Computer Algebra

Sebastian Iwanowski
FH Wedel

3. Modulare Arithmetik
3.2. Anwendungen in der Kryptographie

Referenzen zum Nacharbeiten:

Köpf 5.5

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. Alice weiß etwas, das sie authentifiziert
2. Diese Information will sie nicht herausgeben
3. Sie will aber beweisen, dass sie die Information hat

aus: Seminarvortrag Annuth

Computer Algebra 3

Authentifizierung: Fiat-Shamir-Protokoll

1. Alice wählt ein Modulus n=p*q für eine Restklassemenge und ein zu n teilerfremdes Element s in der Restklassenmenge und berechnet s^2 mod n.
2. Die Zahl s gibt sie unter keinen Umständen preis.
3. Authentifizierung: Sie beweist, dass sie s kennt.

Authentifizierungsprozess:

1. Alice gibt allgemein s^2 mod n und n bekannt, aber nicht die Faktorisierung von n.
2. Alice gibt zusätzlich zu s^2 und n ein frei gewähltes, aber zu n teilerfremdes r^2 mod n bekannt.
   Nun darf Bob fragen:
   entweder a) Was ist s*r mod n ? → Bobs Prüfung $(s*r)^2 \equiv s^2 * r^2 (\mathrm{mod}\ n)?$
   oder b) Was ist r mod n ? → Bobs Prüfung $r_{neu}^2 \equiv r^2 (\mathrm{mod}\ n)?$

3. Wüsste Malloy die Fragen von Bob im Voraus, könnte er mogeln und sich als Alice ausgeben. Darum wird Schritt 2 vielfach durchgeführt.

aus: Seminarvortrag Annuth

Computer Algebra 3

Authentifizierung: Fiat-Shamir-Protokoll

1. Alice wählt ein Modulus n=p*q für eine Restklassemenge und ein zu n teilerfremdes Element s in der Restklassenmenge und berechnet s^2 mod n.
2. Die Zahl s gibt sie unter keinen Umständen preis.
3. Authentifizierung: Sie beweist, dass sie s kennt.

Wie könnte Malloy mogeln?

a) Wenn Malloy weiß, es wird nach r gefragt,
gibt er Bob irgendein von Malloy berechnetes r^2
und auf Bobs Frage dann das gewählte r
Malloys Problem: Die Frage nach s*r könnte er nicht beantworten, da er s nicht kennt

b) Wenn Malloy weiß, es wird nach s*r gefragt,
nimmt er eine Zahl a, quadriert sie, multipliziert das inverse Element von s^2 mit a^2
und gibt Bob das Ergebnis als $r^2 = (s^2)^{-1} \bullet a^2$.
Fragt Bob nach s*r, so antwortet er mit a. Da $r^2 = (s^2)^{-1} \bullet a^2$, gilt: $s^2*(s^2)^{-1}*a^2 = a^2$
Malloys Problem: Die Frage nach r könnte er 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 $N = (N^e \bmod n)^d \bmod n$