Cryptography
CS 555

Topic 1: Course Overview & What is Cryptography

Administrative Note

- Professor Blocki is traveling and will be back on Wednesday.
  - E-mail: jblocki@purdue.edu
- Thanks to Professor Spafford for covering the first lecture!

https://www.cs.purdue.edu/homes/jblocki/courses/555_Spring17/index.html

(also on syllabus)

What is Cryptography?

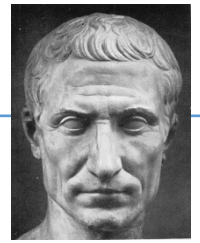
“the art of writing or solving codes” – Concise Oxford English Dictionary

What is Cryptography?

"the art of writing or solving codes" – Concise Oxford English Dictionary

"The study of mathematical techniques for securing digital information, systems and distributed computation against adversarial attacks."

-- Intro to Modern Cryptography



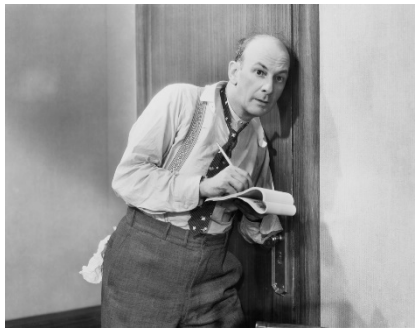
Art

Late 20th century

Science

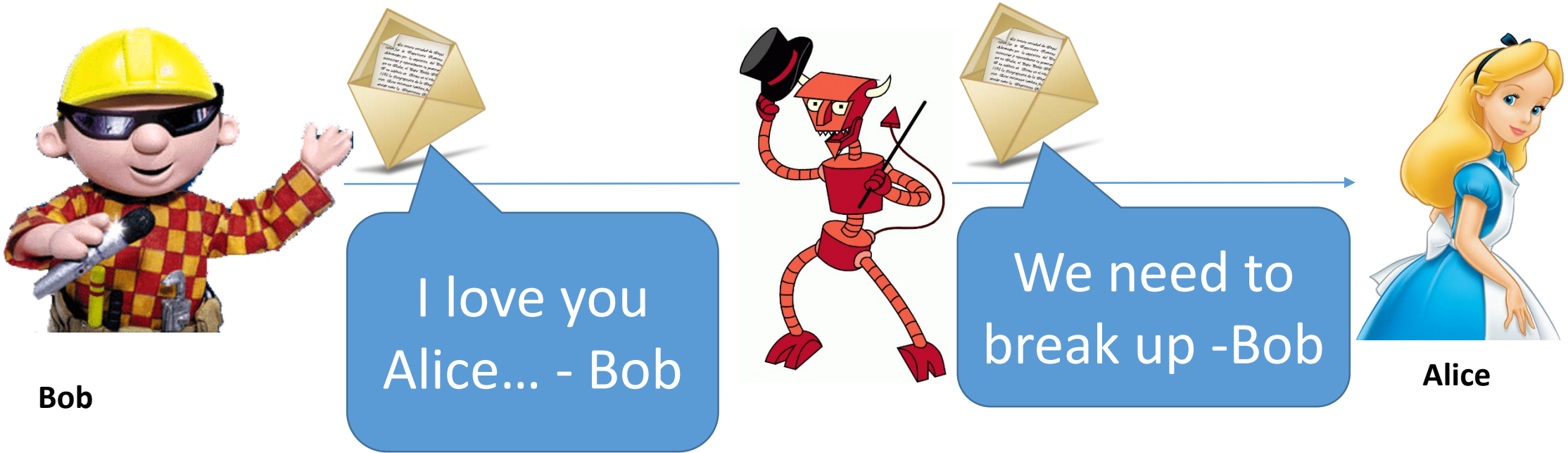
What Does It Mean to “Secure Information”

- Confidentiality (Security/Privacy)
  - Only intended recipient can see the communication



What Does It Mean to “Secure Information”

- Confidentiality (Security/Privacy)
  - Only intended recipient can see the communication
- Integrity (Authenticity)
  - The message was actually sent by the alleged sender



Two Attacker Models

- Passive Attacker
  - Attacker can eavesdrop
  - Protection Requires?
    - Confidentiality

- Active Attacker
  - Has full control over communication channel
  - Protection Requires?
    - Confidentiality & Integrity

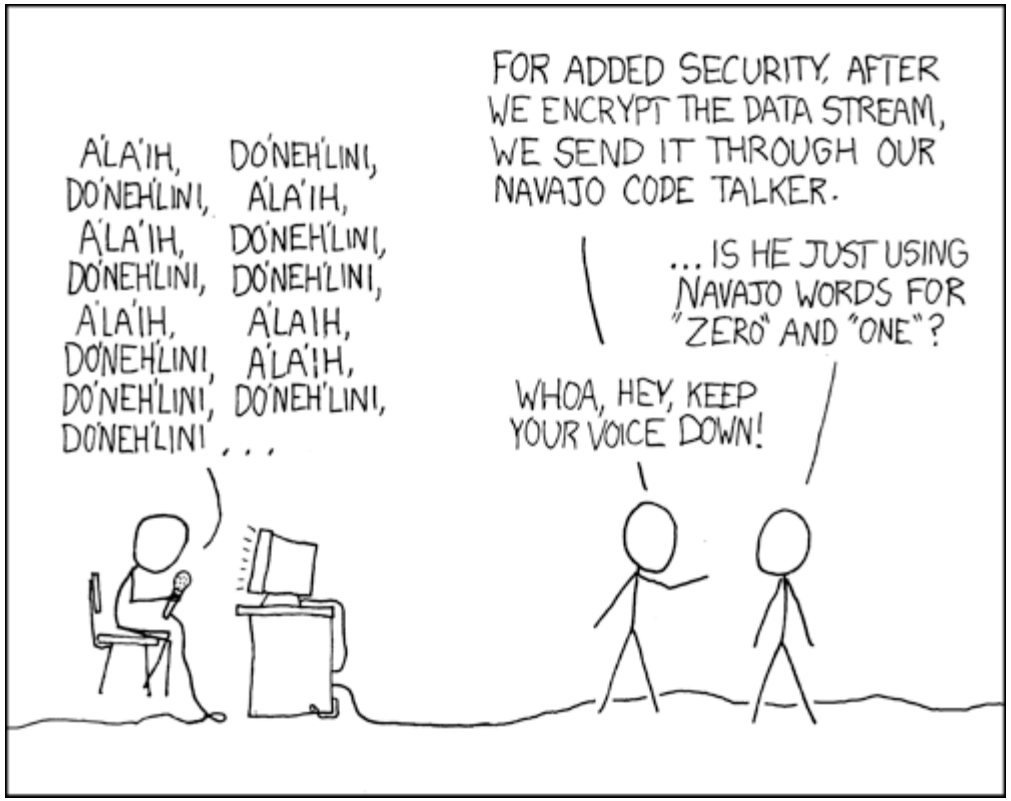
Steganography vs Cryptography

- Steganography
  - Goal: Hide existence of a message
    - Invisible Ink, Tattoo Underneath Hair, …

  - Assumption: Method is secret

Steganography vs Cryptography

- Steganography
  - **Goal:** Hide existence of a message
    - Invisible Ink, Tattoo Underneath Hair, …
  - **Assumption:** Method is secret
- Cryptography
  - **Goal:** Hide the meaning of a message
  - Depends only on secrecy of a (short) key
  - **Kerckhoff's Principle:** Cipher method should not be required to be secret.



Symmetric Key Encryption

- What cryptography has historically been all about (Pre 1970)
- Two parties (sender and receiver) share secret key

- Sender uses key to encrypt (“scramble”) the message before transmission
- Receiver uses the key to decrypt (“unscramble”) and recover the original message

Encryption: Basic Terminology

- Plaintext
  - The original message m
- Plaintext Space (Message Space)
  - The set $\mathcal{M}$ of all possible plaintext messages
  - Example 1: $\mathcal{M} = \{\ 'attack',\ 'retreat',\ 'hold\ current\ position'\}$
  - Example 2: $\mathcal{M} = \{0,1\}^n$ - all $\mathrm{n} - \mathrm{bit\ messages}$
- Ciphertext $\mathrm{c} \in \mathcal{C}$
  - An encrypted ("scrambled") message $\mathrm{c} \in \mathcal{C}$ (ciphertext space)
- Key/Keyspace $\mathrm{k} \in \mathcal{K}$

Private Key Encryption Syntax

- Message Space: $\mathcal{M}$
- Key Space: $\mathcal{K}$
- Three Algorithms
  - $\mathrm{Gen}(R)$ (Key-generation algorithm)
    - Input: Random Bits R
    - Output: Secret key $\mathrm{k} \in \mathcal{K}$
  - $\mathrm{Enc}_{\mathrm{k}}(m)$ (Encryption algorithm)
    - Input: Secret key $\mathrm{k} \in \mathcal{K}$ and message $\mathrm{m} \in \mathcal{M}$
    - Output: ciphertext *c*
  - $\mathrm{Dec}_{\mathrm{k}}(c)$ (Decryption algorithm)
    - Input: Secret key $\mathrm{k} \in \mathcal{K}$ and a ciphertex c
    - Output: a plaintext message $\mathrm{m} \in \mathcal{M}$
- Invariant: $\mathrm{Dec}_{\mathrm{k}}(\mathrm{Enc}_{\mathrm{k}}(\mathrm{m}))=\mathrm{m}$

Typically picks $\mathrm{k} \in \mathcal{K}$ uniformly at random

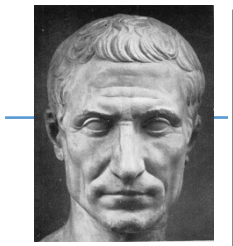
Trusted Parties (e.g., Alice and Bob) must run Gen in advance to obtain secret k.

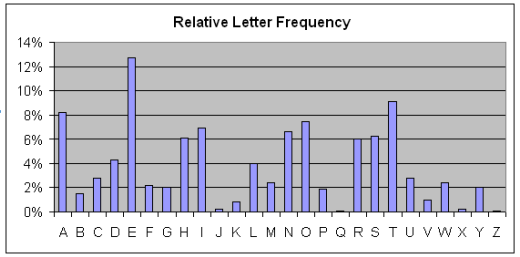
Assumption: Adversary does not get to see output of Gen

Cryptography History

- 2500+ years
- Ongoing battle
  - Codemakers and codebreakers

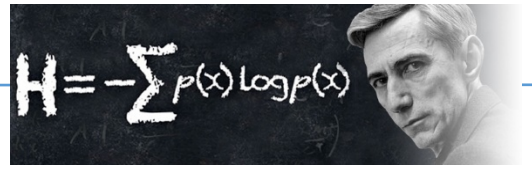
Caesar Shift Cipher (50 BC)





Frequency Analysis

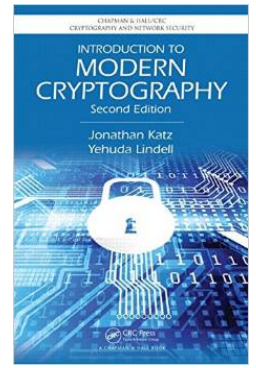
Shannon Entropy/Perfect Secrecy (~1950)



Cipher Machines (1900s)

1970s

Formalization of Modern Crypto (1976+)

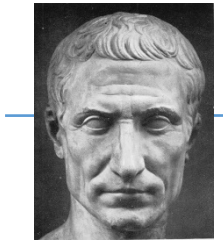


Public Key Crypto/RSA

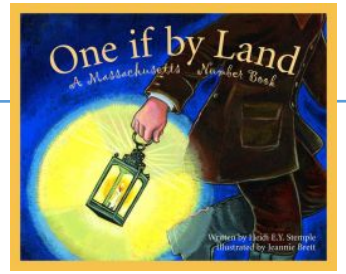
Who Uses Cryptography

- Traditionally: Militias
- Modern Times: Everyone!

Caesar Shift Cipher (50 BC)



Revolutionary War



Modern Crypto

amazon

Course Goals

- Understand the mathematics underlying cryptographic algorithms and protocols
- Understand the power (and limitations) of common cryptographic tools
- Understand the formal approach to security in modern cryptography

Course Background

- Some probability
- Algorithms and complexity
- General Mathematical Maturity
  - Understand what is (is not) a proper definition
  - Know how to write a proof

Coming Up…

- Classic Ciphers + Frequency Analysis

- Before Next Class
  - Read: Katz and Lindell 1.3
  - Plus Katz and Lindell 1.1-1.2 if you haven’t already