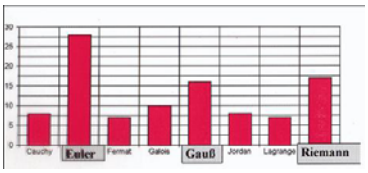
LEUPHANA
UNIVERSITÄT LÜNEBURG

Mathematik für alle



die acht bedeutendsten Mathematiker,

gemessen an nach ihnen benannten Objekten

Bernhard Riemann

Abitur 1846 am Johanneum Lüneburg

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.
Prime numbers n are the numbers with exact two divisors.

Primfaktorzerlegung

Trage deinen Geburtstag – oder eine beliebige Zahl – in dem Kasten ein:

Geburtstag 250 348

Das ist die Primfaktorzerlegung deines Geburtages –oder der Zahl–:

(Angegeben ist jeder Primfaktor und sein Exponent)

{{2, 2}, {7, 1}, {8941, 1}}

www.mathematik-sehen-und-verstehen.de/02krypto/krypto.htm

WolframAlpha Factor[250348]

Primzahlen finden

Nächst größere Primzahl:

Bestimme die nächtgrößere Primzahl. NextPrime[z]

Nächste Primzahl 1 234 567 890 123 456 789

Ergebnis:

1 234 567 890 123 456 817

www.mathematik-sehen-und-verstehen.de/02krypto/krypto.htm

WolframAlpha NextPrime[2014]

Was ist denn mit den Primzahlen?

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

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

Für viel größere Zahlen hat man Chancen für spezielle Primzahltypen.

Größte 2014 bekannte Primzahl

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

eine Zahl mit 17 425 170 (dezimalen) Stellen, die am 2. Februar 2014 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** $2^p - 1$

Diese Größenordnung ist für die Kryptografie unbrauchbar.

Tragende Begriffe der Kryptografie

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

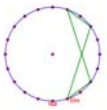
k ist Ordnung von a in Z(m): $a^k \underset{n}{\equiv} 1$ k minimal

Die Potenzen von 3 modulo 20 $3^4 \underset{10}{\equiv} 1$ 4minimal

Potenzen von 3 in Z = {1, 3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049

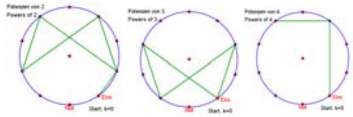
Potenzen von 3 in Z(20)= {1, 3, 9, 7, 1, 3, 9, 7, 1, 3, 9, 7, 1, 3, 9, 7, 1}

3 hat in Z (20) die **Ordnung 4,** denn $a^k \underset{n}{\equiv} 1$



k ist also die „Länge" des Polygons, das die 1 enthält.

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?

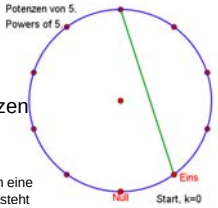
Potenzen von 2 in Z= {1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024
Powers of 2 in Z(10)= {1, 2, 4, 8, 6, 2, 4, 8, 6, 2, 4, 8, 6}
Potenzen von 3 in Z= {1, 3, 9, 27, 81, 243, 729, 2187, 6561,
Powers of 3 in Z(10)= {1, 3, 9, 7, 1, 3, 9, 7, 1, 3, 9, 7, 1}
Potenzen von 4 in Z= {1, 4, 16, 64, 256, 1024, 4096, 16384,
Powers of 4 in Z(10)= {1, 4, 6, 4, 6, 4, 6, 4, 6, 4, 6, 4, 6}
Potenzen von 7 in Z= {1, 7, 49, 343, 2401, 16807, 117649, 823543, 5764801,
Powers of 7 in Z(10)= {1, 7, 9, 3, 1, 7, 9, 3, 1, 7, 9, 3, 1, 7, 9, 3, 1}

Wissenschaftstheorie:
Wir schließen durch „Induktion", lassen uns „hineinführen von der Sache selbst":

Vermutung
Hypothese
Theorie (i.S.WT)

Ist a ungerade, dann gibt es Potenzen $a^k=1$
Ist a gerade, dann gibt es keine Potenzen $a^k=1$

Gegenbeispiel



5 ist ungerade,
dennoch erreichen die Potenzen modulo 10
niemals wieder die 1

Beweis von „niemals": Multipliziere schriftlich eine Zahl mit 5 am Ende mit der Zahl 5, dann entsteht als letzte Ziffer 5.

Potenzen von 5 in Z= {1, 5, 25, 125, 625, 3125, 15625, 78125, 390625, 1953125, 97
Powers of 5 in Z(10)= {1, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5}

Die Vermutung
Hypothese
Theorie (i.S.WT)

Ist a ungerade, dann gibt es Potenzen a^k=1

ist falsch, sie ist durch ein

einziges Gegenbeispiel „falsifiziert".

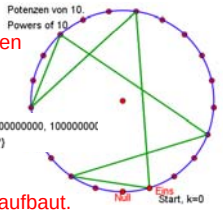
Suche nach einer neuen

Vermutung
Hypothese
Theorie (i.S.WT)

Ist a teilerfremd zu m, dann gibt es Potenzen mit a^k=1 modulo m

Diese Aussage ist verträglich mit den bisherigen Beobachtungen. Wir beobachten weiter.

Der „Falsifikationismus" sucht nach neuen Falsifikationen. (Popper)



Potenzen von 10 in Z= {1, 10, 100, 1000, 10000, 100000, 1000000, 10000000, 100000000, 10000000
Powers of 10 in Z(21)= {1, 10, 16, 13, 4, 19, 1, 10, 16, 13, 4, 19, 1, 10, 16, 13, ?}

Die Mathematiker suchen nach einem **Beweis**, der auf schon Bewiesenem aufbaut.

Beweis

Vermutung
Hypothese
Theorie (i.S.WT)

Ist a teilerfremd zu m, dann gibt es Potenzen mit $a^k=1$ modulo m

Es gibt seit 2300 Jahren den Euklidischen Algorithmus: zur Erzeugung der größten gemeinsamen Teilers ggT(m,a) und zwei ganze Zahlen s und t mit ggT(m,a)=s m + t a. (VSD)
a und m sind teilerfremd heißt: ggT(m,a)=1.

Vielfachsummen-Darstellung.

$1 = sm + ta \quad \| \quad a^2 = a^{2+k}$
$1 \underset{m}{\equiv} ta \quad \| \quad t^k a^k = t^k a^2 \cdot a^k$
$1 = 1 \cdot a^k$
$1 = a^k$

es gibt ein Inverses t zu a

weil es in Z_m nur endlich viele Elemente gibt.

Satz: Ist a teilerfremd zu m, dann gibt es Potenzen mit $a^k=1$ modulo m

Ein bewiesener (mathematischer) Satz, (theorem) ist nie mehr falsch.

Beweis

Vermutung
Hypothese
Theorie (i.S.WT)

Ist a teilerfremd zu m, dann gibt es Potenzen mit
$a^k=1$ modulo m

Es gibt seit 2300 Jahren den Euklidischen Algorithmus: zur Erzeugung der größten gemeinsamen Teilers ggT(m,a) und zwei ganze Zahlen s und t mit ggT(m,a)=s m + t a. (VSD) Vielfachsummen-Darstellung.
a und m sind teilerfremd heißt: ggT(m,a)=1.

$1 = sm + ta \quad \| \quad a^2 = a^{2+k}$

$1 \equiv ta \pmod{m} \quad \| \quad t^t a^t = t^t a^t \cdot a^k$

$1 = 1 \cdot a^k$

$1 = a^k$

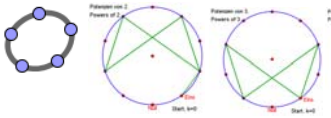
es gibt ein Inverses t zu a

weil es in Z_m nur endlich viele Elemente gibt.

Satz: Ist a teilerfremd zu m, dann gibt es Potenzen mit
$a^k=1$ modulo m

Ein bewiesener (mathematischer) Satz, (theorem) ist nie mehr falsch.

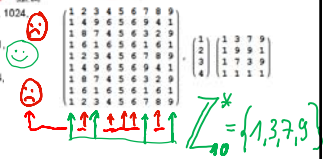
Hat jedes Element von Z(n)eine Ordnung?
Are there elements in Z(n) without an order?



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}



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.

Erweiterter Euklidischer Algorithmus

Erweiterter Euklidischer Algorithmus
Vielfachsummendarstellung VSD: ggT(a,b)= s a + t b

a 20
b 7

Das Ergebnis ist die Liste {ggT(a,b),{s,t}}:

{1, {-1, 3}}

www.mathematik-sehen-und-verstehen.de/02krypto/krypto.htm

ExtendedGcd[7,4,23]

WolframAlpha

Modulare Potenzen

Sehr große und auch negative Basen, Exponenten

Basis 7
Exponent k 4
Modulzahl 23

Ergebnis:

9

$7^4 \equiv \ldots\ldots \pmod{23}$

www.mathematik-sehen-und-verstehen.de/02krypto/krypto.htm

PowerMod[7,4,23]

WolframAlpha

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

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

Prim und nicht prim

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

Was nützt die 1?

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

Anton rechnet $7^4 \cdot 2401$ $7^8 \cdot 5764801$
Anton gibt die Zahl 2401 an Berta
m=5 ist Bertas geheime Nachricht für Anton.
Berta rechnet $5 \cdot 2401 \cdot 12005$,
dies sendet sie Anton.

Anton rechnet: $12005 \cdot 5764801 \cdot 69206436005 \bmod(69206436005,13) \cdot 5$

Wer abhört, kann selbst die Nachricht ausrechnen

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!

Was nützt die 1 und modulo?

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

Anton rechnet 9*3=1 modulo 13
Anton gibt die Zahl 9 und die modulo-Zahl 13 an Berta
m=5 ist Bertas geheime Nachricht für Anton.
Berta rechnet $5 \cdot 9 = 45 \equiv_{13} 6$
dies sendet sie Anton.

Anton rechnet: $6 \cdot 3 = 18 \equiv_{13} 5$

Wer alles abhört, kann selbst die Nachricht ausrechnen

Anton kann jetzt Bertas Nachricht, nämlich die 5, lesen.

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

Die schlechte Nachricht: Das obige Verfahren ist total unsicher!

Eulerscher Satz, Euler's theorem

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

$|\mathbb{Z}_n^*| = \varphi \Rightarrow$ sprich phi

$a^{\varphi} \equiv 1$

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

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

$\leftarrow a^6 \equiv_{14} 1$

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

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

$\leftarrow a^8 \equiv_{15} 1$

Kleiner Satz von Fermat
Fermats little theorem

a ist nicht Vielfaches von p

p prim $\Rightarrow a^{p-1} \equiv_p 1$


Fermat, Pierre
1606-1665

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.

PowerMod[1234,5616,5617] → 3563 ⇒ 5619 ist keine Primzahl

WolframAlpha

PowerMod[1234,5622,5623] → 1 5623 ist Kanditat für Primzahl

NextPrime[5600] → 5623 Mathematica sagt: yes prime

Kleiner Satz von Fermat ist nicht umkehrbar
not conversable

a ist nicht Vielfaches von p

p prim $\Rightarrow a^{p-1} \equiv_p 1$ $\not\Leftarrow$


Fermat, Pierre
1601-1667

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

$15^{340} \equiv_{341} 1$

aber $341 = 11 \cdot 31 \Rightarrow$ nicht prim

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

Primzahl-Tests

- Es gibt noch etliche pfiffige Primzahltests.
  More sophisticated prime tests, i.e. Miller-Rabbin test
- Sie sind auch bei großen Zahlen bis **10^300 effektiv**.
- Sie beruhen auf mathematischer Theorie.
- Die tragenden Themen/ topics heißen
  - Zahlentheorie / number theory
  - Algebra / algebra
  - Theorie der komplexen Funktionen, complex functions

If „little Fermat" gives 1 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.

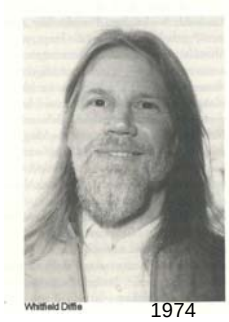
Darauf beruht die Sicherheit in der Kryptografie.

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.

Wie kam es zur modernen Kryptografie?



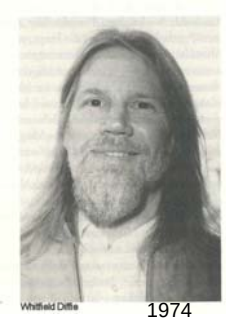
1974

lesen aus

Simon Singh: Codes, Wien, 2001

S. 215 ff (Auch Titel: Geheimschriften)

Diffie-Hellmann Verfahren



1974

Stanford University

Diffie-Hellman Schlüsselvereinbarung

key exchange, better: key agreement

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

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

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

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".

Diffie-Hellman Schlüsselvereinbarung,

key exchange, better: key agreement

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

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

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

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

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".

Beweis der „Durchführbarkeit",

proof of viability,

dass also das Verfahren stets klappt.

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

$k_a = (g^b)^a$

Beweis der „Durchführbarkeit",

proof of viability,

dass also das Verfahren stets klappt.

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

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

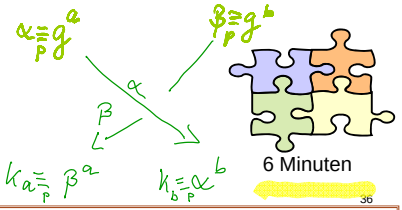
Also $k_a = g^{ba} = g^{ab} = k_b$

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



Vergleichen Sie k
compare k

Nehmen sie evt.
andere Zahlen.

6 Minuten

Wie sieht das in der Realität aus?

Diffie-Hellmann-Verfahren, realisiert in MuPAD
oder in Mathematica oder in TI Nspire CAS, usw.

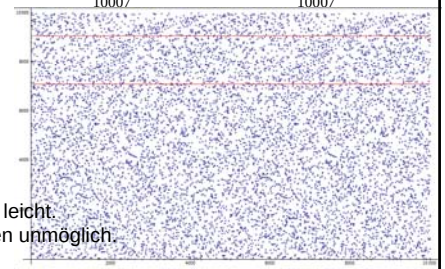
- Das Grund Problem der „alten“ Kryptografie ist gelöst,
- Der Schüssel wird nicht ausgetauscht,
- sondern kryptografisch sicher vereinbart.
- Nun kann man mit dem One-Time-Pad sicher kommunizieren.

Warum hat Mister X keine Chance?

Mister X fängt ab: $p = 10007 \quad g = 6784$
$\alpha = 9088 \quad \beta = 7100$

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

Nutzlos!



Nadel im
Heuhaufen!

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

Das war nur der Anfang

Ronald Rivest, Adi Shamir und Leonard Adleman

RSA-Verschlüsselung
Public-Key-Kryptografie
asymmetrisches Verfahren

lesen
Singh,
231ff

RSA-Public-Key-Verfahren

1.) Schlüsselerzeugungsphase

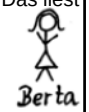
- Anton wählt zwei Primzahlen p und q
- Er rechnet $n := p\,q \qquad \varphi := (p-1)(q-1)$
- Wählt beliebig e mit $e < \varphi$ und e teilerfremd zu φ
- Er berechnet d als Inverses von e im Modul $\mathbb{Z}^*(\varphi)$.
  er hält d streng geheim.

$e \cdot d \equiv 1 \mod \varphi$

Mein öffentliches Schlüsselpaar ist:

(e,n)

Das liest



RSA-Public-Key-Verfahren

Antons Key $(7, 143)$

$p = 11 \quad q = 13$
$n = 143 \quad \varphi = 10 \cdot 12 = 120$
$e = 7 \quad d = 103$

e d=1
mod p

2.) Anwendungsphase: Verschlüsselung

11,13

RSA-Public-Key-Verfahren

2.) Anwendungsungsphase: Verschlüsselung

- Berta will Anton eine Nachricht m senden, die ausschließlich Anton lesen kann.
- Sie rechnet $c :\equiv_n m^e$

m = 13

$C \equiv_{143} 13^7 = 117$

- und sendet c an Anton.

11,13

RSA-Public-Key-Verfahren

Antons Key $(7, 143)$

$p = 11 \quad q = 13$

$n = 143 \quad \varphi = 10 \cdot 12 = 120$

$e = 7 \quad d = 103$

e d=1 mod φ

2.) Anwendungsungsphase: Verschlüsselung

m = 13 $\quad c :\equiv_n m^e \quad c \equiv_{143} 13^7 = 117$

und sendet c an Anton

11,13

$M :\equiv_n c^d \equiv_{143}^{103} 117 \equiv_{143} ?$

RSA-Public-Key-Verfahren

2.) Anwendungsungsphase: Verschlüsselung

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

3.) Anwendungsungsphase: Entschlüsselung

- Anton erhält c und rechnet $M :\equiv_n c^d$

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

Und warum klappt das?

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: $e \cdot d \equiv_\varphi 1$

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

RSA-Public-Key-Verfahren

4.) Zum Beweis

Es sind zwei Moduln im Spiel: Z_n^* $\quad Z_\varphi^*$

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 $e \cdot d \equiv_\varphi 1$ heißt d das Inverse von e modulo φ .

$$M \equiv_n c^d = (m^e)^d = m^{e\,d} \equiv_n m^1 = m$$

Darum klappt das also.

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

Was ist mit der Scheckkarte?

Auf der Karte sind gespeichert:

Kontonummer, Bankleitzahl,
Verfallsdatum,
Fehlbedienungszähler

Triple-DES ← geheimer Schlüssel

Die PIN wird berechnet.

Benutzer gibt die PIN ein

PIN — Sind sie gleich? — PIN

Ein weites Feld

Public-Key-Verfahren

No-Key-Verfahren

Zero-Knowledge-Verfahren

Challenge-and-Response-Verfahren

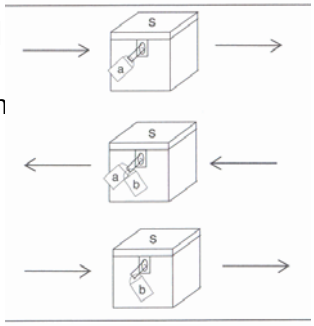


Bild 3.7: Shamir´s No-Key-Protokoll

$s = s^{aa'} \bmod p$ und $s = s^{bb'} \bmod p$.

Was leistet die moderne Kryptografie?

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

Wodurch wird moderne Kryptografie möglich?

Durch:

Mathematik

Zusammen mit Informatik und Technik