

Verschlüsselung durch Exponentiation (POHLIG, HELLMAN, 1976)

- p : eine (grosse) Primzahl
- e : Zahl $0 < e < p$ mit $\text{ggT}(e, p - 1) = 1$
- d Inverses von e in \mathbb{Z}_{p-1}^* , d.h. $d \cdot e \equiv 1 \pmod{p-1}$ ($= \phi(p)$)
- M : numerisch codierter Text
- M in Blöcke M_i mit $0 < M_i < p$ zerlegen ($i=1,2,3,\dots$)
- Codierung (*encryption*)

$$M_i \mapsto C_i := M_i^e \pmod{p}$$

($i=1,2,3,\dots$)

- Decodierung (*decryption*)

$$C_i \mapsto C_i^d \equiv (M_i^e)^d \equiv (M_i)^{e \cdot d} \equiv M_i^{k \cdot \phi(p)+1} \equiv M_i \pmod{p}$$

($i=1,2,3,\dots$)

1

Verschlüsselung

$$\begin{array}{rcl} C_1 & = & 0514^{91} \pmod{7951} = 2174 \\ C_2 & = & 0318^{91} \pmod{7951} = 4468 \\ C_3 & = & 2516^{91} \pmod{7951} = 7889 \\ \vdots & & \vdots \\ C_{11} & = & 1400^{91} \pmod{7951} = 7114 \end{array}$$

Ciphertext

2174 4468 7889 6582 0924 5460 7868 7319 0726 2890 7114

Entschlüsselung

$$\begin{array}{rcl} M_1 & = & 2174^{961} \pmod{7951} = 514 \\ M_2 & = & 4468^{961} \pmod{7951} = 318 \\ M_3 & = & 7889^{961} \pmod{7951} = 2516 \\ \vdots & & \vdots \\ M_{11} & = & 7114^{961} \pmod{7951} = 1400 \end{array}$$

3

numerische Codierung

□	A	B	C	D	...	Y	Z
↓	↓	↓	↓	↓	...	↓	↓
00	01	02	03	04	...	25	26

Parameter: $p = 7951, e = 91, d = 961$

Text: ENCRYPTION REGULATION

Numerisch codierter Text;

$M = 05\ 14\ 03\ 18\ 25\ 16\ 20\ 09\ 15\ 14\ 00\ 18\ 05\ 07\ 21\ 12\ 01\ 20\ 09\ 15\ 14\ 00$

Zerlegung in Blöcke mit je 4 Ziffern

0514 0318 2516 2009 1514 0018 0507 2112 0120 0915 1400

2

Public-Key-Kryptographie

- Ziel: sicherer Informationsaustausch zwischen Teilnehmern $\{Alice, Bob, Caesar, \dots\}$ an einem öffentlichen Netz, bei dem die transportierten (verschlüsselten) Daten abgehört werden können
- Klassisch ("symmetrische Kryptosysteme", z.B. DES): jedes Paar $\langle A, B \rangle$ von Teilnehmern besitzt identische Schlüssel zum Verschlüsseln und Entschlüsseln, die nur diesen bekannt sind
Problem: wie können A und B identische Schlüssel erhalten/erzeugen?

als nicht-technische Lektüre dringendst empfohlen:

S. Singh, *Geheime Botschaften*, dtv, 2001. (Engl.: *The Code Book*)

4

- Public-Key-Idee (“asymmetrisch”, W. Diffie, M. Hellman, 1976):
Schlüssel über das Netz selbst zugänglich machen
 - Jeder Teilnehmer B erzeugt ein Paar $\langle k_E, k_D \rangle$ von Schlüsseln,
 - k_E wird von B öffentlich bekanntgegeben (“Telefonbuch”),
 k_D bleibt Geheimnis von B
 - Will eine Teilnehmerin A am Netz eine Nachricht N in verschlüsselter Form an B schicken, so
 - * besorgt sich A den Schlüssel k_E (unverschlüsselt) aus dem Telefonbuch
 - * verschlüsselt N mittels k_E zu $\mathcal{E}(N, k_E)$ mittels eines geeigneten Verfahrens \mathcal{E} und sendet $\mathcal{E}(N, k_E)$ zu B
 - * B erhält $\mathcal{E}(N, k_E)$ und entschlüsselt dies zu $\mathcal{D}(\mathcal{E}(N, k_E), k_D) = N$ mit Hilfe eines geeigneten Verfahrens \mathcal{D}
 - Sicherheit: mit vernünftigen Aufwand
 - * aus verschlüsselter Nachricht $\mathcal{E}(N, k_E)$ keine Rückschlüsse auf N
 - * aus der Kenntnis von k_E keine Kenntnis von k_D
- möglich, auch wenn Verfahren \mathcal{E} und \mathcal{D} öffentlich bekannt sind

5

Das RSA-Verfahren

R. RIVEST, A. SHAMIR, L. ADLEMAN, A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Communications of the ACM*, 21 (1978), 120–126

O.E.: Nachrichten sind als (Blöcke von) positiven ganzen Zahlen codiert

Jeder Teilnehmer am System

- wählt zwei grosse Primzahlen p und q (typisch: ≥ 100 Dezimalstellen)
- berechnet $n = p \cdot q$ und $\phi(n) = (p - 1)(q - 1)$
- wählt eine grosse “zufällige” ungerade Zahl d mit $1 < d < \phi(n)$ und $\text{ggT}(d, \phi(n)) = 1$
- berechnet $e = d^{-1} \bmod \phi(n)$
- veröffentlicht das Paar $k_E = (e, n)$ als öffentlichen Schlüssel
- hält die Daten (d, p, q) geheim, privater Schlüssel $k_D = (d, n)$
- Verschlüsselung: $\mathcal{E}_{(e,n)} : \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n^* : N \mapsto N^e \bmod n$
- Entschlüsselung: $\mathcal{D}_{(d,n)} : \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n^* : C \mapsto C^d \bmod n$

7

alternative Verwendung asymmetrischer Systeme:

Authentifizieren von (nicht geheimen) Nachrichten, falls

$$\mathcal{D}(\mathcal{E}(N, k_E), k_D) = N = \mathcal{E}(\mathcal{D}(N, k_D), k_E)$$

- B benutzt seinen privaten Schlüssel k_D um Nachricht N zu “verschlüsseln”: $\mathcal{D}(N, k_D)$ (“Signatur”)
- B sendet $\langle N, \mathcal{D}(N, k_D) \rangle$ zu A
- A verschlüsselt die Signatur $\mathcal{D}(N, k_D)$ mit k_E und vergleicht das Ergebnis $\mathcal{E}(\mathcal{D}(N, k_D), k_E)$ mit der Nachricht N

6

Demonstrationsbeispiel

Systemparameter:

$p=$	47	Primzahl
$q=$	59	Primzahl
$n = p \cdot q=$	2773	
$\phi(n)=$	$(p - 1)(q - 1) = 2668$	EULERS Funktion
$d=$	157	$\text{ggT}(d, \phi(n)) = 1$
$e = d^{-1} \bmod \phi(n)=$	17	mittels erweitertem EA
$k_E=$	(17, 2773)	öffentlicher Schlüssel
$k_D=$	(157, 2773)	privater Schlüssel

8

Text

ITS ALL GREEK TO ME

W. SHAKESPEARE, *Julius Cesar*, 1. Akt, 2. Szene

numerisch codierter Text

0920 1900 0112 1200 0718 0505 1100 2015 0013 0500

Verschlüsselung

$$C_1 = 920^{17} \bmod 2773 = 948$$

$$C_2 = 1900^{17} \bmod 2773 = 2342$$

$$C_3 = 0112^{17} \bmod 2773 = 1084$$

$$\vdots \quad \quad \quad \vdots$$

$$C_{10} = 0500^{17} \bmod 2773 = 1665$$

Ciphertext

0948 2342 1084 1444 2663 2390 0778 0774 0219 1655

Klassisches Beispiel 1

Parameter:

$$n = \text{RSA-129} = 114381625757888867669235779976146612010218296721242362562$$

$$561842935706935245733897830597123563958705058989075147599290026879543541$$

$$e = 9007$$

Text:

ITS ALL GREEK TO ME

W. SHAKESPEARE, *Julius Cesar*, 1. Akt, 2. Szene

numerisch codierter Text

09201900011212000718050511002015001305

verschlüsselter Text:

1999351314978051004523171227402606474232040170583914631037037174

0625971608948927504309920962672582675012893554461353823769748026

Entschlüsselung

Ciphertext

0948 2342 1084 1444 2663 2390 0778 0774 0219 1655

$$M_1 = 948^{157} \bmod 2773 = 920$$

$$M_2 = 2342^{157} \bmod 2773 = 1900$$

$$M_3 = 1084^{157} \bmod 2773 = 0112$$

$$\vdots \quad \quad \quad \vdots$$

$$M_{10} = 1665^{157} \bmod 2773 = 0500$$

numerisch codierter Text

$M = 0920 1900 0112 1200 0718 0505 1100 2015 0013 0500$

Text

ITS ALL GREEK TO ME

Klassisches Beispiel 2: das 100 \$ - RSA -Problem

M. GARDNER, "Mathematical Games - A New Kind of Cipher that Would Take Millions of Years to Break", *Scientific American*, 237, 2 (1977), 120-124.

Parameter:

$$n = 114381625757888867669235779976146612010218296721242362562561842$$

$$935706935245733897830597123563958705058989075147599290026879543541$$

$$e = 9007$$

numerisch codierter Text:

9686961375462206147714092225435588290575999112457

4319874695120930816298225145708356931476622883989

628013391990551829945157815154

Faktorisierung von RSA-129

D. ATKINS, M. GRAFF, A. K. LENSTRA, P. LEYLAND et al.,
2. April 1994, mit Aufwand von ca. 5000 mips-Jahren, 8 Monate
Rechenzeit auf ≥ 600 workstations
Methode: “Multiple Polynomial Quadratic Sieve”

RSA-129 ist das Produkt der beiden Primzahlen

$p = 3490529510847650949147849619903898133417764638493387843990820577$
 $q = 32769132993266709549961988190834461413177642967992942539798288533$

Zur Entschlüsselung benötigt man das Inverse d von $e = 9007$ modulo
 $\phi(n) = \phi(p \cdot q) = (p - 1)(q - 1)$

$d = 1066986143685780244428687713289201547807099066339$
 $3786280122622449663106312591177447087334016859746$
 $2306553968544513277109053606095$

13

Nach Entschlüsselung

2008050013010709030023151804190001180500191721050
11309190800151919090618010705

Übersetzung in Text

THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE

15

Die Entschlüsselung

$$M \mapsto M^d \bmod n$$

wird mittels “Schneller Exponentiation” in \mathbb{Z}_n ausgeführt, wobei man die 426
Bit lange Binärdarstellung von d verwendet

100111011001111110010100110010001000001000001110100111100100110
01001111010011100000000000001111110100001101010110001011101111
01010000111110110000001000001110110101010111101010100111110110
11010000111110100000011110100110001011001011001101001010001100
100111010110000101110100101011010000011100000001110001110101010
011011101000111101001110001101011010101010010011101010001001111
000000100111010011000110111110101100100011001111

14

Die Verschlüsselungsabbildung

$$N \mapsto N^e \bmod n$$

wird natürlich auch mittels “Schneller Exponentiation” in \mathbb{Z}_n^* ausgeführt,
wobei $e = 9007$ die Binärdarstellung

10001100101111

hat

16

Die 100\$-Nachricht von RIVEST, SHAMIR, ADLEMAN war signiert mit Hilfe der Entschlüsselungsabbildung:

1671786115038084424601527138916839824543690103235831121783503
8446929062655448792237114490509578608655662496577974840004057020373

Mittels Verschlüsselungsabbildung erhält man

06091819200019151222051800230914190015140500082114041805040004151212011819

im Klartext:

FIRST SOLVER WINS ONE HUNDRED DOLLARS

17

Effizienz

- grosse Primzahlen p, q mittels randomisiertem Primzahltest gewinnen: mittlere Anzahl der Versuche um eine ℓ -stellige Primzahl zu finden ist wegen Primzahlsatz $\in \Theta(\ell)$
- Multiplikationen $n = p \cdot q$ und $\phi(n) = (p-1)(q-1)$
- Exponent d zufällig wählen und mittels EA auf Teilerfremdheit mit $\phi(n)$ testen
- Inverses $e = d^{-1} \bmod \phi(n)$ mittels erweitertem EA berechnen
- Ver- und Entschlüsselung mittels schneller Exponentiation (Quadrieren und Multiplizieren)

19

Korrektheit

- für die Hintereinanderausführung von Verschlüsselung und Entschlüsselung

$$N \xrightarrow{\mathcal{E}_{(e,n)}} N^e \bmod n \xrightarrow{\mathcal{D}_{(d,n)}} (N^e)^d \bmod n$$

für $N \in \mathbb{Z}_n^*$ und $e \cdot d = 1 + k \cdot \phi(n)$

gilt wegen des Satzes von Euler:

$$N^{ed} \equiv N^{1+k \cdot \phi(n)} \equiv N \cdot (N^{\phi(n)})^k \equiv N \cdot 1 \equiv N \bmod n$$

18

Sicherheit

- Wenn es einem Angreifer gelingt, die Faktorisierung $n = p \cdot q$ zu ermitteln, kann er auch $d = e^{-1} \bmod \phi(n)$ mittels EA berechnen
- Bislang keine wirklich effizienten Faktorisierungsalgorithmen bekannt (aber: Quantencomputer? Algorithmus von Shor (1994))
- Ist es wirklich nötig, n zu faktorisieren, um RSA zu brechen? (wenn man n und $\phi(n)$ kennt, kann man p und q berechnen! Wie?)
- RSA hat "Schwachstellen", die man respektieren sollte (z.B. sehr kleine e bzw. d , oder wenn $p-1$ und $q-1$ viele kleine Primteiler haben)

Empfohlene Lektüre:

D. Boneh, *Twenty Years of Attacks on the RSA Cryptosystem*,
Notices of the American Mathematical Society, vol. 46, 203–213, 1999.
<http://www.ams.org/notices/199902/199902-toc.html>

20

aus: Eric Weisstein's Mathworld

⇒ <http://mathworld.wolfram.com/news/2003-12-05/rsa/>

MathWorld Headline News

RSA-576 Factored

By Eric W. Weisstein

December 5, 2003--On December 3, the day after the announcement of the discovery of the largest known prime by the Great Internet Mersenne Prime Search on December 2 (*MathWorld* headline news, [December 2, 2003](#)), a team at the German Federal Agency for Information Technology Security (BIS) announced the factorization of the 174-digit number

1881 9881292060 7963838697 2394616504 3980716356 3379417382
7007633564 2298885971 5234665485 3190606065 0474304531
7388011303 3967161996 9232120573 4031879550 6569962213
0516875930 7650257059

known as RSA-576.

RSA numbers are [composite numbers](#) having exactly two [prime factors](#) (i.e., so-called [semiprimes](#)) that have been listed in the Factoring Challenge of RSA Security®.

21

RSA-Aufgaben

- In einem RSA-System wird der Ciphertext 10 übertragen. Der öffentliche Schlüssel ist $(5, 35)$. Welches war die Nachricht?

Lösung:

- $n = 35 = 5 \cdot 7 \Rightarrow \phi(n) = (5 - 1)(7 - 1) = 24$
- $e = 5 \Rightarrow d = 5^{-1} \bmod 24 = 5$
- $10^5 \bmod 35 = 5 \bmod 35 \Rightarrow M = 5$

- Ein RSA-System hat $(31, 3599)$ als öffentlichen Schlüssel. Welches ist der private Schlüssel?

Lösung:

- $n = 3599 = 59 \cdot 61 \Rightarrow \phi(n) = 58 \cdot 60 = 3480$
- $d = 31^{-1} \bmod 3480 = -499 \bmod 3480 = 3031$ folgt aus eeA mit Bézout-Beziehung

$$4 \cdot 3480 - 449 \cdot 31 = 1$$

- privater Schlüssel $(3031, 3599)$

23

number	digits	prize	factored
RSA-100	100		Apr. 1991
RSA-110	110		Apr. 1992
RSA-120	120		Jun. 1993
RSA-129	129	\$100	Apr. 1994
RSA-130	130		Apr. 10, 1996
RSA-140	140		Feb. 2, 1999
RSA-150	150	withdrawn?	open [see postscript]
RSA-155	155		Aug. 22, 1999
RSA-160	160		Apr. 1, 2003
RSA-576	174	\$10,000	Dec. 3, 2003
RSA-640	193	\$20,000	open
RSA-704	212	\$30,000	open
RSA-768	232	\$50,000	open
RSA-896	270	\$75,000	open
RSA-1024	309	\$100,000	open
RSA-1536	463	\$150,000	open
RSA-2048	617	\$200,000	open

Postscript added August 24, 2004:

RSA-150 was factored into two 75-digit primes by Aoki *et al.* in a [preprint](#) dated April 16, 2004.

22