WELCOME!
Introduction

Cryptography is Magic

History of Cryptography

Math fundamentals
Course Objectives

• Learn how cryptographic primitives work

• Use them correctly, and reason about security
Administrative Details

- Course website: [https://courses.grainger.illinois.edu/cs498ac3/fa2020/](https://courses.grainger.illinois.edu/cs498ac3/fa2020/)

- Has syllabus, instructor and TA info, office hours

- IMPORTANT: Join Piazza! [piazza.com/illinois/fall2020/ececs498ac/home](http://piazza.com/illinois/fall2020/ececs498ac/home)

*I strongly encourage class participation. If you don't understand something in class, please interrupt me and ask questions. Please make abundant use of office hours.*
SSL/TLS
SSL/TLS

Two parts.

• **Handshake protocol**: Use *public key encryption* to establish shared secret key

• **Record layer**: Transmit data using shared secret key *secret-key encryption*
SSL/TLS

Two parts.

• **Handshake protocol**: Use *public key encryption* to establish shared secret key

• **Record layer**: Transmit data using shared secret key *secret-key encryption*

We will: -- see how these encryption schemes work.
   -- understand why we think these are unbreakable.
The Magic of Cryptography
Key Exchange

Key 194658284

UNTRUSTED CHANNEL

EAVESDROPPER

Key 194658284
Zero-Knowledge Proofs

Given a SAT formula:

\[(X_1 \lor X_2 \lor \cdots \lor X_n) \land (Y_1 \lor X_2 \lor \cdots \lor X_n) \land (X_1 \lor Y_2 \lor \cdots \lor X_n) \land (Y_1 \lor Y_2 \lor \cdots \lor X_n) \land \cdots \land (Y_1 \lor Y_2 \lor \cdots \lor Y_n).\]

The clause is satisfiable!

I agree, but I didn’t learn the solution!
Secure Computation
History
Symmetric Ciphers
Substitution Ciphers

Key

- a → g
- b → z
- c → o
- d → r
- e → b

a bad cab → g zq r ogz
What is the size of key space in the substitution cipher assuming 26 letters?

1. $26^2$
2. $26!$
3. $2^{26}$
4. 26
Substitution Ciphers are Easy to Break!

UKBYBIOUZBCUFEEBORUKBYBHOBBRFESPVKBWFOFERVNBCVBZPRUBOFERVNBCVBPCYYFVUFO
FEIKNWFRIKJNUPWRFIPOUNVNIUBRNCCUKBEFWFDFNCHXYBOHOPYXPUBNCOBOYNRVNIWN
CPOJIOFHOPZRVFZIXUJORJRUBZRBCHNCBONCHRJZSFWNVRJRUBZRPUCYFPUKBZPNVNPWPCYVF
ZIXUPUNFCPWRVNBCVBPRYPYNNUNFCPWWJUKBYBIOUZBCUPOUNVNIUBRNCHOPYXPUBNCOBOY
OYNRVNIWNCPOJIOFHOPZRRCRVNBCUNENVVFZIXUNCHPCYVFZIXUPUNFCPZWPUKBZPNVRR

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>N</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>U</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

→ E
→ T
→ A

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UN</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

→ IN
→ AT

digrams

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>UKB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RVN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FZI</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

→ THE

trigrams
Substitution Ciphers are Easy to Break!

UKBYBIPOUZBCUFEEBORUKBYBHOBBRFESPVKBWFOFERVNBCVBZPRUBOFERVNBCVBPCYYFVUFO
FEIKNWFRFIKJNUPWRFIPOUNVNIUBRNCUKBEFWWFDNCHXCYBOHOPYXUBNCUBOYNYRNVNIWN
CPOJIOFHOPZRFVZIXUBORJRUBZRBCWHNBBONCHRCJZSFWNVRJRUBZRRCYZPUKBZPUNVPWPBCYVF
ZIXUPUNFCPCWRNVCVBPRPYYNUNFCPWWJUKBYBIPOUZBCUPOUNVNIUBRNCOPYXUBNCUCUB
OYNRVNIWNCPOJIOFHOPZRNCRVNBCUNENVVZIXUNCHPCYVFZIXUPUNFCPWPZPUKBZPUNVR

<table>
<thead>
<tr>
<th>B</th>
<th>36</th>
<th>→ E</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>34</td>
<td>→ T</td>
</tr>
<tr>
<td>U</td>
<td>33</td>
<td>→ A</td>
</tr>
<tr>
<td>P</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>26</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NC</th>
<th>11</th>
<th>→ IN</th>
</tr>
</thead>
<tbody>
<tr>
<td>PU</td>
<td>10</td>
<td>→ AT</td>
</tr>
<tr>
<td>UB</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>UN</td>
<td>9</td>
<td></td>
</tr>
</tbody>
</table>

digrams

<table>
<thead>
<tr>
<th>UKB</th>
<th>6</th>
<th>→ THE</th>
</tr>
</thead>
<tbody>
<tr>
<td>RVN</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>FZI</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

trigrams
Rotor Machines

$k_2$: $k_1$, shifted
Rotor Machines: Advanced (The Enigma)
Encryption Standards

• Data Encryption Standard (DES): $2^{56}$ keys

• Advanced Encryption Standard (AES): used today

• And many others...
Mathematical Background
Discrete Probability

• $S$ : finite set (e.g., $S = \{0,1\}^n$)

• A probability distribution $Pr$ over $S$ is a function $Pr : S \rightarrow [0,1]$ such that $\sum_{x \in S} Pr(x) = 1$

• Examples
  • Uniform distribution
  • Point distribution
  • Distribution vector

$S = \{0,1\}^n$
$Pr[0] = Pr[1] = \frac{1}{2}$

$S = \{0,1\}^n$
$\xi_{000...0,00...1, .......11111}$

$\forall x \in S$ $Pr[\chi] = \frac{2^{-1}}{2^n}$

$S = \{0,1\}^n$
$Pr[x] = 1$ for $x = 1010 ... 1$ , $Pr[x] = 0$ for all other $x \in S$. 
Events

- For a set $A \subseteq S$, $\Pr [A] = \sum_{x \in A} \Pr (x)$
- The set $A$ is called an event

$S = \{0, 1\}^n$

$A = 0^{n/2} \overset{n/2}{\ldots} \overset{n/2}{0}$

$\frac{1}{2^{n/2}}$ (uniform distribution over $S$)
Events

• For a set $A \subseteq S$, $\Pr[A] = \Sigma_{x \in A} \Pr(x)$
• The set $A$ is called an event

• For events $A_1$ and $A_2$, $\Pr[A_1 \cup A_2] \leq \Pr[A_1] + \Pr[A_2]$
Random Variables

• A random variable $X$ is a function $X : \mathcal{U} \rightarrow \mathcal{V}$

• Let $\mathcal{U}$ be some set, e.g. $\mathcal{U} = \{0,1\}^n$

• We write $r \leftarrow \mathcal{U}$ to denote a uniform random variable over $\mathcal{U}$

  for all $a \in \mathcal{U}$: $\Pr [ r = a ] = 1/|\mathcal{U}| = \frac{1}{2^n}$
Randomized Algorithms

• We will make extensive use of randomized algorithms

• Deterministic algorithm: \( y \leftarrow A(m) \)

• Randomized algorithm: \( y \leftarrow A(m; r) \)

• Eg, to encrypt message \( m \), we will sample \( r \leftarrow \mathcal{S} \) and output \( Enc(m; r) \)
Independent Events

• Events $A$ and $B$ are independent if $\Pr[A \text{ and } B] = \Pr[A] \cdot \Pr[B]$

• Random variables $X, Y$ taking values in $\mathbb{V}$ are independent if
  $\forall (a, b) \in \mathbb{V}: \Pr[X = a \text{ and } Y = b] = \Pr[X = a] \cdot \Pr[Y = b]$
Independent Events

• XOR: bitwise addition mod 2. Example –

\[
\begin{align*}
0 \oplus 0 &= 0 \\
0 \oplus 1 &= 1 \\
1 \oplus 0 &= 1 \\
1 \oplus 1 &= 0 \\
\end{align*}
\]

• If Y some random (not necessarily uniform) variable over \(\{0,1\}^n\), and X an independent uniform variable on \(\{0,1\}^n\), then \(Z := Y \oplus X\) is a uniform variable on \(\{0,1\}^n\)
The One-Time Pad
Symmetric Ciphers

Enc

Dec
Symmetric Ciphers: One Time Pad

• A cipher defined over \((\mathcal{K}, \mathcal{M}, \mathcal{C})\)
  is a pair of efficient algorithms \((E, D)\) where

\[
E: \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}
\]
\[
D: \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}
\]

such that for all \(m \in \mathcal{M}, k \in \mathcal{K}, \ D ( k, E (k, m) ) = m \)

(Correctness)

\[
E (k, m) \rightarrow c
\]
then \(D(k, c) \rightarrow m\)
The One-Time Pad

- Provably Secure Cipher
  \[ \mathcal{K} = \{0,1\}^n, \quad \mathcal{M} = \{0,1\}^n, \quad \mathcal{C} = \{0,1\}^n \]

- Key is sampled uniformly from the set \( \mathcal{K} = \{0,1\}^n \)
  i.e. the key is a random bit string as long as the message

- \( E(k, m) = k \oplus m \)

- \( D(k, c) = k \oplus c \)

- Check correctness

We want:
\[
\begin{aligned}
D(k, E(k, m)) &= m \\
\text{c = (k \oplus m)} \\
k \oplus c &= k \oplus k \oplus m = m
\end{aligned}
\]
The One-Time Pad

• Example

• Check correctness

• What about security?
The One-Time Pad

• Let’s define security for a symmetric cipher. (perfect secrecy)

**Defn 1:** \( \forall m_0, m_1 \in \mathcal{M} \) (of equal size, i.e. \( |m_0| = |m_1| \)) and \( \forall c \in C \)

\[
\Pr_{k \leftarrow K} [ E(k, m_0) = c ] = \Pr_{k \leftarrow K} [ E(k, m_1) = c ]
\]

An attacker, given \( c \), cannot guess \( m \).
The One-Time Pad

• Theorem: The one-time pad satisfies Defn 1 (perfect secrecy).

\[ c_1 = k_1 \oplus m \]
\[ c_2 = k_2 \oplus c_1 \oplus (k_2 \oplus z) \oplus m \]
\[ K = \{0, 1\}^n, \quad M = \{0, 1\}^n \]
\[ C = \{0, 1\}^n. \]

Fix arbitrary \( m_0 \) & arbitrary \( c \).

\[ \Pr [E(k, m_0) = c] = \Pr [E(k, m_1) = c] \]

Similarly, \[ \Pr [E(k, m_1) = c] = \frac{1}{2^n} \]

\[ c = m_0 \oplus k \]

\[ k = m_0 \oplus c \]
The One-Time Pad: Disadvantage

• Observe: $|K| = |M|$

• That means to send a long file, you need to share a long key.
  • And for every file, you need a new key. Why?

• Can you have $|K| < |M|$?

• Shannon: No 😞. For perfect secrecy, you need $|K| \geq |M|$. Why?

Prove: if $|K| < |M|$, then $\exists \ m_0, m_1 \in M, \exists \ c \in C$
  s.t. $\Pr_{k \leftarrow K}[E(k, m_0) = c] \neq \Pr_{k \leftarrow K}[E(k, m_1) = c]$
Conclusion

- Looking ahead: *perfect* secrecy unnecessary, can relax it.

- Assume *hard problems* that cannot be solved by adversaries (i.e. we will assume P! = NP, and in fact something stronger).

- Under these assumptions, we will achieve *provable* security.

- *Conditional* secrecy:
  hardness of problem ------ => secrecy of the scheme.