Guest Lecture

Professor Martin Tompa from the Computer Science and Engineering Department tells us about ...
Today’s topic

Secret Codes,
Unforgeable Signatures,
and
Coin Flipping on the Phone
<table>
<thead>
<tr>
<th>Name</th>
<th>Address 1</th>
<th>Address 2</th>
<th>City</th>
<th>Zip</th>
<th>Phone 1</th>
<th>Phone 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>John J &amp; Barbara G</td>
<td>5815 Ann Arbor NE</td>
<td>SEATTLE 98105</td>
<td>SEATTLE 98105</td>
<td>206 524-3371</td>
<td>206 523-8877</td>
<td></td>
</tr>
<tr>
<td>John R Dr 8001 Sand Point Way NE</td>
<td>SEATTLE 98115</td>
<td></td>
<td>SEATTLE 98115</td>
<td>206 634-2368</td>
<td>206 524-0179</td>
<td></td>
</tr>
<tr>
<td>GATELY H A 3847 Woodlawn N</td>
<td>SEATTLE 98103</td>
<td></td>
<td>SEATTLE 98103</td>
<td>206 634-2368</td>
<td>206 524-0179</td>
<td></td>
</tr>
<tr>
<td>Joe &amp; Kelley 15114 SE 224th</td>
<td>KENT 98042</td>
<td></td>
<td>KENT 98042</td>
<td>253 639-8073</td>
<td>253 946-4303</td>
<td></td>
</tr>
<tr>
<td>Kimberlie 5815 Ann Arbor NE</td>
<td>SEATTLE 98105</td>
<td></td>
<td>SEATTLE 98105</td>
<td>206 520-1590</td>
<td>206 520-1590</td>
<td></td>
</tr>
<tr>
<td>Steve &amp; Christina 31500 1st Ave S</td>
<td>FEDWY 98003</td>
<td></td>
<td>FEDWY 98003</td>
<td>253 946-4303</td>
<td>253 946-4303</td>
<td></td>
</tr>
<tr>
<td>GATENS Clay M</td>
<td>James 2008 SW 348th</td>
<td>FEDWY 9803</td>
<td>FEDWY 98023</td>
<td>253 838-3565</td>
<td>253 838-3565</td>
<td></td>
</tr>
<tr>
<td>GATERS M 11300 3d NE</td>
<td>SEATTLE 98125</td>
<td></td>
<td>SEATTLE 98125</td>
<td>206 363-1482</td>
<td>206 363-1482</td>
<td></td>
</tr>
<tr>
<td>GATES A 721 17th</td>
<td>SEATTLE 98122</td>
<td></td>
<td>SEATTLE 98122</td>
<td>206 320-3705</td>
<td>206 320-3705</td>
<td></td>
</tr>
<tr>
<td>A &amp; C Shoreline</td>
<td></td>
<td></td>
<td>A &amp; C Shoreline</td>
<td>206 362-4366</td>
<td>206 362-4366</td>
<td></td>
</tr>
<tr>
<td>Abraham 820 NE 57th</td>
<td>SEATTLE 98105</td>
<td></td>
<td>SEATTLE 98105</td>
<td>206 729-1580</td>
<td>206 729-1580</td>
<td></td>
</tr>
<tr>
<td>Andrew R 14405 SE 15th</td>
<td>BLVU 98007</td>
<td></td>
<td>BLVU 98007</td>
<td>425 957-7398</td>
<td>425 957-7398</td>
<td></td>
</tr>
<tr>
<td>Barron</td>
<td></td>
<td></td>
<td>Barron</td>
<td>206 901-1947</td>
<td>206 901-1947</td>
<td></td>
</tr>
<tr>
<td>Bertha 3014 NE 98th</td>
<td>SEATTLE 98115</td>
<td></td>
<td>SEATTLE 98115</td>
<td>206 729-0714</td>
<td>206 729-0714</td>
<td></td>
</tr>
<tr>
<td>Evelyn 801 Third</td>
<td></td>
<td></td>
<td>Evelyn 801 Third</td>
<td>206 523-3777</td>
<td>206 523-3777</td>
<td></td>
</tr>
</tbody>
</table>

© Copyright Martin Tompa, 1999
What Is a Cryptosystem?

- Sender: A
- Receiver: B
- Cryptanalyst: (bad guy)

Encryption: $C = E_{AB}(M)$
Decryption: $M = D_{AB}(C)$

<table>
<thead>
<tr>
<th>M</th>
<th>C</th>
<th>$K_{AB}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message</td>
<td>Encryption</td>
<td>Key</td>
</tr>
<tr>
<td>Plaintext</td>
<td>Cyphertext</td>
<td></td>
</tr>
<tr>
<td>Cleartext</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What Is a Public Key Cryptosystem?

A Sender  \( C = E_{AB}(M) \)  A Receiver  \( M = D_{AB}(C) \)

<table>
<thead>
<tr>
<th>M</th>
<th>C</th>
<th>( K_B )</th>
<th>( E_B )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message</td>
<td>Encryption</td>
<td>Key</td>
<td>Public Key</td>
</tr>
<tr>
<td>Plaintext</td>
<td>Cyphertext</td>
<td>Private Key</td>
<td></td>
</tr>
</tbody>
</table>
The RSA Public Key Cryptosystem

- Has proven resilient to all cryptanalytic attacks since.
Receiver’s Set-Up

- Choose 500-digit primes $p$ and $q$ (each 2 more than a multiple of 3).
  
  $p = 5, \ q = 11$

- Let $n = pq$.
  
  $n = 55$

- Let $s = (1/3) \ (2(p - 1)(q - 1) + 1)$.
  
  $s = (1/3) \ (2 \cdot 4 \cdot 10 + 1) = 27$

- Publish $n$.
  
  Keep $p$, $q$ and $s$ secret.
Encrypting a Message

- Break the message into chunks.
  H I C H R I S ...

- Translate each chunk into an integer $M$ ($0 < M < n$).
  8 9 3 8 18 9 19 ...

- Divide $M^3$ by $n$. $E(M)$ is the remainder.
  $M = 8, \ n = 55$
  $8^3 = 512 = 9 \times 55 + 17$
  $E(8) = 17$

© Copyright Martin Tompa, 1999
Decrypting A Cyphertext C

- Divide $C^s$ by $n$. $D(C)$ is the remainder.
  
  \[ C = 17, \quad n = 55, \quad s = 27 \]
  
  \[ 17^{27} = 1,667,711,322,168,688,287,513,535,727,415,473 \]
  
  \[ = 30,322,024,039,430,696,136,609,740,498,463 \times 55 + 8 \]
  
  \[ D(17) = 8 \]

- Translate $D(C)$ into letters.
  
  H
Euler’s Theorem (1736): Suppose

- $p$ and $q$ are distinct primes,
- $n = pq$,
- $0 < M < n$, and
- $k > 0$.

If $M^{k(p-1)(q-1)+1}$ is divided by $n$, the remainder is $M$.

\[
(M^3)^s = (M^3)^{(1/3)(2(p-1)(q-1)+1)} = M^{2(p-1)(q-1)+1}
\]
Leonhard Euler 1707-1783
Why Is It Secure?

- To find \( M = D(C) \), you seem to need \( s \).
- To find \( s \), you seem to need \( p \) and \( q \).
- All you have is \( n = pq \).
- How hard is it to factor a 1000-digit number \( n \)?
  
  With the grade school method, doing 10,000,000 steps per second, it would take ... \( 10^{485} \) years.


1994: RSA129 factored over an 8 month period using 1000 computers on the Internet around the world.

With this method, a 250-digit number would take 100,000,000 times as long.
Signed Messages

❖ How A sends a secret message to B

\[ C = E_B(M) \quad \text{and} \quad M = D_B(C) \]
Signed Messages

❖ How A sends a secret message to B

A \[ C = E_B(M) \]

B \[ M = D_B(C) \]

❖ How A sends a signed message to B

A \[ C = D_A(M) \]

B \[ M = E_A(C) \]
Signed *and* Secret Messages

- How A sends a secret message to B ...
  \[ C = E_B(M) \]
  \[ M = D_B(C) \]

- How A sends a signed secret message to B ...
  \[ C = E_B(D_A(M)) \]
  \[ M = E_A(D_B(C)) \]
**Flipping a Coin Over the Phone**

**A**

Choose random $x$.

$y = E_A(x)$

**B**

Guess if $x$ is even or odd.

Guess if $y = E_A(x)$.

- “even”
- “odd”

Check $y = E_A(x)$.

- B wins if the guess about $x$ was right