Introduction

Rasmus Wismann

March 2017
Outline

● Classic vs. modern cryptography

● Kerckhoff’s principle

● Historic crypto schemes

● Principles of modern cryptography
Classic vs modern cryptography

- Concise Oxford Dictionary, definition of cryptography:
  "The art of writing or solving codes"

- Introduction to modern cryptography, definition of cryptography:
  ○ "The study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks."
Classic Cryptography

- Two parties communicate secretly by using codes/ciphers.
- Security relies on secret keys.
- $Enc_k (m) := c$
- $Dec_k (c) := m$
Kerckhoff’s Principle

“The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.”
Shift Cipher

- Key $k \in \{0,...,25\}$

- $\text{Enc}_k(m_1...m_l) = c_1...c_l$ where $c_i = [(m_i+k) \text{ mod } 26]$

- $\text{Dec}_k(c_1...c_l) = m_1...m_l$ where $m_i = [(c_i-k) \text{ mod } 26]$
Shift Cipher - Example

- $m = \text{“secretmessage”}$
- $k = 6$
- $c = \text{“yklxkskyygmy”}$
Sufficient key-space principle

“Any secure encryption scheme must have a key space that is sufficiently large to make an exhaustive-search attack infeasible.”
Mono-alphabetic substitution cipher

- Uses a mapping between each letter of cleartext and ciphertext. E.g.
  
<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
<th>g</th>
<th>....</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>E</td>
<td>U</td>
<td>A</td>
<td>D</td>
<td>N</td>
<td>B</td>
<td>....</td>
</tr>
</tbody>
</table>

- Key space: $26! \approx 2^{88}$

- Scheme vulnerable to statistical analysis of letter frequency
Principles of Modern Cryptography

Formal definitions

○ Offers a way to compare schemes and evaluate them
○ Security Guarantee
○ Threat Model
Threat Model

- **Ciphertext-only attack**
  - Only access to the ciphertext transmitted between the two communicating parties.

- **Known-plaintext attack**
  - Can obtain some ciphertext/plaintext pairs.

- **Chosen-plaintext attack**
  - Can obtain the corresponding ciphertext to a chosen plaintext.

- **Chosen-ciphertext attack**
  - Can obtain the corresponding plaintext to a chosen ciphertext.
Principles of Modern Cryptography

1. Formal definitions
   ○ Offers a way to compare schemes and evaluate them
   ○ Security Guarantee
   ○ Threat Model

2. Precise assumptions
   ○ Cryptographic schemes rely on assumptions.
   ○ Assumptions should be mathematically precise and concise.
   ○ Comparison

3. Proofs of security
   ○ Some assurance that the scheme is secure relative to the definitions and assumptions