Introduction to Modern Cryptography

9th lecture:
Public-Key Encryption
El Gamal Encryption
last time:
• Private-Key Management
• Public-Key Revolution

9th lecture (today):
• Public-Key Encryption
• El Gamal

- algorithmic number theory
- key distribution, Diffie-Hellmann
- RSA

<table>
<thead>
<tr>
<th></th>
<th>secret key</th>
<th>public key</th>
</tr>
</thead>
<tbody>
<tr>
<td>confidentiality</td>
<td>private-key encryption</td>
<td>public-key encryption</td>
</tr>
<tr>
<td>authentication</td>
<td>message authentication codes (MAC)</td>
<td>digital signatures</td>
</tr>
</tbody>
</table>
last time:
• Private-Key Management
• Public-Key Revolution

9th lecture (today):
• Public-Key Encryption
• El Gamal
Taher Elgamal

*1955

- 1977: BSc from Cairo university
- 1984: PhD from Stanford
- 1996: “Father of SSL” as Chief Scientist of Netscape
- CTO of various companies

- fun fact: “I read number theory books for fun!”
Recent Software Bugs

• Feb 2014: #gotofail in Apple software

• April 2014: Heartbleed in OpenSSL library, see XKCD

• 24 Sep 2014: Shellshock in Unix Bash shell

Bottom line: implementing security-related software is difficult