Introduction to Modern Cryptography

Master of Logic 2012
2nd Quarter Nov / Dec
Christian Schaffner

- me
- pure mathematics at ETH Zurich
- PhD from Aarhus, Denmark
- research: quantum cryptography
- c.schaffner@uva.nl
- plays ultimate frisbee
Maria Velema

- your teaching assistant
- MoL student
- mariavelema@gmail.com

- switched sides of the table
Outline of the Course

• Historical cryptography & principles of modern cryptography
• perfectly-secret encryption
Outline of the Course II

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>secret key</th>
<th>public key</th>
</tr>
</thead>
<tbody>
<tr>
<td></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>


# Outline of the Course II

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Secret Key</th>
<th>Public Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private-key encryption</td>
<td>message authentication codes (MAC)</td>
<td>digital signatures</td>
</tr>
</tbody>
</table>

- reduction proofs
- pseudorandomness
- block ciphers: DES, AES
### Outline of the Course II

#### Confidentiality
- reduction proofs
- pseudorandomness
- block ciphers: DES, AES

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Secret Key</th>
<th>Public Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private-key encryption</td>
<td>RSA</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Message Authentication codes (MAC)</th>
<th>Digital Signatures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public-key encryption</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- digital signatures
Fun Stuff

• zero-knowledge proofs
• multi-party computation (secret sharing, bit commitment, oblivious transfer)
• electronic voting and auctions
• quantum cryptography
• position-based cryptography
• ...
Questions ?
Introduction

• for centuries, cryptography has been an “art of writing codes and solving codes”

• goal: secret communication

• mainly used by military and intelligence

• “modern cryptography”
Claude Elwood Shannon
1916 - 2001

• Father of Information Theory
• Graduate of MIT
• Bell Labs

• juggling, unicycling, chess
• ultimate machine
Silvio Micali, Shafi Goldwasser, Oded Goldreich

- MIT
- Weizmann Institute
- Foundations of Modern Cryptography
Modern Cryptography

• “scientific study of techniques for securing digital information, transactions and distributed computations”

• crypto is everywhere!
Auguste Kerckhoffs
1835 - 1903

- Dutch linguist and cryptographer
- Kerckhoffs’ principle:
  “A cryptosystem should be secure even if everything about the system, except the key, is public knowledge”
- leader of Volapük movement
AES and SHA competitions

- AES: advanced encryption standard
- SHA: secure hash algorithm
- both determined by a public procedure led by the National Institute for Standards and Technology (NIST)
- SHA-3 zoo
Gaius Julius Caesar
100 BC – 44 BC

• not best known for his cryptographic skills
• Roman general
• suffered from epilepsy, or migraine headache
Modular Arithmetic

• Given integers $a$ and $N > 1$ we write $[a \mod N] \in \{0,1,2, ..., N-1\}$ as the remainder of $a$ upon division by $N$
Frequency analysis

Wikipedia source
Blaise de Vigenère
1523–1596

- diplomat and cryptographer
- Vigenère’s cipher
- interested in alchemy
Friedrich Kasiski
1805 – 1881

• Preussian infantry officer
• cryptographer and archeologist
Charles Babbage
1791 – 1871

• mathematician, philosopher, inventor and mechanical engineer
• father of the computer
• designed the “difference machine” and “Analytical Engine”

• counted broken window panes
• hated organ grinders
3 Basic Principles of Modern Cryptography
1. Formulation of Exact Definitions

- “a cryptographic scheme is secure if no adversary of a specified power can achieve a specified break”
  example: encryption

- mathematical definitions vs the real world
  example: power-usage attacks

- cryptographers face a similar problem as Turing: “Am I modeling the right thing?”
2. Reliance on Precise Assumptions

- unconditional security is often impractical (unfortunate state of computational complexity)
- validation of assumptions (independent of cryptography)
  example: factoring
- allows to compare crypto schemes
3. Rigorous Proofs of Security

- Intuition is not good enough. History knows countless examples of broken schemes.

- Bugs vs security holes
  - Software users vs adversaries

- Reduction proofs: Given that Assumption X is true, Construction Y is secure. Any adversary breaking Construction Y can be used as subroutine to violate Assumption X.