten mit einer subexponentiellen Laufzeit von $\exp\left(O\left(\sqrt[3]{(\log N)\cdot(\log\log N)^2}\right)\right)$, beachte: subexponentiell $\hat{=} o(N^\varepsilon) = o(e^{\varepsilon \log N})$ für jedes $\varepsilon > 0$, hier ist $O(\log N)$ die Inputgröße, d.h. die Anzahl Stellen/Ziffern von N).

Mittlerweile sind auch "schnelle" (d.h. subexponentielle) Faktorisierungsalgorithmen mit elliptischen Kurven bekannt. Auf einem Quantencomputer hingegen kann das Problem mit dem Shor-Algorithmus (≈1997) polynomiell schnell gelöst werden.

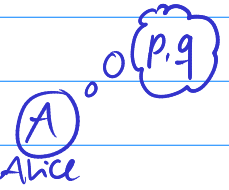
Public-Key-Kryptographie und das RSA-Verfahren

12.4. Die Public-Key-Kryptographie bezeichnet man auch als asymmetrische Kryptographie. Bei diesem Kommunikationsverfahren hat jeder Nutzer einen öffentlichen Schlüssel, den jeder einsehen kann, und einen privaten Schlüssel, den jeder Nutzer geheim hält: Jeder kann verschlüsseln, aber nur der rechtmäßige Empfänger entschlüsseln. Möchte Nutzer (B) eine Nachricht an Nutzer (A) sendet, benutzt er zur Verschlüsselung den öffentlichen Schlüssel von (A), die Entschlüsselung gelingt aber nur (A) mit dem privaten Schlüssel.
Kerckhoffs Prinzip: Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen, sondern von der Geheimhaltung der geheimen Schlüssel.

12.5. Das RSA-Verfahren ist benannt nach einer Arbeit von R.L. Rivest, A. Shamir und L.M. Adleman aus dem Jahr 1978. Seine Sicherheit beruht auf der Schwierigkeit des Faktorisierungsproblems und wird bis heute zur sicheren Kommunikation benutzt.
Die Methode verlangt auch die Möglichkeit, große Primzahlen zu erzeugen, die möglichst zufällig gewählt sein sollen, $N = p \cdot q$ muss so groß sein, dass alle bekannten Faktorisierungsverfahren zu langsam wären.

12.6. RSA: Nutzer (A)lice und (B)ob kommunizieren über einen unsicheren Kanal.

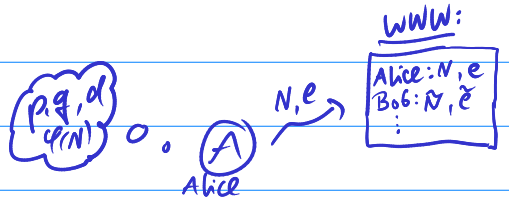
Schritt (1.) (Vorbereitung)



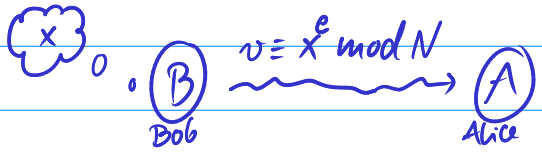
Jeder Nutzer, z.B. (A), wählt zwei große Primzahlen $p \neq q$, etwa gleichgroß mit ähnlicher Stellenanzahl, und berechnet $N = pq$ sowie $\varphi(N) = (p-1)(q-1)$.

Dann wählt (A) eine Zahl e mit $1 < e < \varphi(N)$ und berechnet $1 < d < \varphi(N)$ als Inverses von e mod $\varphi(N)$, d.h. $de \equiv 1 \bmod \varphi(N)$, unter Zuhilfenahme des euklidischen Algorithmus.

(A) hält p, q, φ(N), d geheim und gibt N, e bekannt, z.B. durch Hinterlegung auf einen öffentlichen Schlüsselserver, wo jeder nachsehen kann.



Schritt (2.)



Bob (B) möchte Alice (A) seinen Geheimtext (als eine Zahl x mod N kodiert) schicken. Er besorgt sich die Daten N, e vom Server und verschlüsselt x zu x^e mod N

Dann schickt er ihr das Ergebnis $v \equiv x^e (N)$ zwischen 1 und N.

Schritt (3.)

Alice (A) entschlüsselt den geheimen Text v durch Berechnen von v^d mod N, sie erhält x, weil für ein $k \in \mathbb{Z}$ gilt: $ed = 1 + k \cdot \varphi(N)$, also folgt

$$v^d \equiv (x^e)^d \equiv x^{1 + k \cdot \varphi(N)} \equiv x \cdot \underbrace{\left(x^{\varphi(N)}\right)^k}_{\equiv 1 \,(N) \text{ nach Euler-Fermat, falls } ggT(x,N)=1} \equiv x \quad (N).$$

12.7. Bem.: Die nötigen Berechnungen sind: schnelles modulares Potenzieren mod N, d.h. Berechnungen in der multiplikativen Gruppe $(\mathbb{Z}_N^*, \cdot)$, Berechnen von d mit dem euklidischen Algorithmus, Erzeugen großer Pzen p, q.

12.8. Bem.: Ein Unbefugter, der die Daten N, e, v dieser Kommunikation abfängt, ist nicht in der Lage, x ohne der Kenntnis von d, p, q, φ(N) zu berechnen. Dazu müsste man N faktorisieren.

12.9. **Bem.:** Wie sicher das Verfahren ist, hängt davon ab, wie groß die verwendeten Schlüssel sind. Aktuell ist eine Verschlüsselung, bei der p,q eine Bitlänge von mindestens 512 haben sollten, besonders sicher: 2048 Bit. Empfehlung der Bundesnetzagentur bis Ende 2020: mind. 1976 Bit. Gegen einen Angriff mit dem Quantencomputer hätte man allerdings keine Chance.

12.10. **Bem.:** Auch in den seltenen Fällen $p|x$ oder $q|x$, d.h. $ggT(x,N)>1$, arbeitet das Verfahren korrekt: Ist $(x,pq)>1$, gilt $x=p$ oder $x=q$, O.E. $x=p$.
Dann ist $v^d \equiv x^{ed} = p^{1+k\cdot e(N)} = p\cdot\underbrace{(p^{q-1})^{k(p-1)}}_{\equiv 1\,(q)} = p\cdot(1+lq) \equiv p = x \quad (pq)$, $\underbrace{\quad}_{=N}$ $\equiv 1\,(q)$

12.11. **Bem.:** Das Verfahren kann auch ohne Schlüsselserver benutzt werden. (B) kann (A) erst mitteilen, dass es ihr eine Nachricht schicken will. Dann erst erledigt (A) Schritt (1.) und teilt ihm die Daten N, e mit. Dann wie oben.

Als Vorbereitung für die Anwendung 12.14 wiederholen wir kurz das modulare Wurzelziehen modulo $N=p\cdot q$:

12.12. **Lösung von** $x^2 \equiv a\ (N)$ falls $N=p\cdot q$ und $p\equiv q\equiv 3\ (4)$ prim, $p\neq q$:
Sei $p=4k+3$, $q=4l+3$ mit $k,l\in\mathbb{N}_0$, und sei $k\neq l$.
Sei a ein qu.Rest mod N, d.h. es ex. Lösungen.
Nach dem CRS gilt: $x^2\equiv a\ (N) \iff x^2\equiv a\ (p)$ und $x^2\equiv a\ (q)$, und die jeweiligen Lösungen $\pm a^{k+1}$ mod p und $\pm a^{l+1}$ mod q kann man zusammensetzen zu (maximal) vier Lösungen mod N. Es sind genau 4 Lösungen, die explizit wie folgt bestimmt werden können:
Sind $r,s\in\mathbb{Z}$ geg. mit $rp+sq=1$, d.h. die Bézout-Elemente von p und q, und ist $\pm b$ Lsg. von $x^2\equiv a\ (p)$ [2 Mögl.], $\pm c$ Lsg. von $x^2\equiv a\ (q)$ [2 Mögl.], so liefert die CRS-Formel (Inv. von q mod p, Inv. von p mod q)

$$x = \pm b\,s\,q \pm c\,r\,p$$

genau vier Lösungen von $x^2\equiv a\ (p\cdot q)$. Diese müssen paarweise inkongruent mod pq sein, da wir laut CRS den Ringiso $\mathbb{Z}/pq \cong \mathbb{Z}/p \times \mathbb{Z}/q$ haben und die 4 versch. Lösungspaare (b,c), $(-b,c)$, $(b,-c)$, $(-b,-c)$ deswegen genau 4 Restklassen in $\mathbb{Z}/pq$ entsprechen.

12.13. **Bsp.:** Betr. $p=11$, $q=19$, d.h. $k=2$, $\ell=4$. Wähle $a=47$.

Die Lösungen von $x^2 \equiv 47 \equiv 3 \ (11)$ sind $\pm 3^3 \ (11) \equiv \pm 5 \ (11)$,

die Lösungen von $x^2 \equiv 47 \equiv 9 \ (19)$ sind $\pm 3 \ (19)$.

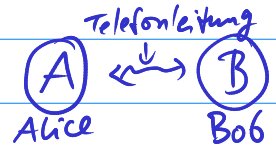
Bézout-El. bestimmen (hier Probieren): Inv. von $19 \equiv 8 \bmod 11$ ist 7, Inv. von $11 \bmod 19$ ist 7.

$\rightsquigarrow$ $s = r = 7$ und $x \equiv \mp 5 \cdot 7 \cdot 19 \mp 3 \cdot 7 \cdot 11 \ (11 \cdot 19)$

ergibt $x \in \{\pm 16, \pm 60\}$. Probe: $16^2 \equiv 47 \ (11 \cdot 19)$ ✓, $60^2 \equiv 47 \ (11 \cdot 19)$ ✓

- Man beachte, dass wir hier benötigen, dass a ein quadratischer Rest mod 11 und mod 19 sein muss. Würde man a zufällig wählen, wäre das nicht unbedingt der Fall; dann ist $x^2 \equiv a \ (N)$ ohnehin unlösbar, falls a kein quadratischer Rest mod $11 \cdot 19$ ist.

12.14. **Problem des fairen Münzwurfknobelns am Telefon:**



Zwei Spieler, Alice (A) und Bob (B) möchten etwas ausknobeln (z.B. wer beim Fernschach beginnen soll und dann einen Vorteil hat, etc.), allerdings sprechen sie sich am Telefon oder mailen sich, und können sich daher nicht sehen. (A) wirft eine Münze, und (B) denkt vorher "Kopf" oder "Zahl", verrät das aber nicht. (*) (A) teilt (B) das Ergebnis mit, und (B) verkündet, wer gewonnen hat: (A), wenn ihr Münzwurfergebnis mit der Wahl von (B) übereinstimmt, ansonsten gewinnt (B).

Sei (B)s geheime Wahl "Zahl".

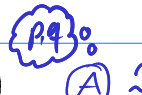
Teilt (A) mit, dass sie "Zahl" geworfen hat, akzeptieren (A) und (B) den Spielausgang, weil dann (A) gewinnt und (B) ihr dies verkündet. Falls (A) jedoch mitteilt, dass sie "Kopf" geworfen hat, teilt (B) mit, dass (A) verloren habe, was (A) natürlich nicht akzeptieren würde.

$\rightsquigarrow$ **Problem:** Wie kann bei Ergebnis "Kopf" Spieler (B) ihre Mitspielerin (A) überzeugen, dass er vor dem Münzwurf die Wahl "Zahl" getroffen hat?

Unsere Antwort: Wenn (B) dann eine Zahl $n = pq$ faktorisieren könnte, deren Primteiler p, q ansonsten nur (A) kennt!

(*): (Wäre (B) live dabei, würde er "Kopf" oder "Zahl" sagen und das Ergebnis sehen. Am Telefon gilt: Würde (A) seine Wahl vorher kennen, so würde (B) ihr mitgeteiltes Münzwurfergebnis u.U. anzweifeln.)

12.15. Das Verfahren funktioniert wie folgt:



Schritt (1.) (A) wählt Primzahlen $p,q \equiv 3 \ (4)$, $p \neq q$, berechnet $n = p \cdot q$ und schickt n an (B) (der Einfachheit halber für (A))

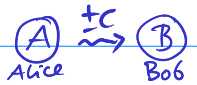
Schritt (2.) (B) wählt $1 \leq b \leq n-1$ zufällig und behält b geheim, er berechnet $a \equiv b^2 \ (n)$, und schickt a an (A)

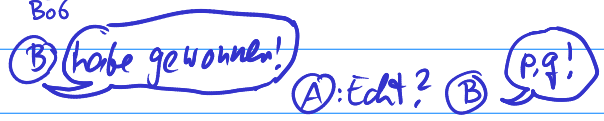
Schritt (3.) (A) berechnet die 4 Lösungen von $x^2 \equiv a \ (n)$ mit der Berechnungsmethode aus 12.12, die 4 Lösungen seien $\pm b, \pm c \in \mathbb{Z}$, (mit b von (B)), die Lösungen $\pm c$ sind andere, die (B) nicht kennt.

Soweit die Vorbereitung; dann der eigentliche Münzwurf:

Schritt (4.) (A) wählt eine der 4 Lösungen zufällig aus (etwa durch Münzwurf!), d.h. entweder $\pm b$ oder $\pm c$, und schickt (B) das Ergebnis. (A) kann nicht wissen, dass (B) die Zahl b gewählt hat. Die Vereinbarung ist nun: Schickt (A) eine der Zahlen $\pm b$, gewinnt (A), schickt (A) eine der Zahlen $\pm c$, gewinnt (B), und das verkündet (B).

ODER





Schritt (5.) Es erfolgt die Verifikation, dass (A) wirklich verloren hat im 2. Fall, dann muss sich (A) davon überzeugen, dass (B) vorher wirklich $\pm b$ gewählt hat: Es kann (A) die Lösungen $\pm b$ einfach mitteilen, falls (A) auch diese berechnet hat. Ev. hat (A) aber nur $\pm c$ berechnet und diese verschickt (der Einfachheit halber). Auch dann kann (A) von (B) überzeugt werden, nämlich durch Prüfen, dass $\pm b$ Lösungen sind. Wenn (A) das nicht prüfen/rechnen möchte, kann (B) anderweitig zur Überzeugung von (A) die von ihr gewählten Primfaktoren von n nennen! Nämlich so:

(B) berechnet $b+c \bmod n$ und

$d = ggT(b+c, n)$ mit dem euklidischen Algo.

Dann ist $d = p$ oder $d = q$. [Denn aus $b^2 \equiv a \equiv c^2 \ (pq)$ folgt:
$pq \mid (b-c)(b+c) = b^2 - c^2$, und da $b \not\equiv \pm c \ (p)$, $b \not\equiv \pm c \ (q)$ folgt $q \mid b+c$ oder $p \mid b+c$,
und $d \neq n$, weil sonst $b \equiv -c \bmod n$ wäre ↯.]

Also kann (B), weil es c kennt, die von (A) gewählten Primfaktoren bestimmen und (A) mitteilen und auf diese Art (A) überzeugen.

Das konnte (B) nur, weil er vorher auch wirklich die nicht von (A) genannte Lösung $\pm b$ hatte. Damit ist das Spiel fair.

Neben dem Faktorisierungsproblem gibt es vor allem ein weiteres, schwer zu lösendes mathematisches Problem, auf dem in der Praxis benutzte Kryptoverfahren beruhen:

12.16. **Das Problem des diskreten Logarithmus (DL-Problem):**

Geg. sei eine abelsche Gruppe, wir beschreiben das Problem multiplikativ und additiv:

In $(G, \cdot, 1)$:	In $(G, +, 0)$:
Sei $x \in G$, $n = ord(x)$, $y \in \langle x \rangle = \{x^l ; l \in \mathbb{Z}\}$.	Sei $x \in G$, $n = ord(x)$, $y \in \langle x \rangle = \{l \cdot x ; l \in \mathbb{Z}\}$.
Bestimme $k \bmod n$ mit $y = x^k$.	Bestimme $k \bmod n$ mit $y = k \cdot x$.
("diskreter Logarithmus")	("diskreter Logarithmus")

12.17. Bem.: Ist eine Gruppe G gegeben, in der das DL-Problem schwer lösbar ist, kann dies für ein Kryptoverfahren genutzt werden.

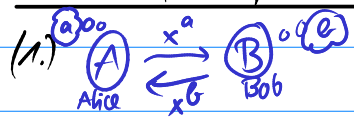
- Im Fall $G = (\mathbb{Z}/n\mathbb{Z}^*, \cdot, \bar{1})$ ist das DL-Problem vergleichbar schwer wie das Faktorisierungsproblem.
- Die Gruppe $(\mathbb{Z}/n\mathbb{Z}^*, \cdot, \bar{1})$ ist zyklisch genau für $n \in \{1, 2, 4\}$ oder $n = p^k$ oder $n = 2p^k$ für ein bel. $k \in \mathbb{N}$ und eine bel. Primzahl $p > 2$, nach dem Satz von Euler über die Existenz von Primitivwurzeln (= Erzeuger von $\mathbb{Z}/n\mathbb{Z}^*$). Man kann auch einfach ein $x \in G$ (mit großer Ordnung in G) wählen und $\tilde{G} = \langle x \rangle$ an stelle G betrachten.

• Im Fall, dass $G = (\tilde{E}(\mathbb{K}), +, \mathcal{O})$ die Gruppe einer (kryptographisch geeigneten elliptischen Kurve ist, ist das DL-Verfahren quasi unlösbar. Die besten bekannten (klass.) Algorithmen sind langsamer als die für das DL-Problem für $\mathbb{Z}_m^*$. Darauf beruht die als höher angesehene Sicherheit bei der Kryptographie mit elliptischen Kurven. → höhere Schlüssellänge bei $\mathbb{Z}_m^*$ erforderlich (bei gleicher Sicherheit)
Wir beschreiben noch die beiden gängigsten Kryptoverfahren, die auf DL beruhen: das Diffie-Hellman-Verfahren und das ElGamal-Verfahren.

12.18. **Der Diffie-Hellman-Schlüsselaustausch:**

Hier vereinbaren (A)lice und (B)ob durch einen öffentlichen Kanal einen gemeinsamen geheimen Schlüssel, die sie dann für ein symmetrisches Kryptoverfahren nutzen können. Geg. sei eine Gruppe G und $x \in G$, sowie $n \in \mathbb{N}$.
Diese Daten seien öffentlich bekannt.

In $(G, \cdot, 1)$:

(1.) 

Alice denkt sich eine Zahl $a \in \{1, \dots, n-1\}$ und schickt $x^a \in G$ an Bob.

Bob denkt sich eine Zahl $b \in \{1, \dots, n-1\}$ und schickt $x^b \in G$ an Alice.

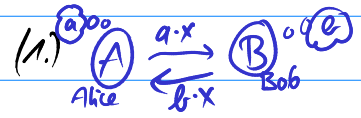
(2.) 

Alice berechnet mit a das Gruppenelement $(x^b)^a$

Bob berechnet mit b das Gruppenelement $(x^a)^b$

Danach besitzen beide den gemeinsamen geheimen Schlüssel $(x^b)^a = x^{ab} = x^{ba}$.

In $(G, +, 0)$:

(1.) 

Alice denkt sich eine Zahl $a \in \{1, \dots, n-1\}$ und schickt $a \cdot x \in G$ an Bob.

Bob denkt sich eine Zahl $b \in \{1, \dots, n-1\}$ und schickt $b \cdot x \in G$ an Alice.

(2.) 

Alice berechnet mit a das Gruppenelement $a \cdot (bx)$

Bob berechnet mit b das Gruppenelement $b \cdot (ax)$

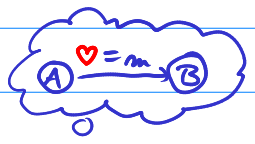
Danach besitzen beide den gemeinsamen geheimen Schlüssel $a \cdot (bx) = abx = b \cdot (ax)$

12.19. **Bem.:** Ein Unbefugter, der die Daten x^a, x^b bzw. ax, bx abhört, kann die geheimen Schlüssel berechnen, wenn er das DL-Problem lösen kann.

Es genügt aber schon, dafür das folgende, ev. leichtere Problem zu lösen:
Diffie-Hellman-Problem (DH-Problem):
Berechne zu $x^a, x^b \in \langle x \rangle \subseteq G$ in $(G, \cdot, 1)$ das Element $x^{ab} \in \langle x \rangle$.
Es ist aber davon auszugehen, dass auch DH ein schweres Problem ist.
(Bem.: "DL lösbar $\Rightarrow$ DH lösbar" ist klar, „$\in$" ist unbekannt.)

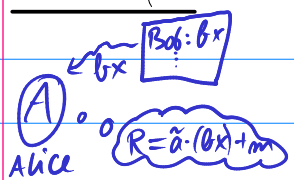
12.20. ElGamal-Verschlüsselung:
Allen Teilnehmern bekannt sei eine abelsche Gruppe $(G, +)$ und ein Gruppenelement $x \in G$ von (großer) Ordnung $n = \mathrm{ord}(x)$.
Jeder Nutzer wählt eine Zufallszahl $a \in \{1, \dots, n-1\}$ als privaten Schlüssel und erzeugt einen öffentlichen Schlüssel $a \cdot x$:

	geheim	öffentlich
Alice	a	ax
Bob	b	bx

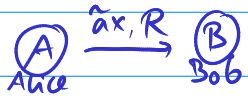


Alice möchte eine geheime Botschaft $m \in G$ an Bob schicken.
Das Verfahren geht wie folgt:

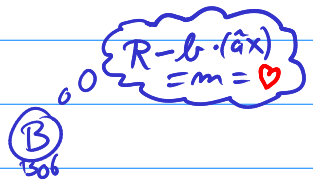
Schritt (1.) Alice wählt eine Zufallszahl $\tilde{a} \in \{1, \dots, n-1\}$ und berechnet $\tilde{a} \cdot x$.
Alice besorgt sich Bobs öffentlichen Schlüssel bx und berechnet $R = \tilde{a} \cdot (bx) + m$.



Schritt (2.) Alice schickt $\tilde{a}x$ und R an Bob.



Schritt (3.) Bob berechnet $b \cdot (\tilde{a}x) = \tilde{a} \cdot (bx)$
und die Nachricht durch $R - b \cdot (\tilde{a}x) = m$.



12.21. Motivation: Eine auf Koblitz/Miller zurückgehende Idee ist nun, dass für die ElGamal-Verfahren eine beliebige zyklische Gruppe $\langle x \rangle$ verwendbar ist, wie etwa die, die von Punkten auf elliptischen Kurven erzeugt werden. Da für (geeignete) elliptische Kurven das DL-Problem bzw. DH-Problem schwieriger als für $\mathbb{Z}_m^*$ ist, gilt diese Art von Verschlüsselungstechnik heute als

besonders sicher und wird vielfältig industriell angewendet; wegen der kleineren Schlüssellänge ist diese auch rechnerisch praktischer als z.B. RSA. Daher eignet sie sich auch besonders für Hardware-/Chipkarten-implementationen.
- Eine Variante des ElGamal-Verfahrens ((EC)DSA) wird zur (elektronischen) Unterschrift/Signatur benutzt; z.B. Personalausweis, etc.

Auf Quantencomputern ist das DL-Problem allerdings schnell lösbar:

12.22. Bem.: • Shors Algo zur Berechnung des diskreten log mod p ermöglicht wiederum, dass die Sicherheit der auf DL beruhenden Algorithmen (Diffie-Hellman, ElGamal) hinfällig werden, sobald ein leistungsfähiger Quantencomputer zur Verfügung steht.
- Der Shor-Algo für DL konnte mittlerweile auch für das DL-Problem auf elliptischen Kurven-Gruppen übertragen werden [Proos/Zalka 2004].
Ein solcher Angriff braucht nur etwa halb so lange wie der klassische Shor-Algorithmus zur Lösung des Faktorisierungsproblems bei einem RSA-Verfahren mit vergleichbarer Sicherheit. Auch der Speicheraufwand eines Quantencomputers (Anzahl benötigter Qubits) ist dabei um (grob) den Faktor 2/3 geringer.
- Bei Aufkommen von Quantencomputern werden die ECC-Verfahren daher Jahre vor den entsprechenden RSA-Verfahren geknackt sein. Dies ist ein Grund, warum wieder eher zur RSA-Technologie geraten wird (mit entsprechend hoher Schlüssellänge).

Primzahltests: Für alle genannten Anwendungen werden große PZen benötigt, numerisch gegeben.

12.23. Grundlage/Heuristik: Hintergrund ist der Kleine Fermatsche Satz, d.h.
p prim $\Rightarrow$ Für alle $a \in \mathbb{Z}$ mit $p \nmid a$ gilt $a^{p-1} \equiv 1 \ (p)$.
Man kann hier versucht sein, die Umkehrung zu nutzen; hier ist „$\Leftarrow$" zwar i.a. falsch, aber dennoch oft richtig: Ist $N = p \cdot q$ zusgesetzt mit $p \neq q$ prim, $U := \{a \in (\mathbb{Z}/N)^* : a^{N-1} \equiv 1 \ (N)\}$, so ist $U = \ker f$, wo $f: a \mapsto a^{N-1}$.
Also ist U echte UG von $(\mathbb{Z}/N)^*$, also $\#U \leq \frac{1}{2} \#(\mathbb{Z}/N)^* = \frac{\varphi(N)}{2}$,
Sofern ex. $a \in (\mathbb{Z}/N)^* \setminus U$. Diese „Zeugen" für die Zusammengesetztheit von N

sind dann durch Probieren leicht zu finden, da sie mehr als die Hälfte aller a ausmachen.
Im ungünstigen Fall $U = (\mathbb{Z}/N)^*$ heißt eine zusammengesetzte Zahl N eine Carmichaelzahl.

12.24. Bem.: Carmichaelzahlen sind ungerade, quadratfrei und bestehen aus mindestens 3 Primfaktoren. Sie erfüllen das Korselt-Kriterium: N Carmichael $\Leftrightarrow \forall p \mid N : p-1 \mid N-1$. (ü)

Die Idee aus 12.23 kann man verfeinern wie folgt:

12.25. Satz (Miller-Rabin-Test): Sei $N > 1$ ungerade, $N-1 = 2^k \cdot m$, m ungerade.
(i) Gilt für jedes $a \in \mathbb{Z}$ mit $(a,N)=1$, dass
$\circledast$ $a^m \equiv 1 \ (N)$ oder ex. $\ell \in \{0,1,\dots,k-1\}$: $a^{2^\ell m} \equiv -1 \ (N)$,
dann ist N eine Primzahl.
(ii) Ist N zus.gesetzt, gilt $\#\{a \in \{1,\dots,N-1\};\ (a,N)=1,\ \circledast\} \le \frac{\varphi(N)}{4}$.

12.26. Bem.: • Erhalte so einen Test: Wähle $a \in (\mathbb{Z}/N)^*$ zufällig. Gilt dann $\circledast$, entscheide "N prim". Die W., dass $\circledast$ gilt (für zufällig gewähltes a) und N trotzdem zus.gesetzt ist, beträgt nur $\le \frac{1}{4}$. Bei t-facher Wdh. also $\le (\frac{1}{4})^t$, was schnell sehr klein ist. N ist dann mit W. $\ge 1 - \frac{1}{4^t}$ eine Primzahl.
• Die Laufzeit dieses probabilistischen Algorithmus ist $O(\log^A N)$ für ein $A > 1$. Er ist also polynomiell (in der Inputgröße $O(\log N)$).

12.27. • Bsp.: $N = 2^{400} - 593$, $t = 100$, ist prim mit W. $\ge 1 - \frac{1}{4^{100}}$, wo $\frac{1}{4^{100}} < 10^{-60}$.
(Später wurde N prim mit determ. Test bestätigt.)

12.28. Def.: Man nennt eine Zahl N mit $\circledast$ für ein a, $(a,N)=1$, eine
starke Pseudo-Primzahl zur Basis a.

12.29. Beweis von Satz 12.25: Betr. $0 < a < N$ mit $(a,N)=1$.
Setze $a_0 := a^m \pmod N$, $a_1 := a_0^2 = a^{2m} \pmod N, \dots,$
$a_i := a_{i-1}^2 = a^{2^i m} \pmod N, \dots, a_k = a_{k-1}^2 = a^{2^k m} = a^{N-1} \pmod N$.
Sei $P_0 := \{a \in (\mathbb{Z}/N)^*;\ a_0 \equiv 1 \ (N)\}$,
$P_i := \{a \in (\mathbb{Z}/N)^*;\ a_{i-1} \equiv -1 \ (N)\}$, $1 \le i \le k$, und $P := \bigcup_{i=0}^{k} P_i$.

- Die P_i sind p.w. disjunkt.
- Ist $a \in P$, folgt $a^{N-1} = a_k \equiv 1 \ (N)$.
- Ist N prim, folgt $P = (\mathbb{Z}/N)^* = \{\bar{1}, \bar{2}, \dots, \overline{N-1}\}$.

Zu (ii): (I) Sei N zunächst eine Carmichaelzahl, d.h. $a^{N-1} \equiv 1 (N)$ für alle $(a,N)=1$.
Nach Bem. 12.24 ist $N = p_1 \cdots p_r$ mit p_i p.w.v. prim, $p_i > 2$.
Haben dann Iso $\psi : (\mathbb{Z}/N)^* \xrightarrow{\sim} (\mathbb{Z}/p_1)^* \times \ldots \times (\mathbb{Z}/p_r)^*$ laut CRS.
Wähle Primitivwurzeln (= Erzenger) $g_i \in (\mathbb{Z}/p_i)^*$ und sei
$a(k_1, \ldots, k_r) \in (\mathbb{Z}/N)^*$ das El. mit $\psi(a(k_1,\ldots,k_r)) = (g_1^{k_1}, \ldots, g_r^{k_r})$.
Nach Bem. 12.24, dem Korselt-Kriterium, ist $\forall i : p_i - 1 \mid N-1$.
Sei also $N-1 = 2^{s_i} m_i (p_i - 1)$ mit ungeradem m_i: für alle $i = 1, \ldots, r$,
OE mit $s_1 \le s_2 \le \ldots \le s_r$. Setze $s := s_1$, dann gilt $a^{(N-1)/2^s} \equiv 1$ für alle
$a \in (\mathbb{Z}/N)^*$, da dies mod $p_1, \ldots, p_r$ gilt, und weiter: $\frac{N-1}{2^s}$ ist gerade (da faktor $p_r - 1$ enthalten).
1. Fall: Für alle i ist $s_i = s$. Dann ist $\frac{N-1}{2^{s+1}}$ ungerades Vielfache von $\frac{p_i - 1}{2}$ für alle i.
Die Menge P liegt dann in $A := \{a \in (\mathbb{Z}/N)^*;\ a^{(N-1)/2^{s+1}} \equiv \pm 1 (N)\}$.
Die Bed. in A gilt genau dann, wenn entweder alle k_i gerade oder
alle k_i ungerade sind, d.h. in 2 von 2^r Fällen der VZ-Verteilung von $a^{(N-1)/2^{s+1}} \bmod p_i$.
gilt diese. Da $r \ge 3$ nach Bem. 12.24, folgt $\#A \le \frac{1}{4} \varphi(N)$,
Also gilt (ii).

2. Fall: $s < s_r$. Dann ist $\frac{N-1}{2^{s+1}}$ ein Vielfaches von $p_r - 1$, also gerade.
Also ex. kein $a \in (\mathbb{Z}/N)^*$ mit $a^{(N-1)/2^{s+1}} \equiv -1 (N)$.
Es folgt $P \subseteq A_{(+1)} := \{a \in (\mathbb{Z}/N)^*;\ a^{(N-1)/2^{s+1}} \equiv 1 (N)\}$.
Außerdem ist $A_{(+1)} \neq (\mathbb{Z}/N)^*$, also $\#A_{(+1)} \le \frac{\varphi(N)}{2}$ da echte UG von $(\mathbb{Z}/N)^*$.
⌜Denn $a(1,0,\ldots,0)$ erfüllt $g_1^{(p_1-1)/2} \equiv -1 (p_1)$, $i > 1 : g_i^0 \equiv 1 (p_i) \rightsquigarrow \frac{N-1}{2^{s+1}} = m_1 \cdot \frac{p_1 - 1}{2}$,
also $a^{(N-1)/2^{s+1}} = (-1, 1, \ldots, 1) \neq 1$, d.h. $a \notin A_{(+1)}$. ⌟

Jetzt ist $P \subseteq B := \{a \in (\mathbb{Z}/N)^*;\ a^{\frac{N-1}{2^{s+2}}} \equiv \pm 1 (N)\} \subseteq A_{(+1)}$.
Für das El. $a(2,0,\ldots,0)$ gilt $a^{(N-1)/2^{s+1}} \equiv 1 (N)$, also $a \in A_{(+1)}$ und
$a^{(N-1)/2^{s+2}} = a(\frac{p_1-1}{2}, 0, \ldots, 0) \neq \pm 1$, also $B \neq A_{(+1)}$.
($g_1^{\frac{2(p_1-1)}{2} m_1} \equiv 1 (p_1)$) Daraus folgt $\#B \le \frac{1}{2} \#A_{(+1)} \le \frac{1}{4} \varphi(N)$.
Also gilt (ii).

(II) Ist N keine Carmichaelzahl, ist $C := \{a \in (\mathbb{Z}/N)^* ; a^{N-1} \equiv 1 (N)\}$ eine echte UG von $(\mathbb{Z}/N)^*$, also $\#C \leq \frac{1}{2}\varphi(N)$, und haben $P \subseteq C$.
Ist nun $[(\mathbb{Z}/N)^* : C] \geq 4$, gilt $\#P \leq \#C \leq \frac{1}{[\dots]} \cdot \#(\mathbb{Z}/N)^* \leq \frac{1}{4}\varphi(N)$ ✓. Daher:
Gen. z.z.: Ist $[(\mathbb{Z}/N)^* : C] < 4$, gilt $\#P \leq \frac{1}{2}\#C$. [Ohne Beweis; geht ähnlich wie (I).]
Auch dann gilt also (ii).

Zu (i): Aus (ii): ist N nicht prim, gilt ⊛ nicht für alle a.
Somit: Gilt ⊛ für alle a, ist N notwendig prim. □

12.30. Bem.: Lange Zeit war offen, ob ein deterministischer PZtest, der polynomiell schnell ist, existiert. Ein solcher Test wurde 2003 überraschend entdeckt von Agrawal, Kayal, Saxena und ist heute bekannt als AKS-Primzahltest; dieser läuft in der Praxis aber (noch) nicht so schnell wie der Miller-Rabin-test, so dass bis heute der letztere angewendet wird.

12.31. Bem.: Unter Ann. der verallgemeinerten Riemannschen Vermutung (GRH) wurde 1985 von E. Bach gezeigt: N zus. gesetzt $\Rightarrow \exists a \leq 2\log^2 N$ mit $a \notin P$.
Sucht man die a gezielt ab bzw. testet $a = 2, 3, \dots$, stößt man sehr bald auf ein $a \notin P$, es sei denn, die verallg. Riemannsche Vermutung ist falsch.
Dieses Ergebnis zeigt, dass der Miller-Rabin-Test (mit $a \leq 2\log^2 N$) für die Praxis völlig ausreichend ist, da die Gültigkeit der Riemannschen Vermutung kaum angezweifelt wird. Mehr über die Riemannsche Vermutung und ihre Bedeutung wird gegen Ende der Vorlesung behandelt (und in der Vorlesung "Analytische Zahlentheorie").