ECE297:11 Lecture 12

RSA – Genesis, operation & security

Public Key (Asymmetric) Cryptosystems

Public key of Bob - $K_B$

Private key of Bob - $k_B$

Alice

Encryption

Network

Decryption

Bob

Trap-door one-way function

Whitfield Diffie and Martin Hellman
“New directions in cryptography,” 1976

PUBLIC KEY

$X$  $f(X)$  $Y$

$X$  $f^{-1}(Y)$

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

1. Know how to break Russian ciphers
2. Use only well-established proven methods
3. Hire 50,000 mathematicians
4. Cooperate with an industry giant
5. Keep as much as possible secret

1. Know nothing about cryptography
2. Think of revolutionary ideas
3. Go for skiing
4. Publish in “Scientific American”
5. Offer a $100 award for breaking the cipher

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 88886692357797531
690690724573339878059712356395870
5089809751475992900626879543541
e = 9007

Award 100 $
RSA keys

<table>
<thead>
<tr>
<th>PUBLIC KEY</th>
<th>PRIVATE KEY</th>
</tr>
</thead>
<tbody>
<tr>
<td>{ e, N }</td>
<td>{ d, P, Q }</td>
</tr>
</tbody>
</table>

N = P \cdot Q \quad P, Q - large prime numbers

e \cdot d \equiv 1 \mod ((P-1)(Q-1))

Why does RSA work? (1)

\[ M' = C^d \mod N = (M^e \mod N)^d \mod N = M \]
decrypted \quad original
message \quad message

\[ e \cdot d \equiv 1 \mod ((P-1)(Q-1)) \]

\[ e \cdot d \equiv 1 \mod \varphi(N) \] \quad Euler’s totient function

Euler’s totient (phi) function (1)

\[ \varphi(N) - number \ of \ integers \ in \ the \ range \ from \ 1 \ to \ N-1 \] that are relatively prime with N

Special cases:

1. P is prime
   \[ \varphi(P) = P-1 \]
   Relatively prime with P: 1, 2, 3, ..., P-1

2. N = P \cdot Q \quad P, Q are prime
   \[ \varphi(N) = (P-1)\cdot(Q-1) \]
   Relatively prime with N: \{1, 2, 3, ..., P-1\} \cup \{P, 2P, ..., (Q-1)P\} \cup \{Q, 2Q, ..., (P-1)Q\}
Euler’s totient (phi) function (2)

Special cases:
3. \( N = P^2 \)  
   \( P \) is prime  
   \[ \varphi(N) = P \cdot (P-1) \]

Relatively prime with \( N \): \( \{1, 2, 3, \ldots, P^2-1\} \) \( \sim \) \( \{P, 2P, 3P, \ldots, (P-1)P\} \)

In general
If \( N = P_1^{e_1} \cdot P_2^{e_2} \cdot P_3^{e_3} \cdots \cdot P_t^{e_t} \)
\[ \varphi(N) = \prod_{i=1}^{t} P_i^{e_i-1} \cdot (P_i-1) \]

Euler’s Theorem

Leonard Euler, 1707-1783

\[ \forall a: \text{gcd}(a, N) = 1 \quad a^{\varphi(N)} \equiv 1 \pmod{N} \]

Euler’s Theorem - Justification (1)

For \( N=10 \)

\( R = \{1, 3, 7, 9\} \)

Let \( a=3 \)

\( S = \{3 \cdot 1 \text{ mod } 10, 3 \cdot 3 \text{ mod } 10, 3 \cdot 7 \text{ mod } 10, 3 \cdot 9 \text{ mod } 10 \} \)
\( = \{3, 9, 1, 7\} \)

For arbitrary \( N \)

\( R = \{x_1, x_2, \ldots, x_{\varphi(N)}\} \)

Let us choose arbitrary \( a \), such that \( \text{gcd}(a, N) = 1 \)

\( S = \{a \cdot x_1 \text{ mod } N, a \cdot x_2 \text{ mod } N, \ldots, a \cdot x_{\varphi(N)} \text{ mod } N\} \)
\( = \) rearranged set \( R \)
Euler’s Theorem - Justification (2)

For $N=10$

\[
R = S = x_1 x_2 x_3 x_4 \equiv (a x_1) (a x_2) (a x_3) (a x_4) \mod N
\]

\[
a^4 \equiv 1 \pmod{N}
\]

For arbitrary $N$

\[
R = S = \prod_{i=1}^{\varphi(N)} x_i \equiv \prod_{i=1}^{\varphi(N)} a x_i \pmod{N}
\]

\[
a^{\varphi(N)} \equiv 1 \pmod{N}
\]

Why does RSA work? (2)

\[
M' = C^d \pmod{N} = (M^e \pmod{N})^d \pmod{N} =
\]

\[
= M^e \cdot d \equiv 1 \pmod{\varphi(N)} =
\]

\[
= M^{e \cdot d} \pmod{N} = M \cdot (M^\varphi(N))^k \pmod{N} =
\]

\[
= M \cdot M^{\varphi(N)} \pmod{N} = M \cdot 1^k \pmod{N} = M
\]

Rivest estimation - 1977

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

\[
40000 \text{ trillion years} = 40 \cdot 10^{15} \text{ years}
\]

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 = 10 ps

Estimated age of the universe: 100 bln years = $10^{11}$ years
Early records in factoring large numbers

<table>
<thead>
<tr>
<th>Years</th>
<th>Number of decimal digits</th>
<th>Number of bits</th>
<th>Required computational power (in MIPS-years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1974</td>
<td>45</td>
<td>149</td>
<td>0.001</td>
</tr>
<tr>
<td>1984</td>
<td>71</td>
<td>235</td>
<td>0.1</td>
</tr>
<tr>
<td>1991</td>
<td>100</td>
<td>332</td>
<td>7</td>
</tr>
<tr>
<td>1992</td>
<td>110</td>
<td>365</td>
<td>75</td>
</tr>
<tr>
<td>1993</td>
<td>120</td>
<td>398</td>
<td>830</td>
</tr>
</tbody>
</table>

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)

Practical implementations of attacks

Factorization, RSA

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of bits of N</th>
<th>Number of decimal digits of N</th>
<th>Method</th>
<th>Estimated amount of computations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1994</td>
<td>430</td>
<td>129</td>
<td>QS</td>
<td>5000 MIPS-years</td>
</tr>
<tr>
<td>1996</td>
<td>433</td>
<td>130</td>
<td>GNFS</td>
<td>750 MIPS-years</td>
</tr>
<tr>
<td>1998</td>
<td>467</td>
<td>140</td>
<td>GNFS</td>
<td>2000 MIPS-years</td>
</tr>
<tr>
<td>1999</td>
<td>467</td>
<td>140</td>
<td>GNFS</td>
<td>8000 MIPS-years</td>
</tr>
</tbody>
</table>
**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

---

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

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

---

**Factoring methods**

<table>
<thead>
<tr>
<th>General purpose</th>
<th>Special purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time of factoring depends only on the size of N</td>
<td>Time of factoring is much shorter if N or factors of N are of the special form</td>
</tr>
</tbody>
</table>

- GNFS - General Number Field Sieve
- QS - Quadratic Sieve
- Continued Fraction Method (historical)
- ECM - Elliptic Curve Method
- Pollard’s p-1 method
- Cyclotomic polynomial method
- SNFS - Special Number Field Sieve
Running time of factoring algorithms

\[ L_{\alpha}(\alpha, c) = \exp \left( (c+o(1)) \left( \ln q \right)^{\alpha} \left( \ln \ln q \right)^{1-\alpha} \right) \]

- For \( \alpha = 0 \)
  \[ L_{\alpha}[0, c] = (\ln q)^{c+o(1)} \]
  Algorithm \text{polynomial} as a function of the number of bits of \( q \)

- For \( \alpha = 1 \)
  \[ L_{\alpha}[1, c] = \exp((c+o(1))(\ln q)) \]
  Algorithm \text{exponential} as a function of the number of bits of \( q \)

- For \( 0 < \alpha < 1 \)
  \[ L_{\alpha}[\alpha, c] = \exp((\alpha+o(1))(\ln q)) \]
  Algorithm \text{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 \( n \geq n_0 \)

General purpose factoring methods

- **Expected running time**
  - QS
    \[ L_{QS}[1/2, 1] = \exp((1+o(1))(\ln N)^{1/2}((\ln \ln N)^{1/2})) \]
  - NFS
    \[ L_{NFS}[1/3, 1.92] = \exp((1.92+o(1))(\ln N)^{1/3}((\ln \ln N)^{2/3})) \]

QS more efficient \( \rightarrow \) NFS more efficient

- Size of the factored number \( N \) in decimal digits (D)
- 100D \rightarrow 110D \rightarrow 120D \rightarrow 130D

RSA Challenge

- Smallest unfactored number
  - **RSA-150**
  - Unused awards accumulate at a rate of $1750 / quarter
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

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

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) |
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

RSA vs. DES: Resistance to attack
Number of operations in the best known attack

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#nfscircuit
### 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

### 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

### 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

\[ 10 \text{ billion} \times \text{several minutes} = \text{tens of years} \]

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

Bernstein’s Machine (6)

<table>
<thead>
<tr>
<th>RSA keylength that can be broken using Bernstein’s machine</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA key lengths that can be broken using classical computers</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>$1 \text{bln} \times 1 \text{day}$</td>
</tr>
</tbody>
</table>

Computational cost = time [days] * memory [$]

RSA Challange

<table>
<thead>
<tr>
<th>Length of N in bits</th>
<th>Length of N in decimal digits</th>
<th>Award for factorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>576</td>
<td>174</td>
<td>$10,000</td>
</tr>
<tr>
<td>640</td>
<td>193</td>
<td>$20,000</td>
</tr>
<tr>
<td>704</td>
<td>212</td>
<td>$30,000</td>
</tr>
<tr>
<td>768</td>
<td>232</td>
<td>$50,000</td>
</tr>
<tr>
<td>896</td>
<td>270</td>
<td>$75,000</td>
</tr>
<tr>
<td>1024</td>
<td>309</td>
<td>$100,000</td>
</tr>
<tr>
<td>1536</td>
<td>463</td>
<td>$150,000</td>
</tr>
<tr>
<td>2048</td>
<td>617</td>
<td>$200,000</td>
</tr>
</tbody>
</table>
Estimation of RSA Security Inc. regarding the number and memory of PCs necessary to break RSA-1024

<table>
<thead>
<tr>
<th>Attack time:</th>
<th>1 year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single machine:</td>
<td>PC, 500 MHz, 170 GB RAM</td>
</tr>
<tr>
<td>Number of machines:</td>
<td>342,000,000</td>
</tr>
</tbody>
</table>