Computer Algebra

Sebastian Iwanowski
FH Wedel

3. Modular Arithmetic
3.2. Applications in Cryptography

Referenzen zum Nacharbeiten:

Köpf 5.5
Dankmeier – Zusatz (Handout-Server)

Computer Algebra 3

Practical applications of modular arithmetic

Authentification:

Fiat-Shamir Scheme

(utilises the difficulty of computing the modular square root)

Key exchange:

Diffie-Hellman Key Exchange

(utilises the difficulty of computing the modular logarithm)

Computer Algebra 3

Practical applications of modular arithmetic

The dilemma of authentification

1. Alice knows something which identifies her.
2. She will not show this knowledge in order to prevent that others pretend her identity.
3. But she wants to prove that she has got this knowledge.

from: Seminarvortrag Annuth

Computer Algebra 3

Authentification: Fiat-Shamir Scheme

1. Alice chooses a modulus n=p*q for a residue class and an element s which is coprime to n and computes s^2 mod n.
2. The number s is her secret she will never reveal.
3. Authentification: Alice proves that she knows s.

Authentification process:

1. Alice publishes s^2 mod n and n, but not the prime factors p and q of n.
2. Alice additionally posts an r^2 mod n which is coprime to n.
   Now Bob may ask:
   either a) What is s*r mod n ? → Bob‘s test $(s*r)^2 \equiv s^2 * r^2 (\text{mod } n)$?
   or b) What is r mod n ? → Bob‘s test $r_{neu}^2 \equiv r^2 (\text{mod } n)$?

3. If Malloy knew Bob‘s queries in advance,
   he could cheat and pretend to be Alice.
   This is why step 2 is executed several times.

Computer Algebra 3

Authentification: Fiat-Shamir Scheme

1. Alice chooses a modulus n=p*q for a residue class and an element s which is coprime to n and computes s^2 mod n.
2. The number s is her secret she will never reveal.
3. Authentification: Alice proves that she knows s.

How can Malloy cheat?

a) If Malloy knows that r is queried,
he may post any r^2 and answer Bob‘s query with the chosen r
Malloy‘s problem: He could not answer the query for s*r because he does not know s.

b) If Malloy knows that s*r is queried,
he may choose any number a, compute a^2, multiply the inverse of s^2 with a^2
und post the result $r^2 = (s^2)^{-1} \bullet a^2$.
If Bob asks for s*r, Malloy answers with a. Since $r^2 = (s^2)^{-1} \bullet a^2$, we get: $s^2 * (s^2)^{-1} * a^2 = a^2$
Malloy‘s problem: He could not answer the query for r.

Computer Algebra 3

Practical applications of modular arithmetic

The problem of key exchange via internet

1. Alice wants to exchange keys with Bob.
2. Nobody else should be eligible to use the keys.
3. The exchange channel is unsafe.

from: Seminarvortrag Annuth

Computer Algebra 3

Diffie-Hellman key exchange

1. Let the modulus n and an element s mod n be public.

2. Alice chooses a private positive integer a and computes $s^a \equiv \alpha (\text{mod } n)$
3. Bob chooses a private positive integer a and computes $s^b \equiv \beta (\text{mod } n)$

4. Alice and Bob exchange α and β via the unsafe channel.

5. Alice computes $\beta^a \equiv s^{ba} \equiv k (\text{mod } n)$
   Bob computes $\alpha^b \equiv s^{ab} \equiv k (\text{mod } n)$

6. k is the common key.

If somebody captures α and β, how should one get a or b?

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

Computer Algebra 3

Asymmetric cryptography: RSA

Details: Köpf 5.5

Alice provides public key e and keeps private key d which serves to decrypt any message encrypted by e

Bob wants to send a message to Alice which only she can read.

- chooses two primes p,q and computes n = p • q
- computes φ = (p-1) • (q-1) and chooses e where gcd(e,φ) = 1
- computes d = e^{-1} mod φ
- publishes n and e, keeps d in secret and deletes p,q,φ

> *d may be computed efficiently, when φ is known.*
>
> **!** *φ is known when the prime factors of n are known.* **!**

- encrypts N by N^e mod n and sends this message to Alice.

- decrypts N = (N^e mod n)^d mod n