Introduction to Modern Cryptography

Master of Logic
3rd Block: Feb/March 2016-17
Outline of the Course

• Historical cryptography & principles of modern cryptography

• perfectly-secret encryption
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
Claude Elwood Shannon
1916 - 2001

- Father of Information Theory
- Graduate of MIT
- Bell Labs
- juggling, unicycling, chess
- ultimate machine
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!
Edward Joseph Snowden
1983 -

• former CIA employee and NSA contractor
• whistleblower
• on (temporary) asylum in Russia

• Traitor or Hero?
Politics of Cyberwar

• In 2013, 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)

You Should Use Both

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

- private-key encryption
- public-key encryption
- digital signatures
# Outline of the Course II

**Secret Key**
- Confidentiality
- Authentication
  - Message authentication codes (MAC)

**Public Key**
- Private-key encryption
- Public-key encryption
- Digital signatures

**Key Distribution**
- Algorithmic number theory
- Key distribution, Diffie-Hellman
- RSA

**Other Topics**
- Reduction proofs
- Pseudorandomness
- Block ciphers: DES, AES
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
- ...

...
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
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.
Questions ?
Python Programming Project: BibTeX Parser
Python Programming Project:

BibTeX Parser

- Block 2 (Nov/Dec), starting asap, 3 ECTS
- Goal: creating the “perfect” bibtex file (for articles in a certain research domain, such as quantum cryptography)
Python Programming Project: BibTeX Parser

- Block 2 (Nov/Dec), starting asap, 3 ECTS
- Goal: creating the “perfect” bibtex file (for articles in a certain research domain, such as quantum cryptography)
- https://github.com/sciunto-org/python-bibtexparser
Python Programming Project:

BibTeX Parser

- Block 2 (Nov/Dec), starting asap, 3 ECTS
- Goal: creating the “perfect” bibtex file (for articles in a certain research domain, such as quantum cryptography)
- https://github.com/sciunto-org/python-bibtexparser
- extensions to this parser:
  - create alphastyle citation keys
  - look up article information from crossref, dblp, arXiv
  - provide various bibtex file formats
  - create a website where articles can be looked up “on the fly”
  - …