Secure Communications

How can a computer send a secret

CS202
Fall 2010
Lecture 39

Secure Telephone Game

- Sender must tell receiver the name of a random playing card
- Message must be "transmitted" from sender to receiver by eavesdroppers
- Outcomes
  - Only sender and receiver know the card
  - Eavesdroppers know the card
  - Neither receiver nor eavesdroppers know card

The Internet

- Internet security
  - Need a secure way to buy things online
  - Need to manage bank account securely
- Messages are received by lots of intermediaries, any could be eavesdroppers
  - Home router => Roommate
  - Building switch => Building manager
  - Local network => ISP employee
  - Backbone => Government

Information Security

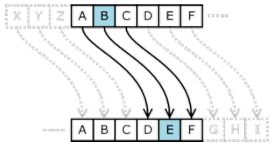
- Confidentiality
  - Eavesdroppers cannot understand messages
- Integrity
  - Eavesdroppers cannot modify message undetectably
- Availability
  - Messages should reach their destination
- Authenticity
  - Sender and receiver are who they say they are

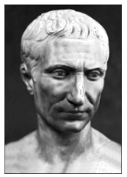
Cryptography

- Encode a message so eavesdroppers cannot understand it
- Idea over 2000 years old
- Shared secret cryptography
  - Sender and receiver have a secret or key that allows them to share encoded messages

Caesar Cipher

Letters in message shifted by a fixed amount





Ex: Clear text -- Attack at noon, agree on shift of 3

Cipher text -- Dwwdfn dw qrrq

How would you crack the code?

Enumerate all 26 possibilities until see reasonable

Shift of 1? Cvvcej cv pqqp

2? Buubdl bu oppo

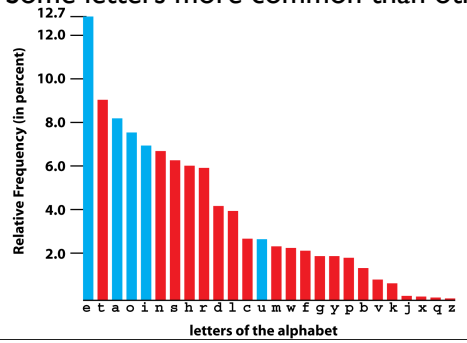
3? Attack at noon – Got it!

Substitution Cipher

- Over 1000 years old
- Replace each letter with another letter or symbol

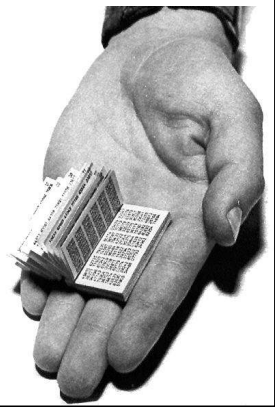
Cracking Substitution Cipher

- Frequency Analysis
- Some letters more common than others



One-time Pad

- Each letter is shifted by a different amount
- Amount to shift each letter is stored on a pad that can only be used once
- Impervious to frequency analysis



Modern Era Small Key Encryption

- Rely on a small key, few thousand bits
- Scramble and shift letters based on series of keys derived from initial key
- Enigma machine
  - Used by Nazi Germany (1940's)
  - Broken by British (Turing), Polish

What about messages between perfect strangers?

What about messages between perfect strangers?

- Amazon cannot send a one-time pad to every customer
- eBay will not call you to agree on a shared secret

Public Key Encryption

- 2 keys for every user
  - public key known to everyone
  - private key know only to the user
- Encrypt/Decrypt
  - Private key can decrypt messages encrypted with public key
  - Public key cannot decrypt messages encoded by the public key
- This is how E-Commerce works

Public Key Authentication

- Items signed by a public key obviously came from owner of private key
- Now Amazon can sign messages

Common Cryptography Themes

- Creating problems often easier solving
  - shifting letters easy, guessing how much they were shifted is hard
- Algorithm can be known by everyone, but cracking is still difficult
  - e.g. one-time pad
- Seeing info does not mean understanding it
  - Encrypted messages easy to detect, hard to crack

What if we want to hide the message entirely?

What if we want to hide the message entirely?

- Steganography
- Hide message in photos
  - store message in least important bits of photo
  - changes picture slightly

Questions?

Alan Turing

- British Genius
  - Founder of modern computer science
  - Helped crack the Enigma machine
- Outed as a gay man in 1952
  - convicted of gross indecency
  - security clearance revoked
  - given choice of hard labor or chemical castration
  - horrible side-effects lead to his suicide in 1954
- British government apologized in 2009