Lecture Notes

Cryptography

Michael Nüsken
b-it
(Bonn-Aachen International Center
for Information Technology)

Winter 2015/2016

Organizational

Course website:

`https://cosec.bit.uni-bonn.de/students/teaching/15ws/15ws-crypto/`

Mailing list for discussions

`15ws-crypto@lists.bit.uni-bonn.de`
Subscribe today!

b-it

Bonn-Aachen International Center
for Information Technology

cosec >students >Teaching >Winter 2015/2016

Cryptography

This course is listed in Aachen Campus as Cryptography, in Bonn Basis as MA-INF1103 Cryptography.

Lecture

Michael Nüsken

Tutorial

Michael Nüsken

Time & Place

- Monday, 12^{45}-14^{15}, B-IT bitmax.
- Thursday, 12^{15}-13^{45}, B-IT bitmax.
- Tutorial: Monday 14^{30}-16^{00}, B-IT bitmax.

First meeting: 2 November 2015, 12^{45}.

Exam

Pre-exam meeting: probably Tuesday, 8 March 2016, 10^{00}, b-it 1.25 (tba).

Exam: Tuesday, 15 March 2016, 10^{00}, b-it tba.

Post-exam meeting: probably Tuesday, 29 March 2016, 10^{00}, b-it 1.25 (tba).

Exam2 (repetitions only): probably Tuesday, 15 April 2016, 10^{00}, b-it tba.

Contents

Cryptography deals with methods for secure data transfer. In earlier times this was the domain of military and intelligence agencies, but today modern cryptography has grown into a key technology, enabling e-commerce and secure internet communications. Its many applications range from credit and debit cards, mobile phones, tv decoders, and electronic money to unforgeable electronic signatures under orders and contracts in the internet. In the course, we first discuss two of the current standard tools, namely AES and RSA. Further topics are key exchange, including group cryptography and discrete logarithm, digital signatures and identification, and cryptographic hash functions.

Exercises

- Sheet 1 (PDF, last updated 02 November 2015, 18:02).
  - File 01-2.txt, last updated 02 November 2015, 18:05.

Literature

- Jonathan Katz & Yehuda Lindell (2008).

About handins, credits and boni

Of course, you know that solving exercises is vital to understand the topics of the course. As an additional motivation, you can earn credits with a small influence on your final mark. Note that to be admitted to the exam you need to earn *at least* 50% of the credits. Experience shows that you should try all exercises and tutorials. Students are

Introduction to Modern Cryptography, CRC Press.

- Mihir Bellare & Shafi Goldwasser (2001). *Lecture Notes on Cryptography*. PDF.
- Johannes A. Buchmann (2004). *Introduction to Cryptography*. Birkhäuser Verlag, 2nd edition. ISBN 0-387-21156-X (hardcover), 0-387-20756-2.
- Douglas R. Stinson (2005). *Cryptography - Theory and Practice*. Discrete Mathematics and its Applications. Chapman & Hall / CRC Press, Boca Raton FL, 3rd edition. ISBN 1584885084, 600pp. Book's page including errata. Parts of this text can be found online with GoogleBooks.
- Nigel Smart (2002), *Cryptography: An Introduction*. McGraw-Hill. ISBN 0-077-09987-7. This first edition is out of print, but a new edition is available online.

Prerequisites

None.

Allocation

4+2 SWS.

- Master in Media Informatics: Computer and Communication Technology, 8 ECTS credits.
- Master in Computer Science at University of Bonn: MA-INF 1103, 9 CP.
  Students have to register this course with POS/BASIS.

The lecture's mailing list

Students are encouraged to ask and answer any questions related to the course on the mailinglist:

15ws-crypto@lists.bit.uni-bonn.de

You can subscribe to and unsubscribe from the mailing list using the information given on the list's Info page.

encouraged to discuss the given exercises among each other. Still, every student has to write up his/her solutions on his/her own. Your solution has to be self-explanatory. Stating the final result is never enough.

Due to the large number of participants we may be forced to correct only some exercises. Which exercises are chosen for correction will be determined after the deadline. Of course, only corrected exercises are considered for computing the credit percentage.

1. You are encouraged to form groups to discuss and solve the exercises. However, you must formulate and write down the solutions *individually*.
2. Always hand in to `us`.
3. Your solution must consists of
   - either: a *single* attached, printable file, best a PDF,
   - or: as text only in the mail body.

   A printout of this single thing *must* contain your name. Your solution can only be graded if the name is on the printout readably.

   (A zipped file is not printable and counts as many files!)

   Please make sure that a printout is *readable*!
4. Make sure that you have uploaded your key to the keyserver according to the first part of Exercise 1.1.
5. Sign the entire mail *including* attachments. (It would be a lot of extra work to check extra signatures for attachments, as our tools do not automatically do that.)

   The second part of Exercise 1.1 was to present *personally* a fingerprint of your signature (&encryption) key. From sheet 2 onwards the bonus for validly signed handins will only awarded when we trust your key. (This trust will be given after we've got your fingerprint; if we do trust your key we will sign it until Friday. You can check for our signature by updating your own key versus the keyserver.)
6. Usually do not encrypt.
7. Any encrypted mail to `us` *must* be encrypted for all recipients.
8. Try to keep the size of your mail fairly below 5MB.

Imprint, webmaster & more

If you do follow these rules and we can *easily verify* your signature then you earn an extra credit (per sheet). Otherwise you earn a malus (per sheet).

1. Obvious: credits are awarded for solutions that arrive within the respective deadline. Any post-deadline submission may be ignored.
2. Admission and boni
   - If you solved 50% of all corrected exercises, you are admitted to the exam.
   - If you solved 70% of all corrected exercises, you earn a single bonus.
   - If you even solved 90% of all corrected exercises, you earn a second bonus.
   - If you pass the exam and the exam is not an oral one, your final mark will be increased by approximately one third point per earned bonus.

Organizational

Hand-ins

- Out: Typically, Monday, 18^{00}.
- In: Friday, 23^{59}.

Bonus

- $\geq 50\%$: Admitted to the exam.
- $\geq 70\%$: One third bonus.
- $\geq 90\%$: Two third bonus.

Final exam

- 15 March 2016.
- $\geq 50\%$ of all points necessary to pass.
- If you pass, we apply the bonus.

Expectations

FUN

Knowledge
with fun
(ASIF)

Why is it so hard
to break crypto?
(Abdullah)

Learn to solve
cicada problem
(Jakob)

To know the math
background
(Christian)

15ws-crypto
2.11.15
(2)

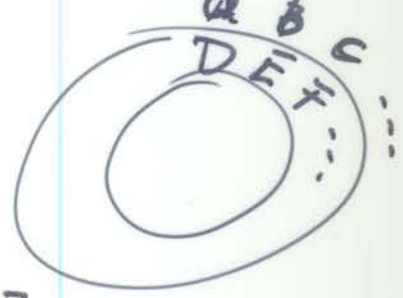
Cesar's cipher (≈ 50 B.C.)

Write down the message letter by letter, but replace each with its third successor:

f o r e s t

I R U H V W

Shift cipher



Instead replace any letter by the k-th successor where $k \in \{0, \dots 25\}$.

```
2nd successor
         attacker
k=2  ↓  CVVCEMGT  ) 2nd predecessor
         attacker ↓
```

An attacker could just try out all keys.

```
dwwdfnhu  )
exxegoiv  |  candidate plain text.
   ⋮      |
attacker  |
buubdefs  )
```

Next best solution

~~Poly~~ a Monoalphabetic cipher

~~a b c d e f g h i ...~~

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
P	A	L	N	K	U	B	D	O	R	S	Q	V	C	T	X	J	W	Z	M	E	G	F ...

attacker

encrypt ↓ PMMPLSKW ↑ decrypt

Better? How many keys?

$26! = 403,291,461,126\ 605\ 635\ 584,000\ 000$

septillion

quadrillion

trillion

billion

million

$\approx 4 \cdot 10^{26} \approx 2^{89}$.

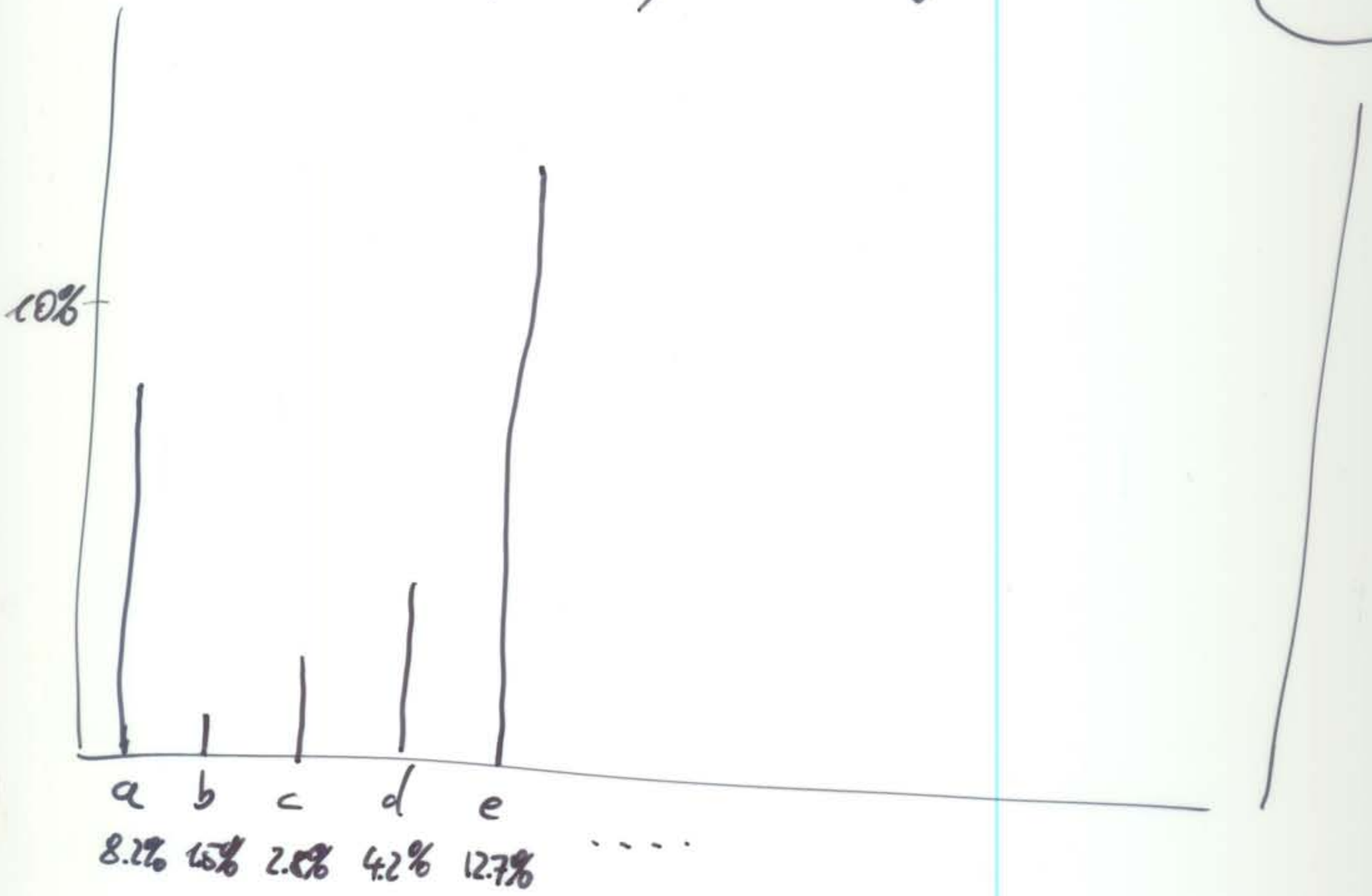
Largest distributed Internet computations:

$\approx 2^{60} - 2^{70}$ operations

(e.g. GIMPS, SETI@home, ...)

Brute force: try all keys. OUT OF REACH!

Break it: frequency analysis



Take the cipher text, assuming it sufficiently long, and compute the frequencies of each cipher text letter.

Probably you find

(e)	K	:	12.1%
(a)	P	:	9.3%
(d)	N	:	3%

Try to map K to e.

This is MUCH faster than brute force.

Anna-Lena: Use varying shift ciphers ...

The unbreakable cipher

Use a key word, say CRYPTO:

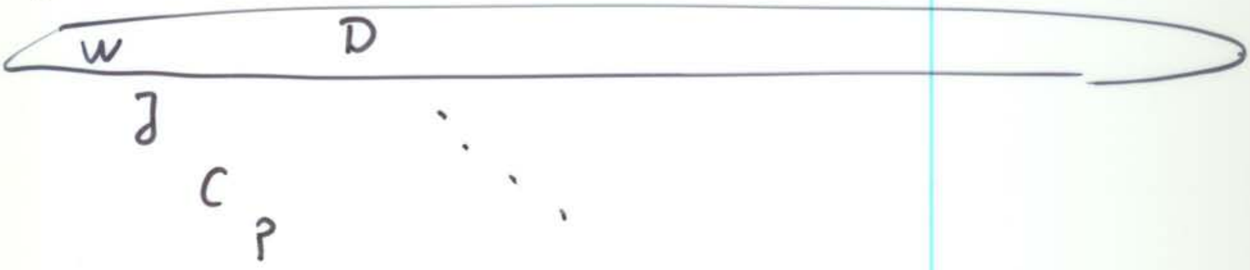
use a keyword say crypto — plaintext
CRYPTOCRYPTOCRYPTOCR — KEY

WJCPD... — CIPHERTEXT

aka. Vigenère cipher, polyalphabetic cipher.

It remained open for more than a century.

Assume we suspect that the length of the keyword is 4. Then:



If our guess is correct then each row is encrypted with the same shift. → Break with previous methods (or new ones ...).

Now use frequency analysis for each row, which should now be encrypted with a shift cipher.

↪ find the key and decrypt.

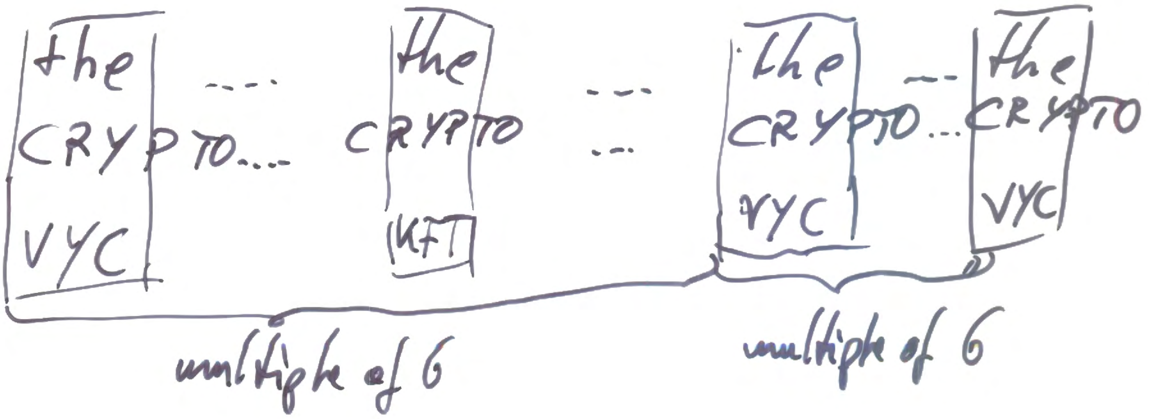
But: how to find the key length?

Julius: Look for repetitions in the cipher text. Then the key length...

KASISKI attack:

- ~~But~~ Find repetitions in the ciphertext.
- The key length probably is a divisor of the distance of the repeated ciphertext parts.

Typical:


the
CRYPTO...
VYC
...
the
CRYPTO
KFT
...
...
the
CRYPTO...
VYC
...
the
CRYPTO
VYC
multiple of 6
multiple of 6