ECE646 Lecture 11

RSA Key Generation

Required Reading

W. Stallings, "Cryptography and Network-Security,"

Chapter 8.3 Testing for Primality

A. Menezes, P. van Oorschot, and S. Vanstone,  
“Handbook of Applied Cryptography”

Chapter 4 Public-Key Parameters
  4.1 Introduction
  4.2 Probabilistic primality tests (you can skip 4.2.2  
     Solvay-Strassen test)
  4.4 Prime number generation (you can skip 4.4.3 and  
     4.4.4)
Generation of the RSA keys

Typically
\[ e = 2^{16} + 1 \]

\[ \gcd(e, P-1) = 1 \]
\[ \gcd(e, Q-1) = 1 \]
\[ \gcd(e-1, P-1) = 2 \]
\[ \gcd(e-1, Q-1) = 2 \]

Extended Euclid’s algorithm

\[ d = e^{-1} \mod (P-1) \cdot (Q-1) \]

RSA as a trap-door one-way function

\[ C = f(M) = M^e \mod N \]
\[ M = f^{-1}(C) = C^d \mod N \]

\[ N = P \cdot Q \]
\[ P, Q - large prime numbers \]
\[ e \cdot d \equiv 1 \mod ((P-1)(Q-1)) \]
Concealment of messages in the RSA cryptosystem

Blakley, Borosh, 1979

At least 9 messages not concealed by RSA!

Number of messages not concealed by RSA:

\[\sigma = (1 + \gcd(e-1, P-1)) \cdot (1 + \gcd(e-1, Q-1))\]

A. \(e=3\)  \(\sigma = 9\)

B. \(\gcd(e-1, P-1) = 2\) and \(\gcd(e-1, Q-1) = 2\)  \(\sigma = 9\)

C. \(\gcd(e-1, P-1) = P-1\) and \(\gcd(e-1, Q-1) = Q-1\)  \(\sigma = P \cdot Q = N\)

It is possible that all messages remain unconcealed by RSA!

Random vs. Incremental Search

Random search

---

Incremental search

starting point chosen at random
Is there a sufficient amount of prime numbers to choose from?

\( \pi(x) \) - the amount of prime numbers smaller than \( x \)

\[
\pi(x) = \frac{x}{\ln(x)}
\]

<table>
<thead>
<tr>
<th>( x )</th>
<th>( \pi(x) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>10^{100}</td>
<td>4.3 \cdot 10^{97}</td>
</tr>
<tr>
<td>10^{150}</td>
<td>2.9 \cdot 10^{147}</td>
</tr>
</tbody>
</table>

Is there a sufficient amount of prime numbers of the given bit length to choose from?

\( \pi_k \) - the amount of prime numbers of the size of \( k \)-bits

\[
\pi_k = \pi(2^k) - \pi(2^{k-1}) \\
\approx 0.5 \cdot \pi(2^k) \\
\approx \pi(2^{k-1})
\]

<table>
<thead>
<tr>
<th>( k )</th>
<th>( \pi_k )</th>
</tr>
</thead>
<tbody>
<tr>
<td>384</td>
<td>7 \cdot 10^{112}</td>
</tr>
<tr>
<td>512</td>
<td>4 \cdot 10^{151}</td>
</tr>
<tr>
<td>1024</td>
<td>2.5 \cdot 10^{305}</td>
</tr>
</tbody>
</table>
Average distance between primes of the given bit length (1)

Average distance between two consecutive primes

Average distance (k) \approx \frac{2^k - 2^{k-1}}{\pi_k} \approx \frac{2^{k-1}}{\pi(2^{k-1})} \approx \ln 2^{k-1} \approx 0.69 \cdot (k-1)

Average distance between primes of the given bit length (2)

<table>
<thead>
<tr>
<th>Number of bits k</th>
<th>Average distance between primes</th>
<th>Average amount of odd numbers to test</th>
</tr>
</thead>
<tbody>
<tr>
<td>256</td>
<td>177</td>
<td>88</td>
</tr>
<tr>
<td>384</td>
<td>265</td>
<td>132</td>
</tr>
<tr>
<td>512</td>
<td>354</td>
<td>177</td>
</tr>
<tr>
<td>1024</td>
<td>709</td>
<td>355</td>
</tr>
</tbody>
</table>
**Euler’s Theorem**

Leonard Euler, 1707-1783

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

**Fermat’s Theorem**

Pierre de Fermat, 1601?-1665

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

Algorithm Fermat primality test

FERMAT(n,t)
INPUT: an odd integer \( n \geq 3 \) and security parameter \( t \geq 1 \).
OUTPUT: an answer “prime” or “composite” to the question: “Is \( n \) prime?”

1. For \( i \) from 1 to \( t \) do the following:
   1.1 Choose a random integer \( a, 2 \leq a \leq n - 2 \).
   1.2 Compute \( r = a^{n-1} \mod n \) using Algorithm 2.143.
   1.3 If \( r \neq 1 \) then return ("composite").
2. Return ("prime").
Carmichael Numbers

A composite integer is a Carmichael number iff

\[ n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k \]

\[ k \geq 3 \]

\[ p_i \text{ are distinct primes, } p_i \neq p_j \text{ for } i \neq j \]

\[ \forall p_i (p_i - 1) \mid (n - 1) \]

Smallest Carmichael number

\[ n = 561 = 3 \cdot 11 \cdot 17 \]

Among all numbers smaller or equal to \(10^{15}\)

There are about \(3 \cdot 10^{13}\) prime numbers

\(10^5\) Carmichael numbers
**Good probabilistic primality test**

∀ n composite  | |W(n)| ≥ |L(n)|

If \(a \in W(n)\) test returns “n composite”
else test returns “n probably prime”
or “n pseudoprime to the base a”

**Miller-Rabin test**

∀ n composite  | |L(n)| ≤ \(\varphi(n)/4 < (n-1)/4\)
Miller-Rabin test

Strong witnesses to the compositness of n

For certain composite numbers, such as
n = 3 · 5 · 7 · . . . · (2k+1)
there are only two strong liars: 1 and n-1

Miller-Rabin test
Mathematical Basis

If n is prime then
1 has only two square roots modulo n
i.e., there are only two numbers, y₁ and y₂, such that
y₁² mod n = 1 and y₂² mod n = 1
y₁=1 and y₂=n-1≡-1 mod n

If n is composite then
1 has at least four square roots modulo n
i.e., there exist numbers, y₁, y₂, y₃, y₄, such that
y₁² mod n = 1, y₂² mod n = 1, y₃² mod n = 1, y₄² mod n = 1,
y₁=1, y₂=n-1≡-1 mod n, y₃ ≠ ± 1 mod n, y₄ ≠ ± 1 mod n
Miller-Rabin test
Algorithm (1)

Find s and r, such that

\[ n - 1 = 2^s \cdot r, \text{ where } r \text{ is odd} \]

For example:

\[ n = 49 \]
\[ n - 1 = 48 = 2^4 \cdot 3 \quad s=4, r=3 \]

\[ n = 61 \]
\[ n - 1 = 60 = 2^2 \cdot 15 \quad s=2, r=15 \]

Miller-Rabin test
Algorithm (2)

Compute

\[ a^{n-1} \mod n = \ldots ((a^r \mod n)^2 \mod n)^2 \mod n \ldots)^2 \mod n = 1 \]

s squarings

\[ \frac{a^r}{(a^r)^2} (a^r)^2 \ldots (a^r)^2^{s-1} (a^r)^2^s \mod n \]

square mod n

square root mod n
Miller-Rabin test

Algorithm (3)

\[\begin{align*}
a^r &\quad (a^r)^2 &\quad (a^r)^2 &\quad (a^r)^2 &\quad \ldots &\quad (a^r)^{s-1} &\quad (a^r)^{2^s} \\ \text{square mod } n & & & & & & \text{mod } n \\
\text{square root mod } n & & & & & & \text{result of test} \\
1 & 1 & 1 & 1 & 1 & 1 & \text{result of test} \\
X & X & -1 & 1 & 1 & 1 & \text{result of test} \\
X & X & 1 & 1 & 1 & 1 & \text{result of test} \\
-1 & 1 & 1 & 1 & 1 & 1 & \text{result of test} \\
X & X & X & X & X & X & \text{result of test} \\
\end{align*}\]

\[X \not\equiv \pm 1 \mod n\]

**probably prime or composite?**

Miller-Rabin test

**Algorithm** Miller-Rabin probabilistic primality test

**Algorithm** Miller-Rabin probabilistic primality test

MILLER-RABIN(n,t)

INPUT: an odd integer \( n \geq 3 \) and security parameter \( t \geq 1 \).

OUTPUT: an answer “prime” or “composite” to the question: “Is \( n \) prime?”

1. Write \( n - 1 = 2^r s \) such that \( r \) is odd.
2. For \( i \) from 1 to \( t \) do the following:
   2.1 Choose a random integer \( a, 2 \leq a \leq n - 2 \).
   2.2 Compute \( y = a^r \mod n \) using Algorithm 2.143.
   2.3 If \( y \neq 1 \) and \( y \neq n - 1 \) then do the following:
      \( j \leftarrow 1 \).
      While \( j \leq s - 1 \) and \( y \neq n - 1 \) do the following:
      Compute \( y \leftarrow y^2 \mod n \).
      If \( y = 1 \) then return (“composite”).
      \( j \leftarrow j + 1 \).
      If \( y \neq n - 1 \) then return (“composite”).
3. Return (“prime”).
-log₂ of the bound on the error probability of declaring a $k$-bit composite number a prime after $t$ iterations of the Miller-Rabin test

<table>
<thead>
<tr>
<th>$k$ = number of bits of $n$</th>
<th>$t$ - number of iterations of the Miller-Rabin test</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>5 14 20 25 29 33 36 39 41 44</td>
</tr>
<tr>
<td>150</td>
<td>8 20 28 34 39 43 47 51 54 57</td>
</tr>
<tr>
<td>200</td>
<td>11 25 34 41 47 52 57 61 65 69</td>
</tr>
<tr>
<td>250</td>
<td>14 29 39 47 54 60 65 70 75 79</td>
</tr>
<tr>
<td>300</td>
<td>19 33 44 53 60 67 73 78 83 88</td>
</tr>
<tr>
<td>400</td>
<td>37 46 55 63 72 80 87 93 99 105</td>
</tr>
<tr>
<td>500</td>
<td>56 63 70 78 85 92 99 106 113 119</td>
</tr>
<tr>
<td>600</td>
<td>75 82 88 95 102 108 115 121 127 133</td>
</tr>
</tbody>
</table>

Minimal number of the Miller-Rabin tests $t$, necessary to obtain the probability of error < $2^{-100}$ for a $k$-bit number $n$

<table>
<thead>
<tr>
<th>$k$</th>
<th>$t$</th>
<th>$k$</th>
<th>$t$</th>
<th>$k$</th>
<th>$t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>160</td>
<td>34</td>
<td>202-208</td>
<td>23</td>
<td>335-360</td>
<td>12</td>
</tr>
<tr>
<td>161-163</td>
<td>33</td>
<td>209-215</td>
<td>22</td>
<td>361-392</td>
<td>11</td>
</tr>
<tr>
<td>164-166</td>
<td>32</td>
<td>216-222</td>
<td>21</td>
<td>393-430</td>
<td>10</td>
</tr>
<tr>
<td>167-169</td>
<td>31</td>
<td>223-231</td>
<td>20</td>
<td>431-479</td>
<td>9</td>
</tr>
<tr>
<td>170-173</td>
<td>30</td>
<td>232-241</td>
<td>19</td>
<td>480-542</td>
<td>8</td>
</tr>
<tr>
<td>174-177</td>
<td>29</td>
<td>242-252</td>
<td>18</td>
<td>543-626</td>
<td>7</td>
</tr>
<tr>
<td>178-181</td>
<td>28</td>
<td>253-264</td>
<td>17</td>
<td>627-746</td>
<td>6</td>
</tr>
<tr>
<td>182-185</td>
<td>27</td>
<td>265-278</td>
<td>16</td>
<td>747-926</td>
<td>5</td>
</tr>
<tr>
<td>186-190</td>
<td>26</td>
<td>279-294</td>
<td>15</td>
<td>927-1232</td>
<td>4</td>
</tr>
<tr>
<td>191-195</td>
<td>25</td>
<td>295-313</td>
<td>14</td>
<td>1233-1853</td>
<td>3</td>
</tr>
<tr>
<td>196-201</td>
<td>24</td>
<td>314-334</td>
<td>13</td>
<td>over 1853</td>
<td>2</td>
</tr>
</tbody>
</table>
Minimal number of the Miller-Rabin tests, $t$, for relatively small numbers $n$

**Definition** Let $p_1, p_2, \ldots, p_t$ denote the first $t$ primes. Then $\psi_t$ is defined to be the smallest positive composite integer which is a strong pseudoprime to all the bases $p_1, p_2, \ldots, p_t$.

The numbers $\psi_t$ can be interpreted as follows: to determine the primality of any integer $n < \psi_t$, it is sufficient to apply the Miller-Rabin algorithm to $n$ with the bases $a$ being the first $t$ prime numbers. With this choice of bases, the answer returned by Miller-Rabin is always correct. Table 4.1 gives the value of $\psi_t$ for $1 \leq t \leq 8$.

<table>
<thead>
<tr>
<th>$t$</th>
<th>$\psi_t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2047</td>
</tr>
<tr>
<td>2</td>
<td>1373653</td>
</tr>
<tr>
<td>3</td>
<td>25326001</td>
</tr>
<tr>
<td>4</td>
<td>3215031751</td>
</tr>
<tr>
<td>5</td>
<td>21523028947</td>
</tr>
<tr>
<td>6</td>
<td>347474900383</td>
</tr>
<tr>
<td>7</td>
<td>341550071328321</td>
</tr>
<tr>
<td>8</td>
<td>341550071728321</td>
</tr>
</tbody>
</table>

Table 4.1: Smallest strong pseudoprimes. The table lists values of $\psi_t$, the smallest positive composite integer that is a strong pseudoprime to each of the first $t$ prime bases, for $1 \leq t \leq 8$.

---

Random vs. Incremental Search

**Random search**

![Random search diagram]

- Primes
- Numbers tested for primality

**Incremental search**

![Incremental search diagram]

- Starting point chosen at random
Using division by small primes

D – Division by small primes
R₂ – Miller-Rabin test with base 2
R – Miller-Rabin test with the random base a

Merten’s Theorem

The proportion of candidate odd integers NOT ruled out by the trial division by all primes ≤ B

\[ \alpha(B) = \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{7}\right) \cdot \ldots \cdot \left(1 - \frac{1}{B}\right) \]

\[ \alpha(B) \approx 1.12 / \ln B \]

For B=256, \( \alpha(B) \approx 0.2 \)

80% of tested numbers discarded by the trial division
### Incremental search for a prime

**Efficient implementation of division by small primes**

<table>
<thead>
<tr>
<th>Set of small primes</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>( n_0 = 91 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( n = 93 )</td>
<td></td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>( n = 95 )</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( n = 97 )</td>
<td></td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>( n = 99 )</td>
<td></td>
<td>1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>( n = 101 )</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>S[k]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>4</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>