


# Cryptography: A Closer Look at Protecting Digital Secrets



JAN 16, 2015

# Outline



- Introduction
  - Philip Chan
- Interactive Demo
  - Ryan Stansifer
- Key ideas of crypto algorithms, attacks, and future
  - Marius Silaghi

# Introduction



PHILIP CHAN

# WWII



- You are a general
  - How to communicate with your troops quickly?

# WWII



- You are a general
  - How do communicate with your troops quickly?
- Pigeons

# WWII



- You are a general
  - How do communicate with your troops quickly?
- Pigeons
- Radio
- What is the common problem?

# WWII



- You are a general
  - How do communicate with your troops quickly?
- Pigeons
- Radio
- What is the common problem?
  - Could be intercepted
  - Which is easier to be intercepted?

# Communication Can be Intercepted



- Make messages not easily readable by your enemy
- But can be read by your troops



# Fast forward to now



- Communication via internet
- Can communication be intercepted?
  - Wired
  - Wireless

# Information Privacy



- Credit card numbers
- Passwords
- Data of Birth
- Email/text to your significant other
- Medical records
- What else?

# Key Idea 1: Encryption and Decryption



- **Before sending a message**
  - Make the message difficult to read
  - Encryption
- **After receiving a message**
  - Translate the encrypted message
  - Decryption

# Very Simple Encryption/Decryption



- Encryption:
  - Replace a letter by the **next** letter in the alphabet
    - ✦ A -> B
    - ✦ B -> C
    - ✦ ...

# Very Simple Encryption/Decryption



- Encryption:

- Replace a letter by the **next** letter in the alphabet

- ✦ A -> B

- ✦ B -> C

- ✦ ...

- Decryption:

- Replace a letter by the **previous** letter in the alphabet

- ✦ B -> A

- ✦ C -> B

- ✦ ...

# Example



<b>original</b>	<b>R</b>	<b>E</b>	<b>D</b>
encrypted	<b>S</b>	<b>F</b>	<b>E</b>

# Example



encrypted	<b>S</b>	<b>F</b>	<b>E</b>

# Example



encrypted	<b>S</b>	<b>F</b>	<b>E</b>
decrypted	<b>R</b>	<b>E</b>	<b>D</b>



# Let's decode these



- BOU
- TLZ
- CJSE

# Let's decode these



- **BOU**
  - ANT
  
- **TLZ**
  - SKY
  
- **CJSE**
  - BIRD

# Back to WWII



- Which machine did the Germans use for encryption?

# Enigma Machine



- <https://www.awesomestories.com/asset/view/Enigma-Machine-German-Codes-in-WWII>

# Breaking Enigma



- **British**
  - Bletchley Park
  - Codebreakers including Alan Turing
  - Broke the code before the Germans realizing it
  - Helped end the war earlier
  
- **Alan Turing?**

# Breaking Enigma



- **British**
  - Bletchley Park
  - Codebreakers including Alan Turing
  - Broke the code before the Germans realizing it
  - Helped end the war earlier
  
- **Alan Turing**
  - Father of Computer Science
  - Movie: Imitation Game

# Fast Forward to Now



- En/decryption is performed by software on electronic computers
  - Not electromechanical machines
- Software implements the en/decryption algorithms (recipes)
- Encrypted messages
  - designed to be very difficult to break
  - Can take “forever” with modern computers

# Key Idea 2: Strong Encryption



- Theoretically/mathematically proven
- Take “forever” for modern computers to break
  - e.g. millions of years
- Harder than winning Powerball 😊
  - One in 292 million



# Back to WWII



- Additional issues to think about
- You got a encrypted message from your general and you decrypted it
  - How do you know it is from your general (not an adversary)?
    - ✦ authentication
  - How do you know it has not been altered (by an adversary)?
    - ✦ integrity

# Fast forward to now



- Similar issues
- You got an email/document/...
  - How do you know it is from the sender (not an adversary)?
    - ✦ authentication
  - How do you know it hasn't been altered (by an adversary)?
    - ✦ integrity
- Encryption can be applied to
  - Authentication
  - Integrity

# Key Idea 3: Beyond Protecting Secrets



- Applications such as
  - Authentication of sender
  - Integrity of data

# Summary of Key Ideas



1. Encryption and decryption
2. Strong encryption
3. Beyond protecting secrets

# Part 2



# More Outreach Efforts



- [cs.fit.edu/~pkc/cs4hs](http://cs.fit.edu/~pkc/cs4hs)
- District-wide tic-tac-toe tournament
  - ✦ Organized by Edgewood in April/May
  - ✦ New teacher – not sure?
  - ✦ Your player against others
- Summer Camps
  - ✦ July