Aspects of ICT for Science: Computer Algebra and Modern Cryptography

Prof. Dr. Wolfram Koepf

Universität Kassel
http://www.mathematik.uni-kassel.de/~koepf

July 30, 2008
Yaounde, Cameroon

Abstract

Topics of This Talk

- The internet is an open system and therefore completely unsecure.
- Therefore, in principle, everybody can wiretap everything.
- How can the internet—nevertheless—be used for such personal things like banking?
- Further applications of modern cryptography are discussed.
- Modern cryptography uses important mathematical algorithms.
- An implementation of the RSA cryptographic system is demonstrated.

Summary

- Secure Cryptography
- Cryptography in the Internet
- Mathematics Behind RSA
- Diffie-Hellman Key Exchange
- Error-Correcting Codes

What is Cryptography?

Cryptography

- With a cryptographic system a message M is encrypted using an encryption function E and a key e:

$$C = E_e(M) \ .$$

  The result C is called cryptogram.

- Decoding is realized by the (corresponding) decryption function D and a key d:

$$D_d(C) = D_d(E_e(M)) = M \ .$$

- The functions E and D should be efficiently computable.
- An important problem is the key exchange.

Asymmetric Cryptography and RSA

Asymmetric = Public-Key Cryptography

- The RSA cryptographic system developed by Rivest, Shamir and Adleman (1978) is an example of an asymmetric cryptographic scheme. Internet Check
- Such procedures were introduced in 1976 by Diffie and Hellman. Internet Check
- For these methods sender and recipient each use their own keys e and d.
- The keys e are made public, whereas the keys d remain secret.
- For such public-key systems exchange of the respective personal decoding keys is therefore not necessary.

Asymmetric Cryptography and RSA

Where is the RSA method utilized?

- The RSA method is used for the login on a remote computer (secure shell (`ssh`)).
- RSA is hidden behind secure e-mail with PGP (Pretty Good Privacy). Internet Check
- It is used for secure data transfer on secure web sites (`https`), for example for online banking. Internet Check
- Hence: Internet shopping and online banking (with `https`!) can be really safe.
- However, be sure to use a Secure Password!
- We would like to test the RSA method. ...RSA Test

Prime Number Test

Fermat's Little Theorem

- For a prime number $p \in \mathbb{P}$ and $a \in \{1, \ldots, p-1\}$ the relation
$$a^p = a \pmod{p}$$
is valid.
- This means that integer division of a^p by p (the modulus) has always the remainder a.

Fermat Test

If this relation is *not* valid for a number $a \in \mathbb{Z}$, then p cannot be a prime number! *Mathematica*

Efficient Computation of Powers

Divide and Conquer Algorithm

- To utilize the Fermat test, modular powers should be computed very efficiently.
- The modular power $a^n \pmod{p}$ is computed efficiently by reducing powers of size n to powers of size $n/2$.
- Such a method is called a *Divide and Conquer Algorithm*.
- Recursive formulation of this algorithm:
  - $a^0 \mod p = 1$
  - $a^n \mod p = (a^{n/2} \mod p)^2 \mod p$ for even n
  - $a^n \mod p = (a^{n-1} \mod p) \cdot a \mod p$ for odd n
- *Mathematica*

Connection with RSA

Mathematics of RSA

- RSA-encryption is given by the function (*e* and *n* public)

$$C = E(M) = M^e \pmod{n} .$$

- The number $n = p \cdot q$ is the product of two secret primes.
- RSA-decryption is carried out by (*d* private)

$$D(C) = C^d \pmod{n} .$$

- Fermat's Little Theorem guarantees that $D(E(M)) = M$.
- Knowing the factors p and q, then d is computable from e.
- RSA is secure if it is true that factorization of large integers is a very hard mathematical problem.

RSA Factoring Challenge

RSA Numbers

- To prove the difficulty of integer factorization the RSA Laboratories set up the RSA Factoring Challenge in 1991.
- The group around Jens Franke of Bonn University solved four of these problems and received two prices of 10.000 US$ and 20.000 US$, respectively.
- The record is the factorization of a 200 decimal digit.
- To establish such a record thousands of PCs are used in parallel for several months, and the best available algorithms are needed.

Diffie-Hellman Key Exchange

Modular Logarithm

- The inverse of the real exponential function $x \mapsto 2^x$ is simple to compute.
- The inverse of the integer exponential function $x \mapsto 2^x$ is also simple to compute.
- However, the inverse of the modular exponential function $x \mapsto 2^x \pmod{p}$ is difficult to compute. *Mathematica*
- The Diffie-Hellman key exchange is secure if the discrete modular logarithm is a very hard mathematical problem.

Diffie-Hellman Key Exchange

Protocol of Diffie-Hellman Key Exchange (1976)

- Anna and Barbara want to exchange a common key. They choose numbers $g \in \mathbb{N}$ and $p \in \mathbb{P}$. These can be assumed to be public.

A chooses $a < p$	B chooses $b < p$
A computes $\alpha := g^a \mod p$	B computes $\beta := g^b \mod p$
A sends α to B	B sends β to A
A computes $s := \beta^a \mod p$	B computes $t := \alpha^b \mod p$

Correctness of algorithm

$$s = \beta^a = (g^b)^a = (g^a)^b = \alpha^b = t\,.$$

Error-Correcting Codes

Why do we need this?

- We have seen that for cryptography it is essential that transmission is realized without any errors.
- A scratched music CD can contain hundreds of thousands of read errors!
- Without error correcting codes you could not at all enjoy the music.
- After error correction a music CD must be completely error free!
- Similarly deep space telecommunications with spacecrafts, satellite broadcasting of TV programs, computer hard drives and RAID systems etc. all need error-correction.

Error-Correcting Codes

Error-Correcting Codes

- For an error-correcting code two bytes might be added to a sequence of bytes (a block) that satisfy two conditions.
- Testing both conditions, one can detect
  - at which position an error occured,
  - and how large the error is.
- Therefore one can correct one error.
- In an analogous manner with more complicated error-correcting codes one can correct several errors per block by adding more redundancy.
- As an example, I have implemented a 2-correcting Reed-Solomon Code. *Mathematica*

Many Thanks for Your Interest!