Lecture 1: Introduction

Viet Tung Hoang

The slides are loosely based on those of Prof. Mihir Bellare, UC San Diego.
Agenda

1. Crypto Usage & Goals
2. Classical Crypto
3. One-time Pad & Perfect Secrecy
4. Modern Crypto
Crypto Use Is Ubiquitous

HTTPS

Secure messaging

Bank of America

WhatsApp

Facebook

ATM

Bitcoin

Tor
A Classical Crypto Goal: Privacy

Privacy: Adversary can’t learn anything from the content that it eavesdrops.
A Classical Crypto Goal: Privacy

Private-key setting: \( K_e = K_d \)

Public-key setting: \( K_e \neq K_d \)
But Privacy Alone Is **Not** Enough

Transfer $5 to account 12345

Transfer $1000 to account 99999

**Authenticity:** Adversary can’t forge valid ciphertexts
Four Fundamental Cryptographic Problems

- Privacy
  - Private-key Encryption
  - Public-key Encryption
- Authenticity
  - MAC
  - Digital Signature
Agenda

1. Crypto Usage & Goals

2. Classical Crypto

3. One-time Pad & Perfect Secrecy

4. Modern Crypto
Caesar Cipher

No key
Broken once scheme is known
Shift Cipher

Use a secret key $K \in \{0, \ldots, 25\}$

Same as Caesar cipher, but shift $K$ positions, instead of 3.

Small Keyspace

Broken by brute force
Substitution Cipher

Key: a permutation \( \pi : \Sigma \rightarrow \Sigma \)

Example: \( \Sigma = \{A, B, C, \ldots, Z\} \)

<table>
<thead>
<tr>
<th>( \pi(x) )</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>A</td>
<td>Z</td>
<td>U</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

26! \approx 2^{88.38} keys for the English alphabet
Sherlock Holmes’s Example

The Adventure of the Dancing Men
Break Substitution Cipher: Frequency Analysis

Only work for large ciphertexts
Improve Attack via Monte Carlo Markov Chain

View keys as nodes in a complex graph

Initial key

True key
Build a Mechanism to Assess Likelihood of Keys

Candidate key $K$

Ciphertext

$Score(K) = 0.3$

Decrypted message

Higher score $\rightarrow$ more likely to be the correct key
Find the Destination via Hill Climbing

- Initial key
  - score = 0.03

- Score progression:
  - score = 0.07
  - score = 0.1
  - score = 0.3
  - score = 0.5
  - score = 0.8

- True key

Diagram:

- Initial key
- Score progression:
- True key
Assess Key Likelihood via Bigram Analysis

“The cat is chasing the mouse”

Bigrams: th he e□ c ca at t□ ...

must consider white space
Assess Key Likelihood via Bigram Analysis

Use an English corpus

$T[“ca”]$: frequency of bigram “ca” in English
Assess Key Likelihood via Bigram Analysis

Candidate key $K$

Ciphertext $M$

Decrypted message $M$

$\text{Score}[K] = \prod T[x]$

bigram $x$ in $M$
Find A Neighbor By Transposition

<table>
<thead>
<tr>
<th>$\mathcal{X}$</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\pi(\mathcal{X})$</td>
<td>E</td>
<td>A</td>
<td>Z</td>
<td>U</td>
<td></td>
</tr>
</tbody>
</table>

Current node

A neighbor

Swap two random entries
Occasionally, one may have to go **down**.

*Initial key*

- score = 0.03

*True key*

- score = 0.07
- score = 0.1
- score = 0.3
- score = 0.5
- score = 0.8

Get Around Local Maximum in Hill Climbing
Get Around Local Maximum in Hill Climbing

Always go

score = 0.3

score = 0.5

Go with probability $= \frac{0.4}{0.5 + 0.4}$

score = 0.4
The Enigma

Broken by British in an effort led by Turing
Agenda

1. Crypto Usage & Goals
2. Classical Crypto
3. One-time Pad & Perfect Secrecy
4. Modern Crypto
Encryption Syntax

Key Gen

Encrypt

Decrypt
Define security?
Perfect Secrecy

**Intuition:** Ciphertext should reveal **no additional info** about plaintext

For every $m$ and $c$:

$$\Pr_{K \leftarrow \mathcal{K}}[\text{Msg} = m \mid \mathcal{E}_K(\text{Msg}) = c] = \Pr[\text{Msg} = m]$$
Achieving Perfect Secrecy: One-time Pad

Key Gen

$K \leftarrow \{0, 1\}^m$

Encrypt

$M \rightarrow K \rightarrow C$

Decrypt

$C \rightarrow K \rightarrow M$

Message space
Behind Every Notion, There Is An Assumption

For every $m$ and $c$:

$$
\Pr_{K \leftarrow \mathcal{K}}[\text{Msg} = m \mid \mathcal{E}_K(\text{Msg}) = c] = \Pr[\text{Msg} = m]
$$

It’s **assumed** that you pick a fresh key for each encryption
Reusing One-time Pad Breaks Security

One can obtain $M \oplus M'$ via $C \oplus C''$

Can recover both $M$ and $M'$ if the messages are English texts and long enough
Bad Usage of One-time Pad: USSR’s reusing of one-time pads led to the decryption of 2900 messages.
Bad Usage of One-time Pads:

PPTP protocol in Windows NT

\[ M \rightarrow K \rightarrow C \rightarrow M' \]

\[ C' \leftarrow K \leftarrow M' \]
Limitation of Perfect Secrecy

If $|\mathcal{M}| > |\mathcal{K}|$ then no scheme is perfectly secret

Impractical
Agenda

1. Crypto Usage & Goals
2. Classical Crypto
3. One-time Pad & Perfect Secrecy
4. Modern Crypto
Modern Crypto: A Lego Approach

Primitives: AES  SHA-2  Factoring  ...

Applications: Encryption  MAC  Digital Signature

Transformers
Modern Crypto: A Computational Science

- Assume computational hardness of a few primitives

  AES  SHA-2  Factoring ...

- Confidence by cryptanalysis
Modern Crypto: Provable Security

- Define security notions for applications
- Prove the transformer meets the notions