CrypTool

A free software program

- **for creating awareness of IT security issues**
- **for learning about and obtaining experience of cryptography**
- **for demonstrating encryption algorithms and analysis procedures**

www.cryptool.de
www.cryptool.com
www.cryptool.org

Claudia Eckert / Thorsten Clausius
Bernd Esslinger / Jörg Schneider / Henrik Koy

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Contents

TECHNISCHE UNIVERSITÄT DARMSTADT

Introduction

1. What is CrypTool?

- a freeware Program with graphical user interface
- a tool for applying and analysing cryptographic algorithms
- with extensive online help, understandable without deep crypto knowledge
- contains nearly all state of the art crypto algorithms
- "playful" introduction to modern and classical cryptography
- not a "hacker tool"

2. Why CrypTool?

- origin in Deutsche Bank's IT security awareness program
- developed in co-operation with universities
- improve IT security related courses in universities and companies

3. Audience

- target group: students of computer science, commercial IT and mathematics
- also aimed at: interested computer users and application developers
- prerequisites: secondary school mathematics or programming skills

TECHNISCHE UNIVERSITÄT DARMSTADT

CrypTool Overview
1. Features

Cryptography

Classical algorithms

- Caesar
- Vigenère
- Hill
- Monoalphabetic substitution
- Homophonic substitution
- Playfair
- Permutation
- Addition
- XOR
- Vernam

To facilitate performing text book examples with CrypTool

- alphabet can be configured
- treatment of white space etc. configurable

Cryptanalysis

Attacks on classical algorithms

- ciphertext only
  - Caesar
  - Vigenère
  - Addition
  - XOR
- known plaintext
  - Hill
  - Playfair
- manual
  - mono-alphabetic substitution

Supporting analysis procedures

- entropy, floating frequency
- histogram, n-gram analysis
- auto-correlation
- ZIP compression test

CrypTool Overview
1. Features

Cryptography

Modern symmetric algorithms
- IDEA, RC2, RC4, DES, 3DES
- last round AES candidates
- AES (=Rijndael)

Asymmetric algorithms
- RSA with X.509 certificates
- RSA demonstration
  - to facilitate performing text book examples with CrypTool
  - alphabet and block length configurable

Hybrid encryption
- RSA combined with AES encryption
- visualised by an interactive data flow diagram

Cryptanalysis

Brute-force attack on symmetric algorithms
- implemented for all algorithms
- assumption:
  entropy of the plain text is small

Attack on RSA encryption
- factor RSA modulus
- workable for bit lengths <= 250

Attack on hybrid encryption
- attack on RSA (see below) or
- attack on AES (see above)

CrypTool Overview
1. Features

Cryptography

Digital Signature
- RSA with X.509 certificates
  - signature procedure visualised by an interactive data flow diagram
- DSA with X.509 certificates
- Elliptic curve DSA, Nyberg-Rueppel

Hash functions
- MD2, MD4, MD5
- SHA, SHA-1, RIPEMD-160

Random generators
- SECUDE
- X^2 modulo N
- Linear Congruence Generator (LCG)
- Inverse Congruence Generator (ICG)

Cryptanalysis

Attack on RSA Signature
- RSA modulus factorisation
- workable up to approx. 250 bit

Attack on hash function/digital signature
- Generation of hash collisions to ASCII texts

Random data analysis
- FIPS-PUB-140-1 test battery
- periodicity, Vitany, entropy
- histogram, n-gram analysis
- auto-correlation
- ZIP compression test

TECHNISCHE UNIVERSITÄT DARMSTADT

CrypTool Overview
2. Software package contents

completely bilingual
English
German

CrypTool program
- all functions integrated in *one* program with uniform graphical user interface
- platforms: Win32 and Linux with WINE emulator
- cryptography based on Secude library (www.secude.com)
- arbitrary precision arithmetic: Miracl library (http://indigo.ie/~mscott/)

AES-Tool
- standalone program for AES encryption (self extracting)

Extensive online help (Winhelp)
- context sensitive online help for *all* program functions and all menu items
- detailed examples of usage for many program features

Script (PDF) with background information on
- encryption algorithms • prime numbers • digital signature
- elliptic curves • public key certification • elementary number theory

Short story "Dialogue of the Sisters" by Dr. C. Elsner

CrypTool Overview
3. New in release 1.3.xx

Most important changes (details: see ReadMe-en.txt):

Release 1.3.00 published January 2002

- completely bilingual English/German
- improved dialog box consistency and comprehensibility
- Windows 9x file size limit removed
- homophonic and permutation encryption
- random generators, random data analysis (FIPS-140-1, periodicity, n-gram)
- AES-Tool: create self-decrypting files (AES)
- demonstration: number theory and RSA crypto system (further improved in 1.3.02)
- PKCS#12 export/import for PSEs

Release 1.3.02 published June 2002

- visualisation of hybrid encryption and decryption
- visualisation of signature creation and verification
- hash value calculation of large files (without loading them into memory)
- visualisation of the sensitivity of hash functions to changes in the hashed data
- short story “Dialogue of the Sisters” by Dr. C. Elsner included

TECHNISCHE UNIVERSITÄT DARMSTADT

CrypTool Overview
3. New in release 1.3.xx

Release 1.3.04 published June 2003

- visualisation of Diffie-Hellman key exchange
- attack on digital signature using hash-collisions (birthday paradox)
- brute-force attack on symmetric ciphers improved
- script updated (primes, factorization) and extended (hash functions, ECC, CrypTool menu tree)
- many small improvements (especially online help) and bug fixes

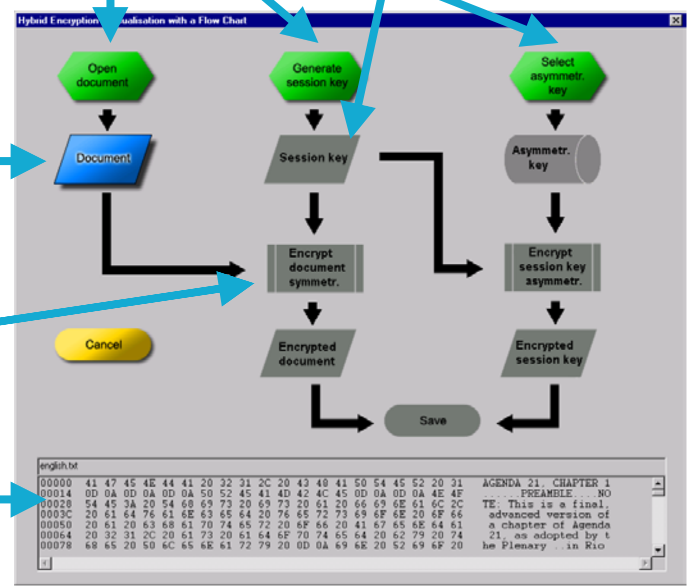
Examples of use
1. Hybrid encryption visualised

Hybrid encryption

- combines advantages of symmetric and asymmetric encryption
  - speed
  - simple and scalable key management
- widely used in practice
  - e-mail (S/MIME, PGP) and file encryption
  - SSL (https)

Visualisation by an interactive data flow diagram

- playful learning leads to deeper understanding



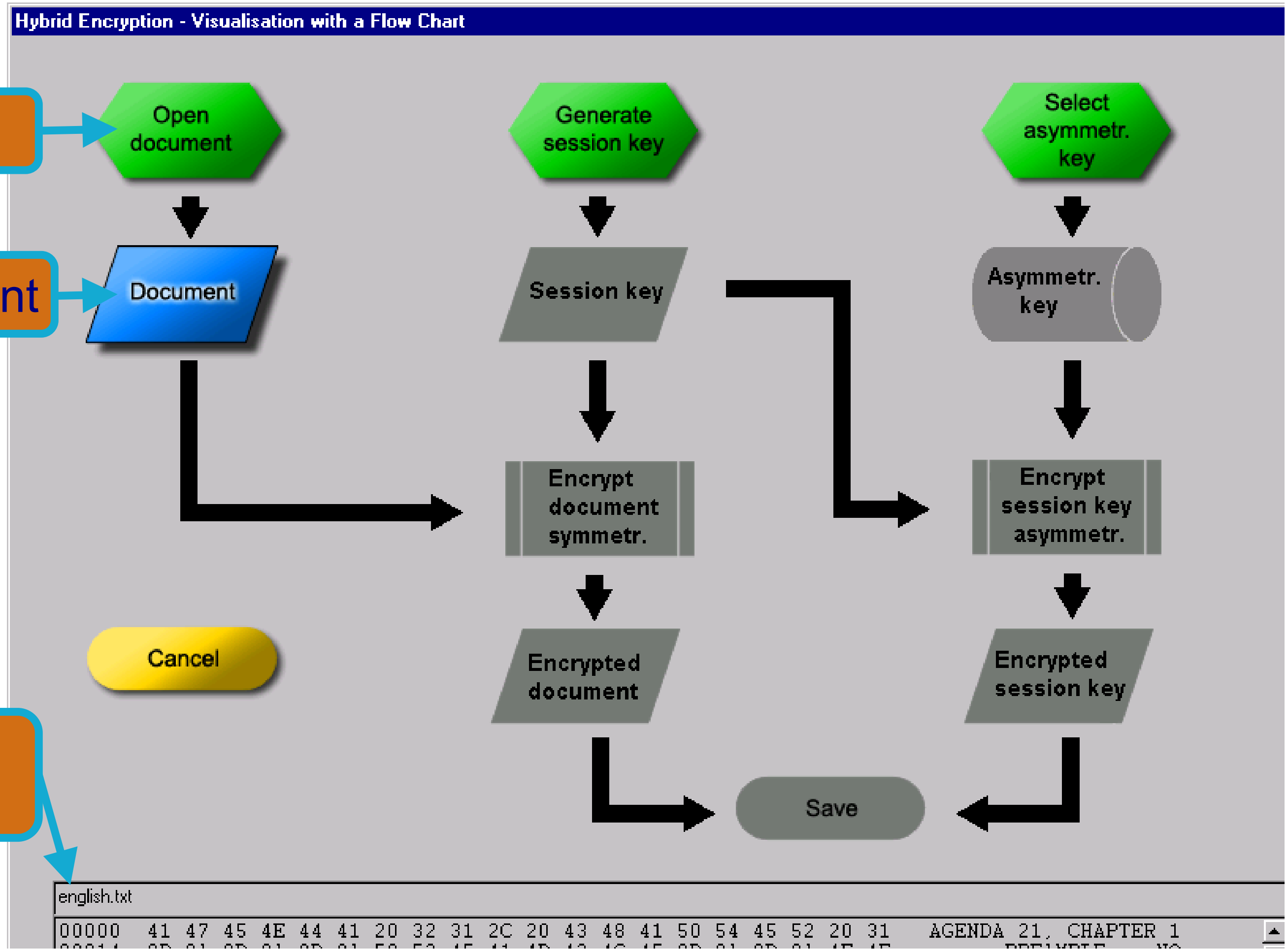
TECHNISCHE UNIVERSITÄT DARMSTADT

Examples of use
1. Hybrid encryption visualised: Preparation

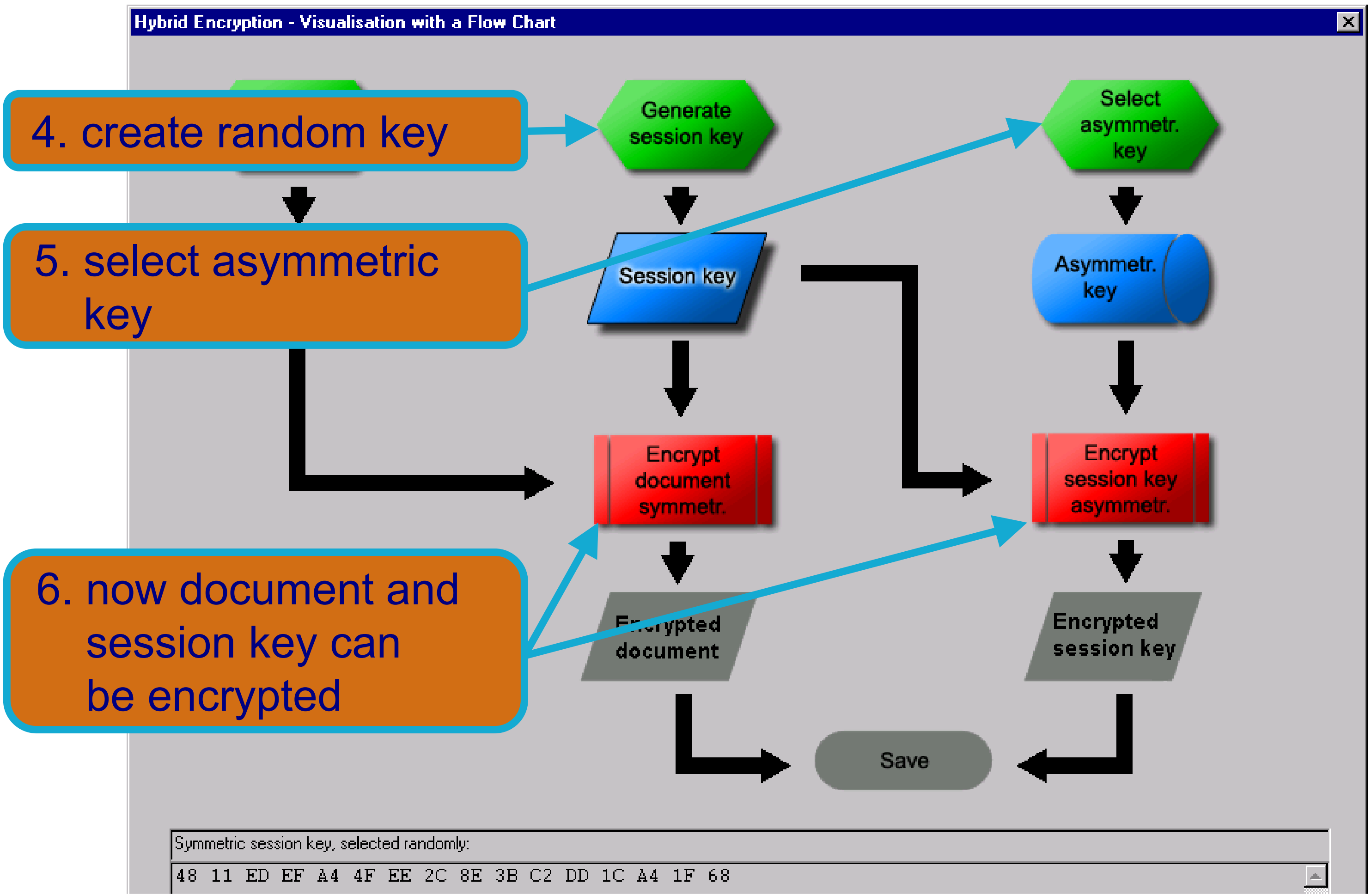
1. select file

2. click on document

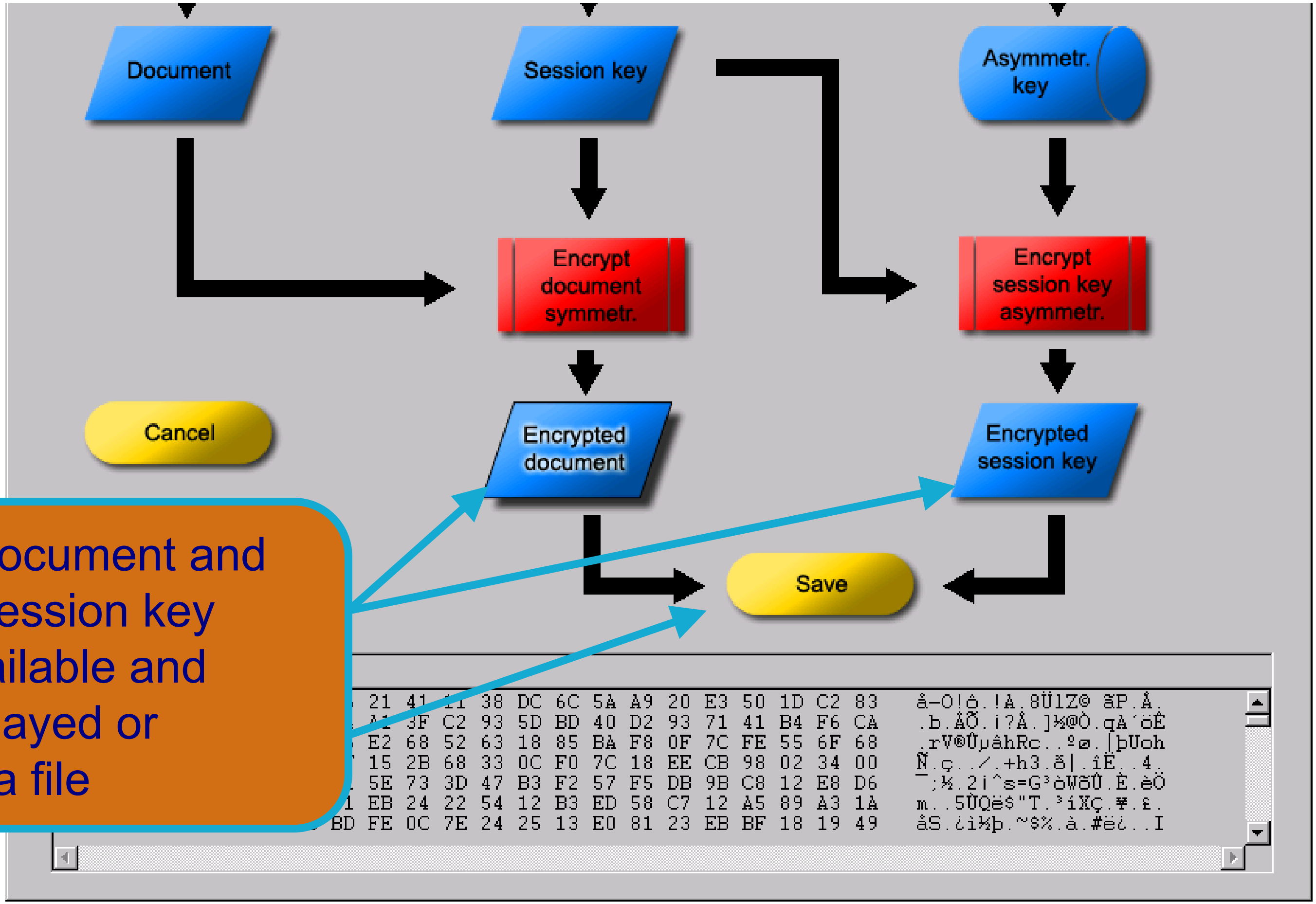
3. contents displayed here



Examples of use
1. Hybrid encryption visualised: Cryptography



Examples of use
1. Hybrid encryption visualised: Result



7. encrypted document and encrypted session key are now available and can be displayed or written into a file

TECHNISCHE UNIVERSITÄT DARMSTADT

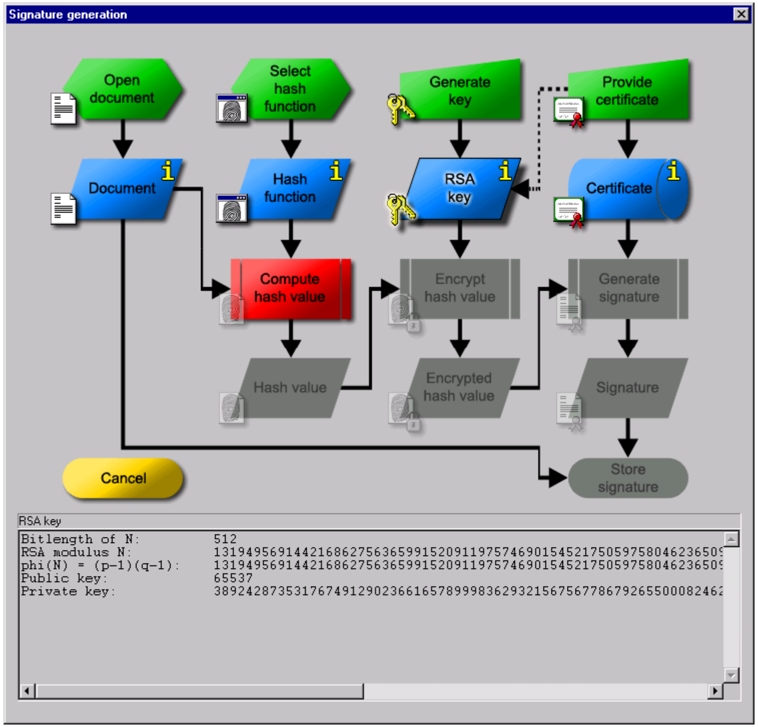
Examples of use
2. Digital signature visualised

Digital signature

- increasingly important
  - equivalence with manual signature (digital signature law)
  - increasingly used by industry, government and consumers
- few people know how it works

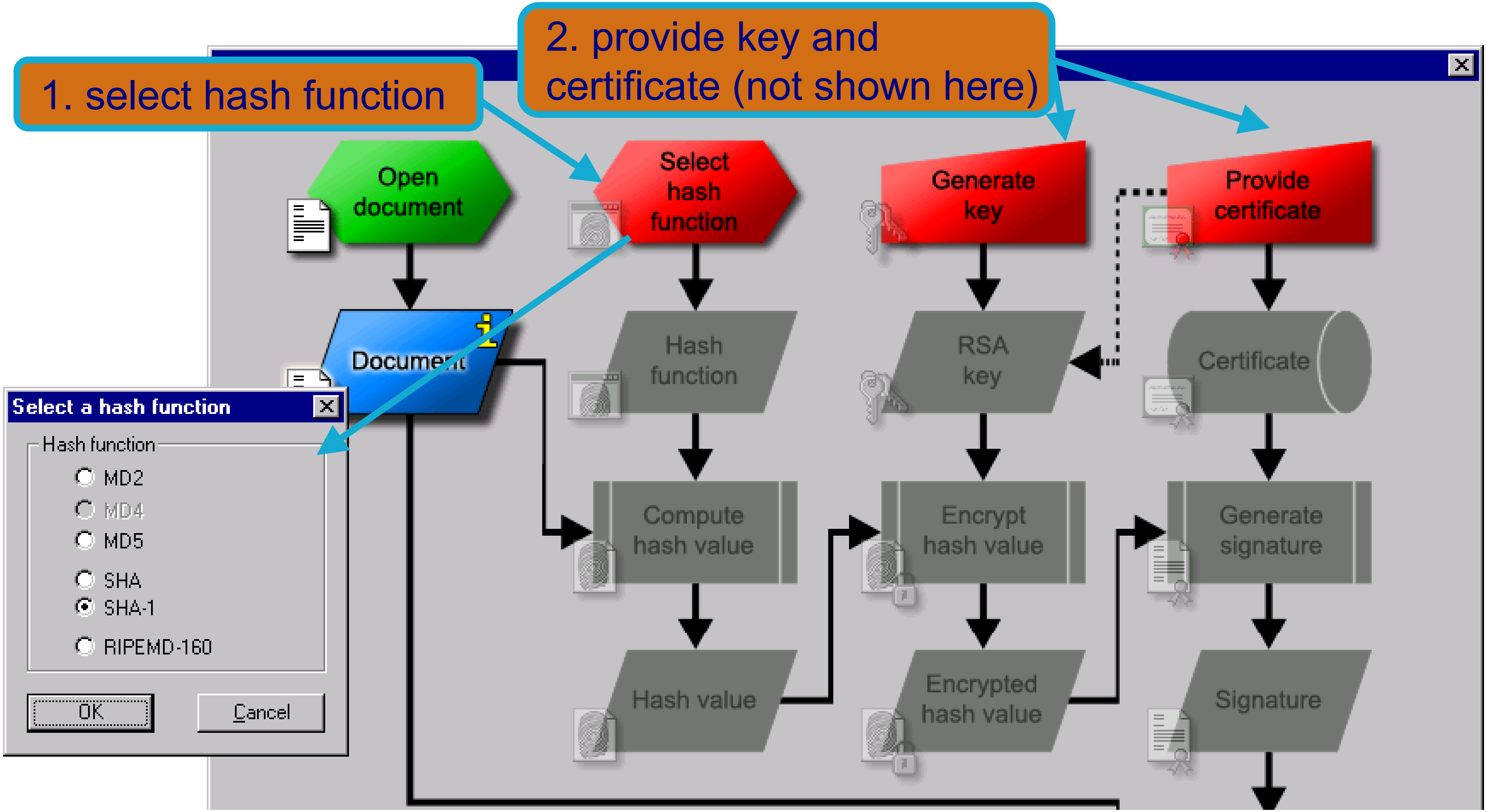
Visualisation in CrypTool

- interactive data flow diagram
- similar to the visualisation of hybrid encryption



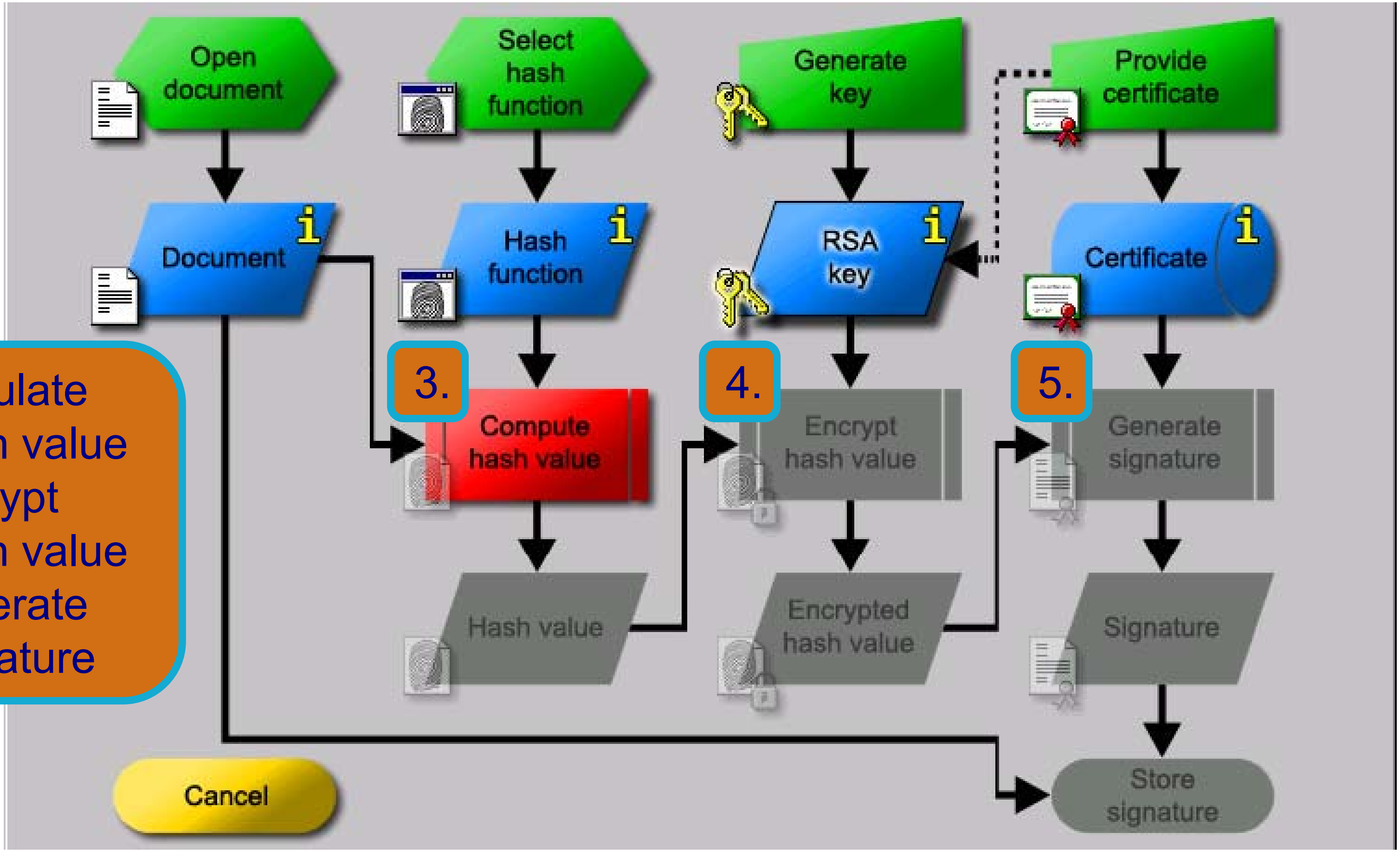
TECHNISCHE UNIVERSITÄT DARMSTADT

Examples of use
2. Digital signature visualised: Preparation



TECHNISCHE UNIVERSITÄT DARMSTADT

Examples of use
2. Digital signature visualised: Cryptography

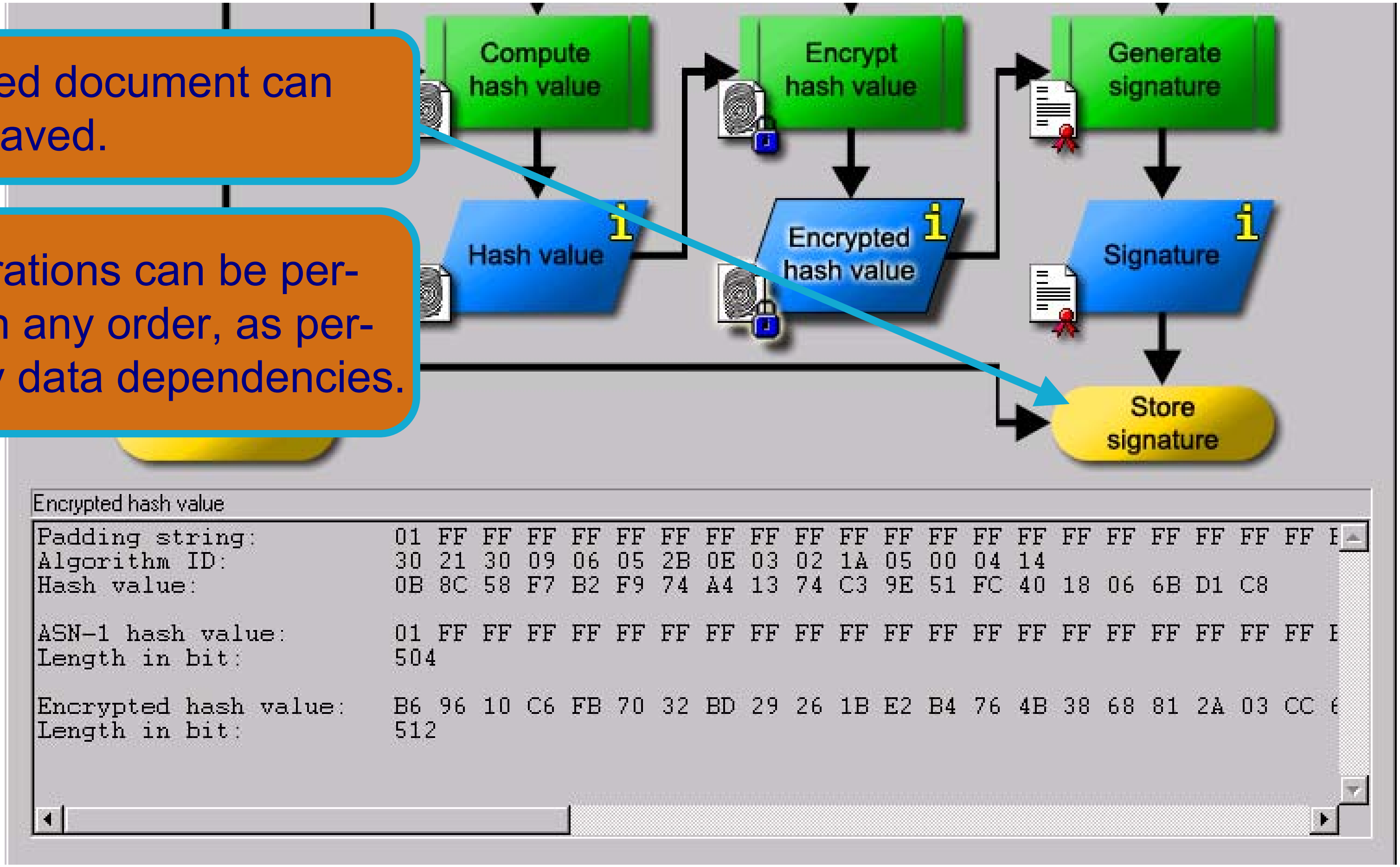


3. calculate hash value
4. encrypt hash value
5. generate signature

Examples of use
2. Digital signature visualised: Result

The signed document can now be saved.

The operations can be performed in any order, as permitted by data dependencies.



TECHNISCHE UNIVERSITÄT DARMSTADT

Examples of use
3. Attack on RSA encryption with short RSA modulus

Example from *Song Y. Yan*, Number Theory for Computing, Springer, 2000

- public key
  - RSA modulus N = 63978486879527143858831415041 (95 bit, 29 decimal digits)
  - public exponent e = 17579
- cipher text (block length = 14):
  - C_1 = 45411667895024938209259253423,
    C_2 = 16597091621432020076311552201,
    C_3 = 46468979279750354732637631044,
    C_4 = 32870167545903741339819671379
- the text shall be deciphered!

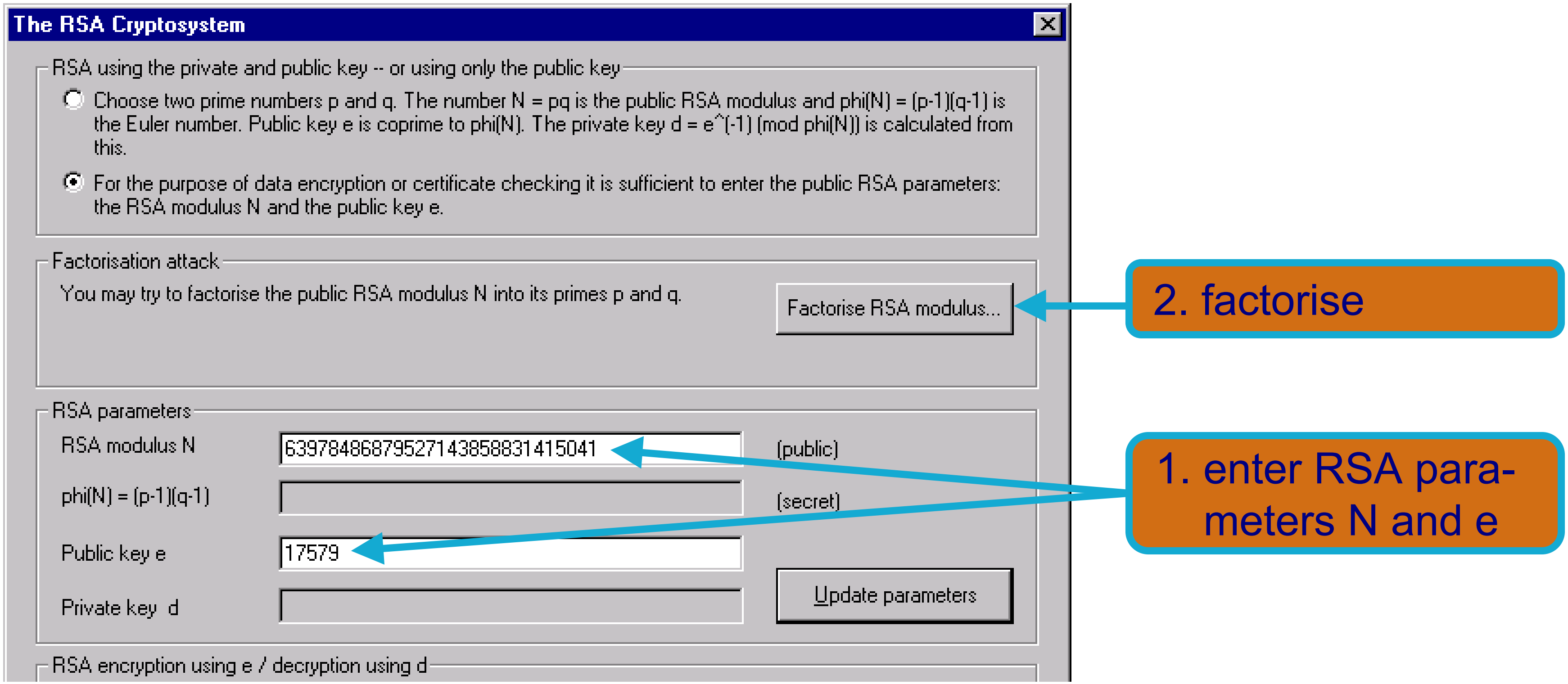
Solution using CrypTool (more detailed in online help examples section):

- enter public parameters into "RSA cryptosystem" (menu indiv. procedures)
- button "factorise the RSA modulus" yields prime factors pq = N
- based on that information private exponent $d=e^{-1} \bmod (p-1)(q-1)$ is determined
- decrypt the cipher text with d: $M_i = C_i^d \bmod N$

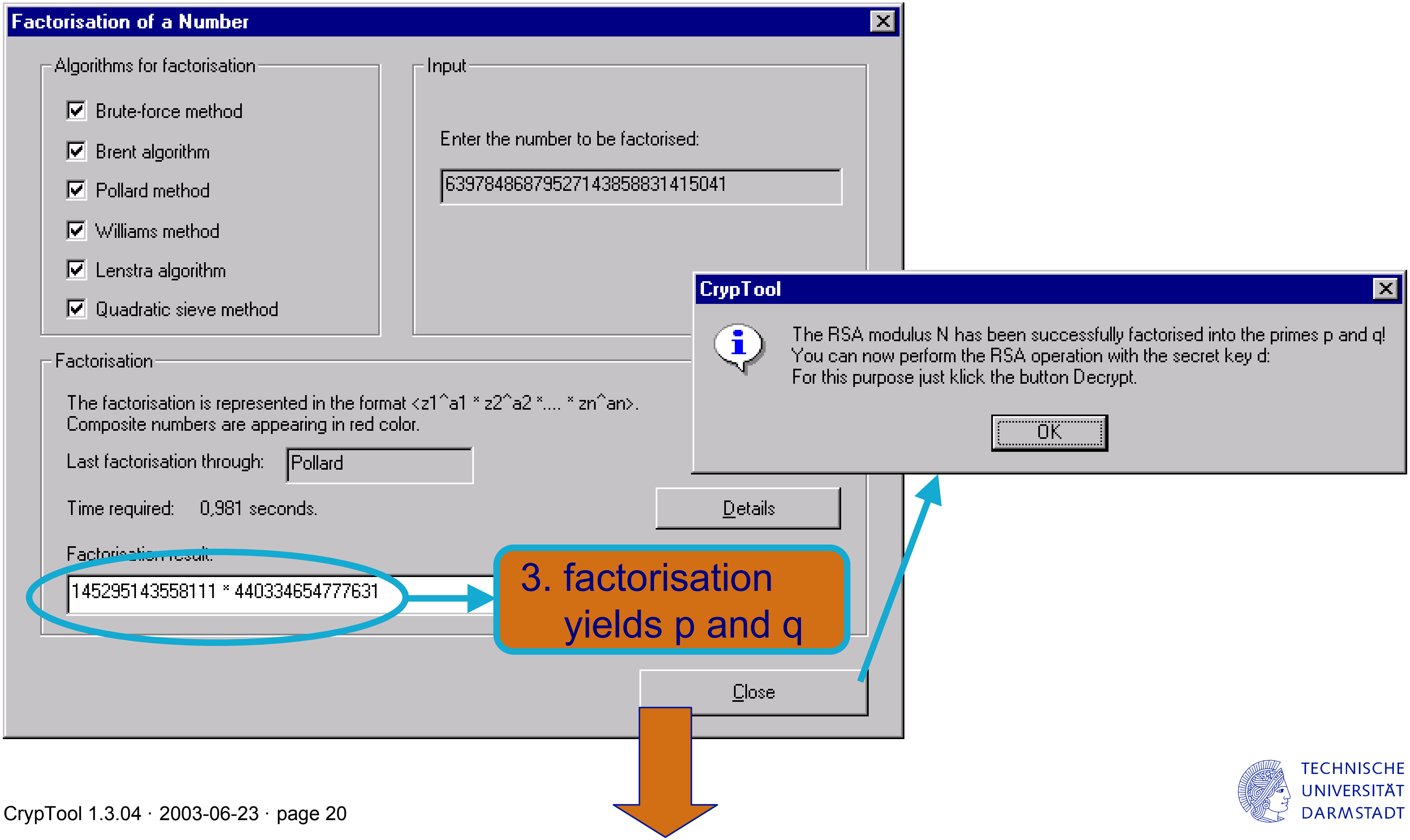
The attack with CrypTool is workable for RSA moduli up to 250 bit

TECHNISCHE
UNIVERSITÄT
DARMSTADT

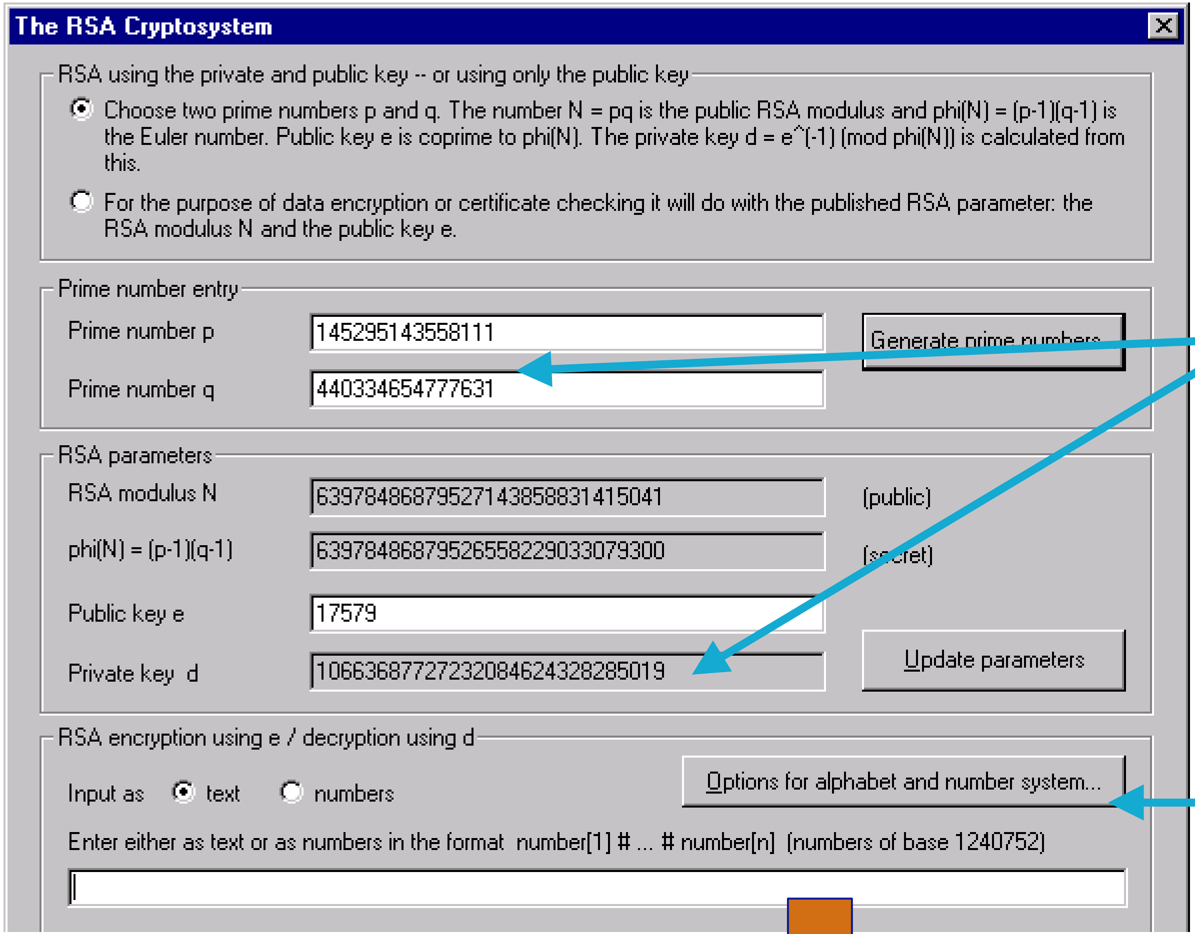
Examples of use:
3. Short RSA modulus: enter public RSA parameters



Examples of use:
3. Short RSA modulus: factorise RSA modulus



Examples of use:
3. Short RSA modulus: determine private key d

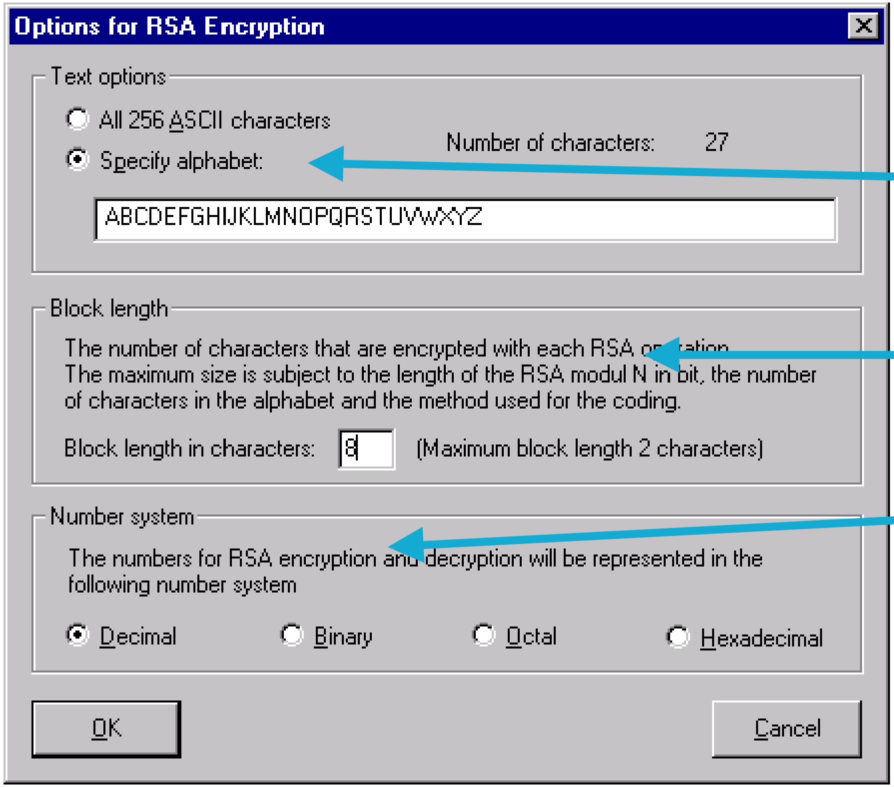


4. p and q have been entered automatically and secret key d has been calculated

5. adjust options

TECHNISCHE UNIVERSITÄT DARMSTADT

Examples of use:
3. Short RSA modulus: adjust options

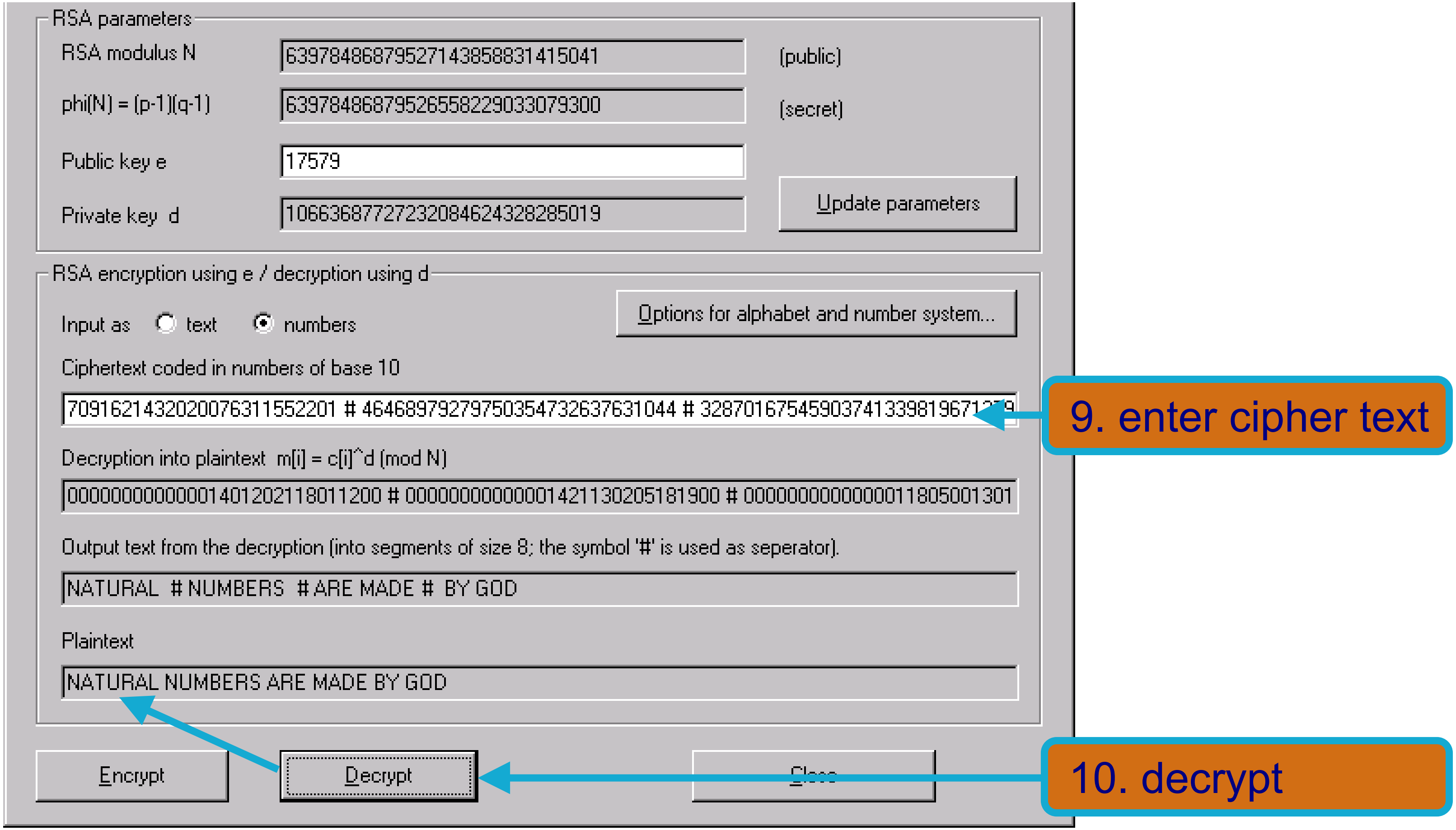


6. select alphabet

7. select coding method

8. select block length

Examples of use:
3. Short RSA modulus: decrypt cipher text



TECHNISCHE UNIVERSITÄT DARMSTADT

Examples of use
4. Analysis of encryption used in the PSION 5 PDA

Attack on the encryption option in the PSION 5 PDA word processing application

Starting point: an encrypted file on the PSION

Requirements

- encrypted English or German text
- depending on method and key length, 100 bytes up to several kB of text

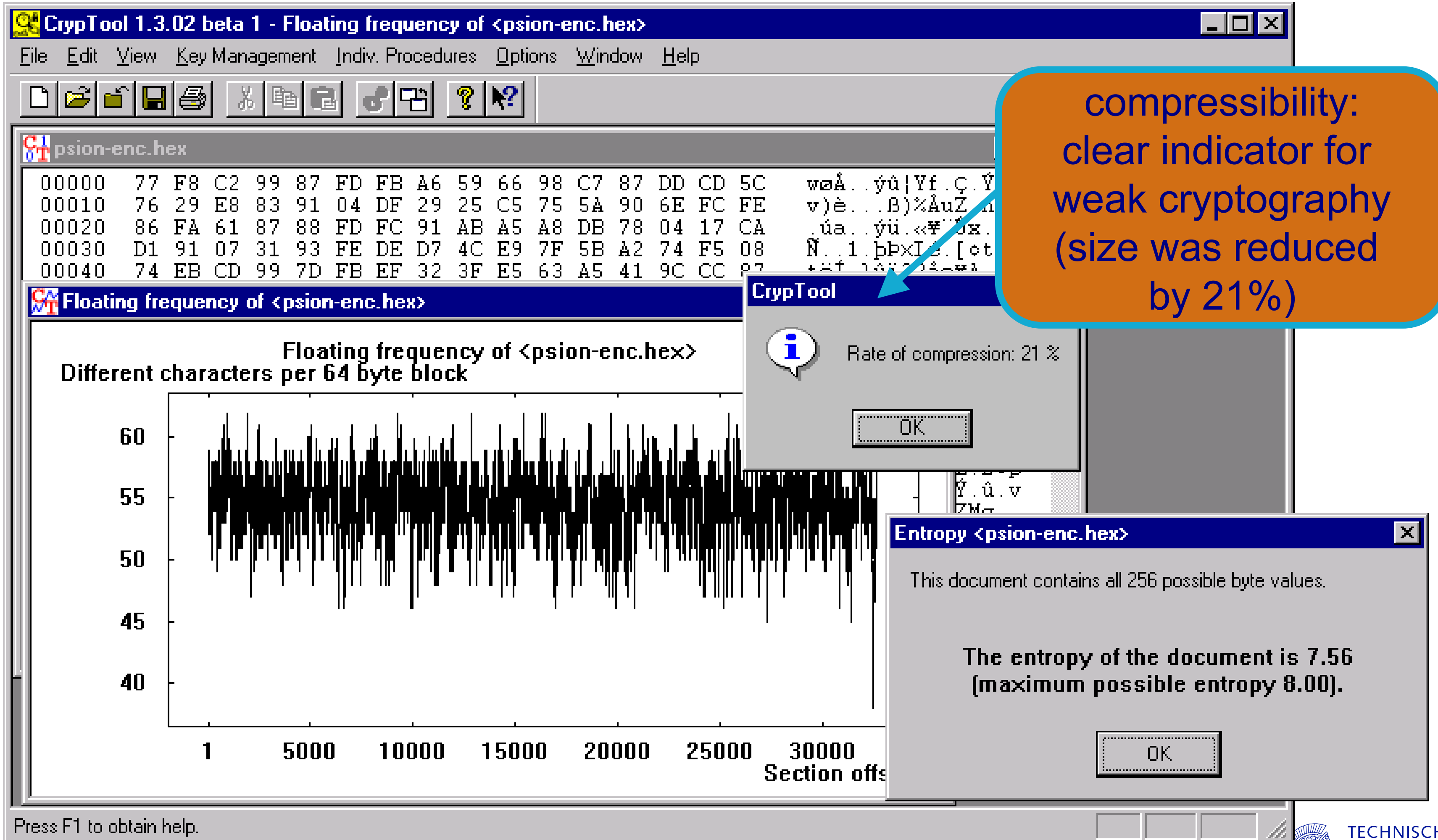
Procedure

- pre-analysis
  - entropy
  - floating entropy
  - compression test

  $\Rightarrow$ probably classical encryption algorithm
- auto-correlation
- try out automatic analysis with classical methods

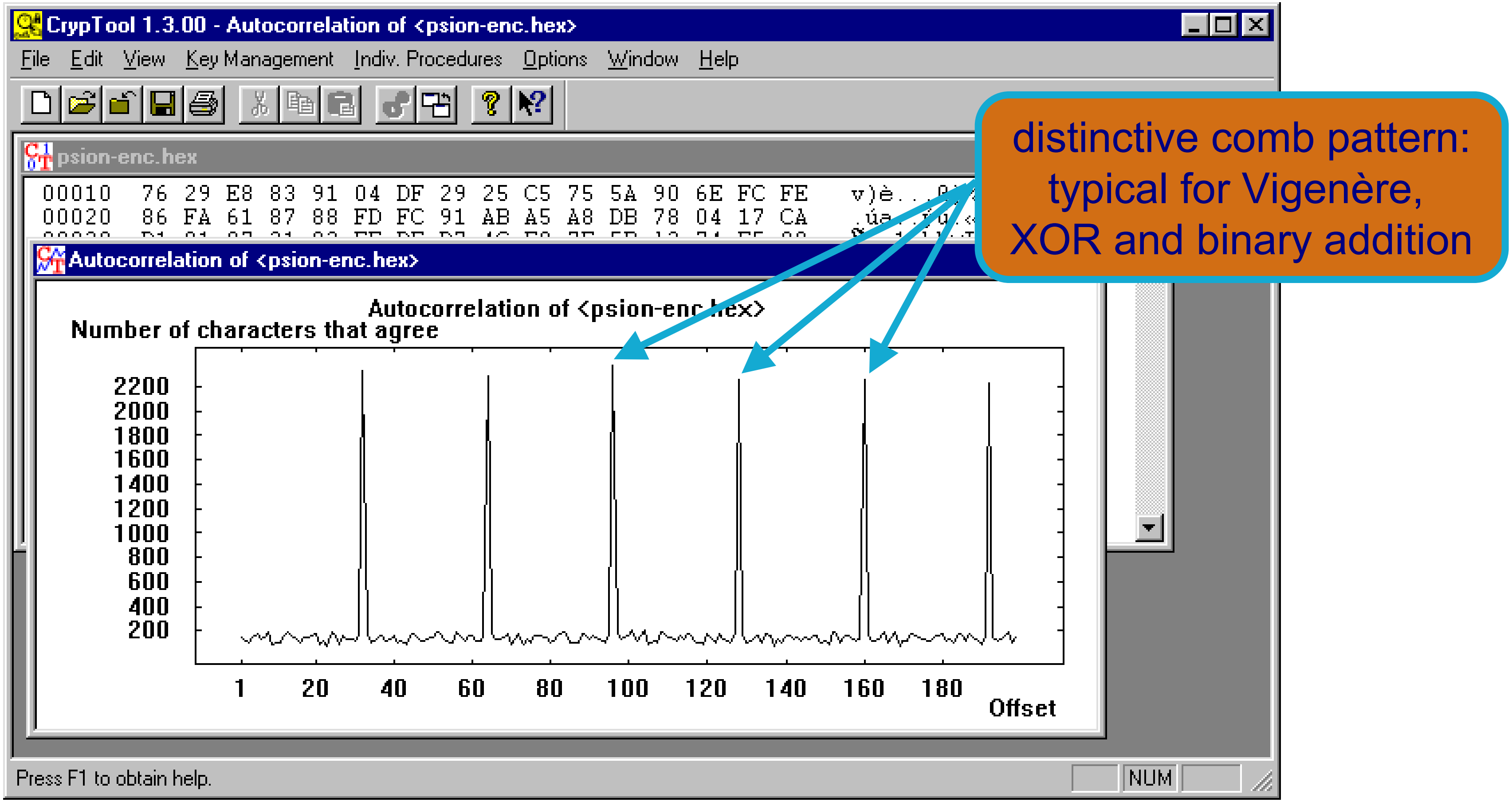
TECHNISCHE UNIVERSITÄT DARMSTADT

Examples of use
4. PSION PDA: determine entropy, compression test



TECHNISCHE UNIVERSITÄT DARMSTADT

Examples of use
4. PSION PDA: determine auto-correlation



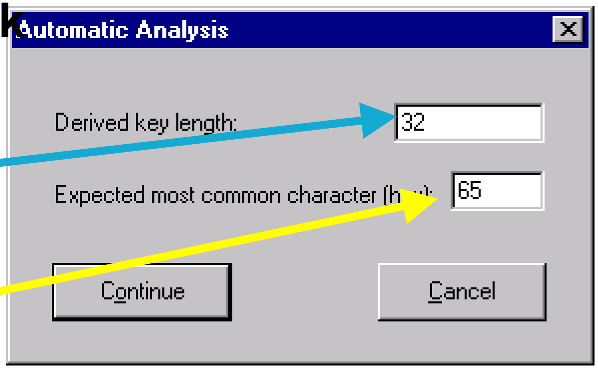
TECHNISCHE UNIVERSITÄT DARMSTADT

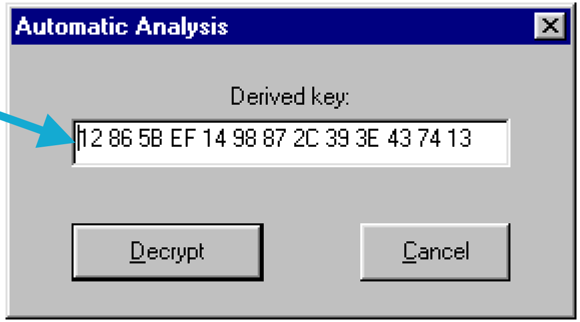
Examples of use
4. PSION PDA: automatic analysis

Automatic analysis using XOR: does not work

Automatic analysis using Binary Addition:

- CrypTool calculates the key length using auto-correlation: 32 bytes
- The user can choose which character is expected to occur most frequently: "e" = 0x65 (ASCII code)
- Analysis calculates the most likely key (based on the assumptions about distribution)
- Results: good, but not perfect



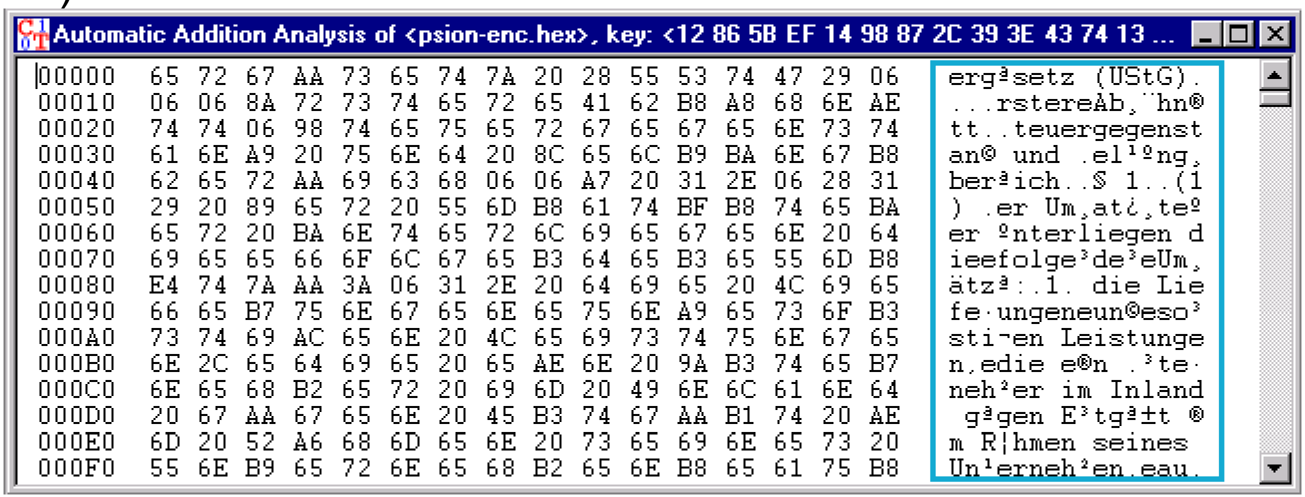


TECHNISCHE UNIVERSITÄT DARMSTADT

Examples of use
4. PSION PDA: results of automatic analysis

Results of automatic analysis with assumption “binary addition”:

- results good, but not perfect: 24 out of 32 key bytes correct.
- the key length was correctly determined.
- the password entered was not 32 bytes long.
  $\Rightarrow$ PSION Word derives the actual key from the password.
- manual post-processing produces the encrypted text (not shown)



TECHNISCHE UNIVERSITÄT DARMSTADT

Examples of use
4. PSION PDA: determining the remaining key bytes

Copy key to clipboard during automatic analysis

In automatic analysis hexdump,

- determine incorrect byte positions, e.g. 0xAA at position 3
- guess and write down corresponding correct bytes: „e“ = 0x65

In encrypted initial file hexdump,

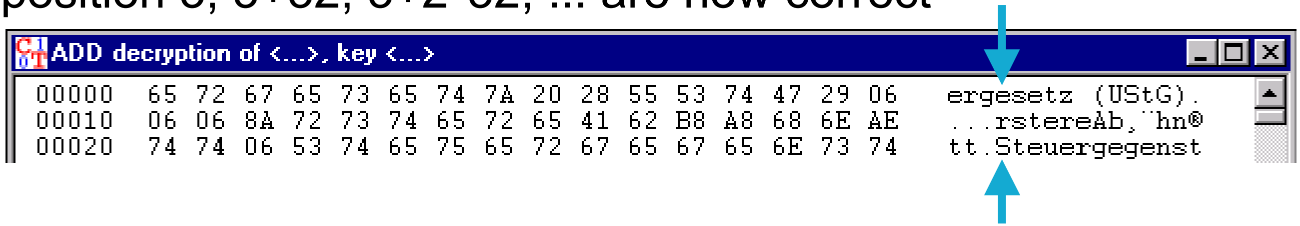
- determine initial bytes from the calculated byte positions: 0x99
- calculate correct key bytes with CALC.EXE: 0x99 - 0x65 = 0x34

Correct key from the clipboard

- 12865B341498872C393E43741396A45670235E111E907AB7C0841...

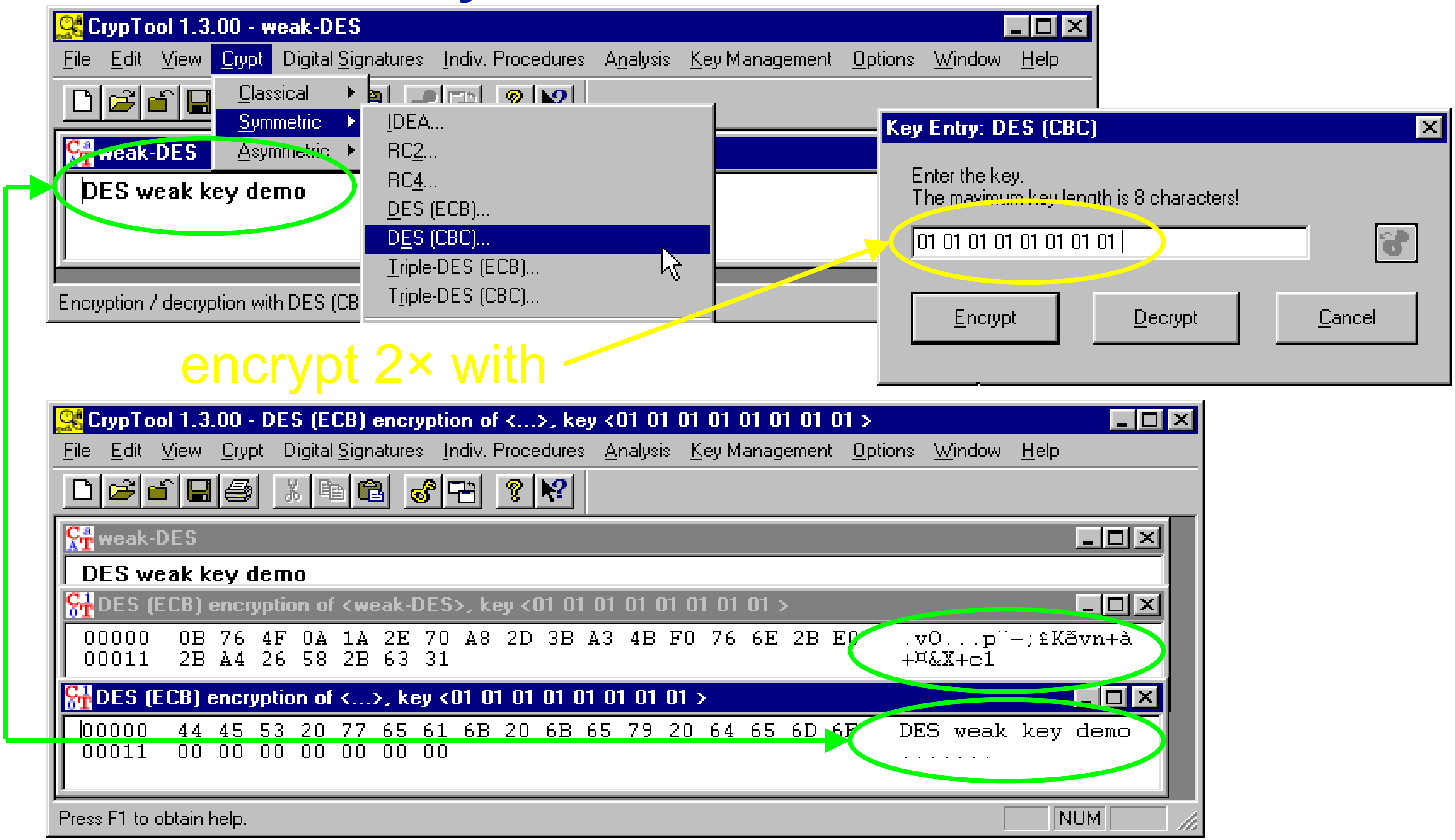
Decrypt encrypted initial document using binary addition

- bytes at position 3, 3+32, 3+2*32, ... are now correct



TECHNISCHE UNIVERSITÄT DARMSTADT

Examples of use
5. Weak DES keys

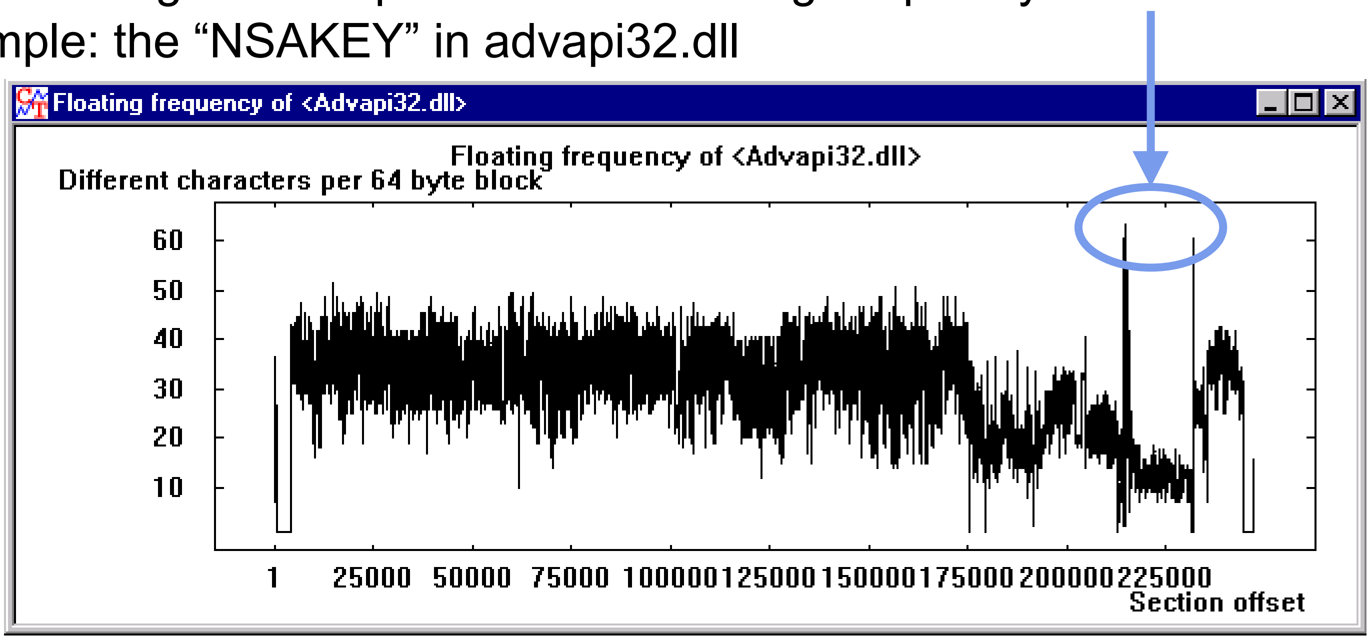


Examples of use
6. Locate key material

The function “Floating frequency” is suitable for locating key material and encrypted areas in files.

Background:

- key data is “more random” than text or program code
- can be recognised as peaks in the “floating frequency”
- example: the “NSAKEY” in advapi32.dll



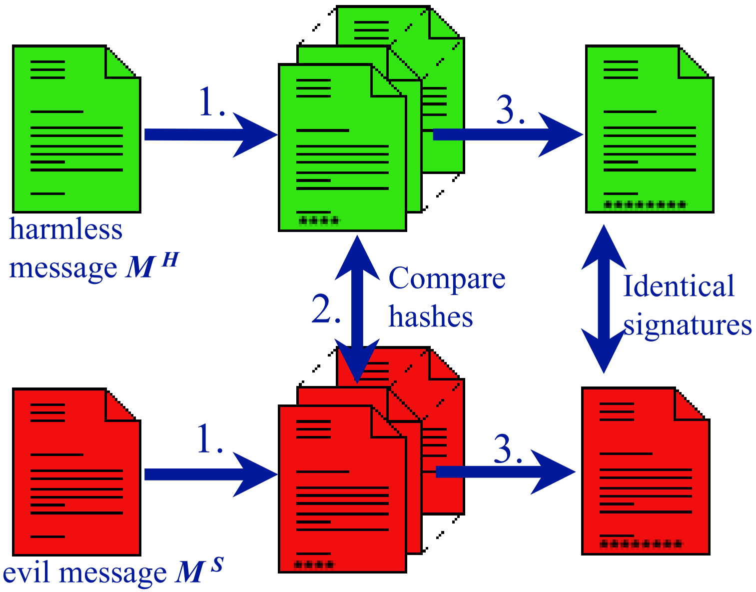
Examples of use
7. Attack on digital signature: idea

Attack on the digital signature of an ASCII text based on hash collision search

Idea:

- ASCII-Texts can be modified by changing/inserting ***non-printable*** characters, without changing the visible content
- modify two texts in parallel until a hash collision is found
- exploit the birthday paradox (birthday attack)
- generic attack applicable to all hash functions
- can be run in parallel on many machines (not implemented)
- implemented in CrypTool by Jan Blumenstein as part of his bachelor thesis “*Methods and tools for attacks on digital signatures*” (German), 2003.

Examples of use
7. Attack on digital signature: idea (2)



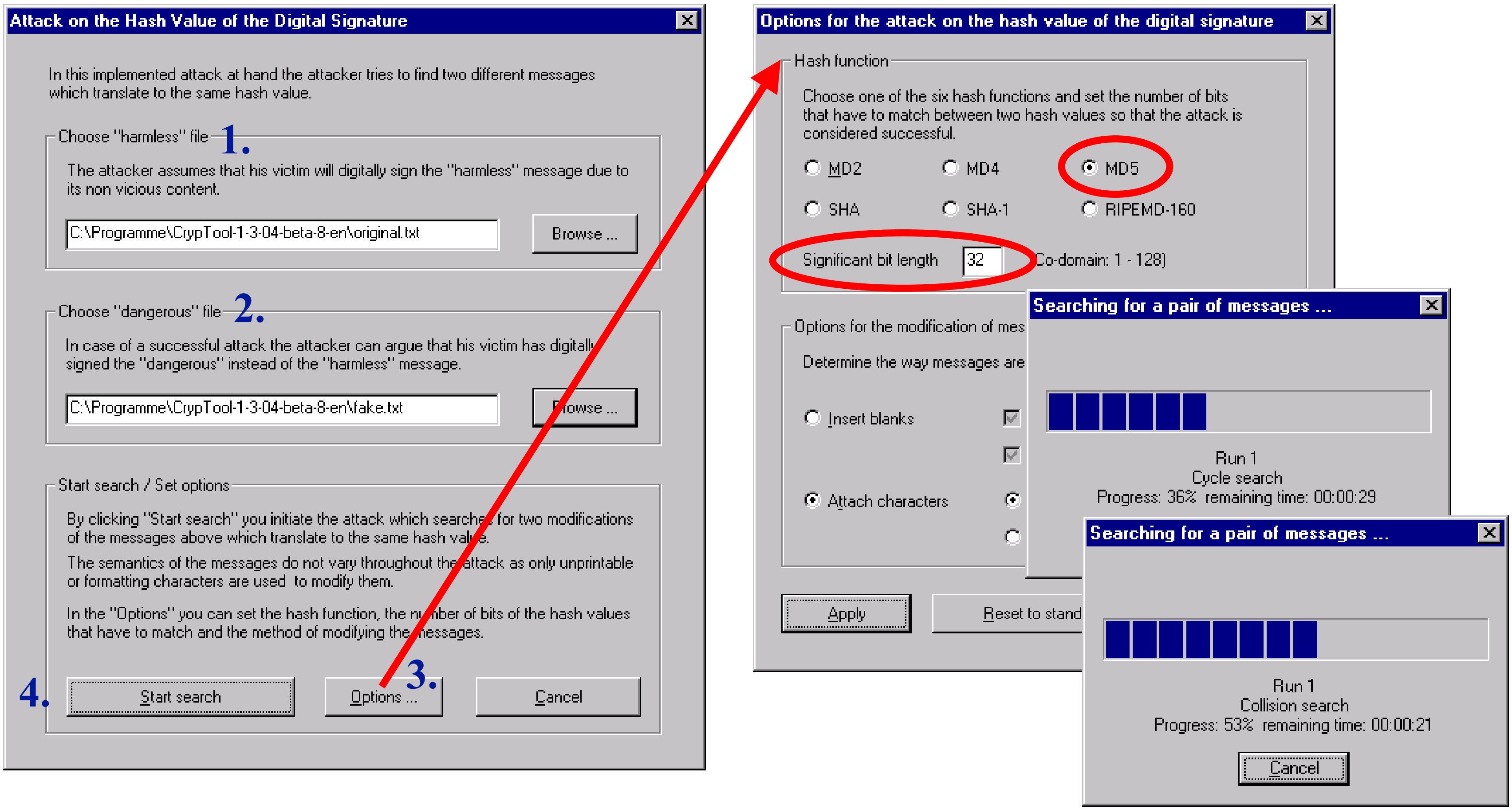
1. **Modification:** starting from a message *M* create N different messages M_1, ..., M_N with the same "content" as *M*.
2. **Search:** find modified messages M_i^H und M_j^S with the same hash value.
3. **Attack:** the signatures of those two documents M_i^H und M_j^S are the same.

We know from the birthday paradox that for hash values of bit length n:

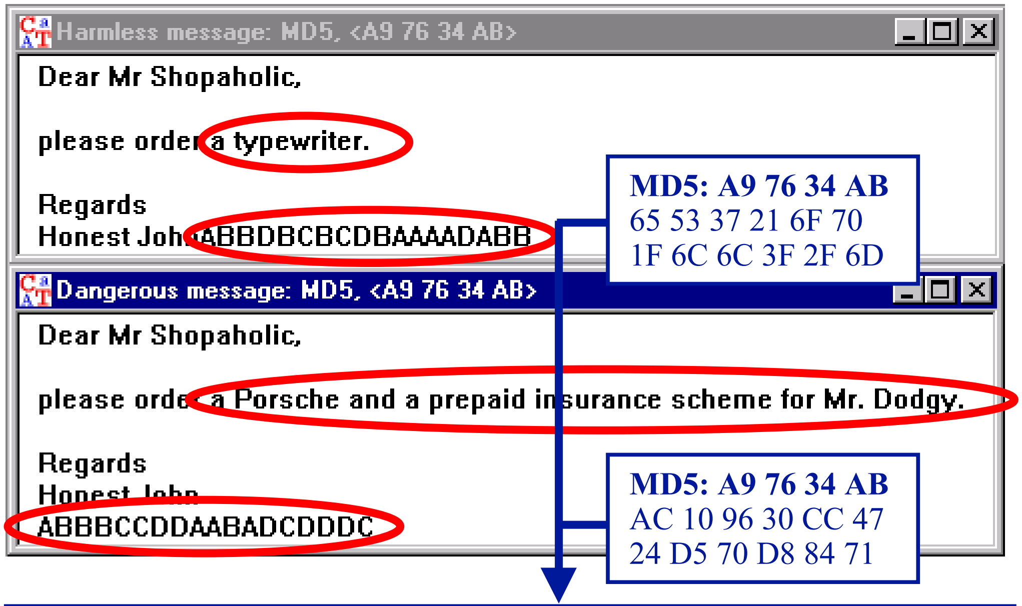
- search collision between M^H and M_1^S, ..., M_N^S : N $\approx 2^n$
- search collision between M_1^H, ..., M_N^H and M_1^S, ..., M_N^S : N $\approx 2^{n/2}$

TECHNISCHE UNIVERSITÄT DARMSTADT

Examples of use
7. Attack on digital signature: attack



Examples of use
7. Attack on digital signature: results



The first 32 bits of the hash values are identical.

Experimental results

- 72 Bit *partial collision* (equality of the first 72 hash value bits) were found in a couple of days on a single PC.
- Signatures using hash values of up to 128 bit can be attacked today using massive parallel search!

Further development

Work in process

- visualisation of challenge-response authentication
- attack on single-sided authentication with CR and weak encryption
- mass pattern search

Planned for near future

- visualisation of SSL protocol
- visualisation of Man-in-the-Middle attack
- demonstration of a side-channel attack

Planned for remote future

- visualisation of different security protocols (e.g. Kerberos)
- visualisation of attacks on these different security protocols
- port to Linux or Java
- many more ideas can be found in the readme file, chapter 6

Contact addresses

Prof. Dr. Claudia Eckert
Technical University Darmstadt
Faculty of Computer Science
IT Security
Wilhelminenstr. 7

64283 Darmstadt, Germany
claudia.eckert@
sec.informatik.tu-darmstadt.de

Bernhard Esslinger
- University of Siegen
  Faculty of Economics
- Deutsche Bank AG
  Head of Information Security

bernhard.esslinger@db.com
besslinger@web.de

Thorsten Clausius
Technical University Darmstadt
thorsten.clausius@
sec.informatik.tu-darmstadt.de

Jörg Cornelius Schneider
Deutsche Bank AG
joerg-cornelius.schneider@db.com
js@joergschneider.com

www.cryptool.de

www.cryptool.org

www.cryptool.com

Mailing list: cryptool-list@sec.informatik.tu-darmstadt.de