

## ECE 646 - Lecture 9

### RSA – Genesis, operation & security

1

---

---

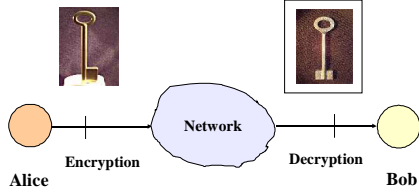
---

---

### Public Key (Asymmetric) Cryptosystems

Public key of Bob -  $K_B$

Private key of Bob -  $k_B$



2

---

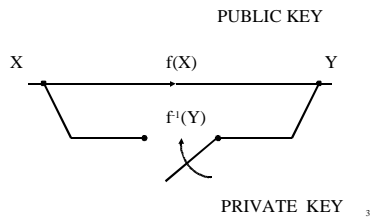
---

---

---

### Trap-door one-way function

Whitfield Diffie and Martin Hellman  
"New directions in cryptography," 1976



3

---

---

---

---

**Professional (NSA) vs. amateur (academic)  
approach to designing ciphers**

- |   |  |
|---|--|
| 1. Know how to break Russian ciphers        | 1. Know nothing about cryptology               |
| 2. Use only well-established proven methods | 2. Think of revolutionary ideas                |
| 3. Hire 50,000 mathematicians               | 3. Go for skiing                               |
| 4. Cooperate with an industry giant         | 4. Publish in "Scientific American"            |
| 5. Keep as much as possible secret          | 5. Offer a \$100 award for breaking the cipher |

4

---

---

---

---



---

---

---

---



---

---

---

---




---



---



---



---

**Challenge published in Scientific American**

Ciphertext: 1977

9686 9613 7546 2206 1477 1409 2225 4355  
 8829 0575 9991 1245 7431 9874 6951 2093  
 0816 2982 2514 5708 3569 3147 6622 8839  
 8962 8013 3919 9055 1829 9451 5781 5145

**Public key:**

N = 114381625757 88886766923577997614  
 661201021829672124236256256184293  
 570693524573389783059712356395870  
 5058989075147599290026879543541

e = 9007 (129 decimal digits)

*Award \$100*

---



---

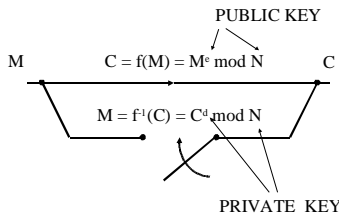


---



---

**RSA as a trap-door one-way function**




---



---



---



---

## More Number Theory

- Recall “The Ring  $\mathbb{Z}_m$ ” from Lecture 5
- Assume  $m = 26$ 
  - What are the elements of  $\mathbb{Z}_m$ ?
  - How many elements have a multiplicative inverse?
  - How can we determine this number?
  - What is the condition for an element of  $\mathbb{Z}_m$  to have a multiplicative inverse?

10

---

---

---

---

## Euler's Phi Function

**Definition:** The number of integers in  $\mathbb{Z}_m$  relatively prime to  $m$  is denoted by  $\phi(m)$ .

11

---

---

---

---

## Example

$$m = 6; \mathbb{Z}_6 =$$

12

---

---

---

---

## Example 2

$$m = 5; \mathbb{Z}_5 =$$

17

---

---

---

---

**Theorem:** If  $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_n^{e_n}$  where  $p_i$  are prime numbers and  $e_i$  are integers, then:

$$\phi(m) = \prod_{i=1}^n (p_i^{e_i} - p_i^{e_i-1})$$

Example:

$$m = 40 = 8 \cdot 5 = 2^3 \cdot 5 = p_1^{e_1} \cdot p_2^{e_2}$$

$$\phi(m) = (2^3 - 2^2)(5^1 - 5^0) = (8 - 4)(5 - 1) = 4 \cdot 4 = 16$$

22

---

---

---

---

*Leonard Euler, 1707-1783*

## Euler's Theorem

If  $\gcd(a, m) = 1$ , then:

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Example:

$$m = 6; a = 5$$

$$\phi(6) = \phi(3 \cdot 2) = (3 - 1)(2 - 1) = 2$$

$$5^{\phi(6)} = 5^2 = 25 \equiv 1 \pmod{6}$$

23

---

---

---

---

### Euler's Theorem - Justification (1)

#### For N=10

$$R = \{1, 3, 7, 9\}$$

Let  $a=3$

$$S = \{ 3 \cdot 1 \bmod 10, \\ 3 \cdot 3 \bmod 10, 3 \cdot 7 \bmod 10, \\ 3 \cdot 9 \bmod 10 \} \\ = \{3, 9, 1, 7\}$$

#### For arbitrary N

$$R = \{x_1, x_2, \dots, x_{\phi(N)}\}$$

Let us choose arbitrary  $a$ , such that  $\gcd(a, N) = 1$

$$S = \{a \cdot x_1 \bmod N, a \cdot x_2 \bmod N, \dots, \\ a \cdot x_{\phi(N)} \bmod N\} \\ = \text{rearranged set } R$$

24

---



---



---



---

### Euler's Theorem - Justification (2)

#### For N=10

$$R = S$$

$$x_1 \cdot x_2 \cdot x_3 \cdot x_4 \equiv \\ (a \cdot x_1) \cdot (a \cdot x_2) \cdot (a \cdot x_3) \cdot (a \cdot x_4) \bmod N$$

$$x_1 \cdot x_2 \cdot x_3 \cdot x_4 \equiv \\ a^4 \cdot x_1 \cdot x_2 \cdot x_3 \cdot x_4 \bmod N$$

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

#### For arbitrary N

$$R = S$$

$$\prod_{i=1}^{\phi(N)} x_i \equiv \prod_{i=1}^{\phi(N)} a \cdot x_i \pmod{N}$$

$$\prod_{i=1}^{\phi(N)} x_i \equiv a^{\phi(N)} \cdot \prod_{i=1}^{\phi(N)} x_i \pmod{N}$$

$$a^{\phi(N)} \equiv 1 \pmod{N}$$

25

---



---



---



---

### RSA Setup

- Choose two large primes  $p, q$ .
- Compute  $n = p \cdot q$
- Compute  $\phi(n) = (p-1)(q-1)$
- Choose random  $e$ ;  
 $0 < e < \phi(n)$  with  $\gcd(e, \phi(n)) = 1$   
 (note  $e$  has inverse in  $\mathbb{Z}_{\phi(n)}$ ).
- Compute inverse  $d = e^{-1} \bmod \phi(n)$   
 $e \cdot d \equiv 1 \bmod \phi(n)$

26

---



---



---



---

### RSA keys

PUBLIC KEY

PRIVATE KEY

$\{ e, n \}$    $\{ d, p, q \}$

$n = p \cdot q$       $p, q$  - large prime numbers

$e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$

27

---

---

---

---

---

### RSA Encryption / Decryption

• Encryption  $y = C, x = M$

$$y = e_{k_{pub}}(x) = x^e \pmod n$$

$$x \in \mathbb{Z}_n = 0, 1, \dots, n-1$$

• Decryption  $x = d_{k_{priv}}(y) = y^d \pmod n$

28

---

---

---

---

---

### Example

on board

29

---

---

---

---

---

### Why does RSA work? (1)

$$M' = C^d \bmod N = (M^e \bmod N)^d \bmod N \stackrel{?}{=} M$$

decrypted message original message

$$e \cdot d \equiv 1 \pmod{(P-1)(Q-1)}$$



$$e \cdot d \equiv 1 \pmod{\phi(N)}$$

Euler's totient function

30

---

---

---

---

---

### Why does RSA work? (2)

$$\begin{aligned} M' &= C^d \bmod n = (M^e \bmod n)^d \bmod n = \\ &= M^{e \cdot d} \bmod n = \begin{vmatrix} e \cdot d \equiv 1 \pmod{\phi(n)} \\ e \cdot d = 1 + k \cdot \phi(n) \end{vmatrix} = \\ &= M^{1+k \cdot \phi(n)} \bmod n = M \cdot (M^{\phi(n)})^k \bmod n = \\ &= M \cdot (M^{\phi(n)} \bmod n)^k \bmod n = \\ &= M \cdot 1^k \bmod n = M \\ \text{iff } \gcd(M, n) &= \gcd(M, p \cdot q) = 1 \end{aligned}$$

31

---

---

---

---

---

### Why does RSA work (3)

- if  $\gcd(M, n) = \gcd(M, p \cdot q) \neq 1$

Either  $M = r \cdot p$  or  $M = s \cdot q$

where  $r, s$  are integers such that:  $r < q, s < p$

assume  $M = r \cdot p \Rightarrow \gcd(M, q) = 1$

$$\begin{aligned} (M^{\phi(n)})^k &= (M^{(q-1)(p-1)})^k = (M^{\phi(q)(p-1)})^k \\ &= ((M^{\phi(q)})^{p-1})^k \equiv 1^{(p-1)k} = 1 \pmod{q} \end{aligned}$$

$$(M^{\phi(n)})^k \equiv 1 \pmod{q} \Rightarrow (M^{\phi(n)})^k = 1 + c \cdot q; c \text{ is integer}$$

$$\begin{aligned} M \cdot (M^{\phi(n)})^k &= M + M \cdot c \cdot q = x + r \cdot p \cdot c \cdot q = x + r \cdot c \cdot p \cdot q \\ &= x + r \cdot c \cdot n \equiv x \pmod{n} \end{aligned}$$

$$M \cdot (M^{\phi(n)})^k \equiv x \pmod{n} \quad 32$$

---

---

---

---

---

**Rivest estimation - 1977**

The best known algorithm for factoring a 129-digit number requires:

**40 000 trillion years**  
**=  $40 \cdot 10^{15}$  years**

assuming the use of a supercomputer being able to perform

1 multiplication of 129 decimal digit numbers in 1 ns

*Rivest's assumption translates to the delay of a single logic gate  $\approx 10$  ps*

**Estimated age of the universe: 100 bln years =  $10^{11}$  years**

33

---

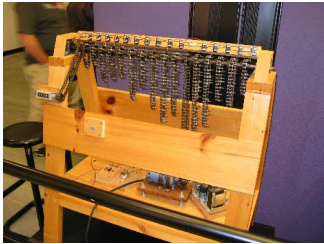
---

---

---

**Lehmer Sieve**

**Bicycle chain sieve [D. H. Lehmer, 1928]**



Computer Museum, Mountain View, CA

---

---

---

---



Machine à Congruences [E. O. Carissan, 1919]

---

---

---

---

### Supercomputer Cray



Computer Museum, Mountain View, CA

---

---

---

---

### Early records in factoring large numbers

Years	Number of decimal digits	Number of bits	Required computational power (in MIPS-years)
1974	45	149	0.001
1984	71	235	0.1
1991	100	332	7
1992	110	365	75
1993	120	398	830

37

---

---

---

---

### How to factor for free?

*A. Lenstra & M. Manasse, 1989*

- Using the spare time of computers, (otherwise unused)
- Program and results sent by e-mail (later using WWW)

38

---

---

---

---

<b>Practical implementations of attacks</b>				
<b>Factorization, RSA</b>				
<b>Year</b>	<b>Number of bits of N</b>	<b>Number of decimal digits of N</b>	<b>Method</b>	<b>Estimated amount of computations</b>
1994	430	129	QS	5000 MIPS-years
1996	433	130	GNFS	750 MIPS-years
1998	467	140	GNFS	2000 MIPS-years
<b>1999</b>	<b>467</b>	<b>140</b>	<b>GNFS</b>	<b>8000 MIPS-years</b>

---



---



---



---

**Breaking RSA-129**

**When:** August 1993 - 1 April 1994, **8 months**

**Who:** D. Atkins, M. Graff, A. K. Lenstra, P. Leyland  
+ 600 volunteers from the entire world

**How:** **1600 computers**  
from Cray C90, through 16 MHz PC,  
to fax machines

*Only 0.03% computational power of the Internet*

**Results of cryptanalysis:**

*"The magic words are squeamish ossifrage"*

An award of \$100 donated to Free Software Foundation<sup>40</sup>

---



---



---



---

**Elements affecting the progress  
in factoring large numbers**

- computational power  
1977-1993 increase of about 1500 times
- computer networks  
Internet
- **better algorithms**

---



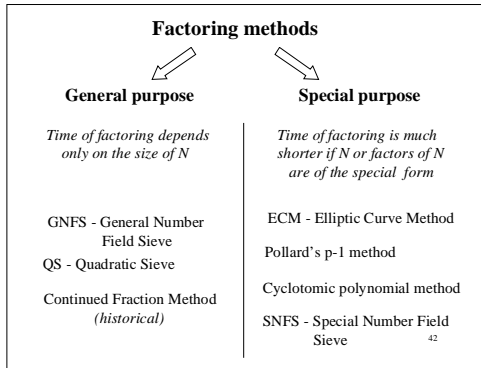
---



---



---




---

---

---

---

---

**Running time of factoring algorithms**

$L_q[\alpha, c] = \exp((c+o(1)) \cdot (\ln q)^{-\alpha} \cdot (\ln \ln q)^{1-\alpha})$

**For  $\alpha=0$**   
 $L_q[0, c] = (\ln q)^{c+o(1)}$

**For  $\alpha=1$**   
 $L_q[1, c] = \exp((c+o(1)) \cdot (\ln q))$

**For  $0 < \alpha < 1$**

Algorithm **polynomial** as a function of the number of bits of  $q$

Algorithm **exponential** as a function of the number of bits of  $q$

Algorithm **subexponential** as a function of the number of bits of  $q$

$f(n) = o(1)$  if for any positive constant  $c > 0$  there exist a constant  $n_0 > 0$ , such that  $0 \leq f(n) < c$ , for all  $n \geq n_0$  <sup>43</sup>

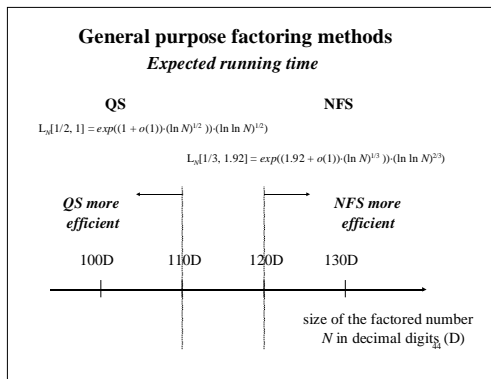
---

---

---

---

---




---

---

---

---

---

### First RSA Challenge

RSA-100  
 RSA-110  
 RSA-120  
 RSA-130  
 RSA-140  
 RSA-150  
 RSA-160  
 RSA-170  
 RSA-180  
 RSA-190  
RSA-200  
 RSA-210  
 .....  
 RSA-450  
 RSA-460  
 RSA-470  
 RSA-480  
 RSA-490  
 RSA-500

Largest number factored to date

**RSA-200**    May 2005

---



---



---



---

### Second RSA Challenge

Length of N in bits	Length of N in decimal digits	Award for factorization
<del>576</del>	<del>174</del>	<del>\$10,000</del>
<del>640</del>	<del>193</del>	<del>\$20,000</del>
704	212	\$30,000
768	232	\$50,000
896	270	\$75,000
1024	309	\$100,000
1536	463	\$150,000
2048	617	\$200,000

---



---



---



---

### Number of bits vs. number of decimal digits

$$10^{\#digits} = 2^{\#bits}$$

$$\#digits = (\log_{10} 2) \cdot \#bits \approx 0.30 \cdot \#bits$$

256 bits = 77 D  
 384 bits = 116 D  
 512 bits = 154 D  
 768 bits = 231 D  
 1024 bits = 308 D  
 2048 bits = 616 D

---



---



---



---

### Factoring 512-bit number

512 bits = 155 decimal digits  
old standard for key sizes in RSA

17 March - 22 August 1999

Group of Herman te Riele  
Centre for Mathematics and Computer Science  
(CWI), Amsterdam

First stage 2 months

168 workstations SGI and Sun, 175-400 MHz  
120 Pentium PC, 300-450 MHz, 64 MB RAM  
4 stations Digital/Compaq, 500 MHz

Second stage

Cray C916 - 10 days, 2.3 GB RAM <sup>48</sup>

---

---

---

---

---

### Factoring RSA-576

512 bits = 155 decimal digits

When?

Announced: December 3, 2003

Who?

J. Franke and T. Kleinjung  
Bonn University  
Max Planck Institute for Mathematics in Bonn  
Experimental Mathematics Institute in Essen

P. Montgomery and H. te Riele - CWI  
F. Bahr, D. Leclair, P. Leyland and R. Wackerbarth

German Federal Agency for Information  
Technology Security (BIS) <sup>49</sup>

---

---

---

---

---

### Factoring RSA-200

200 decimal digits = 664 bits

When?

Dec 2003 - May 2005

Who?

CWI (Netherlands), Bonn University,  
Max Planck Institute for Mathematics in Bonn  
Experimental Mathematics Institute in Essen  
German Federal Agency for Information  
Technology Security (BIS)

Effort?

First stage About 1 year on various machines, equivalent to  
55 years on Opteron 2.2 GHz CPU

Second stage

3 months on a cluster of 80 2.2 GHz Opterons  
connected via a Gigabit network <sup>50</sup>

---

---

---

---

---

**Factoring RSA-640**

**When?** 640 bits = 193 decimal digits  
June 2005 - Nov 2005

**Who?** *CWI (Netherlands), Bonn University,  
Max Planck Institute for Mathematics in Bonn  
Experimental Mathematics Institute in Essen  
German Federal Agency for Information  
Technology Security (BIS)*

**Effort?**

First stage 3 months on 80 Opteron 2.2 GHz CPUs

Second stage  
1.5 months on a cluster of 80 2.2 GHz Opterons  
connected via a Gigabit network

51

---

---

---

---

---

**For the most recent records see**

**Factorization Announcements at**

<http://www.crypto-world.com/FactorAnnouncements.html>

52

---

---

---

---

---

**TWINKLE**  
**“The Weizmann INstitute Key Locating Engine”**

*Adi Shamir, Eurocrypt, May 1999  
CHES, August 1999*

**Electrooptical device capable to speed-up  
the first phase of factorization from 100 to 1000 times**

**If ever built it would increase the size of the key  
that can be broken from 100 to 200 bits**

**Cost of the device (assuming that the prototype was  
earlier built) - \$5000**

53

---

---

---

---

---

### Recommended key sizes for RSA

**Old standard:**

Individual users

~~512 bits~~  
(155 decimal digits)

**New standard:**

Individual users

768 bits  
(231 decimal digits)

Organizations (short term)

1024 bits  
(308 decimal digits)

Organizations (long term)

2048 bits  
(616 decimal digits)<sub>54</sub>

---

---

---

---

### Keylengths in public key cryptosystems that provide the same level of security as AES and other secret-key ciphers

Arjen K. Lenstra, Eric R. Verheul  
„*Selecting Cryptographic Key Sizes*”  
*Journal of Cryptology*

Arjen K. Lenstra  
„*Unbelievable Security: Matching AES Security Using Public Key Systems*”  
ASIACRYPT' 2001

55

---

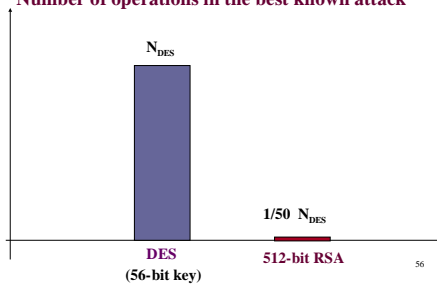
---

---

---

### RSA vs. DES: Resistance to attack

Number of operations in the best known attack



56

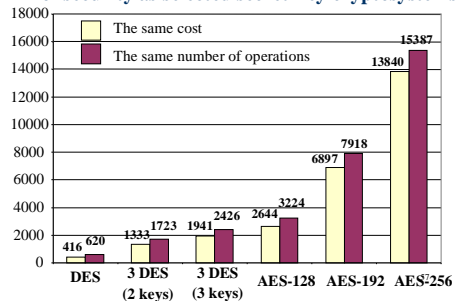
---

---

---

---

**Keylengths in RSA providing the same level of security as selected secret-key cryptosystems**




---



---

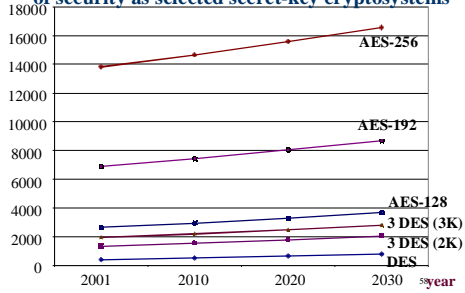


---



---

**Keylengths in RSA providing the same level of security as selected secret-key cryptosystems**




---



---



---



---

**Practical progress in factorization**

**March 2002, Financial Cryptography Conference**

**Nicko van Someren, CTO nCipher Inc.**  
 announced that his company developed software  
 capable of breaking 512-bit RSA key  
 within **6 weeks**  
 using computers available in a single office

---



---



---



---

### Bernstein's Machine (1)

Fall 2001

**Daniel Bernstein**, professor of mathematics at University of Illinois in Chicago submits a grant application to NSF and publishes fragments of this application as an article on the web

D. Bernstein, *Circuits for Integer Factorization: A Proposal*

<http://cr.yp.to/papers.html#npscircuit>

60

---

---

---

---

### Bernstein's Machine (2)

March 2002

- Bernstein's article "discovered" during *Financial Cryptography Conference*
- Informal panel devoted to analysis of consequences of the Bernstein's discovery
- Nicko Van Someren (nCipher) estimates that machine costing \$ **1 billion** is able to break **1024-bit RSA** within **several minutes**

61

---

---

---

---

### Bernstein's Machine (3)

March 2002

- **alarming voices** on e-mailing discussion lists calling for revocation of all currently used 1024-bit keys
- **sensational articles** in newspapers about Bernstein's discovery

62

---

---

---

---

### Bernstein's Machine (4)

April 2002

#### Response of the RSA Security Inc.:

Error in the estimation presented at the conference:  
according to formulas from the Bernstein's article  
machine costing

**\$ 1 billion** is able to break  
**1024-bit RSA** within

**10 billion x several minuts = tens of years**

According to estimations of Lenstra i Verheul, machine  
breaking **1024-bit RSA** within **one day**  
would cost **\$ 160 billion** in 2002

63

---

---

---

---

---

### Bernstein's Machine (5)

Carl Pomerance, Bell Labs:

„...fresh and fascinating idea...”

Arjen Lenstra, Citibank & U. Eindhoven:

„...I have no idea what is this all fuss about...”

Bruce Schneier, Counterpane:

„ ... enormous improvements claimed are more a result  
of redefining efficiency than anything else...”

64

---

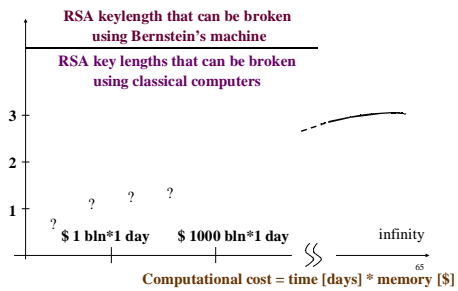
---

---

---

---

### Bernstein's Machine (6)



---

---

---

---

---

**Estimation of RSA Security Inc. regarding  
the number and memory of PCs  
necessary to break RSA-1024**

**Attack time: 1 year**

**Single machine: PC, 500 MHz, 170 GB RAM**

**Number of machines: 342,000,000**

66

---

---

---

---

**TWIRL** *February 2003*

*Adi Shamir & Eran Tromer, Weizmann Institute of Science*

Hardware implementation of the sieving phase of  
Number Field Sieve (NFS)

**Assumed technology:**

CMOS, 0.13  $\mu\text{m}$   
clock 1 GHz

30 cm semiconductor wafers at the cost of \$5,000 each

67

---

---

---

---

**TWIRL**

*A. Shamir, E. Tromer  
Crypto 2003*

**Tentative estimations  
(no experimental data):**

**512-bit RSA:**

**< 10 minutes  
\$ 10 k**

**1024-bit RSA:**

**< 1 year  
\$ 10 million**

68

---

---

---

---

Estimated recurring costs with  
current technology (US\$×year)

by Eran Tromer, May 2005

	768-bit	1024-bit
Traditional PC-based	1.3×10 <sup>7</sup>	10 <sup>12</sup>
TWINKLE	8×10 <sup>6</sup>	
TWIRL	5×10 <sup>3</sup>	10 <sup>6</sup>
Mesh-based	3×10 <sup>4</sup>	
SHARK		2.3×10 <sup>8</sup>

But: NRE, chip size, chip transport networks...<sup>69</sup>

---

---

---

---

---

Workshop Series

**SHARCS - Special-purpose Hardware  
for Attacking Cryptographic Systems**

1st edition: Paris, February 24-25, 2005  
2nd edition: Cologne, April 03-04, 2006

See

<http://www.ruhr-uni-bochum.de/itsc/tanja/SHARCS/>

70

---

---

---

---

---

Recommendations of RSA Security Inc.

May 6, 2003

Validity period	Minimal RSA key length (bits)	Equivalent symmetric key length (bits)
2003-2010	1024	80
2010-2030	2048	112
2030-	3072	128

71

---

---

---

---

---

**Five security levels  
allowed by American government**  
NIST SP 800-56

Level	RSA / DH	ECC	Symmetric ciphers
I	1024	160	80
II	2048	224	112
III	3072	256	128
IV	8192	384	192
V	15360	512	256 <sup>72</sup>

---



---



---



---

**ACM A.M. Turing Award  
2002**



**R. Rivest  
A. Shamir  
L. Adleman**

“For Seminal Contributions  
to the Theory and Practical Applications of  
Public Key Cryptography”

73

---



---



---



---

**On-line Turing Award Lectures**

[http://www.acm.org/awards/turing\\_citations/rivest-shamir-adleman.html](http://www.acm.org/awards/turing_citations/rivest-shamir-adleman.html)



Dr. Leonard M. Adleman  
*University of Southern California*  
**Pre RSA Days**

Dr. Ronald L. Rivest  
*Massachusetts Institute of Technology*  
**Early RSA Days**

Dr. Adi Shamir  
*The Weizmann Institute*  
**Cryptology: A Status Report**

74

---



---



---



---



---

---

---

---

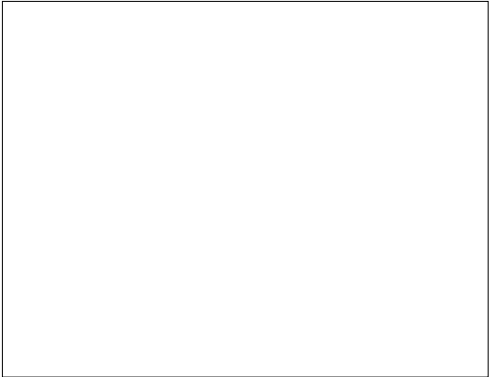


---

---

---

---



---

---

---

---