

Prüfungsprotokoll (Modulprüfung MSc Informatik)

Kurs: 01321 –Mathematische Grundlagen der Kryptographie

Datum: 26.03.2012

Prüfer: Prof. Dr. Luise Unger

Dauer: ca. 25 Minuten

Note: 1,0

Fragen:

- **Worum geht es in der Kryptographie und wie kann man sie mathematisch beschreiben?**
 - Sichere Kommunikation über unsicheren Kanal
 - 5-Tupel beschreiben (musste ich auch aufschreiben)
- **Worin unterscheiden sich symmetrische und asymmetrische Verschlüsselung?**
 - symmetrisch: Ein Schlüssel, d_k aus e_k leicht ableitbar
 - asymmetrisch: Zwei Schlüssel, geheime Zusatzinformation benötigt
- **Was ist monoalphabetische und was polyalphabetische Verschlüsselung?**
 - monoalphabetisch: Ein Klartextsymbol wird auf genau ein Geheimsymbol abgebildet; Beispiel: Verschiebe-Kryptosystem (erklärt)
 - polyalphabetisch: Buchstabenfolgen werden abgebildet; verschleiern die Buchstabenhäufigkeit; Beispiel: Vigenère-Kryptosystem
- **Bekanntes Beispiel für asymmetrische Verschlüsselung ist RSA. Bitte einmal aufschreiben und erklären.**
 - Hier sollte man auch den kleinen Satz von Fermat ($a^{p-1} \bmod p = 1$) und seine Erweiterung ($M^{k(p-1)(q-1)+1} \bmod pq = M$) aufschreiben können.
- **Wie wird die Zahl e beim RSA berechnet?**
 - ggT über Euklidischen Algorithmus
- **Wie wird die Zahl d beim RSA berechnet?**
 - Über den erweiterten Euklidischen Algorithmus
- **Wie wird die Chiffrierung ($y = x^e \bmod m$) berechnet?**
 - Durch wiederholtes Quadrieren, bei dem nicht jede Potenz berechnet wird, sondern nur x^2, x^4, \dots
- **Wieso wird RSA als sicher eingestuft?**
 - Primfaktorzerlegung großer Zahlen → nicht effizient lösbar
- **Wie findet man die Primzahlen p und q ?**
 - Primzahltests: Fermat-Test erklärt
- **Was sind Carmichael Zahlen und was ist so gemein an denen?**
 - Für ein beliebiges b ist immer $b^{n-1} \bmod n = 1$ erfüllt und es gibt unendlich viele davon.
- **Welche Primzahltests gibt es noch und welcher wird in der Praxis verwendet?**
 - In der Praxis wird Rabin-Miller-Test verwendet
 - Es gibt außerdem noch den Solovay-Strassen-Test
- **Was gibt es noch für ein Problem auf dem Kryptosysteme beruhen?**
 - Diskreter-Logarithmus-Problem; erklärt über endlichen Körpern

- **Was sind endliche Körper?**
 - Körper mit endlich vielen Elementen
 - Charakteristik ist immer eine Primzahl p (musste noch erklären, was eine Charakteristik ist)
 - Anzahl der Elemente ist p^n (musste ich genauer erklären)
- **Gibt es zu jedem p^n einen endlichen Körper?**
 - Ja
- **Gibt es einen endlichen Körper mit 6 Elementen?**
 - Nein
- **Wir hatten ja noch ein Kryptosystem kennengelernt, das sich dann als Flop herausgestellt hat. Wie heißt das und worauf basierte das?**
 - Knapsack-Kryptosystem
 - Basiert auf dem Teilmengen-Summen-Problem ($\sum_{i=0}^n a_i x_i = s$)
 - Kann über den LLL-Algorithmus gebrochen werden (Kurz noch etwas über Berechnung reduzierter Basen und kurzen ersten Vektor, der sehr oft die Lösung ist, erzählt.)

Fazit:

Frau Prof. Dr. Unger hat am Anfang über Smalltalk und über Fragen zu meiner Arbeit und meinem Studium zunächst einmal die Situation gelockert und mir die Anspannung etwas genommen.

Die Fragen waren alle sehr auf die Kryptographie und nicht so sehr auf die Mathematik bedacht. Ich studiere im Master of Science in Informatik. Evtl. sind die Fragen bei Mathematik-Studenten etwas anders gestellt. Das kann ich aber nicht beurteilen.

Obwohl ich bei einigen mathematischen Definitionen einige Patzer drin hatte, hat mir Frau Prof. Dr. Unger stets mit kleinen Tipps weitergeholfen.

Ich finde die Benotung sehr großzügig, da ich wie gesagt ein paar Patzer bei den mathematischen Definitionen hatte.

Mein Eindruck war, dass es sehr wichtig ist die Zusammenhänge verstanden zu haben und die Kryptographie. Die mathematischen Details sollte man zwar grob verstanden haben, aber in allen Einzelheiten musste man sie nicht wiedergeben.

Die bisherigen Prüfungsprotokolle haben mir sehr beim Lernen geholfen. Also schreibt auch ihr welche für die zukünftigen Studenten!

Gedächtnisprotokoll Fachprüfung (Master)

Kurs: 1321 – Mathematische Grundlagen der Kryptographie
Prüfer: Prof. Unger (Beisitzerin: Frau Hartlieb)
Datum: 12.12.2011
Dauer: ca. 25 Minuten
Note: 1,0

Inhalt der Prüfung:

- Worum geht es in der Kryptographie? Wie wird die Kryptographie in der Mathematik beschrieben?
- Es gibt verschiedene Kryptosysteme: symmetrische und asymmetrische. Worauf bezieht sich die Symmetrie bei einem symmetrischen Kryptosystem?
- Wie werden Primzahlen bestimmt?
- Welche Primzahltests kennen Sie?
- Wie funktioniert RSA im Detail?
- Schreiben Sie den Satz von Euler und kleine Satz von Fermat auf.
- Wieso wird RSA als sicher betrachtet?
 - Wie wird der ggT berechnet?
 - Wie wird das d von $e \cdot d = 1 \pmod{\varphi(m)}$ berechnet?
 - Wie wird $x^e \pmod{m}$ berechnet?
 - Gibt es Kryptosysteme, die auf einem anderen Problem beruhen?
- Beschreiben Sie das Diffie-Hellman-Verfahren.
- Was können Sie mir über endliche Körper sagen?
- Wie sehen die Elemente eines endlichen Körpers F_p aus?
- Was ist die Charakteristik?

Fazit:

Prof. Unger ist eine freundliche und faire Prüferin. Die Fragen sind klar formuliert. Ich habe bei der Beantwortung der Fragen immer wieder kleine Ungenauigkeiten gehabt, bei denen Sie gleich nachgehakt hat, so dass ich mich selber korrigieren konnte. Bei der detaillierten Beschreibung des RSA habe ich einen Fehler gemacht, der sich aber nicht auf die Note ausgewirkt hat. Wichtig ist, dass man die wesentlichen Inhalte des Kurses verstanden hat und diese im Zusammenhang erläutern kann - vor allem beim RSA.

Ich kann Prof. Unger als Prüferin weiterempfehlen.

Viel Erfolg bei Deiner Prüfung,

Alexander

SS2011 Prüfungsprotokoll "Mathematische Grundlagen der Kryptografie"

Prüferin: Fr. Prof. Dr. Unger

Beisitzerin: Fr. Dr. Harlieb

Dauer: max. 20 Minuten

Note: 1,0

Prüfungsprotokoll:

- Was ist Kryptografie, wie wird die Kryptografie in Mathematik "gegossen"?
- Definition eines Kryptosystems
- Symmetrische vs. Asymmetrische Kryptosysteme
- RSA beschreiben.
- Wie findet man denn Primzahlen?
- Welcher Primzahltest wird verwendet?
- Warum ist RSA (vermutlich) sicher?
- Fragen zur effizienten Berechnung der einzelnen Komponenten des RSA Kryptosystems
- Was wird denn mit dem Erweiterten Euklidischen Algorithmus berechnet?
- Was ist denn die Charakteristik?
- Welche Eigenschaften haben denn endliche Körper?
- Gibt es zu jedem n (für p^n) einen endlichen Körper?
- Was ist denn ein primitives Element?
- Was ist das DLP?
- Beschreiben Sie ein Kryptosystem oder Schlüsselaustauschsystem auf Basis des DLP.

Generell eher ein Wechselgespräch als sture Fragenrunde.

Sehr angenehme Prüferin; sehr angenehme Prüfungsatmosphäre.

Prüfungsprotokoll zu Mathematische Grundlagen der Kryptographie (01321)

Prüfer: Prof. Luise Unger

Datum: 05.10.2009

Note: 1,0

Worum geht es in der Kryptografie, was ist denn ein Kryptosystem?

- Zweck des Ganzen, Codes, Chiffren etc. beschrieben und Definition eines Kryptosystems als Quintupel wiedergegeben.

Was ist der Unterschied zwischen symmetrisch und asymmetrisch?

- Bei asymmetrischen KS benötigt die Umkehrfunktion $d(K)$ eine Zusatzinformation, die nur der Empfänger kennt.

Welche symmetrischen KS kennen Sie denn?

- Alle im Kurstext genannten aufgezählt.

Darunter gibt es mono- und polyalphabetische KS. Was bedeutet das?

- Unterschied beschrieben, Vigenere als Beispiel erklärt.

Beschreiben Sie mal RSA im Detail!

- Hier hatte ich einen kurzen Blackout und habe stattdessen angefangen, ElGamal zu erklären. Prof. Unger half mir auf die Sprünge. RSA erklärt, im Anschluss Satz von Euler und kleinen Satz von Fermat wiedergegeben.

Welches Problem liegt RSA zugrunde, welche schweren Probleme gibt es sonst noch?

- Faktorisierung großer Primzahlen und diskreten Logarithmus grob umrissen.

Letzteres betrifft endliche Körper. Welche Eigenschaften haben denn endliche Körper?

- Einige Eigenschaften aufgezählt.

Was sind Charakteristik, Primring und primitive Elemente?

- Definitionen wiedergegeben.

Dann konstruieren Sie doch mal einen Körper mit 8 Elementen!

- Mit ein paar hilfreichen Kommentaren kam ich bis $F_2[T] / \dots$

Prof. Unger verriet mir den Rest der Lösung $F_2[T] / (T^3 + T + 1)$ und ließ mich nur noch erklären, warum dieses Polynom offensichtlich irreduzibel ist (weil es keine Nullstelle hat).

Wie sehen denn die Elemente dieses Körpers aus?

- Restklassenringe mit Polynomen u.a. vom Grad < 3

So genau will ich es gar nicht hören. Was ist eine elliptische Kurve?

- Erklärt, dass elliptische Kurven grafisch schön vorstellbare Gruppen sind, dabei eine Kurve aufs Blatt gezeichnet und anhand zweier Punkte die Addition definiert.

Kennen Sie ein Schlüsselaustauschverfahren?

- Diffie-Hellman erklärt.

Was ist das Knapsack-KS und wo war das Problem damit?

Knapsack und Teilmengen-Summen-Problem erklärt, Analyse mittels LLL-Algorithmus grob umrissen.

Die Zeit ist um.

Gedächtnisprotokoll: Grundlagen der Kryptografie (01321)

Prüferin: Prof. Unger

Beisitzerin: Dr. Silke Hartlieb

Datum: 8.10.2009

Prüfungsdauer: 20-25 Minuten

Note: 1.0

Folgende Fragen hat Frau Unger gestellt:

- Was ist überhaupt Kryptografie/ wozu braucht man sie? (allgemein & Definition)
- Wir haben im Kurs symmetrische KS und asymmetrische KS behandelt, erklären Sie die Unterschiede und nennen Sie Beispiele!
- Was ist der Unterschied zwischen monoalphabetischen und polyalphabetischen KS? Erläutern Sie jeweils ein Beispiel. (Habe affines KS und Hill-KS erklärt)
- Auf welchem mathematischen Problem basiert die RSA-Verschlüsselung? (Primfaktorzerlegung/ Erläuterung)
- Erläutern Sie die RSA-Verschlüsselung. (Fermat-Satz und seine Erweiterung nicht vergessen!)
- Wie findet man Primzahlen? (alle 3 Tests genannt/ Fermat-Test erläutert)
- Auf welchem anderen mathematischen Problem basieren weitere Public-Key-KS? (Diskreter-Logarithmus-Problem definieren!)
- Nennen und erläutern Sie ein Beispiel (Habe Diffie-Hellman über endlichen Körpern erläutert)
- Was sind endliche Körper? Welche Eigenschaften haben Sie?
- Erklären Sie wie man die Elemente des F_8 findet (als Faktoring der Polynome über dem endlichen Körper F_2 modulo einer irreduziblen Funktion mit $\text{Grad}(f)=3$)
Ich hatte als irreduzible Funktion $T^3 + T^2 + 1$ gewählt und somit 8 Polynome vom $\text{Grad} < 3$ als Elemente ausgewiesen.
- Wie berechnen Sie jetzt das Produkt $(T^2+T+1) * (T^2+1)$? (multiplizieren und dann eine Polynomdivision durch (T^3+T^2+1) und den Rest als Lösung hinschreiben)

Fazit:

Die Prüfung ging schneller vorbei, als ich es mir gedacht hatte und, obwohl ich sehr nervös war und schnell gesprochen habe, verlief die Prüfung sehr zufriedenstellend. Die Fragen der Prüferin sind sehr fair gestellt, bei Unklarheit kann man leicht nachfragen und bekommt auch Hilfestellungen. Wichtig ist, dass man bei der Vorbereitung die Zusammenhänge lernt und versteht. Die Verschlüsselungssysteme sollte man nicht nur erklären können, sondern die Mathematik, die dahinter steckt beherrschen.

Hilfreich bei der Prüfung war auch, dass ich bei der ein oder anderen Frage auch erkennen ließ, dass ich die wesentlichen Bausteine verstanden hatte und hier und da Querverweise herstellen konnte; somit musste man mir nicht jedes Wort aus der Nase ziehen und die Prüferin fragte die Themen nicht einzeln ab. Im Großen und Ganzen waren es wenige Fragen, die im Rahmen eines angenehmen Wechselgespräches gestellt wurden. Frau Unger ist eine sehr sympathische Prüferin, die ich sofort weiterempfehlen würde.

Wünsche euch viel Glück für eure Prüfung und wenn euch die Protokolle geholfen haben, dann schreibt eurerseits auch welche, damit nachfolgende Studenten auch diese Hilfestellung in Anspruch nehmen können!

Ein Dankeschön an meine Vorgänger, die mir mit ihren Protokollen sehr geholfen haben bei der Prüfungsvorbereitung!

Prüfungsprotokoll zu Mathematische Grundlagen der Kryptographie (01321)

Prüfer: Prof. Luise Unger

Datum: 07.11.2006

Note: 2,0

Erklären Sie Mal, was Kryptographie ist, wie man symmetrische und asymmetrische Kryptographie unterscheidet und nennen sie jeweils Beispiele!

- Auf diese Frage habe ich erstmal relativ frei erzählt: Ich führte erstmal (mit wenigen schriftlichen Erläuterungen) ein KS als Quintupel ein. Dann habe ich gesagt, dass man bei symmetrischen KS die Entschlüsselungsfunktion leicht aus der korrespondierenden Verschlüsselungsfunktion herleiten kann, bei asymmetrischen Verschlüsselungen nicht. Ich habe die symmetrischen KS in monoalphabetische und polyalphabetische Verschlüsselungen eingeteilt und jeweils ein von mir ausgesuchtes Beispiel erklärt (nämlich Cäsar und Vigenere) und auch erwähnt, wie man monoalphabetische Verschlüsselungen allgemein knackt, beim Brechen von Vigenere wurde ich dann gebremst.

Das geht mir jetzt schon zu sehr in's Detail. Geben Sie doch Mal ein Beispiel für eine asymmetrische Verschlüsselung!

- Ich habe hier die RSA-Verschlüsselung erklärt, d.h. erstmal öffentlichen und privaten Schlüssel definiert und dann Ver- und Entschlüsselung beschrieben. Warum die Entschlüsselung funktioniert, musste ich genauer erklären (also dass $e * d \equiv 1 \pmod{\phi(n)}$ und dass $\phi(n)$ die Gruppenordnung ist und mit dem Satz von Fermat)

Kennen Sie noch andere asymmetrische KS?

- Ich habe dann gesagt, dass RSA auf dem Problem beruht, dass große Zahlen schwer zu faktorisieren sind. Andere KS bauen darauf auf, dass der Diskrete Logarithmus in einigen Gruppen (vermutlich) schwer zu berechnen ist.

OK, was ist denn erstmal der Diskrete Logarithmus?

- Definiert.

- Danach habe ich mit der ursprünglichen Frage weitergemacht. Der Diffie-Hellman-Schlüsselaustausch beruht auf der Schwierigkeit des Diskreten Logarithmus. Ich habe dann den DH erläutert.

Auf was für Gruppen haben wir dieses KS denn angewendet?

- Auf elliptische Kurven und auf $\mathbb{Z}/p\mathbb{Z}^*$.

Wir haben es nicht nur auf $\mathbb{Z}/p\mathbb{Z}^*$ angewendet, sondern allgemein auf die Einheitengruppen endlicher Körper. Was sind denn endliche Körper?

- Bei dieser Frage habe ich mir meine Note versaut ;-). Ich habe hier sinngemäß behauptet, $\mathbb{Z}/n\mathbb{Z}$ wäre auch für nicht-prime n ein Körper. Natürlich hat Prof. Unger da nachgehakt und nachdem ich erstmal nichts Sinnvolles von mir gegeben habe, konnte ich dann wenigstens noch beschreiben, wie man $\mathbb{F}_2[x]$ erzeugt (Nämlich als Faktorring der Polynome über \mathbb{F}_2 modulo dem von einem irreduziblen Polynom 3. Grades erzeugten Ring).

Und wie ist das nun mit den elliptischen Kurven?

- Ich habe nach Charakteristik in die drei Fälle eingeteilt (2, 3, >3), wobei nur zwei davon für die Kryptographie relevant sind. Für >3 habe ich die Menge dann genauer mit Voraussetzungen und Formel beschrieben. Die Gruppenoperationen habe ich dann in \mathbb{R}^2 anhand einer Skizze beschrieben.

Was ist denn das Knapsack-KS?

- Habe erstmal das Knapsack-Problem beschrieben und gesagt, dass es allgemein NP-hart ist. Wenn die betrachtete Folge aber supraaufsteigend ist, ist es leicht zu lösen. Auf Nachfrage habe ich dann beschrieben, was bei einer Verschlüsselung nun eigentlich die Nachricht ist. Summarisch habe ich dann die Entschlüsselung erklärt.

Wie wurde das Knapsack-KS gebrochen?

- Anhand der Matrix der Basisvektoren des Gitters wie im Skript habe ich gezeigt, dass der Vektor $(x_1, \dots, x_n, 0)$ im Gitter liegt und recht kurz ist. Mit dem LLL-Algorithmus kann man einen sehr kurzen Vektor finden und die Chancen sind gut, dass es genau der Vektor mit dem Klartext ist.

OK, die Zeit ist um.

Diese Prüfung war für mich eine Wiederholung zur Notenverbesserung eines Freiversuchs. Da ich in der ersten Prüfung eine 1,7 hatte (und dort etwas schlechter vorbereitet war), habe ich mir keinen Gefallen getan. Ich empfinde die Bewertung durchaus als gerecht, da ich mir mit den endlichen Körpern schon einen sehr dicken Patzer geleistet habe (das hat Prof. Unger auch in der Notenbegründung erwähnt). Dieser Fehler war zwar auf meine Nervosität zurückzuführen (wäre ich ruhiger gewesen, hätte ich gemerkt, dass ich Unsinn rede), aber ich glaube nicht, dass ich bei einem anderen Prüfer weniger nervös gewesen wäre. Insgesamt bekam ich bisher im Vergleich zu allen Mathe-Professoren bei Prof. Unger leicht überdurchschnittlich gute Noten, im Vergleich zu den Informatik-Professoren waren sie aber unterdurchschnittlich. Die Kurse von Prof. Unger sind sehr gut zu lesen und auch so hat der Kurs Spaß gemacht.

Diplomprüfung „Mathematische Grundlagen der Kryptographie“ (1321) im Nebenfach
Prüferin: Prof. Dr. Unger
Beisitzerin: Dr. Silke Hartlieb
Datum: 14.09.06
Dauer: 25 min
Note: 1.3

- Es gibt symmetrische und asymmetrische Kryptosysteme. Worin unterscheiden sich die?
- Erklären Sie ein monoalphabetisches Kryptosystem. (affines Kryptosystem erklärt)
- Erklären Sie ein polyalphabetisches Kryptosystem. (Vignere-Chiffre erklärt)
- Erklären Sie ein asymmetrisches Kryptosystem. (RSA erklärt)
- Welche anderen asymmetrischen Kryptosysteme kennen sie?
- Erklären Sie das Knapsackkryptosystem.
- Wie wurde das Knapsackkryptosystem denn geknackt?
- Welche Eigenschaft reduzierter Basen war dafür besonders wichtig?
- Was ist das diskret Logarithmusproblem? (ganz allgemein erklärt)
- Es gibt Gruppen, für die das Problem ganz einfach zu lösen ist. Bei welchen Gruppen ist das Problem schwer? (IK-Kreuz, Elliptische Kurven bzw. deren Untergruppen)
- Wir hatten drei Kryptosysteme dazu. Erklären Sie eines davon. (ElGamal erklärt)
- Was sind effiziente Algorithmen?
- Welche kennen Sie?
- Erklären Sie das wiederholte Quadrieren.
- Wir brauchen öfter Primzahlen. Wie findet man die? (allgemeines Vorgehen und Fermat/Rabin-Miller erklärt)

Frau Unger ist eine sehr angenehme Prüferin, die mir meine Nervosität sehr schnell genommen hat. Die Kryptosysteme und den Primzahltest konnte ich mir selber herausuchen.

Viel Glück und Erfolg bei Eurer Prüfung.

Kurs: 01321 Mathematische Grundlagen der Kryptographie

Betreuung: LG Algebra, Frau Dr. Silke Hartlieb

Prüfung: Informatik Diplom II, Fachprüfung Mathematik im Nebenfach

Termin: 7.7.2005 10 Uhr

Dauer: etwa 30 Minuten

Prüferin: Prof. Dr. Luise Unger

Note: 1.0

Prof. Unger: Beschreiben Sie symmetrische und asymmetrische Kryptosysteme (i.f. KS), nennen Sie Unterschiede, Vor- und Nachteile, nennen Sie Beispiele!

Antwort: angeboten, die formale Definition eines KS als Quintupel hinzuschreiben, dann aber auf verbale Beschreibung beschränkt: Klartextmenge, Geheimtextmenge, Schlüsselmenge, Menge von Verschlüsselungs- bzw. von Entschlüsselungsabbildungen. Unterschied sym/asym: wer symmetrisch verschlüsseln kann, kann auch entschlüsseln, die Entschlüsselungsabbildung ist aus der Verschlüsselungsabbildung ableitbar. Wer asymmetrisch verschlüsselt, kann nicht entschlüsseln, ohne dass er einen anderen, weiteren, zusätzlichen Schlüssel kennt. Erklärt, dass monoalphabetische KS grundsätzlich Permutationen sind, die Abbildungsdefinition über Schlüssel eigentlich nur eine Merkhilfe darstellt. Als Beispiele Verschiebe-KS (Caesar) und affines KS genannt, letzteres auch kurz hingeschrieben. Erläutert, daß monoalphabetische KS geknackt werden können, ohne daß man den Schlüssel explizit ermittelt, über (vermutete) Strukturmerkmale des Klartextes, die sich in evtl. veränderter, aber weiter erkennbarer Form im Geheimtext wiederfinden, insbesondere Buchstabenverteilung (e ist immer der häufigste usw.).

Polyalphabetisch durch Vigenère-KS beispielhaft erklärt: Text wird sozusagen zeichenweise als Spalten geschrieben und jede Spalte mit einem anderen Schlüssel monoalphabetisch verschlüsselt. Erklärt, daß die Spaltenbreite bzw. ein Vielfaches davon über kurze häufig vorkommende Worte im Geheimtext erkennbar ist (Kasiski-Test). Erläutert, wie der Koinzidenzindex benutzt werden kann um zu erkennen, ob mono- oder polyalphabetisch verschlüsselt wurde. Geschlossen damit, dass aufgrund dieser Möglichkeiten symmetrische KS heute nur noch in Verwendung sind, wenn die Möglichkeit besteht, den Schlüssel sehr häufig zu wechseln.

Prof. Unger: und was sind nun demgegenüber Vor- und Nachteile der asymmetrischen Systeme?

Antwort: Vorteil ist die Sicherheit; asymmetrische Systeme erfüllen die Forderung, daß man den Algorithmus nicht geheim halten muß, weil selbst in Kenntnis von Algorithmus und öffentlichem Schlüssel die Entschlüsselung nur mit unangemessenem Rechenaufwand möglich ist.

Nachteil ist der deutlich höhere Rechenaufwand für Ver- und Entschlüsselung.

Prof. Unger: nennen Sie Beispiele und erklären Sie, warum der Rechenaufwand beim Knacken so hoch ist!

Antwort: RSA als Beispiel, erwähnt, daß dieses in Pretty Good Privacy verwendet wird. Verallgemeinerung des kleinen Satz von Fermat eingeführt: Primzahlen p und q , ihr Produkt teilt $a^c - a$ für beliebige a , wenn c kongruent zu 1 modulo $\phi(pq)$ ist. Dies ist Grundlage für RSA: öffentlicher Schlüssel ist $m=pq$ und eine ganze Zahl e , die teilerfremd zu $\phi(pq)$ und daher in $\mathbb{Z}/\phi(pq)\mathbb{Z}$ invertierbar ist. Geheimtext ist x^e , Empfänger kennt den geheimen Schlüssel d mit $(ed) \bmod \phi(pq) = 1$ und

kann $x^{ed} = x$ bilden. Um aus $m = \phi(pq)$ ermitteln und dadurch das zu e inverse d bilden zu können, muß (so wird vermutet) die Faktorisierung von m berechnet werden, und dieses Problem ist NP hart.

Prof. Unger fragt nach einem weiteren rechenaufwendigen Problem und einem Beispiel für KS.

Antwort: die KS nach Diffie-Hellman, Massey-Omura und ElGamal genannt, sie beruhen auf dem Diskreter-Logarithmus-Problem (DLP), (auf Nachhaken dieses hingeschrieben in der Form für multiplikative Gruppen), Schlüsselaustausch nach Diffie-Hellman gezeigt.

Prof. Unger fragt nach einer weiteren Grundmenge neben den endlichen Körpern, die für KS eingeführt wurde.

Antwort: Frage zielte offenbar auf die elliptischen Kurven. Definiert als Teilmenge eines Körpers, für die Kryptographie sind nur die endlichen Körper wesentlich, unterschiedliche Definition für $\text{char}(K) = 2$ bzw. $\text{char}(K) > 3$ hingeschrieben (dabei zunächst den "Punkt bei unendlich" vergessen), die unterschiedlichen Randbedingungen für a und b hingeschrieben, erklärt, wie daraus eine additive Gruppe wird (Prof.

Unger: das Assoziativgesetz glauben wir jetzt einfach), neutrales Element (dabei den "Punkt bei unendlich" in der Definition ergänzt).

(Prof. Unger: zeigen Sie die Addition einfach an einer Zeichnung im \mathbb{R}^2 !) Kurve gezeichnet, einen Punkt P , Inverses dazu als $-P$ (Prof.

Unger korrigiert dies zu $-P$), Prinzip der drei Schnittpunkte erläutert, Spezialfall der Tangente.

Prof. Unger fragt nach einem weiteren Kryptosystem, das "mit etwas Mathematik dazu" im Kurs eingeführt wurde, das sich dann aber als Flop erwiesen hat.

Antwort: Knapsackproblem, will direkt auf Gitter zu sprechen kommen.

Prof. Unger fragt zuerst noch die Beschreibung des Knapsack-Problems ab.

Ich gebe die Definition als Teilmengen-Summen-Problem, erwähne die NP-Vollständigkeit und erläutere, daß das Problem leicht lösbar ist, wenn die Folge der Teilmengen superaufsteigend ist. Definiere superaufsteigend und erläutere, daß die Idee der Verschlüsselung darin bestand, eine superaufsteigende Folge als gewöhnliche Folge zu verschleiern. Prof. Unger fragt nach dem Verfahren. Ich grabe noch irgendwas von Multiplizieren und Modularisieren aus, aber die genaue Formel habe ich nicht im Kopf.

Prof. Unger fragt, wie denn nun das System geknackt wurde.

Antwort: Gitterdefinition, Determinante des Gitters hergeleitet, Problem der kurzen Vektoren erwähnt.

Prof. Unger fragt, da die Zeit praktisch abgelaufen ist, direkt nach dem LLL-Algorithmus. Dieser liefert eine reduzierte Basis. Will das definieren, aber Prof. Unger fragt direkt nach der für das Knacken von Knapsack entscheidenden Eigenschaft: der kurze 1. Vektor, der häufig die Lösung des Knapsack-Problems liefert; um das zu erläutern, Matrix mit den Gittervektoren aufgezeichnet.

Fazit: Frau Prof. Unger ist eine ausgesprochen angenehme Prüferin. Sie ließ mich - im Rahmen der verfügbaren Zeit - selbständig erklären, wo sie Zwischenfragen stellte, hatte das häufig den Charakter eines Wechselgesprächs, nicht von vorbereiteten Prüfungsfragen. Mir kam diese Prüfungsatmosphäre sehr entgegen.

Von den Gebieten des Kurses wurde fast ausschließlich die Kryptosysteme behandelt. Algorithmen-Effizienz brachte ich kurz am Rande zur Sprache, aber ohne alle Definitionen. Algebra kam praktisch nicht vor, außer im letzten Teil bei der Gitter-Definition. Ich sprach Frau Prof. Unger hierauf nach der Prüfung an, und sie meinte, daß sich das so ergeben hat und auch völlig anders laufen könnte.