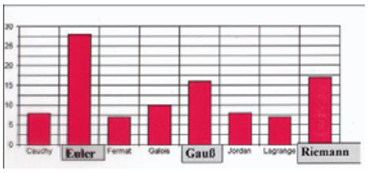
LEUPHANA
UNIVERSITÄT LÜNEBURG

Mathematik für alle



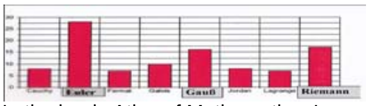
die acht bedeutendsten Mathematiker,
gemessen an nach ihnen benannten Objekten

Bernhard Riemann

Abitur 1846 am Johanneum Lüneburg

Bernhard Riemann

one of the most famous mathematicians



In the book: Atlas of Mathematics, I counted
in the index the number of items with the name
of mathematicians like Eulier's …, Gauß's… Riemann's…
The result is seen above. Riemann had been a student of Gauß
ca 1850. But here in Lüneburg in the Gymnasium Johanneum
he made his Abitur-Exam.
For further information see
http://en.wikipedia.org/wiki/Bernhard_Riemann
http://haftendorn.uni-lueneburg.de/mathe-lehramt/geschichte/riemann/riemann.htm
http://www.johanneum-lueneburg.de/englpage/chronik/riemann/riemann.htm (english)

Mathematik für alle

LEUPHANA
UNIVERSITÄT LÜNEBURG

1 Million Dollar gibt die Clay-Stiftung

für den Beweis der **Riemann**schen Vermutung über die Primzahlverteilung

Dies ist eins von 7 offenen Problemen des 21. Jh.

Open problem: Riemann's hypothesis
http://en.wikipedia.org/wiki/Riemann_hypothesis

Bernhard Riemann

Was sind Primzahlen? What are primes?

-	2	3	-	5	-	7	-	-	-	11	-	13	-	-	-	17	-	19	-	-	-	23	-	-	-	-	-	29	-
31	-	-	-	-	-	37	-	-	-	41	-	43	-	-	-	47	-	-	-	-	-	53	-	-	-	-	-	59	-
61	-	-	-	-	-	67	-	-	-	71	-	73	-	-	-	-	-	79	-	-	-	83	-	-	-	-	-	89	-
-	-	-	-	-	-	97	-	-	-	101	-	103	-	-	-	107	-	109	-	-	-	113	-	-	-	-	-	-	-
-	-	-	-	-	-	127	-	-	-	131	-	-	-	-	-	137	-	139	-	-	-	-	-	-	-	-	-	149	-
151	-	-	-	-	-	157	-	-	-	-	-	163	-	-	-	167	-	-	-	-	-	173	-	-	-	-	-	179	-
181	-	-	-	-	-	-	-	-	-	191	-	193	-	-	-	197	-	199	-	-	-	-	-	-	-	-	-	-	-
211	-	-	-	-	-	-	-	-	-	-	-	223	-	-	-	227	-	229	-	-	-	233	-	-	-	-	-	239	-
241	-	-	-	-	-	-	-	-	-	251	-	-	-	-	-	257	-	-	-	-	-	263	-	-	-	-	-	269	-
271	-	-	-	-	-	277	-	-	-	281	-	283	-	-	-	-	-	-	-	-	-	293	-	-	-	-	-	-	-
-	-	-	-	-	-	307	-	-	-	311	-	313	-	-	-	317	-	-	-	-	-	-	-	-	-	-	-	-	-
331	-	-	-	-	-	337	-	-	-	-	-	-	-	-	-	347	-	349	-	-	-	353	-	-	-	-	-	359	-
-	-	-	-	-	-	367	-	-	-	-	-	373	-	-	-	-	-	379	-	-	-	383	-	-	-	-	-	389	-
-	-	-	-	-	-	397	-	-	-	401	-	-	-	-	-	-	-	409	-	-	-	-	-	-	-	-	-	419	-
421	-	-	-	-	-	-	-	-	-	431	-	433	-	-	-	-	-	439	-	-	-	443	-	-	-	-	-	449	-
-	-	-	-	-	-	457	-	-	-	461	-	463	-	-	-	467	-	-	-	-	-	-	-	-	-	-	-	479	-
-	-	-	-	-	-	487	-	-	-	491	-	-	-	-	-	-	-	499	-	-	-	503	-	-	-	-	-	509	-

Sie sind nicht teilbar durch andere Zahlen, außer durch 1.
they are not divisible by other numbers, without by 1.

Primzahlen sind die Zahlen mit genau zwei Teilern.
Primes are the numbers with exact two divisors.

Was ist denn mit den Primzahlen?

Sie spielen in der
Kryptografie
!!!!!! die !!!!!!
zentrale Rolle.

Primzahlprüfung ist bei kleinen Zahlen leicht.
Für „krytografische" Zahlen hat man Primzahltest (bis ca. 500 Stellen) siehe weiter unten.

Für viel größere Zahlen hat man Chancen für spezielle Primzahltypen.

Whats Important with Primes?

They play
!!!!! the!!!!!
decisive role
in cryptography

To test, that a number is prime, is easy.
For numbers in cryptography one has pimality tests.
(ca. 500 digits) see below.

For larger numbers you have chances for spezial primes.

Größte 2013 bekannte Primzahl

$$2^{57\,885\,161}-1$$

eine Zahl mit 17 425 170 (dezimalen) Stellen, die am 2. Februar 2013 auf einem Computer der mathematischen Fakultät an der Universität von Minnesota, gefunden wurde. Curtis Cooper hatte das Programm des GIMPS-Projekts als Bildschirmschoner seinem Rechner eingerichtet. Die Für Seine Entdeckung dieser Primzahl erhielt er 3000 Dollar. Als man zum ersten Mal mehr als 10 Millionen Dezimalstellen überschritten hatte, gab es von der Electronic Frontier Foundation einen Preis von 100.000 US-Dollar.

Man sucht unter den **Mersenne-Zahlen** 2^p-1

Largest Known Prime Number 2013

$$2^{57\,885\,161}-1$$

a number with 17 425 170 (decimal) digits. It was found the 2. february 2013 with a Computer of the mathematischen faculty of mathematics of the university of Minnesota. Curtis Cooper had the programm of the GIMPS-projekt as screensaver on his computer. For his detection he won 3000 Dollar. At the first time one had more then 10 Millionen digits, the Electronic Frontier Foundation offers a prize of 100.000 US-Dollar.

One search only in **Mersenne-Zahlen** 2^p-1 .

Diese Größenordnung ist für die Kryptografie unbrauchbar.

Tragende Begriffe der Kryptografie:

Wir haben schon gelernt:

$Z(n)=\mathbb{Z}_n=\{0,1,2,3,...,n-1\}$ Rechnen modulo n.

k ist Ordnung von a in Z(m): $a^k \underset{n}{\equiv} 1$ k minimal

3 hat die Ordnung 4 in Z (20): $3^4 \underset{20}{\equiv} 1$

$3^8 \underset{20}{\equiv} 1;\quad 3^{40} \underset{20}{\equiv} 1;\quad 3^{72} \underset{20}{\equiv} 1;\quad 3^{7200} \underset{20}{\equiv} 1;$

$3^9 \underset{20}{\equiv} 3;\quad 3^{43} \underset{20}{\equiv} 9;\quad 3^{75} \underset{20}{\equiv} 9;\quad 3^{7204} \underset{20}{\equiv} 1$

denn $3^9=3^{8+1}=3^8\cdot 3^1 \underset{20}{\equiv} 1\cdot 3=3$

In den Exponenten von a rechnet man modulo Ordnung von a.

This Magnitude is for Cryptography Complete Useless.

Main concepts of crytography:

We learned before:

$Z(n)=\mathbb{Z}_n=\{0,1,2,3,...,n-1\}$ cacolating modulo n.

k is Order of a in Z(m): $a^k \underset{n}{\equiv} 1$ k minimal

3 has the order 4 in Z (20): $3^4 \underset{20}{\equiv} 1$

$3^8 \underset{20}{\equiv} 1;\quad 3^{40} \underset{20}{\equiv} 1;\quad 3^{72} \underset{20}{\equiv} 1;\quad 3^{7200} \underset{20}{\equiv} 1;$

$3^9 \underset{20}{\equiv} 3;\quad 3^{43} \underset{20}{\equiv} 9;\quad 3^{75} \underset{20}{\equiv} 9;\quad 3^{7204} \underset{20}{\equiv} 1$

because $3^9=3^{8+1}=3^8\cdot 3^1 \underset{20}{\equiv} 1\cdot 3=3$

In the exponents of a you have to calculate modulo order of a.

Übungen --- exercises:

Ordnung von a in Z(m) $a^k \underset{m}{\equiv} 1$ Also ist $a^{n\cdot k} \underset{m}{\equiv} 1$

Also ist:

$20^7 \underset{29}{\equiv} 1$ $20^{14} \underset{29}{\equiv}$ $20^{28} \underset{29}{\equiv}$ $20^{7772} \underset{29}{\equiv}$

$17^4 \underset{29}{\equiv} 1$ $17^{100} \underset{29}{\equiv}$ $17^{253} \underset{29}{\equiv}$

$8^5 \underset{31}{\equiv} 1$ $8^{25} \equiv$ $8^{26} \equiv$ $8^{24} \equiv$

In der oberen „Etage“ Vielfache der Ordnung ignorieren.
In the upper storey you must leave multiples of the order.

Übungen --- Exercises:

Ordnung von a in Z(m) $a^k \underset{m}{\equiv} 1$ Also ist $a^{n\cdot k} \underset{m}{\equiv} 1$

Also ist:

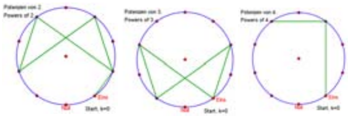
$20^7 \underset{29}{\equiv} 1$ $20^{14} \underset{29}{\equiv} 1$ $20^{28} \underset{29}{\equiv} 1$ $20^{7772} \underset{29}{\equiv} 400 \underset{29}{\equiv} 23$

$17^4 \underset{29}{\equiv} 1$ $17^{100} \underset{29}{\equiv} 1$ $17^{253} \underset{29}{\equiv} 17$

$8^5 \underset{31}{\equiv} 1$ $8^{25} \underset{31}{\equiv} 1$ $8^{26} \underset{31}{\equiv} 8$ $8^{24} \underset{31}{\equiv} 64 \underset{31}{\equiv} 2$

In der oberen „Etage“ Vielfache der Ordnung ignorieren.
In the upper storey you must leave multiples of the order.

Hat jedes Element von Z(n)eine Ordnung?
Are there elements in Z(n) without an order?



Start bei 1

Rückkehr zur 1?
Back to the 1?

Potenzen von 2 in Z= {1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024,
Powers of 2 in Z(10)= {1, 2, 4, 8, 6, 2, 4, 8, 6, 2, 4, 8, 6}
Potenzen von 3 in Z= {1, 3, 9, 27, 81, 243, 729, 2187, 6561,
Powers of 3 in Z(10)= {1, 3, 9, 7, 1, 3, 9, 7, 1, 3, 9, 7, 1}
Potenzen von 4 in Z= {1, 4, 16, 64, 256, 1024, 4096, 16384,
Powers of 4 in Z(10)= {1, 4, 6, 4, 6, 4, 6, 4, 6, 4, 6, 4, 6}

1	2	3	4	5	6	7	8	9
1	4	9	6	5	6	9	4	1
1	8	7	4	5	6	3	2	9
1	6	1	6	5	6	1	6	1
1	2	3	4	5	6	7	8	9
1	4	9	6	5	6	9	4	1
1	8	7	4	5	6	3	2	9
1	6	1	6	5	6	1	6	1
1	2	3	4	5	6	7	8	9

$$\begin{pmatrix}1\\2\\3\\4\end{pmatrix} \quad \begin{pmatrix}1&3&7&9\\1&9&9&1\\1&7&3&9\\1&1&1&1\end{pmatrix}$$

$\mathbb{Z}_{10}^{*}=\{1,3,7,9\}$

Nein, Zahlen, die mit n einen gemeinsamen Teiler haben, müssen wir weglassen.

Übrig bleibt dann Z*(n)

No, but we leave all numbers with a common divisor with n. 13

Prim und nicht prim

Potenz-Tafel von Zstern modulo 11
Zstern(11) hat 10 Elemente

1	2	3	4	5	6	7	8	9	10
1	4	9	5	3	3	5	9	4	1
1	8	5	9	4	7	2	6	3	10
1	5	4	3	9	9	3	4	5	1
1	10	1	1	1	10	10	10	1	10
1	9	3	4	5	5	4	3	9	1
1	7	9	5	3	8	6	2	4	10
1	3	5	9	4	4	9	5	3	1
1	6	4	3	9	2	8	7	5	10
1	1	1	1	1	1	1	1	1	1

Potenz-Tafel von Zstern modulo 12
Zstern(12) hat 4 Elemente

1	5	7	11
1	1	1	1
1	5	7	11
1	1	1	1

$\mathbb{Z}_{12}^{*}=\{1,5,7,11\}$

Z*(n) enthält nur die zu n **teilerfremden** Elemente,
that are the to n **relatively prime** elements.

Ist n keine Primzahl, hat Z* weniger als n-1 Elemente. $|\mathbb{Z}_n^*| \leq n-1$

lies: Z n stern read: Z n star

p ist prim $\Rightarrow |\mathbb{Z}_p^*| = \{1,2,3,\ldots,p-1\}$

Fachausdruck: prime Restklassengruppe
mathematical word; prime residue group

14

Wie findet man die Ordnung?

Potenz-Tafel von Zstern modulo 13
Zstern(13) hat 12 Elemente

k												
1	1	2	3	4	5	6	7	8	9	10	11	12
2	1	4	9	3	12	10	10	12	3	9	4	1
3	1	8	1	12	8	8	5	5	1	12	5	12
4	1	3	3	9	1	9	9	1	9	3	3	1
5	1	6	9	10	5	2	11	8	3	4	7	12
6	1	12	1	1	12	12	12	12	1	1	12	1
7	1	11	3	4	8	7	6	5	9	10	2	12
8	1	9	9	3	1	3	3	1	3	9	9	1
9	1	5	1	12	5	5	8	8	1	12	8	12
10	1	10	3	9	12	4	4	12	9	3	10	1
11	1	7	9	10	8	11	2	5	3	4	6	12
12	1	1	1	1	1	1	1	1	1	1	1	1

a

$a^k \bmod 13 = \square$

$7^5 \bmod 13 = 11$

$a^{p-1} \underset{p}{\equiv} 1$

Man sucht in einer Spalte die erste 1.
Die Zeilennummer ist dann die Ordnung.

Search in the column of a the first 1.
The number of the row ist the order of a.

Ord(12)=2
Ord(3)=3 Ord(9)=3
Ord(5)=4 Ord(8)=4
Ord(4)=6 Ord(10)=6
Ord(2)=12 Ord(6)=12
Ord(7)=12 Ord(11)=12

$\mathbb{Z}_{13}^{*}$

15

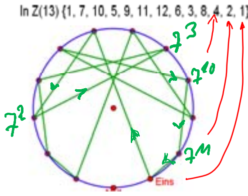
Potenzen in Z(n)

In Z(n) sind die Zahlen von1 bis n-1.

Die Potenzen von 7 modulo 13

In Z {1, 7, 49, 343, 2401, 16807, 117649, 823543, 5764801, 40353607, 282475249, 1977326743, 13841287201}
In Z(13) {1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1}

7^{10} 7^{11} 7^{12}



$7^{12} \underset{13}{\equiv} 1$

Die Ordnung von 7 in Z(13) ist 12.

Darum ist dann z.B. $7^4 \cdot 7^8 \underset{13}{\equiv} 1$

Was nütz die 1? What ist useful with 1?

16

Was nützt die 1?

Idee: Anton weiß also: $7^4 \cdot 7^8 \underset{13}{\equiv} 1$ denn $7^{12} \underset{13}{\equiv} 1$

Anton rechnet $7^4 \to 2401$ $7^8 \to 5764801$
Anton gibt die Zahl 2401 an Berta
m=9 ist Bertas geheime Nachricht für Anton.
Berta rechnet $9 \cdot 2401 \to 21609$,
dies sendet sie Anton.

Anton rechnet: $21609 \cdot 5764801$

$\mathrm{mod}(124571584809, 13) \to 9$

Anton kann jetzt Bertas Nachricht, nämlich die 9, lesen.

Die gute Nachricht: Produkte, die 1 ergeben, helfen beim Entschlüsseln.

Die schlechte Nachricht: Das obige Verfahren ist total unsicher 17

What ist Useful with 1?

Idea: Anton knows: $7^4 \cdot 7^8 \underset{13}{\equiv} 1$ because $7^{12} \underset{13}{\equiv} 1$

Antoncalculates $7^4 \to 2401$ $7^8 \to 5764801$
Anton gives this number 2401 to Berta
m=9 ist Bertas secret message for Anton.
Berta calculates $9 \cdot 2401 \to 21609$,
this she sends to Anton.

Anton calculates $21609 \cdot 5764801$

$\mathrm{mod}(124571584809, 13) \to 9$

Now Anton can read Bertas message, namely the 9.

The good message: produkts, which have the result 1, help in the decryption.

The bad message: The method we have seen is total insecure! 18

Prim und nicht prim

$|\mathbb{Z}_{13}| = 12$

Potenz-Tafel von Zstern modulo 13
Zstern(13 *) hat* 12 *Elemente*

1	2	3	4	5	6	7	8	9	10	11	12
1	4	9	3	12	10	10	12	3	9	4	1
1	8	1	12	8	8	5	5	1	12	5	12
1	3	3	9	1	9	9	1	9	3	3	1
1	6	9	10	5	2	11	8	3	4	7	12
1	12	1	1	12	12	12	12	1	1	12	1
1	11	3	4	8	7	6	5	9	10	2	12
1	9	9	3	1	3	3	1	3	9	9	1
1	5	1	12	5	5	8	8	1	12	8	12
1	10	3	9	12	4	4	12	9	3	10	1
1	7	9	10	8	11	2	5	3	4	6	12
1	1	1	1	1	1	1	1	1	1	1	1

$a^{12} \underset{13}{\equiv} 1$

Potenz-Tafel von Zstern modulo 9
Zstern(9 *) hat* 6 *Elemente*

1	2	4	5	7	8
1	4	7	7	4	1
1	8	1	8	1	8
1	7	4	4	7	1
1	5	7	2	4	8
1	1	1	1	1	1

$a^6 \underset{9}{\equiv} 1$

$|\mathbb{Z}_9^*| = 6$

Potenz-Tafel von Zstern modulo 10
Zstern(10 *) hat* 4 *Elemente*

1	3	7	9
1	9	9	1
1	7	3	9
1	1	1	1

$a^4 \underset{10}{\equiv} 1$

$|\mathbb{Z}_{10}^*| = 4$

Eulerscher Satz, Euler‘s theorem

- In der letzten Zeile der Potenztafeln stehen immer nur Einsen.
- In the last row of the power table there is only Number 1.

$|\mathbb{Z}_n^*| = \varphi$ sprich phi $\Rightarrow$ $\boxed{a^\varphi \equiv 1}$

Potenz-Tafel von Zstern modulo 14
Zstern(14 *) hat* 6 *Elemente*

1	3	5	9	11	13
1	9	11	11	9	1
1	13	13	1	1	13
1	11	9	9	11	1
1	5	3	11	9	13
1	1	1	1	1	1

$|\mathbb{Z}_{14}^*| = 6$

$\leftarrow a^6 \underset{14}{\equiv} 1$

Potenz-Tafel von Zstern modulo 15
Zstern(15 *) hat* 8 *Elemente*

1	2	4	7	8	11	13	14
1	4	1	4	4	1	4	1
1	8	4	13	2	11	7	14
1	1	1	1	1	1	1	1
1	2	4	7	8	11	13	14
1	4	1	4	4	1	4	1
1	8	4	13	2	11	7	14
1	1	1	1	1	1	1	1

$|\mathbb{Z}_{15}^*| = 8$

$\leftarrow a^8 \underset{15}{\equiv} 1$

Kleiner Satz von Fermat
Fermats little theorem

1606-1665

a ist nicht Vielfaches von p

p prim $\Longrightarrow a^{p-1} \underset{p}{\equiv} 1$

Bei Primzahlen p kennt man das φ

Es ist um 1 kleiner als p $\varphi = p - 1$

Hurra! Das ergibt einen Primzahlenprüfer. We have a prime tester . If the result is1, then p is candidat for prime.

WolframAlpha

PowerMod[1234,5618,5619] $\longrightarrow$ 7 5619 ist keine Primzahl

PowerMod[1234,5622,5623] $\longrightarrow$ 1 5623 ist Kanditat für Primzahl

NextPrime[5600] $\longrightarrow$ 5623 Mathematica sagt: yes prime

Kleiner Satz von Fermat ist nicht umkehrbar
not conversable

a ist nicht Vielfaches von p

p prim $\Longrightarrow a^{p-1} \underset{p}{\equiv} 1$

$\not\Longleftarrow$

1601-1667

denn $2^{340} \underset{341}{\equiv} 1 \Rightarrow 341$ Kandidat für prim

$15^{340} \underset{341}{\equiv} 1$

aber $341 = 11 \cdot 31$

$\Rightarrow$ nicht prim

aber $3^{340} \underset{341}{\equiv} 56 \Rightarrow 341$ nicht prim

Primzahl-Tests

- Es gibt noch etliche pfiffige Primzahltests. z.B. Miller-Rabbin test
- Sie sind auch bei großen Zahlen bis **10^300 effektiv**.
- Sie beruhen auf mathematischer Theorie.
- Die tragenden Themen heißen
  - Zahlentheorie
  - Algebra
  - Theorie der komplexen Funktionen

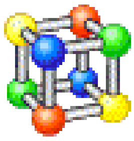
Wenn der „kleine Fermat“ trotz Variation der Basis 1 liefert, muss man einen anderen Test nehmen.

Primality Tests

- There are a lot of sophisticated primalty tests. i.e. Miller-Rabbin test
- They are effective up to **10^300**.
- They are based on mathematical theory.
- The main topics are
  - number theory
  - algebra
  - theory of complex functions

If „little Fermat“ gives 1 although you have taken several base numbers then you must take another test.

Wie lange dauert das Suchen eine Faktors bei großen Zahlen mit 200 Stellen?



How long will it take to search factors when the number has 200 digits?

„Einfach Durch-Suchen“ ist nicht effektiv möglich.

Darauf beruht die Sicherheit in der Kryptografie.

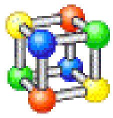
Alternative Methoden sind für große Zahlen nicht erfolgreich genug.

Mathematiker und Informatiker haben da z.Z. keine Hoffnung

To search brute force is not effective, there is no fast algorithm in sight.
That‘s the security of cryptography.

25

How Long will it Take to Search Factors when the Number has 200 Digits?



„Brute force searching“ is not possible in an effective manner and time.

That‘s the reason for secuity in cryptography.

Alternative methods are nowadays not successful for giant numbers.

There is no fast algorithm in sight

Mathematicial and computer scientists are not hopeful.

26

Wie kam es zur modernen Kryptografie?

1974

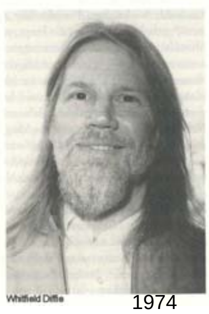
lesen aus

Simon Singh: Codes, Wien, 2001

S. 215 ff (Auch Titel: Geheimschriften)

27

Diffie‘s and Hellmann‘s Method



1974

Stanford

University

28

Diffie-Hellman Schlüsselvereinbarung

key exchange, better: key agreement

Protokoll: Anton und Berta vereinbaren offen eine Primzahl p und ‚eine Grundzahl g 2

Dann wählen sie sich geheim eine Zahl a, bzw. b, bilden 13

5 3

$g^a \underset{p}{\equiv} : \alpha$, bzw. $g^b \underset{p}{\equiv} : \beta$

Anton bildet

$k_a : \underset{p}{\equiv} \beta^a$

Berta bildet

$k_b : \underset{p}{\equiv} \alpha^b$

Diffie und Hellmann nennen ihr Verfahren "Schlüsselvereinbarung" und empfehlen nun die Verwendung eines symmetrischen kryptografischen Verfahrens.

Now it is possible to take a symmetric algorithm like „one time pad“.

29

Diffie-Hellman Schlüsselvereinbarung,

key exchange, better: key agreement

Protokoll: Anton und Berta vereinbaren offen eine Primzahl p und eine Grundzahl g 2

Dann wählen sie sich geheim eine Zahl a, bzw. b, bilden 13

5 3

$g^a \underset{p}{\equiv} : \alpha$, bzw. $g^b \underset{p}{\equiv} : \beta$

$2^5 \underset{13}{\equiv} 6 = \alpha$ $\qquad$ $2^3 \underset{13}{\equiv} 8 = \beta$

Anton bildet

$k_a : \underset{p}{\equiv} \beta^a$

$8^5 \underset{13}{\equiv} 8^2 \cdot 8^2 \cdot 8 = 64 \cdot 64 \cdot 8 \underset{13}{\equiv} (-1)(-1) \cdot 8 \underset{13}{\equiv} 8$

Berta bildet

$k_b : \underset{p}{\equiv} \alpha^b$

$6^3 \underset{13}{\equiv} 36 \cdot 6 \underset{13}{\equiv} 10 \cdot 6 \underset{13}{\equiv} -5 \underset{13}{\equiv} 8$

Diffie und Hellmann nennen ihr Verfahren "Schlüsselvereinbarung" und empfehlen nun die Verwendung eines symmetrischen kryptografischen Verfahrens.

Now it is possible to take a symmetric algorithm like „one time pad“.

30

Beweis der „Durchführbarkeit“,
proof of viability,
dass also das Verfahren stets klappt.

$k_a :\underset{p}{\equiv} \beta^a \qquad \beta :\underset{p}{\equiv} g^b \qquad k_b :\underset{p}{\equiv} \alpha^b \qquad \alpha :\underset{p}{\equiv} g^a$

$k_a = (g^b)^a = g^{ba}$

Beweis der „Durchführbarkeit“,
proof of viability,
dass also das Verfahren stets klappt.

$k_a :\underset{p}{\equiv} \beta^a \qquad \beta :\underset{p}{\equiv} g^b \qquad k_b :\underset{p}{\equiv} \alpha^b \qquad \alpha :\underset{p}{\equiv} g^a$

$k_a = (g^b)^a = g^{ba} \qquad k_b = (g^a)^b = g^{ab}$

Also $k_a = g^{ba} = g^{ab} = k_b$

Vierer-Übung

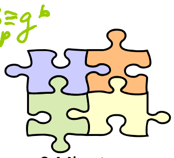
4 Studis bilden eine Gruppe

Primzahl p=11, Grundzahl g=4

Die, die oben sitzen, spielen Anton a=9,
The two upper sitting play Anton
die unten sitzen spielen Berta b=8
the two lower sitting play Berta

$\alpha \underset{p}{\equiv} g^a \qquad \beta \underset{p}{\equiv} g^b$

$\alpha \qquad \beta$



Vergleichen Sie k
compare k

Nehmen sie evt.
andere Zahlen.

$k_a \underset{p}{\equiv} \beta^a \qquad k_b \underset{p}{\equiv} \alpha^b$

6 Minuten

Diffie Hellmann Schlüsselvereinbarung,
Key Agreement

Protokoll: Anton und Berta vereinbaren offen eine Primzahl p und eine Grundzahl g 11 4
Dann wählen sie sich geheim eine Zahl a, bzw. b, bilden 11

$4^9 \underset{11}{\equiv} 3 \qquad g^a \underset{p}{\equiv}: \alpha$, bzw. 9 8 $g^b \underset{p}{\equiv}: \beta \qquad 4^8 \underset{11}{\equiv} 9$

und senden sich offen das Ergebnis zu.

9 3

Anton bildet
$k_a :\underset{p}{\equiv} \beta^a$
$9^9 \equiv 5$

Berta bildet
$k_b :\underset{p}{\equiv} \alpha^b$
$3^8 \equiv 5$

Diffie und Hellmann nennen ihr Verfahren "Schlüsselvereinbarung" und empfehlen nun die Verwendung eines symmetrischen kryptografischen Verfahrens.

Wie sieht das in der Realität aus?

Diffie-Hellmann-Verfahren, realisiert in MuPAD

oder in Mathematica oder in TI Nspire CAS, usw.

- Das Grund Problem der „alten“ Kryptografie ist gelöst,
- Der Schüssel wird nicht ausgetauscht,
- sondern kryptografisch sicher vereinbart.
- Nun kann man mit dem One-Time-Pad sicher kommunizieren.

What‘s Reality?

Diffie Hellmann method, realised in MuPAD

or in mathematica or in TI Nspire CAS or so on.

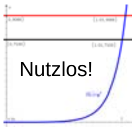
- The main problem of the „old“ cryptography is solved,
- the key is not changed,
- but agreed in a safe cryptographical way.
- Now one can cummunicate safely with one time pad..

Warum hat Mister X keine Chance?

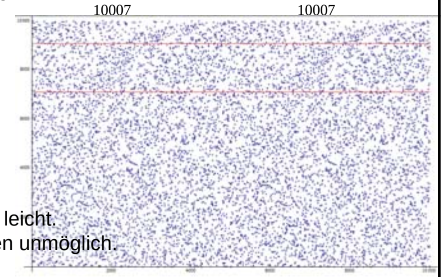
Mister X fängt ab: $p = 10007 \quad g = 6784$

$\alpha = 9088 \quad \beta = 7100$

Er versucht zu lösen: $6784^a \underset{10007}{\equiv} 9088$ oder $6784^b \underset{10007}{\equiv} 7100$



Nutzlos!



Nadel im Heuhaufen!

Bei 10^5 Punkten leicht.
Bei 10^{200} Punkten unmöglich.

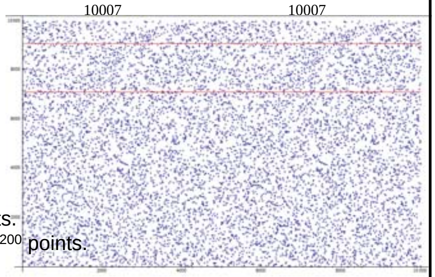
No Chance for Mister X?

Mister X taps: $p = 10007 \quad g = 6784$

$\alpha = 9088 \quad \beta = 7100$

He tries to solve: $6784^a \underset{10007}{\equiv} 9088$ oder $6784^b \underset{10007}{\equiv} 7100$

useless!



Needle in a haystack!

Easy by 10^5 points.
Unpossible by 10^{200} points.

Das war nur der Anfang, aber nun:

Ronald Rivest, Adi Shamir und Leonard Adleman.

RSA-Verschlüsslung

Public-Key-Kryptografie

asymmetrisches Verfahren

lesen Singh, 231ff

That had been the Beginning, but now:

Ronald Rivest, Adi Shamir und Leonard Adleman.

RSA-ciphering

Public-Key-cryptography

asymmetric method

lesen Singh, 231ff

RSA-Public-Key-Verfahren

1.) Schlüsselerzeugungsphase

- Anton wählt zwei Primzahlen p und q
- Er rechnet $n := p\,q \quad \varphi := (p-1)(q-1)$
- Wählt beliebig e mit $e < \varphi$ und e teilerfremd zu φ
- Er berechnet d als Inverses von e im Modul $\mathbb{Z}^*(\varphi)$. er hält d streng geheim.

$e \cdot d \underset{\varphi}{\equiv} 1$

Mein öffentliches Schlüsselpaar ist:

$$(e,n)$$

Das liest

RSA Public Key Method

1.) Generation of the key

- Anton choose two primes p and q
- He calculate $n := p\,q \quad \varphi := (p-1)(q-1)$
- arbitrary e with $e < \varphi$ and e relatively prime to φ teilerfremd zu d
- He calculate d as the inverse von e im Modul $\mathbb{Z}^*(\varphi)$ His d must be very secret.

$e \cdot d \underset{\varphi}{\equiv} 1$

My public key is the pair:

$$(e,n)$$

read it

RSA-Public-Verschlüsselung

2.) Anwendungsungsphase: Verschlüsselung

- Berta will Anton eine Nachricht m senden, die ausschließlich Anton lesen kann.
- Sie rechnet $c :\underset{n}{\equiv} m^e$
- und sendet c an Anton.

Berta

Anton

RSA Public Key Method

2.) operating phase: encryption

- Berta will send a message m to Anton, which Anton can read exclusively.
- She calculates $c :\underset{n}{\equiv} m^e$
- and sends c to Anton.

Berta

Anton

RSA-Public-Key-Verfahren

2.) Anwendungsungsphase: Verschlüsselung

- Berta will Anton eine Nachricht m senden, die ausschließlich Anton lesen kann.
- Sie rechnet $c :\underset{n}{\equiv} m^e$
- und sendet c an Anton.

3.) Anwendungsungsphase: Entschlüsselung

- Anton erhält c und rechnet $M :\underset{n}{\equiv} c^d$

Anton liest M, denn es gilt $M = m$

Und warum klappt das?

Berta

Anton

RSA Public Key Method

2.) operating phase: encryption

- Berta will send a message m to Anton, which Anton can read exclusively.
- She calculates $c :\underset{n}{\equiv} m^e$
- and sends c to Anton.

2.) operating phase: decryption

- Anton receive c and calculate $M :\underset{n}{\equiv} c^d$

Anton read M ,because there is: $M = m$

Why does it work?

Berta

Anton

RSA-Public-Key-Verfahren

4.) Zum Beweis

Es sind zwei Moduln im Spiel: Z_n^* und Z_φ^*

Dabei ist $\varphi = (p-1)\cdot(q-1)$ die Ordnung von Z_n^*

allg. das kleinste gemeinsame Vielfache aller Ordnungen.

Beim Potenzieren modulo n kann man also in den Exponenten modulo φ rechnen. — Eulerscher Satz

Man bestimmt zu **e** aus Z_n^* ein **d** so, dass gilt: $e \cdot d \underset{\varphi}{\equiv} 1$

In dieser Vorlesung und der Klausur ist d gegeben.
Man muss allenfalls nachrechnen.

RSA Public Key Method

4.) proof

there are two Moduls: Z_n^* and Z_φ^*

It is $\varphi = (p-1)\cdot(q-1)$ the Order of Z_n^*

That means the number of Elements, it is generally the lowes common multiple of the orders of all elements.

In potentiating modulo n you can calculate in the exponents modulo φ. — Eulerscher Satz

For **e** aus Z_n^* you have to find **d** so, that: $e \cdot d \underset{\varphi}{\equiv} 1$

In this lecture and the exam d is given, you must only poof.

RSA-Public-Key-Verfahren

4.) Zum Beweis

Es sind zwei Moduln im Spiel: Z_n^* Z_φ^*

Dabei ist $\varphi = (p-1)\cdot(q-1)$ die Ordnung von Z_n^*

das ist die Elementezahl , allg. das kleinste gemeinsame Vielfache aller Ordnungen .

Wegen $e \cdot d \underset{\varphi}{\equiv} 1$ heißt d das Inverse von e modulo φ .

$$M \underset{n}{\equiv} c^d = (m^e)^d = m^{e\,d} \underset{n}{\equiv} m^1 = m$$

Darum klappt das also.

RSA Public Key Method

4.) proof

there are two Moduls: Z_n^* and Z_φ^*

It is $\varphi = (p-1)\cdot(q-1)$ the Order of Z_n^*
That means the number of Elements, it is generally the lowest common multiple of the orders of all elements.

because $e \cdot d \underset{\varphi}{\equiv} 1$ the name of d is the inverse of e modulo φ .

$$M \underset{n}{\equiv} c^d = (m^e)^d = m^{e\,d} \underset{n}{\equiv} m^1 = m$$

That's why it works.

Was ist mit der Scheckkarte?

Die PIN wird nicht zur Bank übertragen, sondern aus Kontonummer und Bankleitzahl berechnet.
s.u.

Unterschriftsberechtigter:	HBCI mit PIN/TAN
Medium:	HBCI mit PIN/TAN
Konto:	Privatgiro - 00521133
BLZ:	24050110
PIN	*****

What's whith the Credit Card?

The PIN is not transported to the bank, but it is calculated with account number and bank code number.

Unterschriftsberechtigter:	HBCI mit PIN/TAN
Medium:	HBCI mit PIN/TAN
Konto:	Privatgiro - 00521133
BLZ:	24050110
PIN	*****

Was ist mit der Scheckkarte?

Auf der Karte sind gespeichert:

Kontonummer, Bankleitzahl, Verfallsdatum, Fehlbedienungszähler

Triple-DES ← geheimer Schlüssel

Benutzer gibt die PIN ein

Die PIN wird berechnet.

PIN > Sind sie gleich? < PIN

What's whith the Credit Card?

Upon the card are served

account number, bank code number, expiration date, a counter for false use

Triple-DES ← secret key

user give the PIN

The PIN is calculated.

PIN > are they equal? < PIN

Ein weites Feld

Public-Key-Verfahren

No-Key-Verfahren

Zero-Knowledge-Verfahren

Challenge-and-Response-Verfahren

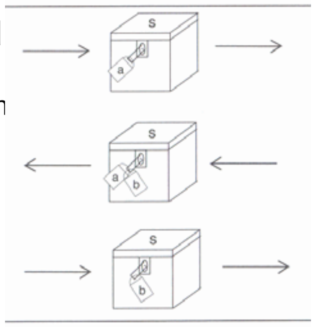


Bild 3.7: Shamir´s No-Key-Protokoll

$s = s^{aa'} \bmod p$ und $s = s^{bb'} \bmod p$. $s^{a \cdot b \cdot a' \cdot b'} \equiv_p s$

An Unending Field

public-key-method

no-key-method

zero-knowledge-method

challenge-and-response-method

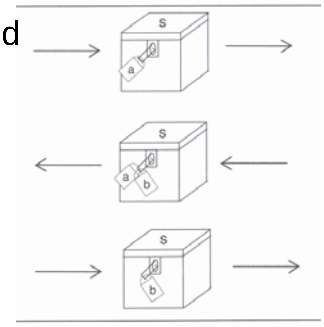


Bild 3.7: Shamir´s No-Key-Protokoll

$s = s^{aa'} \bmod p$ und $s = s^{bb'} \bmod p$. $s^{a \cdot b \cdot a' \cdot b'} \equiv_p s$

Was leistet die moderne Kryptografie?

- Geheimhaltung, sichere Kommunikation
- Echtheitsprüfungen (Authentifikation)
  - der Nachrichten
  - von Personen
  - digitale Signatur
- Anonymität
  - Elektronisches Geld,
  - Elektronische Wahlen....

What Can Modern Cryptography Achieve?

- to keep secrets, safe communikation
- Authentifikation
  - of the messages
  - of the persons
  - digitale signatur
- Anonymity
  - elektronic money,
  - elektronic voting....

Wodurch wird moderne Kryptografie möglich?

Durch:

Mathematik

Zusammen mit Informatik und Technik

Whereby is Modern Cryptography Possible?

by:

Mathematics

together with computer science and technology