Computer Algebra

Sebastian Iwanowski
FH Wedel

3. Modulare Arithmetik
3.2. Anwendungen in der Kryptographie

Referenzen zum Nacharbeiten:

Köpf 4.6, 5.5, Kaplan 5 (nur zur Vertiefung, wird hier nicht behandelt)
Seminararbeit 4 (Hendrik Annuth)
Seminararbeit 3, Kapitel 4 (Thomas Stuht)

Computer Algebra 3

Praktische Anwendungen der modularen Arithmetik im Bereich der Kryptographie

Authentifizierung:

Fiat-Shamir-Protokoll

(nutzt das Berechnungsproblem der modularen Quadratwurzel)

Schlüsselaustausch:

Diffie-Hellman-Schlüsselaustausch

(nutzt das Berechnungsproblem des modularen Logarithmus)

aus: Seminarvortrag Annuth

Computer Algebra 3

Praktische Anwendungen der modularen Arithmetik im Bereich der Kryptographie

Das Dilemma der Authentifizierung

1. Ich weiß etwas, das mich authentifiziert
2. Diese Information will ich nicht herausgeben
3. Ich will aber beweisen, dass ich die Information habe

aus: Seminarvortrag Annuth

Computer Algebra 3

Authentifizierung: Fiat-Shamir-Protokoll

1. Ich wähle ein n=p*q für meine Restklassemenge und ein Element s in dieser und quadriere s mod n.
2. Die Zahl s gebe ich unter keinen Umständen preis.
3. Authentifizierung: Ich beweise, dass ich s kenne.

Authentifizierungsprozess:

1. Ich gebe allgemein s^2 mod n und n bekannt
2. Ich gebe zusätzlich zu s^2 und n ein frei gewähltes r^2 mod n bekannt
   Nun darfst du fragen:
   entweder a) Was ist s*r mod n ? → deine Prüfung $(s*r)^2 \equiv s^2 * r^2 (\mathrm{mod}\ n)?$
   oder b) Was ist r mod n ? → deine Prüfung $r_{neu}^2 \equiv r^2 (\mathrm{mod}\ n)?$

3. Wüsste jemand deine Fragen im Voraus,
   könnte er mogeln und sich als mich ausgeben.
   Darum wird Schritt 2 vielfach durchgeführt.

aus: Seminarvortrag Annuth

Computer Algebra 3

Authentifizierung: Fiat-Shamir-Protokoll

1. Ich wähle ein n=p*q für meine Restklassemenge und ein Element s in dieser und quadriere s mod n.
2. Die Zahl s gebe ich unter keinen Umständen preis.
3. Authentifizierung: Ich beweise, dass ich s kenne.

Wie könnte man mogeln?

a) Wenn ich weiß, es wird nach r gefragt,
gebe ich dir irgendein von mir berechnetes r^2
und auf deine Frage, dann das gewählte r
Mein Problem: Die Frage nach s*r könnte ich dann nicht beantworten, da ich s nicht kenne

b) Wenn ich weiß, es wird nach s*r gefragt,
nehme ich eine Zahl a und quadriere sie, multipliziere das
inverse Element von s^2 mit a^2 und gebe dir das Ergebnis als $r^2 = (s^2)^{-1} \bullet a^2$.
Fragst du nach s*r gebe ich dir a. Da $r^2 = (s^2)^{-1} \bullet a^2$, gilt: $s^2*(s^2)^{-1}*a^2 = a^2$
Mein Problem: Die Frage nach r könnte ich nicht beantworten.

aus: Seminarvortrag Annuth

Computer Algebra 3

Praktische Anwendungen der modularen Arithmetik im Bereich der Kryptographie

Das Problem des Schlüsselaustauschs

1. Alice will mit Bob einen geheimen Schlüssel austauschen.
2. Niemand anders darf den Schlüssel kennen.
3. Der Austauschweg ist unsicher.

aus: Seminarvortrag Annuth

Computer Algebra 3

Diffie-Hellman-Schlüsselaustausch

1. Eine Moduluszahl n und ein Element s mod n sei allgemein bekannt.

2. Alice wählt geheim eine natürliche Zahl a und berechnet $s^a \equiv \alpha \pmod{n}$
3. Bob wählt geheim eine natürliche Zahl b und berechnet $s^b \equiv \beta \pmod{n}$

4. Alice und Bob schicken sich gegenseitig α und β zu

5. Alice berechnet nun $\beta^a \equiv s^{ba} \equiv k \pmod{n}$
   und Bob berechnet nun $\alpha^b \equiv s^{ab} \equiv k \pmod{n}$

6. K wird als gemeinsamer Schlüssel verwendet.

Wenn jemand α und β abfängt, wir errechnet er dann a oder b?

$$\log_s \beta \equiv ? \vee \log_s \alpha \equiv ?$$

aus: Seminarvortrag Annuth

Computer Algebra 3

Asymmetrische Verschlüsselung: RSA

Details: Köpf 5.5

Alice stellt öffentlichen Schlüssel e zur Verschlüsselung bereit, behält geheimen Schlüssel d, mit dem sie jede mit e verschlüsselte Nachricht entschlüsseln kann

Bob will Nachricht an Alice senden, Welche nur sie lesen kann.

- wählt zwei große Primzahlen p,q und berechnet $n = p \bullet q$
- berechnet $\varphi = (p-1) \bullet (q-1)$ und wählt e mit $ggt(e,\varphi) = 1$
- berechnet $d = e^{-1} \bmod \varphi$
- gibt n und e öffentlich bekannt, hält d geheim und löscht p,q,φ

d kann effizient berechnet werden, wenn φ bekannt ist.

! *φ ist bekannt, wenn die Faktorisierung von n bekannt ist.* !

- verschlüsselt Nachricht N durch $N^e \bmod n$ und sendet diese Nachricht an Alice.
- entschlüsselt Nachricht $N = (N^e \bmod n)^d \bmod n$

Computer Algebra 3

Entschlüsselung von RSA-Codes:

Faktorisierung ganzer Zahlen

- Probedivision

  mit Test, ob Division überhaupt erfolgversprechend ist
  exponentielle Laufzeit

  Details: Vortrag Stuht Kapitel 4

- Primzahltest

  Rabin-Miller-Test zum Bestimmen, ob Zahl wahrscheinlich Primzahl ist

  Details: Köpf 4.6

- Spezielle Faktorisierungsverfahren für große Faktoren

  sprengt den Rahmen dieser Vorlesung

  Details: Kaplan 5

Asymptotisch effiziente Algorithmen zur Faktorisierung sind nicht bekannt!