Introduction to Modern Cryptography

Master of Logic 2014
1st Quarter Sep / Oct
Christian Schaffner

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

• your teaching assistant
• ILLC PhD student
• malvin@w4eg.de
• https://w4eg.de/malvin/

• switched sides of the table
Practicalities

- final grade consists of 50-50:
- weekly homework, to be graded
- final exam in week of 20/10/14 - 24/10/14
- details on course homepage: http://homepages.cwi.nl/~schaffne/courses/crypto/2014/
Expectations

We expect from you

• be on time
• code of honor (do not cheat)
• ask questions!
Expectations

We expect from you
• be on time
• code of honor (do not cheat)
• ask questions!

You can expect from us
• be on time
• make clear what goals are
• listen to you and respond to email requests
• keep website up to date
Questions ?
Outline of the Course

• Historical cryptography & principles of modern cryptography

• perfectly-secret encryption
Outline of the Course II

<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>
Outline of the Course II

- 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></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

- 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></td>
<td>public-key encryption</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>authentication</th>
<th></th>
<th>digital signatures</th>
</tr>
</thead>
<tbody>
<tr>
<td>message authentication codes (MAC)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Fun Stuff

- bitcoin (guest lecture by Marc Stevens, CWI)
- 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!
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
Edward Joseph Snowden
1983 -

- former CIA employee and NSA contractor
- whistleblower
- on (temporary) asylum in Russia
- Traitor or Hero?
Politics of Cyberwar

• Snowden leaked many thousand top secret documents to various media, documenting a
• mass surveillance programs by secret services from all over the world
Politics of Cyberwar

FAA702 Operations
Two Types of Collection

Upstream
- Collection of communications on fiber cables and infrastructure as data flows past.
  (FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

PRISM
- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.
Politics of Cyberwar

- **Methods:** (in decreasing order of difficulty)
  - Break cryptography
  - Influence industrial standards
  - Pressure manufacturers to make insecure devices
  - Infiltrate hardware and software (communication infrastructure, computers, smartphones etc.)
Politics of Cyberwar

- **Methods:** (in decreasing order of difficulty)
  - **Break** cryptography
  - **Influence** industrial standards
  - **Pressure** manufacturers to make insecure devices
  - **Infiltrate** hardware and software (communication infrastructure, computers, smartphones etc.)

- **Why** mass surveillance?
  - Other than to combat terrorism, these surveillance programs have been employed to **assess the foreign policy** and economic stability of other countries, and to **gather "commercial secrets"**.
Why worry?

• „I have nothing to hide“ is a very naive reaction.
Why worry?

- „I have nothing to hide“ is a very naive reaction.
- Think about what your smartphone knows about you.
Why worry?

• „I have nothing to hide“ is a very naive reaction.
• Think about what your smartphone knows about you.
• Tell me something that your smartphone does not know about you.
Why worry?

- „I have nothing to hide“ is a very naive reaction.
- Think about what your smartphone knows about you.
- Tell me something that your smartphone does not know about you.
Why worry?

- „I have nothing to hide“ is a very naive reaction.
- Think about what your smartphone knows about you.
- Tell me something that your smartphone does not know about you.

**Facebook to Pay $19 Billion for WhatsApp**
Why Worry?

• „I have nothing to hide“ is a very naive reaction.
• Everyone‘s personal privacy is at stake!
• George Orwell‘s surveillance state from his book 1984 has become reality...
Why Worry?

- „I have nothing to hide“ is a very naive reaction.
- Everyone’s personal privacy is at stake!
- George Orwell’s surveillance state from his book 1984 has become reality...

- "They (the NSA) can use the system to go back in time and scrutinize every decision you've ever made, every friend you've ever discussed something with, and attack you on that basis to sort of derive suspicion from an innocent life and paint anyone in the context of a wrongdoer." – Edward Snowden
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 
  \[ \lfloor a \mod N \rfloor \in \{0, 1, 2, \ldots, N-1\} \]
  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.