Factoring integers, Producing primes and the RSA cryptosystem

University of Pedagogy

Ho Chi Minh City

Trường Đại Học Sư Phạm

Thành Phố Hồ Chí Minh

December 12, 2005

RSA_{2048} = 25195908475657893494027183240048398571429282126204
032027777137836043662020707595556264018525880784406918290641249
515082189298559149176184502808489120072844992687392807287776735
971418347270261896375014971824691165077613379859095700097330459
748808428401797429100642458691817195118746121515172654632282216
869987549182422433637259085141865462043576798423387184774447920
739934236584823824281198163815010674810451660377306056201619676
256133844143603833904414952634432190114657544454178424020924616
515723350778707749817125772467962926386356373289912154831438167
899885040445364023527381951378636564391212010397122822120720357

RSA_{2048} = 25195908475657893494027183240048398571429282126204
032027777137836043662020707595556264018525880784406918290641249
5150821892985591491761845028084891200728449926873928072877776735
9714183472702618963750149718246911650776133798590957000973304597
4880842840179742910064245869181719511874612151517265463228221686
9987549182422433637259085141865462043576798423387184774447920739
9342365848238242811981638150106748104516603773060562016196762561
3384414360383390441495263443219011465754445417842402092461651572
3350778707749817125772467962926386356373289912154831438167899885
04044536402352738195137863656439121201039712282212072035 7

RSA_{2048} is a 617 (decimal) digit number

$$
\begin{aligned}
RSA_{2048} = {} & 25195908475657893494027183240048398571429282126204\\
& 032027777137836043662020707595556264018525880784406918290641249\\
& 515082189298559149176184502808489120072844992687392807287776735\\
& 971418347270261896375014971824691165077613379859095700097330459\\
& 748808428401797429100642458691817195118746121515172654632282216\\
& 869987549182422433637259085141865462043576798423387184774447920\\
& 739934236584823824281198163815010674810451660377306056201619676\\
& 256133844143603833904414952634432190114657544454178424020920924616\\
& 515723350778707749817125772467962926386356373289912154831438167\\
& 899885040445364023527381951378636564391212010397122822120720357
\end{aligned}
$$

RSA_{2048} is a 617 (decimal) digit number

`http://www.rsasecurity.com/rsalabs/node.asp?id=2093`

$$RSA_{2048} = p \cdot q, \quad p, q \approx 10^{308}$$

$$RSA_{2048} = p \cdot q, \quad p, q \approx 10^{308}$$

PROBLEM: *Compute p and q*

$$RSA_{2048} = p \cdot q, \quad p, q \approx 10^{308}$$

PROBLEM: *Compute p and q*

PRICE: 200.000 US$ ($\sim 15,894.00$ VND)!!

$$RSA_{2048}{=}p \cdot q, \quad p, q \approx 10^{308}$$

PROBLEM: *Compute p and q*

PRICE: 200.000 US\$ ($\sim 15,894.00$ VND)!!

Theorem. If $a \in \mathbb{N} \quad \exists!\ p_1 < p_2 < \cdots < p_k$ *primes*

s.t. $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$$RSA_{2048}=p\cdot q, \quad p,q\approx 10^{308}$$

$\boxed{\textbf{PROBLEM: } \textit{Compute } p \textit{ and } q}$

PRICE: 200.000 US\$ ($\sim 15,894.00$ VND)!!

Theorem. If $a\in\mathbb{N}$ $\exists!\ p_1<p_2<\cdots<p_k$ *primes* s.t. $a=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$

Regrettably: RSAlabs believes that factoring in one year requires:

number	computers	memory
RSA_{1620}	1.6×10^{15}	120 Tb
RSA_{1024}	$342,000,000$	170 Gb
RSA_{760}	215,000	4Gb.

http://www.rsasecurity.com/rsalabs/node.asp?id=2093

http://www.rsasecurity.com/rsalabs/node.asp?id=2093

Challenge Number	Prize ($US)
RSA_{576}	\$10,000
RSA_{640}	\$20,000
RSA_{704}	\$30,000
RSA_{768}	\$50,000
RSA_{896}	\$75,000
RSA_{1024}	\$100,000
RSA_{1536}	\$150,000
RSA_{2048}	\$200,000

http://www.rsasecurity.com/rsalabs/node.asp?id=2093

Challenge Number	Prize ($US)	Status
RSA_{576}	$10,000	Factored December 2003
RSA_{640}	$20,000	Not Factored
RSA_{704}	$30,000	Not Factored
RSA_{768}	$50,000	Not Factored
RSA_{896}	$75,000	Not Factored
RSA_{1024}	$100,000	Not Factored
RSA_{1536}	$150,000	Not Factored
RSA_{2048}	$200,000	Not Factored

History of the "Art of Factoring"

History of the "Art of Factoring"

- 220 BC Greeks (Eratosthenes of Cyrene)

History of the "Art of Factoring"

- 220 BC Greeks (Eratosthenes of Cyrene)
- 1730 Euler $2^{2^5}+1=641\cdot 6700417$

History of the "Art of Factoring"

- 220 BC Greeks (Eratosthenes of Cyrene)
- 1730 Euler $2^{2^5}+1=641\cdot 6700417$
- 1750–1800 Fermat, Gauss (Sieves - Tables)

History of the "Art of Factoring"

- 220 BC Greeks (Eratosthenes of Cyrene)
- 1730 Euler $2^{2^5} + 1 = 641 \cdot 6700417$
- 1750–1800 Fermat, Gauss (Sieves - Tables)
- 1880 Landry & Le Lasseur: $2^{2^6} + 1 = 274177 \times 67280421310721$

History of the "Art of Factoring"

- 220 BC Greeks (Eratosthenes of Cyrene)
- 1730 Euler $2^{2^5} + 1 = 641 \cdot 6700417$
- 1750–1800 Fermat, Gauss (Sieves - Tables)
- 1880 Landry & Le Lasseur: $2^{2^6} + 1 = 274177 \times 67280421310721$
- 1919 Pierre and Eugène Carissan (Factoring Machine)

History of the "Art of Factoring"

- 220 BC Greeks (Eratosthenes of Cyrene)
- 1730 Euler $2^{2^5} + 1 = 641 \cdot 6700417$
- 1750–1800 Fermat, Gauss (Sieves - Tables)
- 1880 Landry & Le Lasseur: $2^{2^6} + 1 = 274177 \times 67280421310721$
- 1919 Pierre and Eugène Carissan (Factoring Machine)
- 1970 Morrison & Brillhart
  $2^{2^7} + 1 = 59649589127497217 \times 5704689200685129054721$

History of the "Art of Factoring"

- 220 BC Greeks (Eratosthenes of Cyrene)
- 1730 Euler $2^{2^5}+1 = 641 \cdot 6700417$
- 1750–1800 Fermat, Gauss (Sieves - Tables)
- 1880 Landry & Le Lasseur: $2^{2^6}+1 = 274177 \times 67280421310721$
- 1919 Pierre and Eugène Carissan (Factoring Machine)
- 1970 Morrison & Brillhart
  $2^{2^7}+1 = 59649589127497217 \times 5704689200685129054721$
- 1980, Richard Brent and John Pollard $2^{2^8}+1 = 1238926361552897 \times 93461639715357977769163558199606896584051237541638188580280321$

History of the "Art of Factoring"

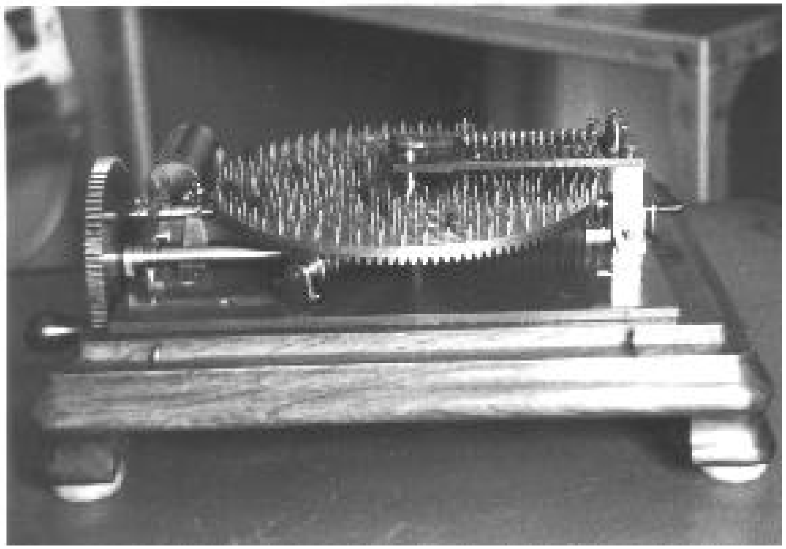
- 220 BC Greeks (Eratosthenes of Cyrene)
- 1730 Euler $2^{2^5}+1 = 641 \cdot 6700417$
- 1750–1800 Fermat, Gauss (Sieves - Tables)
- 1880 Landry & Le Lasseur: $2^{2^6}+1 = 274177 \times 67280421310721$
- 1919 Pierre and Eugène Carissan (Factoring Machine)
- 1970 Morrison & Brillhart
  $2^{2^7}+1 = 59649589127497217 \times 5704689200685129054721$
- 1980, Richard Brent and John Pollard $2^{2^8}+1 = 1238926361552897 \times$
  $93461639715357977769163558199606896584051237541638188580280321$
- 1982 Quadratic Sieve **QS** (Pomerance) $\rightsquigarrow$ Number Fields Sieve **NFS**

History of the "Art of Factoring"

- 220 BC Greeks (Eratosthenes of Cyrene)
- 1730 Euler $2^{2^5}+1=641\cdot 6700417$
- 1750–1800 Fermat, Gauss (Sieves - Tables)
- 1880 Landry & Le Lasseur: $2^{2^6}+1=274177\times 67280421310721$
- 1919 Pierre and Eugène Carissan (Factoring Machine)
- 1970 Morrison & Brillhart
  $2^{2^7}+1=59649589127497217\times 5704689200685129054721$
- 1980, Richard Brent and John Pollard $2^{2^8}+1=1238926361552897\times 93461639715357977769163558199606896584051237541638188580280321$
- 1982 Quadratic Sieve **QS** (Pomerance) $\rightsquigarrow$ Number Fields Sieve **NFS**
- 1987 Elliptic curves factoring **ECF** (Lenstra)

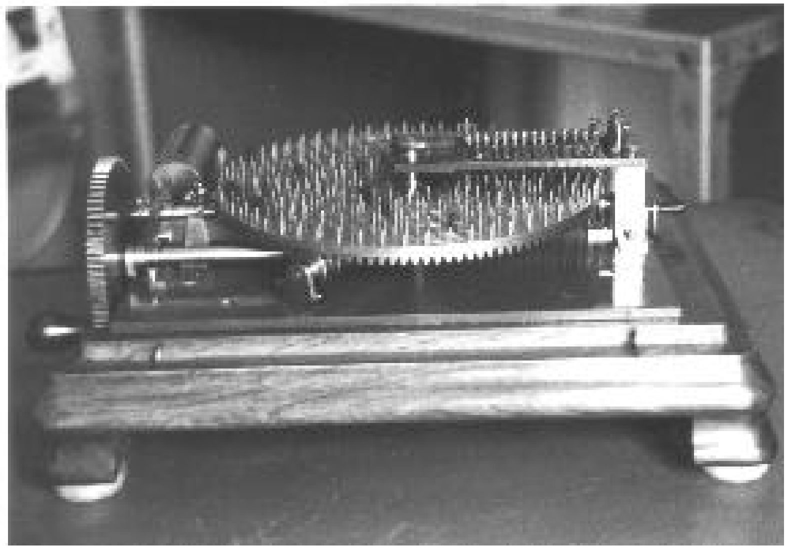
Carissan's ancient Factoring Machine

Carissan's ancient Factoring Machine



Hình 1: Conservatoire Nationale des Arts et Métiers in Paris

Carissan's ancient Factoring Machine



Hình 1: Conservatoire Nationale des Arts et Métiers in Paris

http://www.math.uwaterloo.ca/ shallit/Papers/carissan.html

Hình 2: Lieutenant Eugène Carissan

Hình 2: Lieutenant Eugène Carissan

$$225058681 = 229 \times 982789 \qquad \text{2 minutes}$$

$$3450315521 = 1409 \times 2418769 \qquad \text{3 minutes}$$

$$3570537526921 = 841249 \times 4244329 \qquad \text{18 minutes}$$

Contemporary Factoring 1/2

Contemporary Factoring 1/2

1. 1994, Quadratic Sieve (QS): (8 months, 600 voluntaries, 20 countries)
   D.Atkins, M. Graff, A. Lenstra, P. Leyland

$$
\begin{aligned}
RSA_{129} &= 114381625757888867669235779976146612010218296721242362562561842935706\\
&\quad 935245733897830597123563958705058989075147599290026879543541 =\\
&= 3490529510847650949147849619903898133417764638493387843990820577\times\\
&\quad 32769132993266709549961988190834461413177642967992942539798288533
\end{aligned}
$$

Contemporary Factoring 1/2

❶ 1994, Quadratic Sieve (QS): (8 months, 600 voluntaries, 20 countries)
D.Atkins, M. Graff, A. Lenstra, P. Leyland

$$\begin{aligned} RSA_{129} &= 114381625757888867669235779976146612010218296721242362562561842935706 \\ &\quad 935245733897830597123563958705058989075147599290026879543541 = \\ &= 3490529510847650949147849619903898133417764638493387843990820577 \times \\ &\quad 32769132993266709549961988190834461413177642967992942539798288533 \end{aligned}$$

❷ (February 2 1999), Number Fields Sieve (NFS): (160 Sun, 4 months)

$$\begin{aligned} RSA_{155} &= 1094173864157052742180970732204035761200373294544920599091384213147634998428 \\ &\quad 893478471799725789126733249762575289978183379707653724402714674353159335433897 = \\ &= 102639592829741105772054196573991675900716567808038066803341933521790711307779 \times \\ &\quad 106603488380168454820927220360012878679207958575989291522270608237193062808643 \end{aligned}$$

Contemporary Factoring 1/2

❶ 1994, Quadratic Sieve (QS): (8 months, 600 voluntaries, 20 countries)

D.Atkins, M. Graff, A. Lenstra, P. Leyland

$$RSA_{129} = 114381625757888867669235779976146612010218296721242362562561842935706\\935245733897830597123563958705058989075147599290026879543541 =\\= 3490529510847650949147849619903898133417764638493387843990820577\times\\32769132993266709549961988190834461413177642967992942539798288533$$

❷ (February 2 1999), Number Fields Sieve (NFS): (160 Sun, 4 months)

$$RSA_{155} = 1094173864157052742180970732204035761200373294544920599091384213147634998428\\8934784717997257891267332497625752899781833797076537244027146743531593354333897 =\\= 102639592829741105772054196573991675900716567808038066803341933521790711307779\times\\106603488380168454820927220360012878679207958575989291522270608237193062808643$$

❸ (December 3, 2003) (NFS): J. Franke et al. (174 decimal digits)

$$RSA_{576} = 1881988129206079638386972394616504398071635633794173827007633564229888597152346\\65485319060606504743045317388011303396716199692321205734031879550656996221305168759307650257059 =\\= 398075086424064937397125500550386491199064362342526708406385189575946388957261768583317\times\\472772146107435302536223071973048224632914695302097116459852171130520711256363590397527$$

Contemporary Factoring 1/2

1. 1994, Quadratic Sieve (QS): (8 months, 600 voluntaries, 20 countries)
   D.Atkins, M. Graff, A. Lenstra, P. Leyland

$$RSA_{129} = 114381625757888867669235779976146612010218296721242362562561842935706\\935245733897830597123563958705058989075147599290026879543541 =\\= 3490529510847650949147849619903898133417764638493387843990820577 \times\\32769132993266709549961988190834461413177642967992942539798288533$$

2. (February 2 1999), Number Fields Sieve (NFS): (160 Sun, 4 months)

$$RSA_{155} = 109417386415705274218097073220403576120037329454492059909138421314763499842\\88934784717997257891267332497625752899781833797076537244027146743531593354333897 =\\= 102639592829741105772054196573991675900716567808038066803341933521790711307779 \times\\106603488380168454820927220360012878679207958575989291522270608237193062808643$$

3. (December 3, 2003) (NFS): J. Franke et al. (174 decimal digits)

$$RSA_{576} = 1881988129206079638386972394616504398071635633794173827007633564229888597152346\\65485319060606504743045317388011303396716199692321205734031879550656996221305168759307650257059 =\\= 398075086424064937397125500550386491199064362342526708406385189575946388957261768583317 \times\\472772146107435302536223071973048224632914695302097116459852171130520711256363590397527$$

4. (May 9,2005) (NFS): F. Bahr, et al (663 binary digits)

$$RSA_{200} = 27997833911221327870829467638722601621070446786955428537560009929326128400107609345671052955360 8\\56061822351910951365788637105954482006576775098580557613579098734950144178863178946295187237869221823983 =\\3532461934402770121272604978198464368671197400197625023649303468776121253679423200058547956528088349 \times\\7925869954478333033347085841480059687737975857364219960734330341455767872818152135381409304740185467$$

Contemporary Factoring 2/2

Contemporary Factoring 2/2

Elliptic curves factoring (ECM) H. Lenstra (1985) - small factors (50 digits)

Contemporary Factoring 2/2

Elliptic curves factoring (ECM) H. Lenstra (1985) - small factors (50 digits)

❻ (1993) A. Lenstra, H. Lenstra, Jr., M. Manasse, and J. Pollard $2^{2^9}+1 = 2424833 \times 7455602825647884208337395736200454918783366342657 \times p99$

Contemporary Factoring 2/2

Elliptic curves factoring (ECM) H. Lenstra (1985) - small factors (50 digits)

- ❻ (1993) A. Lenstra, H. Lenstra, Jr., M. Manasse, and J. Pollard $2^{2^9}+1 = 2424833 \times 7455602825647884208337395736200454918783366342657 \times p99$
- ❻ (April 6, 2005) (ECM) B. Dodson $3^{466}+1$ is divisible by $709601635082267320966424084955776789770864725643996885415676682297$;

Contemporary Factoring 2/2

Elliptic curves factoring (ECM) H. Lenstra (1985) - small factors (50 digits)

- ❻ (1993) A. Lenstra, H. Lenstra, Jr., M. Manasse, and J. Pollard $2^{2^9} + 1 = 2424833 \times 7455602825647884208337395736200454918783366342657 \times p99$
- ❻ (April 6, 2005) (ECM) B. Dodson $3^{466} + 1$ is divisible by $709601635082267320966424084955776789770864725643996885415676682297$;
- ❼ (Sept. 5, 2005) (ECM) K. Aoki & T. Shimoyama $10^{311} - 1$ is divisible by $4344673058714954477761314793437392900672885445361103905548950933$

Contemporary Factoring 2/2

Elliptic curves factoring (ECM) H. Lenstra (1985) - small factors (50 digits)

- ❻ (1993) A. Lenstra, H. Lenstra, Jr., M. Manasse, and J. Pollard $2^{2^9}+1 = 2424833 \times 7455602825647884208337395736200454918783366342657 \times p99$
- ❻ (April 6, 2005) (ECM) B. Dodson $3^{466}+1$ is divisible by $709601635082267320966424084955776789770864725643996885415676682297$;
- ❼ (Sept. 5, 2005) (ECM) K. Aoki & T. Shimoyama $10^{311}-1$ is divisible by $4344673058714954477761314793437392900672885445361103905548950933$

For updates see Paul Zimmerman's "*Integer Factoring Records*":

`http://www.loria.fr/ zimmerma/records/factor.html`

Contemporary Factoring 2/2

Elliptic curves factoring (ECM) H. Lenstra (1985) - small factors (50 digits)

- ❻ (1993) A. Lenstra, H. Lenstra, Jr., M. Manasse, and J. Pollard $2^{2^9} + 1 = 2424833 \times 7455602825647884208337395736200454918783366342657 \times p99$
- ❻ (April 6, 2005) (ECM) B. Dodson $3^{466} + 1$ is divisible by 709601635082267320966424084955776789770864725643996885415676682297;
- ❼ (Sept. 5, 2005) (ECM) K. Aoki & T. Shimoyama $10^{311} - 1$ is divisible by 4344673058714954477761314793437392900672885445361103905548950933

For updates see Paul Zimmerman's "*Integer Factoring Records*":

`http://www.loria.fr/ zimmerma/records/factor.html`

More infoes about fatroring in

`http://www.crypto-world.com/FactorWorld.html`

Contemporary Factoring 2/2

Elliptic curves factoring (ECM) H. Lenstra (1985) - small factors (50 digits)

- ❻ (1993) A. Lenstra, H. Lenstra, Jr., M. Manasse, and J. Pollard $2^{2^9}+1 = 2424833 \times 7455602825647884208337395736200454918783366342657 \times p99$
- ❻ (April 6, 2005) (ECM) B. Dodson $3^{466}+1$ is divisible by $709601635082267320966424084955776789770864725643996885415676682297$;
- ❼ (Sept. 5, 2005) (ECM) K. Aoki & T. Shimoyama $10^{311}-1$ is divisible by $4344673058714954477761314793437392900672885445361103905548950933$

For updates see Paul Zimmerman's "*Integer Factoring Records*":

`http://www.loria.fr/ zimmerma/records/factor.html`

More infoes about fatroring in

`http://www.crypto-world.com/FactorWorld.html`

Update on "factorization of Fermat Numbers":

`http://www.prothsearch.net/fermat.html`

Last Minute News

Last Minute News

Date: Thu, 10 Nov 2005 22:07:26 -0500
From: Jens Franke <franke@math.uni-bonn.de>
To: NMBRTHRY@LISTSERV.NODAK.EDU

We have factored RSA640 by GNFS. The factors are

16347336458092538484431338838650908598417836700330
92312181110852389333100104508151212118167511579

and

19008712816648221131268515739354139754718967899685
15493666638539088027103802104498957191261465571

We did lattice sieving for most special q between 28e7 and 77e7 using factor base bounds of 28e7 on the algebraic side and 15e7 on the rational side. The bounds for large primes were 2 34. This produced 166e7 relations. After removing duplicates 143e7 relations remained. A filter job produced a matrix with 36e6 rows and columns, having 74e8 non-zero entries. This was solved by Block-Lanczos.

Sieving has been done on 80 2.2 GHz Opteron CPUs and took 3 months. The matrix step was performed on a cluster of 80 2.2 GHz Opterons connected via a Gigabit network and took about 1.5 months.

Calendar time for the factorization (without polynomial selection) was 5 months.

More details will be given later.

F. Bahr, M. Boehm, J. Franke, T. Kleinjung

RSA

Adi Shamir, Ron L. Rivest, Leonard Adleman (1978)

The RSA cryptosystem

The RSA cryptosystem

1978 R. L. Rivest, A. Shamir, L. Adleman (Patent expired in 1998)

The RSA cryptosystem

1978 R. L. Rivest, A. Shamir, L. Adleman (Patent expired in 1998)

Problem: Alice wants to send the message $\mathcal{P}$ to Bob so that Charles cannot read it

The RSA cryptosystem

1978 R. L. Rivest, A. Shamir, L. Adleman (Patent expired in 1998)

Problem: Alice wants to send the message $\mathcal{P}$ to Bob so that Charles cannot read it

$$\boxed{\begin{array}{ccc} A\ (Alice) & \longrightarrow & B\ (Bob) \\ & \uparrow & \\ & C\ (Charles) & \end{array}}$$

The RSA cryptosystem

1978 R. L. Rivest, A. Shamir, L. Adleman (Patent expired in 1998)

Problem: Alice wants to send the message $\mathcal{P}$ to Bob so that Charles cannot read it

$$\boxed{\begin{array}{ccc} A\ (Alice) & \longrightarrow & B\ (Bob) \\ & \uparrow & \\ & C\ (Charles) & \end{array}}$$

❶

❷

❸

❹

The RSA cryptosystem

1978 R. L. Rivest, A. Shamir, L. Adleman (Patent expired in 1998)

Problem: Alice wants to send the message $\mathcal{P}$ to Bob so that Charles cannot read it

$$\begin{array}{ccc} A\ (Alice) & \longrightarrow & B\ (Bob) \\ & \uparrow & \\ & C\ (Charles) & \end{array}$$

1. KEY GENERATION   Bob has to do it
2.
3.
4.

The RSA cryptosystem

1978 R. L. Rivest, A. Shamir, L. Adleman (Patent expired in 1998)

Problem: Alice wants to send the message $\mathcal{P}$ to Bob so that Charles cannot read it

$$\begin{array}{ccc} A\ (Alice) & \longrightarrow & B\ (Bob) \\ & \uparrow & \\ & C\ (Charles) & \end{array}$$

1. KEY GENERATION — Bob has to do it
2. ENCRYPTION — Alice has to do it
3.
4.

The RSA cryptosystem

1978 R. L. Rivest, A. Shamir, L. Adleman (Patent expired in 1998)

Problem: Alice wants to send the message $\mathcal{P}$ to Bob so that Charles cannot read it

$$\begin{array}{ccc} A\ (Alice) & \longrightarrow & B\ (Bob) \\ & \uparrow & \\ & C\ (Charles) & \end{array}$$

1. KEY GENERATION — Bob has to do it
2. ENCRYPTION — Alice has to do it
3. DECRYPTION — Bob has to do it
4.

The RSA cryptosystem

1978 R. L. Rivest, A. Shamir, L. Adleman (Patent expired in 1998)

Problem: Alice wants to send the message $\mathcal{P}$ to Bob so that Charles cannot read it

$$\begin{array}{ccc} A\ (Alice) & \longrightarrow & B\ (Bob) \\ & \uparrow & \\ & C\ (Charles) & \end{array}$$

1. KEY GENERATION — Bob has to do it
2. ENCRYPTION — Alice has to do it
3. DECRYPTION — Bob has to do it
4. ATTACK — Charles would like to do it

Bob: Key generation

Bob: Key generation

Bob: Key generation

- He chooses randomly p and q primes $(p, q \approx 10^{100})$
-
-
-
-

Bob: Key generation

- He chooses randomly p and q primes $(p, q \approx 10^{100})$
- He computes $M = p \times q$, $\varphi(M) = (p-1) \times (q-1)$
-
-
-

Bob: Key generation

- He chooses randomly p and q primes $(p, q \approx 10^{100})$
- He computes $M = p \times q$, $\varphi(M) = (p-1) \times (q-1)$
- He chooses an integer e s.t.
-
-

Bob: Key generation

✍ He chooses randomly p and q primes $(p, q \approx 10^{100})$

✍ He computes $M = p \times q$, $\varphi(M) = (p-1) \times (q-1)$

✍ He chooses an integer e s.t.

$$0 \leq e \leq \varphi(M) \quad \text{and} \quad \gcd(e, \varphi(M)) = 1$$

✍

✍

Bob: Key generation

- He chooses randomly p and q primes $(p, q \approx 10^{100})$
- He computes $M = p \times q$, $\varphi(M) = (p-1) \times (q-1)$
- He chooses an integer e s.t.

  $$0 \leq e \leq \varphi(M) \text{ and } \gcd(e, \varphi(M)) = 1$$

  NOTE. One could take $e = 3$ and $p \equiv q \equiv 2 \bmod 3$

Bob: Key generation

- He chooses randomly p and q primes $(p, q \approx 10^{100})$
- He computes $M = p \times q$, $\varphi(M) = (p-1) \times (q-1)$
- He chooses an integer e s.t.

  $$0 \le e \le \varphi(M) \quad \text{and} \quad \gcd(e, \varphi(M)) = 1$$

  NOTE. One could take $e = 3$ and $p \equiv q \equiv 2 \bmod 3$

  Experts recommend $e = 2^{16} + 1$
-
-

Bob: Key generation

- He chooses randomly p and q primes $(p, q \approx 10^{100})$
- He computes $M = p \times q$, $\varphi(M) = (p-1) \times (q-1)$
- He chooses an integer e s.t.

$$0 \le e \le \varphi(M) \quad \text{and} \quad \gcd(e, \varphi(M)) = 1$$

NOTE. One could take $e = 3$ and $p \equiv q \equiv 2 \bmod 3$

Experts recommend $e = 2^{16} + 1$

- He computes arithmetic inverse d of e modulo $\varphi(M)$
-

Bob: Key generation

- He chooses randomly p and q primes $(p, q \approx 10^{100})$
- He computes $M = p \times q$, $\varphi(M) = (p-1) \times (q-1)$
- He chooses an integer e s.t.

$$0 \leq e \leq \varphi(M) \quad \text{and} \quad \gcd(e, \varphi(M)) = 1$$

NOTE. One could take $e = 3$ and $p \equiv q \equiv 2 \bmod 3$

Experts recommend $e = 2^{16} + 1$

- He computes arithmetic inverse d of e modulo $\varphi(M)$

(i.e. $d \in \mathbb{N}$ (unique $\leq \varphi(M)$) s.t. $e \times d \equiv 1 \pmod{\varphi(M)}$)

-

Bob: Key generation

✍ He chooses randomly p and q primes $\quad (p, q \approx 10^{100})$

✍ He computes $M = p \times q$, $\varphi(M) = (p-1) \times (q-1)$

✍ He chooses an integer e s.t.

$$0 \leq e \leq \varphi(M) \quad \text{and} \quad \gcd(e, \varphi(M)) = 1$$

NOTE. One could take $e = 3$ and $p \equiv q \equiv 2 \bmod 3$

Experts recommend $e = 2^{16} + 1$

✍ He computes arithmetic inverse d of e modulo $\varphi(M)$

(i.e. $d \in \mathbb{N}$ (unique $\leq \varphi(M)$) s.t. $e \times d \equiv 1 \pmod{\varphi(M)}$)

✍ Publishes (M, e) **public key** and hides **secret key** d

Bob: Key generation

- He chooses randomly p and q primes $\qquad (p, q \approx 10^{100})$
- He computes $\quad M = p \times q,\ \varphi(M) = (p-1) \times (q-1)$
- He chooses an integer e s.t.

  $$0 \leq e \leq \varphi(M) \ \text{ and } \ \gcd(e, \varphi(M)) = 1$$

  NOTE. One could take $e = 3$ and $p \equiv q \equiv 2 \bmod 3$

  Experts recommend $e = 2^{16} + 1$
- He computes arithmetic inverse d of e modulo $\varphi(M)$

  (i.e. $d \in \mathbb{N}$ (unique $\leq \varphi(M)$) s.t. $e \times d \equiv 1 \pmod{\varphi(M)}$)
- Publishes (M, e) **public key** and hides **secret key** d

Problem: How does Bob do all this?- We will go came back to it!

Alice: Encryption

Alice: Encryption

Represent the message $\mathcal{P}$ as an element of $\mathbb{Z}/M\mathbb{Z}$

Alice: Encryption

Represent the message $\mathcal{P}$ as an element of $\mathbb{Z}/M\mathbb{Z}$

(for example) $\boxed{A \leftrightarrow 1 \quad B \leftrightarrow 2 \quad C \leftrightarrow 3 \quad \ldots \quad Z \leftrightarrow 26 \quad AA \leftrightarrow 27 \ldots}$

Alice: Encryption

Represent the message $\mathcal{P}$ as an element of $\mathbb{Z}/M\mathbb{Z}$

(for example) $\boxed{A \leftrightarrow 1 \quad B \leftrightarrow 2 \quad C \leftrightarrow 3 \quad \ldots \quad Z \leftrightarrow 26 \quad AA \leftrightarrow 27 \ldots}$

$$\texttt{SAIGON} \leftrightarrow 19 \cdot 26^5 + 26^4 + 9 \cdot 26^3 + 7 \cdot 26^2 + 15 \cdot 26 + 14 = 226366440$$

Note. Better if texts are not too short. Otherwise one performs some *padding*

Alice: Encryption

Represent the message $\mathcal{P}$ as an element of $\mathbb{Z}/M\mathbb{Z}$

(for example) $\boxed{A \leftrightarrow 1 \quad B \leftrightarrow 2 \quad C \leftrightarrow 3 \quad \ldots \quad Z \leftrightarrow 26 \quad AA \leftrightarrow 27 \ldots}$

$$\texttt{SAIGON} \leftrightarrow 19 \cdot 26^5 + 26^4 + 9 \cdot 26^3 + 7 \cdot 26^2 + 15 \cdot 26 + 14 = 226366440$$

Note. Better if texts are not too short. Otherwise one performs some *padding*

$$\boxed{\mathcal{C} = E(\mathcal{P}) = \mathcal{P}^e \pmod{M}}$$

Alice: Encryption

Represent the message $\mathcal{P}$ as an element of $\mathbb{Z}/M\mathbb{Z}$

(for example) $\boxed{A \leftrightarrow 1 \quad B \leftrightarrow 2 \quad C \leftrightarrow 3 \quad \dots \quad Z \leftrightarrow 26 \quad AA \leftrightarrow 27 \dots}$

$$\texttt{SAIGON} \leftrightarrow 19 \cdot 26^5 + 26^4 + 9 \cdot 26^3 + 7 \cdot 26^2 + 15 \cdot 26 + 14 = 226366440$$

Note. Better if texts are not too short. Otherwise one performs some *padding*

$$\boxed{\mathcal{C} = E(\mathcal{P}) = \mathcal{P}^e \pmod{M}}$$

Example: $p = 9049465727$, $q = 8789181607$, $M = 79537397720925283289$, $e = 2^{16} + 1 = 65537$, $\mathcal{P} = \texttt{SAIGON}$:

Alice: Encryption

Represent the message $\mathcal{P}$ as an element of $\mathbb{Z}/M\mathbb{Z}$

(for example) $\boxed{A \leftrightarrow 1 \quad B \leftrightarrow 2 \quad C \leftrightarrow 3 \quad \ldots \quad Z \leftrightarrow 26 \quad AA \leftrightarrow 27 \ldots}$

$$\texttt{SAIGON} \leftrightarrow 19 \cdot 26^5 + 26^4 + 9 \cdot 26^3 + 7 \cdot 26^2 + 15 \cdot 26 + 14 = 226366440$$

Note. Better if texts are not too short. Otherwise one performs some *padding*

$$\boxed{\mathcal{C} = E(\mathcal{P}) = \mathcal{P}^e \pmod{M}}$$

Example: $p = 9049465727$, $q = 8789181607$, $M = 79537397720925283289$, $e = 2^{16} + 1 = 65537$, $\mathcal{P} = \texttt{SAIGON}$:

$$E(\texttt{SAIGON}) = 226366440^{65537} \pmod{79537397720925283289}$$

$$= 71502481501746956206 = \mathcal{C} = \texttt{ZPOYWXZXDNCGUBA}$$

Bob: Decryption

Bob: Decryption

$$\boxed{\mathcal{P} = D(\mathcal{C}) = \mathcal{C}^d \pmod{M}}$$

Bob: Decryption

$$\boxed{\mathcal{P} = D(\mathcal{C}) = \mathcal{C}^d \pmod{M}}$$

Note. Bob decrypts because he is the only one that knows d.

Bob: Decryption

$$\boxed{\mathcal{P} = D(\mathcal{C}) = \mathcal{C}^d \pmod{M}}$$

Note. Bob decrypts because he is the only one that knows d.

Theorem. (Euler) If $a, m \in \mathbb{N}$, $\gcd(a, m) = 1$,

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

If $n_1 \equiv n_2 \bmod \varphi(m)$ then $a^{n_1} \equiv a^{n_2} \bmod m$.

Bob: Decryption

$$\boxed{\mathcal{P} = D(\mathcal{C}) = \mathcal{C}^d \pmod{M}}$$

Note. Bob decrypts because he is the only one that knows d.

Theorem. (Euler) If $a, m \in \mathbb{N}$, $\gcd(a, m) = 1$,

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

If $n_1 \equiv n_2 \bmod \varphi(m)$ then $a^{n_1} \equiv a^{n_2} \bmod m$.

Therefore $(ed \equiv 1 \bmod \varphi(M))$

$$\boxed{D(E(\mathcal{P})) = \mathcal{P}^{ed} \equiv \mathcal{P} \bmod M}$$

Bob: Decryption

$$\boxed{\mathcal{P} = D(\mathcal{C}) = \mathcal{C}^d \pmod{M}}$$

Note. Bob decrypts because he is the only one that knows d.

Theorem. (Euler) If $a, m \in \mathbb{N}$, $\gcd(a, m) = 1$,

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

If $n_1 \equiv n_2 \bmod \varphi(m)$ then $a^{n_1} \equiv a^{n_2} \bmod m$.

Therefore $(ed \equiv 1 \bmod \varphi(M))$

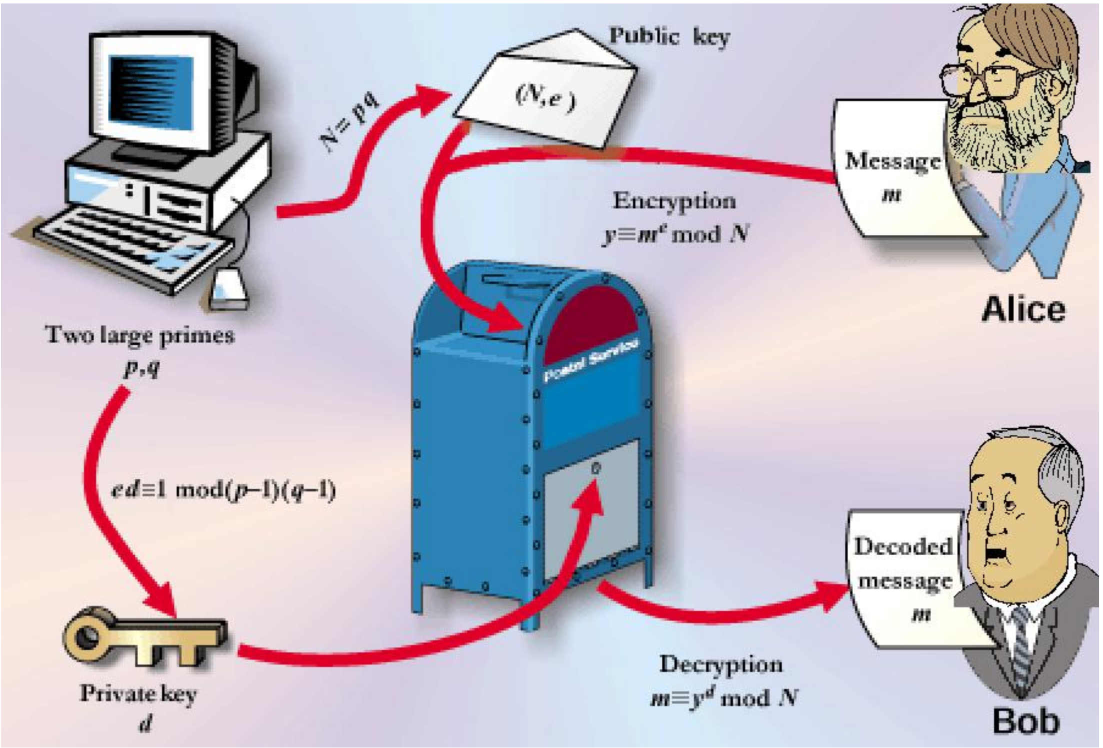
$$\boxed{D(E(\mathcal{P})) = \mathcal{P}^{ed} \equiv \mathcal{P} \bmod M}$$

Example(cont.): $d = 65537^{-1} \bmod \varphi(9049465727 \cdot 8789181607) = 57173914060643780153$

$D(\texttt{ZPOYWXZXDNCGUBA}) =$

$71502481501746956206^{57173914060643780153} (\bmod 79537397720925283289) =$ SAIGON

RSA at work


Public key
(N,e)
N=pq
Message
m
Encryption
y≡m^e mod N
Alice
Two large primes
p,q
ed≡1 mod(p−1)(q−1)
Postal Service
Decoded
message
m
Private key
d
Decryption
m≡y^d mod N
Bob

Repeated squaring algorithm

Repeated squaring algorithm

Problem: How does one compute $a^b \bmod c$?

Repeated squaring algorithm

Problem: How does one compute $a^b \bmod c$?

$$715024815017469562 06^{5717391406064378015 3}(\bmod 795373977209252832 89)$$

Repeated squaring algorithm

Problem: How does one compute $a^b \bmod c$?

$$7150248150174695620 6^{5717391406064378015 3} \pmod{7953739772092528328 9}$$

✍

✍

✍

Repeated squaring algorithm

Problem: How does one compute $a^b \bmod c$?

$$715024815017469562 06^{571739140606437801 53} \pmod{79537397720925283289}$$

- Compute the binary expansion $b = \sum_{j=0}^{[\log_2 b]} \epsilon_j 2^j$
-
-

Repeated squaring algorithm

Problem: How does one compute $a^b \bmod c$?

$$7150248150174695620^{5717391406064378015}3 \pmod{7953739772092528328}9)$$

- Compute the binary expansion $b = \sum_{j=0}^{[\log_2 b]} \epsilon_j 2^j$

$5717391406064378015 3 = 110001100101110010100010111110101011110011011000100100011000111001$

Repeated squaring algorithm

Problem: How does one compute $a^b \bmod c$?

$$71502481501746956206^{5717391406064378015 3}(\bmod 795373977209252832 89)$$

- Compute the binary expansion $b = \sum_{j=0}^{[\log_2 b]} \epsilon_j 2^j$

$5717391406064378015 3$=1100011001011100101000101111101010111100110110001001000110001110 01

- Compute recursively $a^{2^j} \bmod c, j = 1, \ldots, [\log_2 b]$:

-

Repeated squaring algorithm

Problem: How does one compute $a^b \bmod c$?

$$71502481501746956206^{5717391406064378015 3}\pmod{7953739772092528328 9}$$

- Compute the binary expansion $b = \sum_{j=0}^{[\log_2 b]} \epsilon_j 2^j$

$5717391406064378015 3 = 1100011001011100101000101111101010111100110110001001000110001110 01$

- Compute recursively $a^{2^j} \bmod c,\ j = 1, \ldots, [\log_2 b]$:

$$a^{2^j} \bmod c = \left(a^{2^{j-1}} \bmod c\right)^2 \bmod c$$

-

Repeated squaring algorithm

Problem: How does one compute a^b mod c?

$$715024815017469562 06^{57173914060643780153} \pmod{79537397720925283289}$$

- Compute the binary expansion $b = \sum_{j=0}^{[\log_2 b]} \epsilon_j 2^j$

  57173914060643780153=110001100101110010100010111110101011110011011000100100011000111001

- Compute recursively a^{2^j} mod $c, j = 1, \ldots, [\log_2 b]$:

$$a^{2^j} \bmod c = \left(a^{2^{j-1}} \bmod c\right)^2 \bmod c$$

- Multiply the a^{2^j} mod c with $\epsilon_j = 1$

Repeated squaring algorithm

Problem: How does one compute $a^b \bmod c$?

$$715024815017469562 06^{5717391406064378015 3}$$

$$7150248150174695620 6^{57173914060643780153} \pmod{79537397720925283289}$$

- Compute the binary expansion $b = \sum_{j=0}^{[\log_2 b]} \epsilon_j 2^j$

57173914060643780153=110001100101110010100010111110101011110011011000100100011000111001

- Compute recursively $a^{2^j} \bmod c, j = 1, \ldots, [\log_2 b]$:

$$a^{2^j} \bmod c = \left(a^{2^{j-1}} \bmod c\right)^2 \bmod c$$

- Multiply the $a^{2^j} \bmod c$ with $\epsilon_j = 1$

$$a^b \bmod c = \left(\prod_{j=0,\epsilon_j=1}^{[\log_2 b]} a^{2^j} \bmod c\right) \bmod c$$

$$\boxed{\#\{\textbf{oper. in } \mathbb{Z}/c\mathbb{Z} \textbf{ to compute } a^b \bmod c\} \leq 2\log_2 b}$$

$$\boxed{\#\{\textbf{oper. in } \mathbb{Z}/c\mathbb{Z} \textbf{ to compute } a^b \bmod c\} \leq 2\log_2 b}$$

`ZPOYWXZXDNCGUBA` is decrypted with 131 operations in

$$\mathbb{Z}/79537397720925283289\mathbb{Z}$$

$$\boxed{\#\{\textbf{oper. in } \mathbb{Z}/c\mathbb{Z} \textbf{ to compute } a^b \bmod c\} \leq 2\log_2 b}$$

`ZPOYWXZXDNCGUBA` is decrypted with 131 operations in

$$\mathbb{Z}/79537397720925283289\mathbb{Z}$$

Pseudo code: $e_c(a, b) = a^b \bmod c$

$$\boxed{\#\{\textbf{oper. in } \mathbb{Z}/c\mathbb{Z} \textbf{ to compute } a^b \bmod c\} \leq 2\log_2 b}$$

`ZPOYWXZXDNCGUBA` is decrypted with 131 operations in

$$\mathbb{Z}/795373977209252832 89\mathbb{Z}$$

PSEUDO CODE: $e_c(a,b) = a^b \bmod c$

$e_c(a,b)$	`=`	`if`	$b=1$	`then`	$a \bmod c$
		`if`	$2 \mid b$	`then`	$e_c(a, \frac{b}{2})^2 \bmod c$
		`else`			$a * e_c(a, \frac{b-1}{2})^2 \bmod c$

$$\#\{\textbf{oper. in } \mathbb{Z}/c\mathbb{Z} \textbf{ to compute } a^b \bmod c\} \leq 2\log_2 b$$

`ZPOYWXZXDNCGUBA` is decrypted with 131 operations in

$$\mathbb{Z}/795373977209252832 89\mathbb{Z}$$

PSEUDO CODE: $e_c(a,b) = a^b \bmod c$

$$\boxed{\begin{array}{lllll} e_c(a,b) & \texttt{=} & \texttt{if} & b=1 & \texttt{then} & a \bmod c \\ & & \texttt{if} & 2|b & \texttt{then} & e_c(a,\frac{b}{2})^2 \bmod c \\ & & \texttt{else} & & & a * e_c(a,\frac{b-1}{2})^2 \bmod c \end{array}}$$

To encrypt with $e = 2^{16}+1$, only 17 operations in $\mathbb{Z}/M\mathbb{Z}$ are enough

Key generation

Key generation

Problem. Produce a random prime $p \approx 10^{100}$

Probabilistic algorithm (type Las Vegas)
1. Let $p = \textsc{Random}(10^{100})$
2. If ISPRIME(p)=1 then OUTPUT=p else goto 1

Key generation

Problem. Produce a random prime $p \approx 10^{100}$

Probabilistic algorithm (type Las Vegas)
1. Let $p = \textsc{Random}(10^{100})$
2. If ISPRIME(p)=1 then OUTPUT=p else goto 1

subproblems:

Key generation

Problem. Produce a random prime $p \approx 10^{100}$

	Probabilistic algorithm (type Las Vegas)
1.	Let $p = \textsc{Random}(10^{100})$
2.	If ISPRIME(p)=1 then OUTPUT=p else goto 1

subproblems:

A. How many iterations are necessary?

(i.e. how are primes distributes?)

Key generation

Problem. Produce a random prime $p \approx 10^{100}$

Probabilistic algorithm (type Las Vegas)	
1.	Let $p = \text{RANDOM}(10^{100})$
2.	If $\text{ISPRIME}(p)$=1 then $\text{OUTPUT}=p$ else goto 1

subproblems:

A. How many iterations are necessary?

(i.e. how are primes distributes?)

B. How does one check if p is prime?

(i.e. how does one compute $\text{ISPRIME}(p)$?) $\rightsquigarrow$ Primality test

Key generation

Problem. Produce a random prime $p \approx 10^{100}$

	Probabilistic algorithm (type Las Vegas)
1.	Let $p = \text{RANDOM}(10^{100})$
2.	If ISPRIME(p)=1 then OUTPUT=p else goto 1

subproblems:

A. How many iterations are necessary?

(i.e. how are primes distributes?)

B. How does one check if p is prime?

(i.e. how does one compute ISPRIME(p)?) $\rightsquigarrow$ Primality test

False Metropolitan Legend: Check primality is equivalent to factoring

A. Distribution of prime numbers

A. Distribution of prime numbers

$$\pi(x) = \#\{p \leq x \text{ t. c. } p \text{ is prime}\}$$

A. Distribution of prime numbers

$$\pi(x) = \#\{p \leq x \text{ t. c. } p \text{ is prime}\}$$

Theorem. (Hadamard - de la vallee Pussen - 1897)

$$\pi(x) \sim \frac{x}{\log x}$$

A. Distribution of prime numbers

$$\pi(x) = \#\{p \leq x \text{ t. c. } p \text{ is prime}\}$$

Theorem. (Hadamard - de la vallee Pussen - 1897)

$$\pi(x) \sim \frac{x}{\log x}$$

Quantitative version:

Theorem. (Rosser - Schoenfeld) if $x \geq 67$

$$\frac{x}{\log x - 1/2} < \pi(x) < \frac{x}{\log x - 3/2}$$

A. Distribution of prime numbers

$$\pi(x) = \#\{p \leq x \text{ t. c. } p \text{ is prime}\}$$

Theorem. (Hadamard - de la vallee Pussen - 1897)

$$\pi(x) \sim \frac{x}{\log x}$$

Quantitative version:

Theorem. (Rosser - Schoenfeld) if $x \geq 67$

$$\frac{x}{\log x - 1/2} < \pi(x) < \frac{x}{\log x - 3/2}$$

Therefore

$$0.0043523959267 < Prob\left((\textsc{Random}(10^{100}) = \texttt{prime}\right) < 0.004371422086$$

If P_k is the probability that among k random numbers $\leq 10^{100}$ there is a prime one, then

If P_k is the probability that among k random numbers $\leq 10^{100}$ there is a prime one, then

$$P_k = 1 - \left(1 - \frac{\pi(10^{100})}{10^{100}}\right)^k$$

If P_k is the probability that among k random numbers$\leq 10^{100}$ there is a prime one, then

$$P_k = 1 - \left(1 - \frac{\pi(10^{100})}{10^{100}}\right)^k$$

Therefore

$$0.663942 < P_{250} < 0.66554440$$

If P_k is the probability that among k random numbers $\leq 10^{100}$ there is a prime one, then

$$P_k = 1 - \left(1 - \frac{\pi(10^{100})}{10^{100}}\right)^k$$

Therefore

$$0.663942 < P_{250} < 0.66554440$$

To speed up the process: One can consider only odd random numbers not divisible by 3 nor by 5.

If P_k is the probability that among k random numbers $\leq 10^{100}$ there is a prime one, then

$$P_k = 1 - \left(1 - \frac{\pi(10^{100})}{10^{100}}\right)^k$$

Therefore

$$0.663942 < P_{250} < 0.66554440$$

To speed up the process: One can consider only odd random numbers not divisible by 3 nor by 5.

Let

$$\Psi(x, 30) = \#\left\{n \leq x \text{ s.t. } \gcd(n, 30) = 1\right\}$$

To speed up the process: One can consider only odd random numbers not divisible by 3 nor by 5.

To speed up the process: One can consider only odd random numbers not divisible by 3 nor by 5.

Let

$$\Psi(x, 30) = \#\{n \leq x \text{ s.t. } \gcd(n, 30) = 1\}$$

then

To speed up the process: One can consider only odd random numbers not divisible by 3 nor by 5.

Let

$$\Psi(x,30) = \#\{n \leq x \text{ s.t. } \gcd(n,30)=1\}$$

then

$$\frac{4}{15}x - 4 < \Psi(x,30) < \frac{4}{15}x + 4$$

To speed up the process: One can consider only odd random numbers not divisible by 3 nor by 5.

Let

$$\Psi(x, 30) = \#\{n \leq x \text{ s.t. } \gcd(n, 30) = 1\}$$

then

$$\frac{4}{15}x - 4 < \Psi(x, 30) < \frac{4}{15}x + 4$$

Hence, if P'_k is the probability that among k random numbers $\leq 10^{100}$ coprime with 30, there is a prime one, then

To speed up the process: One can consider only odd random numbers not divisible by 3 nor by 5.

Let

$$\Psi(x,30) = \#\{n \leq x \text{ s.t. } \gcd(n,30)=1\}$$

then

$$\frac{4}{15}x - 4 < \Psi(x,30) < \frac{4}{15}x + 4$$

Hence, if P'_k is the probability that among k random numbers $\leq 10^{100}$ coprime with 30, there is a prime one, then

$$P'_k = 1 - \left(1 - \frac{\pi(10^{100})}{\Psi(10^{100},30)}\right)^k$$

To speed up the process: One can consider only odd random numbers not divisible by 3 nor by 5.

Let

$$\Psi(x,30) = \#\{n \le x \text{ s.t. } \gcd(n,30)=1\}$$

then

$$\frac{4}{15}x - 4 < \Psi(x,30) < \frac{4}{15}x + 4$$

Hence, if P'_k is the probability that among k random numbers $\le 10^{100}$ coprime with 30, there is a prime one, then

$$P'_k = 1 - \left(1 - \frac{\pi(10^{100})}{\Psi(10^{100},30)}\right)^k$$

and

$$0.98365832 < P'_{250} < 0.98395199$$

B. Primality test

B. Primality test

Fermat Little Theorem. If p is prime, $p \nmid a \in \mathbb{N}$

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

B. Primality test

Fermat Little Theorem. If p is prime, $p \nmid a \in \mathbb{N}$

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

NON-primality test

$$M \in \mathbb{Z}, \quad 2^{M-1} \not\equiv 1 \bmod M \Rightarrow \quad M \text{composite!}$$

B. Primality test

Fermat Little Theorem. If p is prime, $p \nmid a \in \mathbb{N}$

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

NON-primality test

$$M \in \mathbb{Z}, \quad 2^{M-1} \not\equiv 1 \bmod M \Rightarrow \quad M \text{composite!}$$

EXAMPLE: $2^{RSA_{2048}-1} \not\equiv 1 \bmod RSA_{2048}$

Therefore RSA_{2048} is composite!

B. Primality test

Fermat Little Theorem. If p is prime, $p \nmid a \in \mathbb{N}$

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

NON-primality test

$$M \in \mathbb{Z}, \quad 2^{M-1} \not\equiv 1 \bmod M \Rightarrow \quad M \text{composite!}$$

EXAMPLE: $2^{RSA_{2048}-1} \not\equiv 1 \bmod RSA_{2048}$

Therefore RSA_{2048} is composite!

Fermat little Theorem does not invert. Infact

B. Primality test

Fermat Little Theorem. If p is prime, $p \nmid a \in \mathbb{N}$

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

NON-primality test

$$M \in \mathbb{Z}, \quad 2^{M-1} \not\equiv 1 \bmod M \Rightarrow \quad M \text{composite!}$$

EXAMPLE: $2^{RSA_{2048}-1} \not\equiv 1 \bmod RSA_{2048}$

Therefore RSA_{2048} is composite!

Fermat little Theorem does not invert. Infact

$$2^{93960} \equiv 1 \pmod{93961} \quad \text{but} \quad 93961 = 7 \times 31 \times 433$$

Strong pseudo primes

Strong pseudo primes

From now on $m \equiv 3 \bmod 4$ (just to simplify the notation)

Strong pseudo primes

From now on $m \equiv 3 \bmod 4$ (just to simplify the notation)

Definition. $m \in \mathbb{N}$, $m \equiv 3 \bmod 4$, composite is said strong pseudo prime (SPSP) in base a if

$$a^{(m-1)/2} \equiv \pm 1 \pmod{m}.$$

Strong pseudo primes

From now on $m \equiv 3 \bmod 4$ (just to simplify the notation)

Definition. $m \in \mathbb{N}$, $m \equiv 3 \bmod 4$, composite is said strong pseudo prime (SPSP) in base a if

$$a^{(m-1)/2} \equiv \pm 1 \pmod{m}.$$

Note. If $p > 2$ prime $\Longrightarrow \quad a^{(p-1)/2} \equiv \pm 1 \pmod{p}$

Let $\boxed{\mathcal{S} = \{a \in \mathbb{Z}/m\mathbb{Z} \text{ s.t. } \gcd(m,a) = 1, a^{(m-1)/2} \equiv \pm 1 \pmod{m}\}}$

Strong pseudo primes

From now on $m \equiv 3 \bmod 4$ (just to simplify the notation)

Definition. $m \in \mathbb{N}$, $m \equiv 3 \bmod 4$, composite is said strong pseudo prime (SPSP) in base a if

$$a^{(m-1)/2} \equiv \pm 1 \pmod{m}.$$

Note. If $p > 2$ prime $\Longrightarrow \quad a^{(p-1)/2} \equiv \pm 1 \pmod{p}$

Let $\boxed{\mathcal{S} = \{a \in \mathbb{Z}/m\mathbb{Z} \text{ s.t. } \gcd(m,a) = 1, a^{(m-1)/2} \equiv \pm 1 \pmod{m}\}}$

①

②

③

④

Strong pseudo primes

From now on $m \equiv 3 \bmod 4$ (just to simplify the notation)

Definition. $m \in \mathbb{N}$, $m \equiv 3 \bmod 4$, composite is said strong pseudo prime (SPSP) in base a if

$$a^{(m-1)/2} \equiv \pm 1 \pmod{m}.$$

Note. If $p > 2$ prime $\Longrightarrow$ $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$

Let $\boxed{\mathcal{S} = \{a \in \mathbb{Z}/m\mathbb{Z} \text{ s.t. } \gcd(m,a) = 1, a^{(m-1)/2} \equiv \pm 1 \pmod{m}\}}$

① $\mathcal{S} \subseteq (\mathbb{Z}/m\mathbb{Z})^*$ subgroup

②

③

④

Strong pseudo primes

From now on $m \equiv 3 \bmod 4$ (just to simplify the notation)

Definition. $m \in \mathbb{N}$, $m \equiv 3 \bmod 4$, composite is said strong pseudo prime (SPSP) in base a if

$$a^{(m-1)/2} \equiv \pm 1 \pmod{m}.$$

Note. If $p > 2$ prime $\Longrightarrow$ $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$

Let $\boxed{\mathcal{S} = \{a \in \mathbb{Z}/m\mathbb{Z} \text{ s.t. } \gcd(m,a) = 1, a^{(m-1)/2} \equiv \pm 1 \pmod{m}\}}$

① $\mathcal{S} \subseteq (\mathbb{Z}/m\mathbb{Z})^*$ subgroup

② If m is composite $\Longrightarrow$ proper subgroup

③

④

Strong pseudo primes

From now on $m \equiv 3 \bmod 4$ (just to simplify the notation)

Definition. $m \in \mathbb{N}$, $m \equiv 3 \bmod 4$, composite is said strong pseudo prime (SPSP) in base a if

$$a^{(m-1)/2} \equiv \pm 1 \pmod{m}.$$

Note. If $p > 2$ prime $\Longrightarrow \quad a^{(p-1)/2} \equiv \pm 1 \pmod{p}$

Let $\boxed{\mathcal{S} = \{a \in \mathbb{Z}/m\mathbb{Z} \text{ s.t. } \gcd(m,a) = 1, a^{(m-1)/2} \equiv \pm 1 \pmod{m}\}}$

① $\mathcal{S} \subseteq (\mathbb{Z}/m\mathbb{Z})^*$ subgroup

② If m is composite $\Longrightarrow$ proper subgroup

③ If m is composite $\Longrightarrow \quad \#\mathcal{S} \leq \frac{\varphi(m)}{4}$

④

Strong pseudo primes

From now on $m \equiv 3 \bmod 4$ (just to simplify the notation)

Definition. $m \in \mathbb{N}$, $m \equiv 3 \bmod 4$, composite is said strong pseudo prime (SPSP) in base a if

$$a^{(m-1)/2} \equiv \pm 1 \pmod{m}.$$

Note. If $p > 2$ prime $\Longrightarrow \quad a^{(p-1)/2} \equiv \pm 1 \pmod{p}$

Let $\boxed{\mathcal{S} = \{a \in \mathbb{Z}/m\mathbb{Z} \text{ s.t. } \gcd(m,a) = 1, a^{(m-1)/2} \equiv \pm 1 \pmod{m}\}}$

① $\mathcal{S} \subseteq (\mathbb{Z}/m\mathbb{Z})^*$ subgroup

② If m is composite $\Longrightarrow$ proper subgroup

③ If m is composite $\Longrightarrow \quad \#\mathcal{S} \leq \frac{\varphi(m)}{4}$

④ If m is composite $\Longrightarrow \quad Prob(m \text{ SPSP in base } a) \leq 0,25$

Miller–Rabin primality test

Miller–Rabin primality test

Let $m \equiv 3 \bmod 4$

Miller–Rabin primality test

Let $m \equiv 3 \bmod 4$

MILLER RABIN ALGORITHM WITH k ITERATIONS
$N = (m-1)/2$
`for` $j = 0$ `to` k `do` $a =$`Random`(m)
`if` $a^N \not\equiv \pm 1 \bmod m$ `then OUPUT=(`m `composite): END`
`endfor OUTPUT=(`m `prime)`

Miller–Rabin primality test

Let $m \equiv 3 \bmod 4$

Miller Rabin algorithm with k iterations
$N = (m-1)/2$
`for` $j = 0$ `to` k `do` $a =$`Random`(m)
`if` $a^N \not\equiv \pm 1 \bmod m$ `then OUPUT=(`m `composite): END`
`endfor OUTPUT=(`m `prime)`

Monte Carlo primality test

Miller–Rabin primality test

Let $m \equiv 3 \bmod 4$

MILLER RABIN ALGORITHM WITH k ITERATIONS
$N = (m-1)/2$
`for` $j = 0$ `to` k `do` $a =$`Random`(m)
`if` $a^N \not\equiv \pm 1 \bmod m$ `then OUPUT=(`m `composite): END`
`endfor OUTPUT=(`m `prime)`

Monte Carlo primality test

$Prob$(Miller Rabin says m `prime` and m is composite) $\lessapprox \frac{1}{4^k}$

Miller–Rabin primality test

Let $m \equiv 3 \bmod 4$

MILLER RABIN ALGORITHM WITH k ITERATIONS
$N = (m-1)/2$
`for` $j = 0$ `to` k `do` $a =$`Random`(m)
`if` $a^N \not\equiv \pm 1 \bmod m$ `then OUPUT=(`m `composite): END`
`endfor OUTPUT=(`m `prime)`

Monte Carlo primality test

$Prob$(Miller Rabin says m `prime` and m is composite) $\lessapprox \frac{1}{4^k}$

In the real world, software uses Miller Rabin with $k = 10$

Deterministic primality tests

Deterministic primality tests

Theorem. (Miller, Bach) If m is composite, then

$$\textbf{GRH} \Longrightarrow \ \exists a \leq 2\log^2 m \text{ s.t. } \ a^{(m-1)/2} \not\equiv \pm 1 \pmod{m}.$$

(i.e. *m is not SPSP in base a.*)

Deterministic primality tests

Theorem. (Miller, Bach) If m is composite, then

$$\textbf{GRH} \Longrightarrow \exists a \leq 2\log^2 m \text{ s.t. } a^{(m-1)/2} \not\equiv \pm 1 \pmod{m}.$$

(i.e. *m is not SPSP in base a.*)

Consequence: "Miller–Rabin de–randomizes on GRH" ($m \equiv 3 \bmod 4$)

Deterministic primality tests

Theorem. (Miller, Bach) If m is composite, then

$$\textbf{GRH} \Longrightarrow\ \exists a \leq 2\log^2 m \text{ s.t. } a^{(m-1)/2} \not\equiv \pm 1 \pmod{m}.$$

(i.e. *m is not SPSP in base a.*)

Consequence: "Miller–Rabin de–randomizes on GRH" ($m \equiv 3 \bmod 4$)

`for`	$a = 2$ `to` $2\log^2 m$		`do`
	`if` $a^{(m-1)/2} \not\equiv \pm 1 \bmod m$		`then`
			`OUPUT=(`m `composite): END`
`endfor`			`OUTPUT=(`m `prime)`

Deterministic primality tests

Theorem. (Miller, Bach) If m is composite, then

$$\textbf{GRH} \Longrightarrow\ \exists a \le 2\log^2 m \text{ s.t. } a^{(m-1)/2} \not\equiv \pm 1 \pmod{m}.$$

(i.e. *m is not SPSP in base a.*)

Consequence: "Miller–Rabin de–randomizes on GRH" ($m \equiv 3 \bmod 4$)

`for`	$a = 2$ `to` $2\log^2 m$		`do`
	`if` $a^{(m-1)/2} \not\equiv \pm 1 \bmod m$		`then`
			`OUPUT=(`m `composite): END`
`endfor`			`OUTPUT=(`m `prime)`

Deterministic Polynomial time algorithm

Deterministic primality tests

Theorem. (Miller, Bach) If m is composite, then

$$\textbf{GRH} \Longrightarrow \ \exists a \leq 2\log^2 m \text{ s.t. } \ a^{(m-1)/2} \not\equiv \pm 1 \pmod{m}.$$

(i.e. *m is not SPSP in base a.*)

Consequence: "Miller–Rabin de–randomizes on GRH" ($m \equiv 3 \bmod 4$)

`for`	$a = 2$ `to` $2\log^2 m$		`do`
	`if` $a^{(m-1)/2} \not\equiv \pm 1 \bmod m$		`then`
			`OUPUT=(`m `composite): END`
`endfor`			`OUTPUT=(`m `prime)`

Deterministic Polynomial time algorithm

It runs in $O(\log^5 m)$ operations in $\mathbb{Z}/m\mathbb{Z}$.

Certified prime records

Certified prime records

Top 10 Largest primes:

Certified prime records

Top 10 Largest primes:

1	$2^{25964951}-1$	7816230	Nowak	2005	Mersenne	42?
2	$2^{24036583}-1$	7235733	Findley	2004	Mersenne	41?
3	$2^{20996011}-1$	6320430	Shafer	2003	Mersenne	40?
4	$2^{13466917}-1$	4053946	Cameron	2001	Mersenne	39
5	$27653\times 2^{9167433}+1$	2759677	Gordon	2005		
6	$28433\times 2^{7830457}+1$	2357207	SB7	2004		
7	$2^{6972593}-1$	2098960	Hajratwala	1999	Mersenne	38
8	$5359\times 2^{5054502}+1$	1521561	Sundquist	2003		
9	$4847\times 2^{3321063}+1$	999744	Hassler	2005		
10	$2^{3021377}-1$	909526	Clarkson	1998	Mersenne	37

Certified prime records

Top 10 Largest primes:

1	$2^{25964951}-1$	7816230	Nowak	2005	Mersenne	42?
2	$2^{24036583}-1$	7235733	Findley	2004	Mersenne	41?
3	$2^{20996011}-1$	6320430	Shafer	2003	Mersenne	40?
4	$2^{13466917}-1$	4053946	Cameron	2001	Mersenne	39
5	$27653\times 2^{9167433}+1$	2759677	Gordon	2005		
6	$28433\times 2^{7830457}+1$	2357207	SB7	2004		
7	$2^{6972593}-1$	2098960	Hajratwala	1999	Mersenne	38
8	$5359\times 2^{5054502}+1$	1521561	Sundquist	2003		
9	$4847\times 2^{3321063}+1$	999744	Hassler	2005		
10	$2^{3021377}-1$	909526	Clarkson	1998	Mersenne	37

✍ Mersenne's Numbers: $M_p = 2^p - 1$

Certified prime records

Top 10 Largest primes:

1	$2^{25964951} - 1$	7816230	Nowak	2005	Mersenne	42?
2	$2^{24036583} - 1$	7235733	Findley	2004	Mersenne	41?
3	$2^{20996011} - 1$	6320430	Shafer	2003	Mersenne	40?
4	$2^{13466917} - 1$	4053946	Cameron	2001	Mersenne	39
5	$27653 \times 2^{9167433} + 1$	2759677	Gordon	2005		
6	$28433 \times 2^{7830457} + 1$	2357207	SB7	2004		
7	$2^{6972593} - 1$	2098960	Hajratwala	1999	Mersenne	38
8	$5359 \times 2^{5054502} + 1$	1521561	Sundquist	2003		
9	$4847 \times 2^{3321063} + 1$	999744	Hassler	2005		
10	$2^{3021377} - 1$	909526	Clarkson	1998	Mersenne	37

- Mersenne's Numbers: $M_p = 2^p - 1$
- For more see

http://primes.utm.edu/primes/

The AKS deterministic primality test

The AKS deterministic primality test

Department of Computer Science & Engineering,
I.I.T. Kanpur, Agost 8, 2002.

The AKS deterministic primality test

Department of Computer Science & Engineering,
I.I.T. Kanpur, Agost 8, 2002.

Nitin Saxena, Neeraj Kayal and Manindra Agarwal

The AKS deterministic primality test

Department of Computer Science & Engineering,
I.I.T. Kanpur, Agost 8, 2002.

Nitin Saxena, Neeraj Kayal and Manindra Agarwal
New deterministic, polynomial–time, primality test.

The AKS deterministic primality test

Department of Computer Science & Engineering,
I.I.T. Kanpur, Agost 8, 2002.

Nitin Saxena, Neeraj Kayal and Manindra Agarwal
New deterministic, polynomial–time, primality test.

Solves #1 open question in computational number theory

The AKS deterministic primality test

Department of Computer Science & Engineering,
I.I.T. Kanpur, Agost 8, 2002.

Nitin Saxena, Neeraj Kayal and Manindra Agarwal

New deterministic, polynomial–time, primality test.

Solves #1 open question in computational number theory

http://www.cse.iitk.ac.in/news/primality.html

How does the AKS work?

How does the AKS work?

Theorem. (AKS) Let $n \in \mathbb{N}$. Assume q, r primes, $S \subseteq \mathbb{N}$ finite:

- $q|r-1$;
- $n^{(r-1)/q} \bmod r \notin \{0,1\}$;
- $\gcd(n, b-b') = 1, \quad \forall b, b' \in S$ (distinct);
- $\binom{q+\#S-1}{\#S} \geq n^{2\lfloor\sqrt{r}\rfloor}$;
- $(x+b)^n = x^n + b$ in $\mathbb{Z}/n\mathbb{Z}[x]/(x^r-1), \quad \forall b \in S$;

Then n is a power of a prime

Bernstein formulation

How does the AKS work?

Theorem. (AKS) Let $n \in \mathbb{N}$. Assume q, r primes, $S \subseteq \mathbb{N}$ finite:

- $q | r - 1$;
- $n^{(r-1)/q} \bmod r \notin \{0, 1\}$;
- $\gcd(n, b - b') = 1, \quad \forall b, b' \in S$ (distinct);
- $\binom{q+\#S-1}{\#S} \geq n^{2\lfloor\sqrt{r}\rfloor}$;
- $(x + b)^n = x^n + b$ in $\mathbb{Z}/n\mathbb{Z}[x]/(x^r - 1), \quad \forall b \in S$;

Then n is a power of a prime — Bernstein formulation

Fouvry Theorem (1985) $\Longrightarrow \quad \exists r \approx \log^6 n, s \approx \log^4 n$

How does the AKS work?

Theorem. (AKS) Let $n \in \mathbb{N}$. Assume q, r primes, $S \subseteq \mathbb{N}$ finite:

- $q|r-1$;
- $n^{(r-1)/q} \bmod r \notin \{0,1\}$;
- $\gcd(n, b-b') = 1, \quad \forall b, b' \in S$ (distinct);
- $\binom{q+\#S-1}{\#S} \geq n^{2\lfloor\sqrt{r}\rfloor}$;
- $(x+b)^n = x^n + b$ in $\mathbb{Z}/n\mathbb{Z}[x]/(x^r-1), \quad \forall b \in S$;

Then n is a power of a prime

Bernstein formulation

Fouvry Theorem (1985) $\Rightarrow \quad \exists r \approx \log^6 n, s \approx \log^4 n$

$\Rightarrow \quad$ AKS runs in $O(\log^{17} n)$ operations in $\mathbb{Z}/n\mathbb{Z}$.

How does the AKS work?

Theorem. (AKS) Let $n \in \mathbb{N}$. Assume q, r primes, $S \subseteq \mathbb{N}$ finite:

- $q|r-1$;
- $n^{(r-1)/q} \bmod r \notin \{0,1\}$;
- $\gcd(n, b-b') = 1, \quad \forall b, b' \in S$ (distinct);
- $\binom{q+\#S-1}{\#S} \geq n^{2\lfloor\sqrt{r}\rfloor}$;
- $(x+b)^n = x^n + b$ in $\mathbb{Z}/n\mathbb{Z}[x]/(x^r-1), \quad \forall b \in S$;

Then n is a power of a prime — Bernstein formulation

Fouvry Theorem (1985) $\Rightarrow \quad \exists r \approx \log^6 n, s \approx \log^4 n$

$\Rightarrow$ AKS runs in $O(\log^{17} n)$ operations in $\mathbb{Z}/n\mathbb{Z}$.

Many simplifications and improvements: Bernstein, Lenstra, Pomerance.....

Why is RSA safe?

Why is RSA safe?

☞

☞

☞

Why is RSA safe?

- It is clear that if Charles can factor M,
-
-

Why is RSA safe?

- It is clear that if Charles can factor M,
  then he can also compute $\varphi(M)$ and then also d so to decrypt messages
-
-

Why is RSA safe?

- It is clear that if Charles can factor M,
  then he can also compute $\varphi(M)$ and then also d so to decrypt messages
- Computing $\varphi(M)$ is equivalent to completely factor M. In fact
-

Why is RSA safe?

- It is clear that if Charles can factor M,
  then he can also compute $\varphi(M)$ and then also d so to decrypt messages
- Computing $\varphi(M)$ is equivalent to completely factor M. In fact

$$p, q = \frac{M - \varphi(M) + 1 \pm \sqrt{(M - \varphi(M) + 1)^2 - 4M}}{2}$$

-

Why is RSA safe?

- It is clear that if Charles can factor M,
  then he can also compute $\varphi(M)$ and then also d so to decrypt messages
- Computing $\varphi(M)$ is equivalent to completely factor M. In fact

$$p, q = \frac{M - \varphi(M) + 1 \pm \sqrt{(M - \varphi(M) + 1)^2 - 4M}}{2}$$

- **RSA Hypothesis.** The only way to compute efficiently

Why is RSA safe?

- It is clear that if Charles can factor M,
  then he can also compute $\varphi(M)$ and then also d so to decrypt messages
- Computing $\varphi(M)$ is equivalent to completely factor M. In fact

$$p, q = \frac{M - \varphi(M) + 1 \pm \sqrt{(M - \varphi(M) + 1)^2 - 4M}}{2}$$

- **RSA Hypothesis.** The only way to compute efficiently

$$x^{1/e} \bmod M, \quad \forall x \in \mathbb{Z}/M\mathbb{Z}$$

Why is RSA safe?

- It is clear that if Charles can factor M,
  then he can also compute $\varphi(M)$ and then also d so to decrypt messages
- Computing $\varphi(M)$ is equivalent to completely factor M. In fact

$$p, q = \frac{M - \varphi(M) + 1 \pm \sqrt{(M - \varphi(M) + 1)^2 - 4M}}{2}$$

- **RSA Hypothesis.** The only way to compute efficiently

  $$x^{1/e} \bmod M, \quad \forall x \in \mathbb{Z}/M\mathbb{Z}$$

  (i.e. decrypt messages) is to factor M

Why is RSA safe?

- It is clear that if Charles can factor M,
  then he can also compute $\varphi(M)$ and then also d so to decrypt messages
- Computing $\varphi(M)$ is equivalent to completely factor M. In fact

$$p, q = \frac{M - \varphi(M) + 1 \pm \sqrt{(M - \varphi(M) + 1)^2 - 4M}}{2}$$

- **RSA Hypothesis.** The only way to compute efficiently

  $$x^{1/e} \bmod M, \quad \forall x \in \mathbb{Z}/M\mathbb{Z}$$

  (i.e. decrypt messages) is to factor M

  In other words

Why is RSA safe?

- It is clear that if Charles can factor M, then he can also compute $\varphi(M)$ and then also d so to decrypt messages
- Computing $\varphi(M)$ is equivalent to completely factor M. In fact

$$p, q = \frac{M - \varphi(M) + 1 \pm \sqrt{(M - \varphi(M) + 1)^2 - 4M}}{2}$$

- **RSA Hypothesis.** The only way to compute efficiently

  $$x^{1/e} \bmod M, \quad \forall x \in \mathbb{Z}/M\mathbb{Z}$$

  (i.e. decrypt messages) is to factor M

  In other words

  The two problems are polynomially equivalent

Two kinds of Cryptography

Two kinds of Cryptography

- **Private key (or symmetric)**
  - Lucifer
  - DES
  - AES

Two kinds of Cryptography

- **Private key (or symmetric)**
  - Lucifer
  - DES
  - AES
- **Public key**
  - RSA
  - Diffie–Hellmann
  - Knapsack
  - NTRU