Cryptography

Jordan Zink

Carnegie Mellon University

jzink@andrew.cmu.edu

15-112: Spring 2015

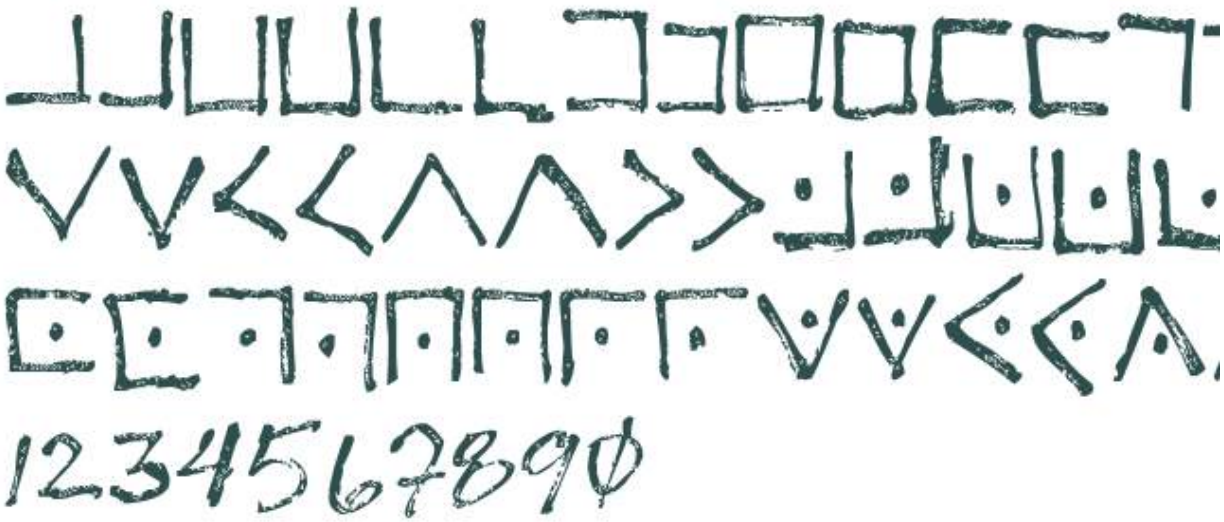
Outline

- Basics of Cryptography
- Classic Cryptography
- The Engima Machine
- Modern Cryptography
- The Future and Limits of Cryptography
- What it means for you
- Plus some code along the way!

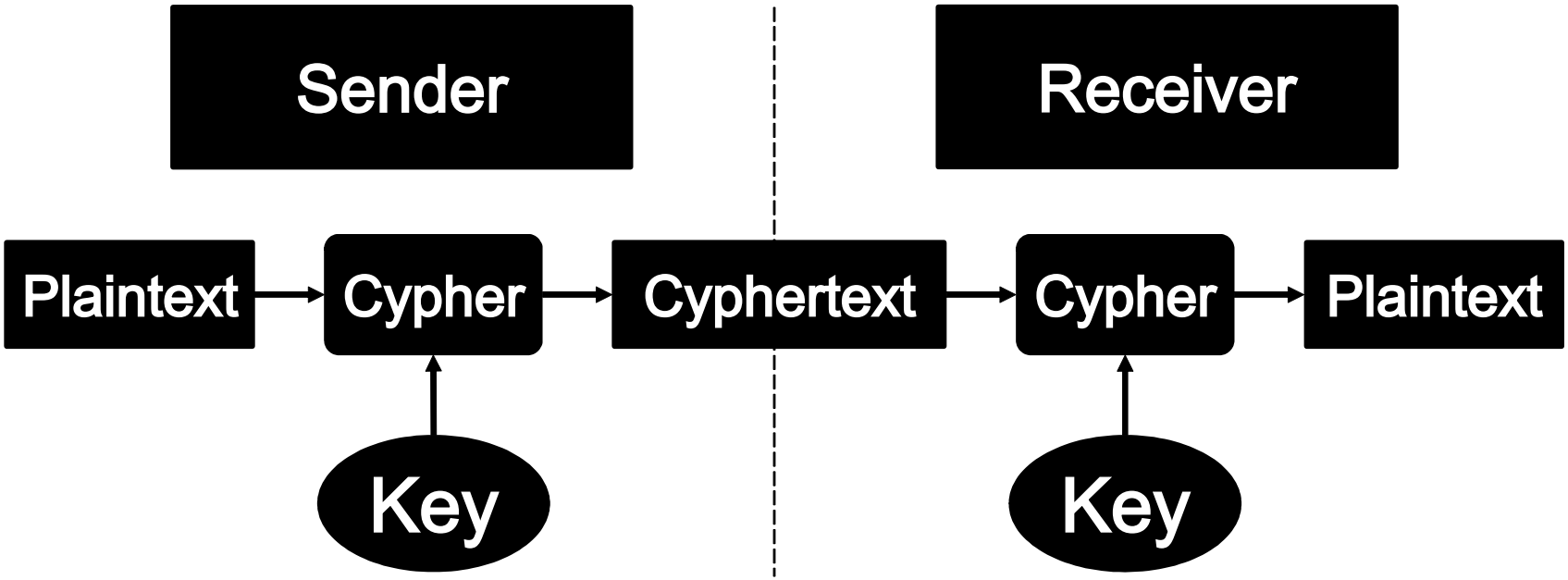
Basics of Cryptography

What Cryptography Is (and Isn't)

- Cryptography is the science of secure communication
- Cryptography is **not** Steganography
  - Steganography is older, and in most cases easier to break
  - Cryptography is the natural progression



Terminology



Adversary tries to deduce plaintext from ciphertext

Classic Cryptography

Classic Cryptography - Transposition Cipher

- Very simple
- All letters stay the same; just rearrange them
- For instance, “Carpe Diem” could become “Eprac Meid”

Classic Cryptography - Transposition Cipher

- Very simple
- All letters stay the same; just rearrange them
- For instance, “Carpe Diem” could become “Eprac Meid”

```
def lameCipher(s):
    return " ".join([w[::-1] for w in s.split(" ")])
```

Classic Cryptography - Transposition Cipher

- A bit better with a Scytale
- Wrap parchment ribbon around a properly sized staff to form plaintext
- Used by the Greeks a lot, especially Spartans
- Still easy to break

Classic Cryptography - Transposition Cipher

- A bit better with a Scytale
- Wrap parchment ribbon around a properly sized staff to form plaintext
- Used by the Greeks a lot, especially Spartans
- Still easy to break

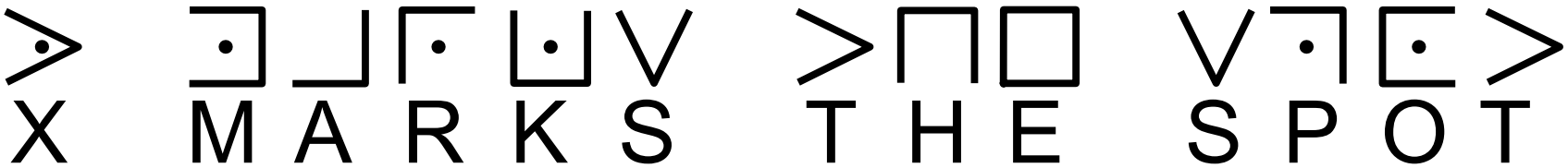
```
def lessLameCipler(s, scytaleSize):
    cyphertext = ""
    for i in xrange(scytaleSized):
        cyphertext += s[i::scytaleSize]
    return cyphertext
```

Classic Cryptography - Caesar Shift

- Simple but better than transposition
- Shift every letter in the alphabet by one
- For example, “Carpe Diem” would become “Dbsqf Ejfn”
- Used in antiquity (hence name)
- Weak if single shift (just undo)
- Even if shift is unknown, only 25 possibilities

Classic Cryptography - Substitution Cipher

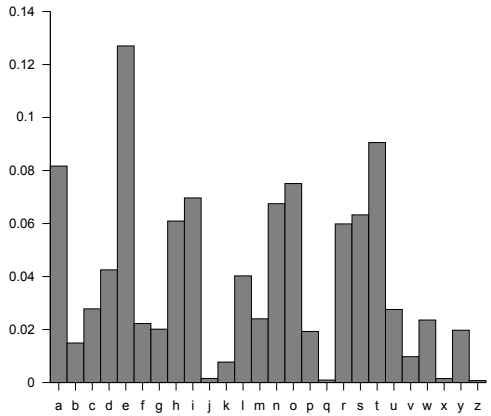
- Generalization of Caesar Shift
- Idea is that every letter maps to another letter based on some key
- Doesn't even need to map to original set of letters



How Do We Break a Substitution Cipher?

How Do We Break a Substitution Cipher?

- Try everything? Brute Force Attack
  - 403291461126605635584000000 possibilities if 26 letters
- Guess words, fill in the key as we go, try again if we do something wrong (backtracking)
- Analyze letter frequency. The most common letter is probably E...
  - Known as frequency analysis, and was first intelligent cryptanalysis



A Better Substitution Cipher

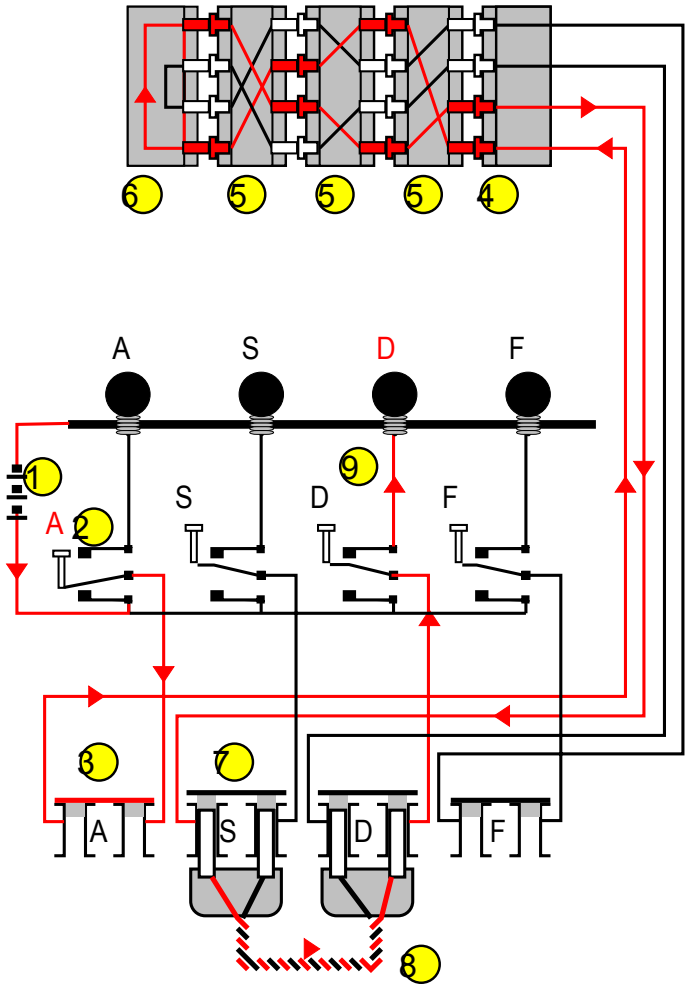
- Substitution Cipher due to single letter-to-letter mapping
- Can be made better by changing mapping during encryption
- This is a poly-alphabetic substitution cipher
- Best example is the Vigenere Cipher

Enigma Machine

The Enigma Machine

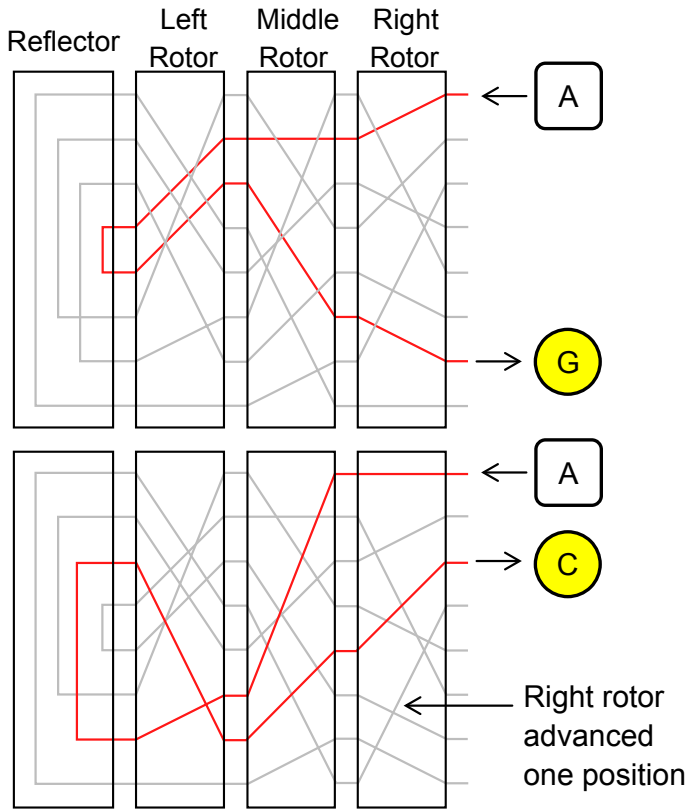
- Invented in Germany in 1918
- Originally marketed to many customers but eventually became standard German military encryption device
- Looked similar to typewriter with a light board of the alphabet

The Enigma Machine - How It Works



The Enigma Machine - Advantages

- Was a powerful poly-alphabetic cipher due to stepping action
- Reflector made encryption and decryption identical processes
- Keys could be relatively small and easy to transfer



Breaking Enigma

Modern Cryptography

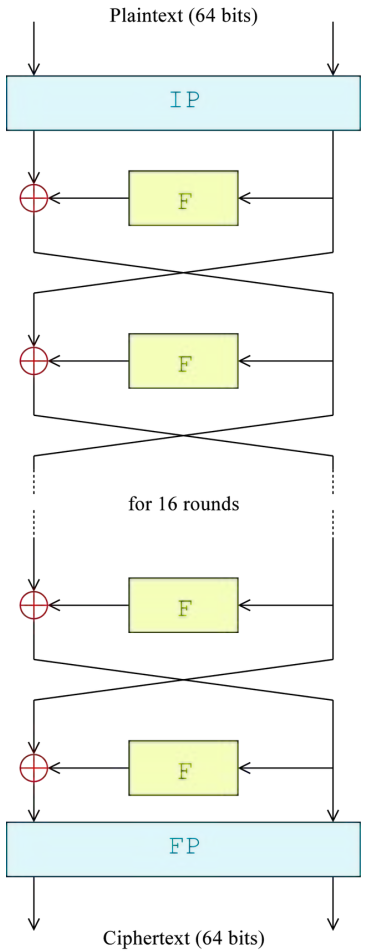
Modern Cryptography

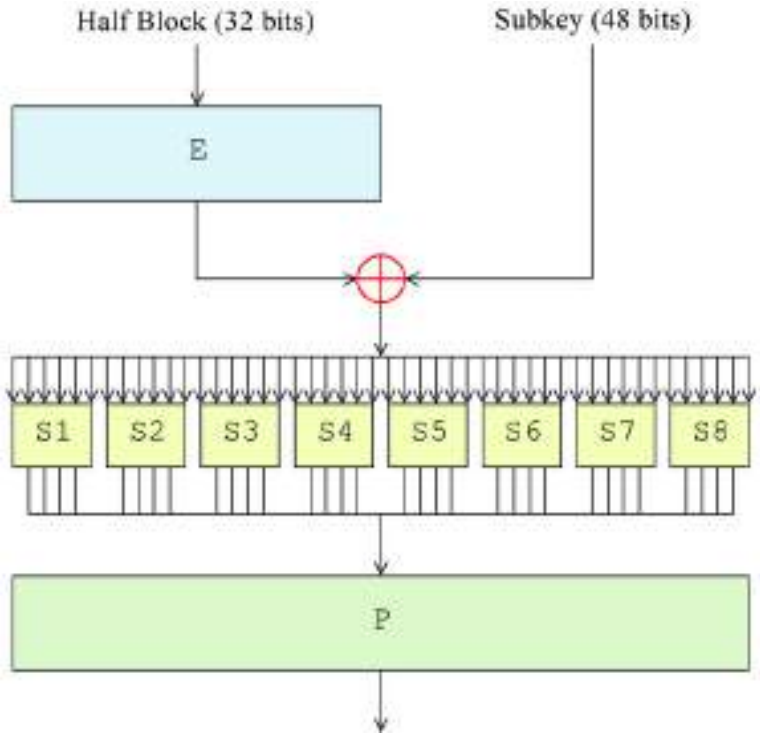
- With the power of computers, classic cryptography (even poly-alphabetic substitution ciphers like Enigma) can be broken with a brute force attack
- Lots of research has gone into how to make ciphers which can still be secure
- Two main types of modern ciphers
  - Symmetric Key
  - Asymmetric Key (also known as Public Key)

Symmetric Key Cryptography

- Both encryption and decryption rely on the same key
- Pretty much all classic cryptography is symmetric key
- If key remains hidden, could be very secure. Key management is a hassle though
- Data Encryption Standard (DES) was first major cryptographic standard in 1979

How Does DES Work?

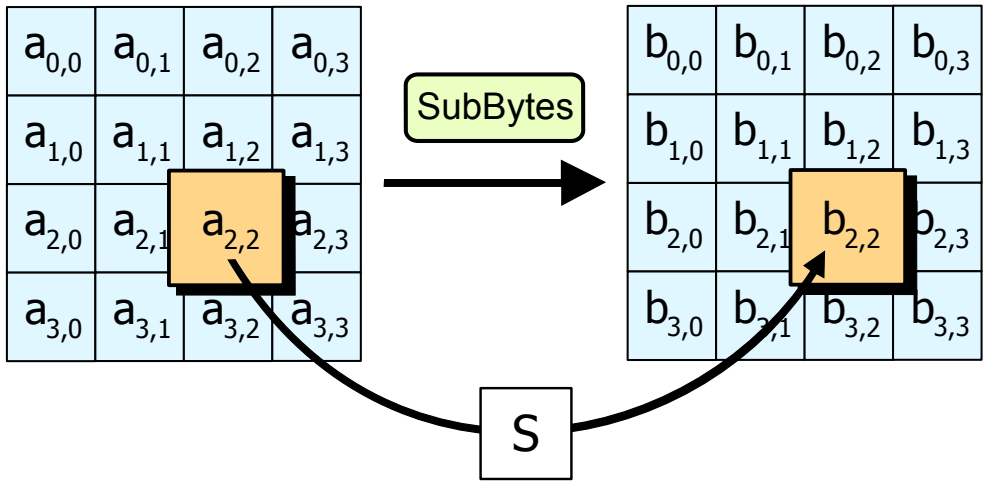




Uh...kinda complicated and boring

Symmetric Key Cryptography

- DES has been considered broken since 1999
  - Key size of 56 bits is too small
- Advanced Encryption Standard (AES) replaced DES in the government space in 2002
- As a general rule, power of a symmetric cipher is in the key size
  - Most likely, computers will catch up to AES key size



Asymmetric (Public) Key Cryptography

- Radically different way to think of cryptography
- Have two different keys: a public one and a private one
- Anyone can use the public key to encrypt, but only private one can decrypt
- I imagine it like a mail drop as opposed to lock box model of symmetric key
- First practical system was RSA in 1977
  - Name comes from Rivest, Shamir, and Adleman

RSA - How it Works

- Pick two primes p and q. Compute $n = p * q$
- Compute $\varphi(n)$, which equals $(p-1)(q-1)$
- Pick a random e such that $1 \leq e \leq \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$
- Solve for d where $d * e \equiv 1 \mod \varphi(n)$
  - Use extended Euclid's algorithm for this

For encryption, take the plaintext as a number, raise it to the e, and mod it by n.
For decryption, take the ciphertext as a number, raise it to the d, and mod it by n.

RSA

- Easy to hand out keys
- Scheme also allows for verifying ones identity since e and d are interchangeable
- Whole idea is built on idea that numbers are hard to factor when only a few prime factors
- All information to crack a ciphertext is publicly available!

Aside: Authentication and Passwords

Authentication

- Authentication is proving who you are
  - Confirming a claimed identity
- Very important in the digital age of anonymity
- Just showed one way with RSA
- Comes in three different forms
  - Multiple forms might be used in high security locations

Authentication - Forms

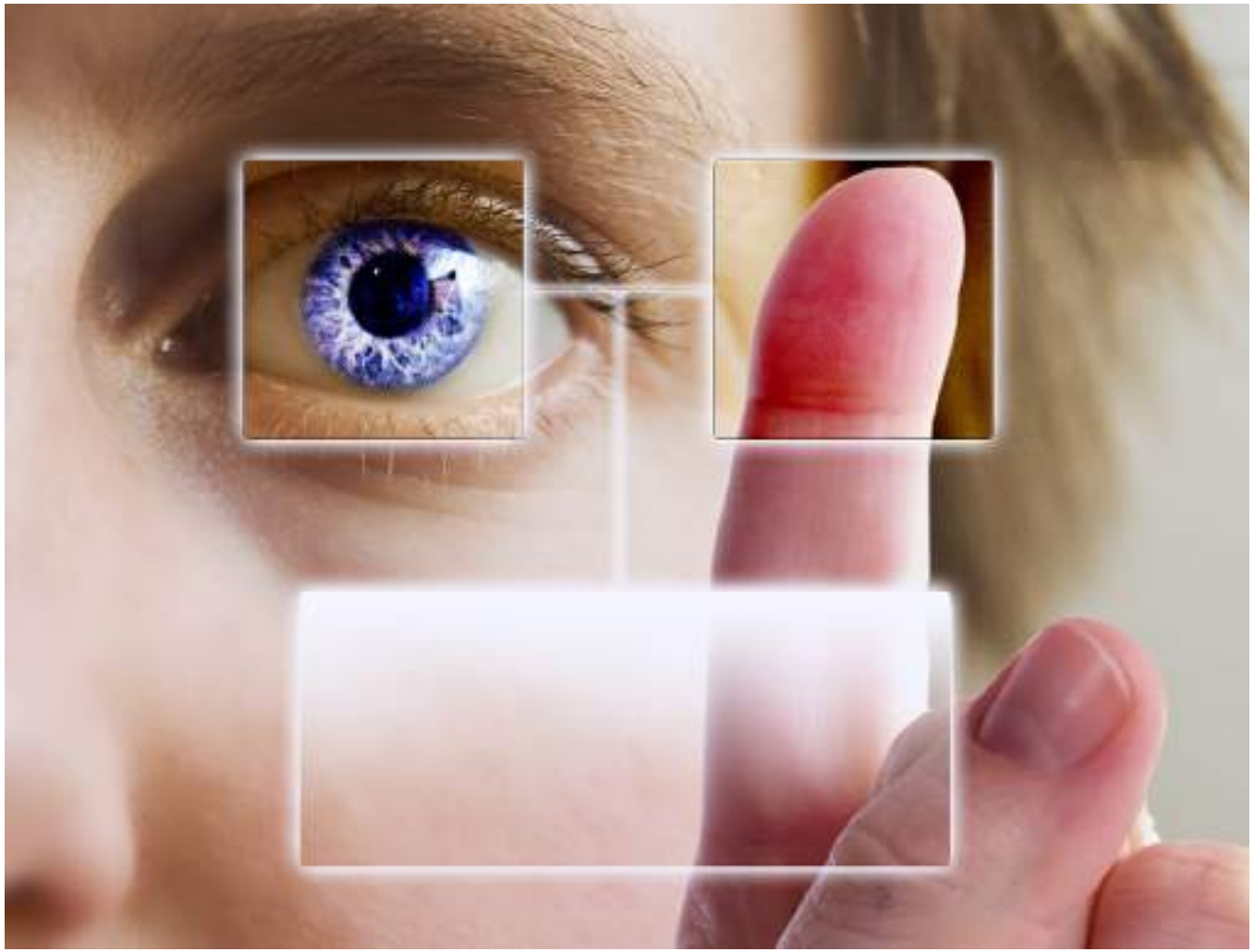
Knowledge Factor - What you **know** (e.g. password)

Authentication - Forms

Ownership Factor - What you **have** (e.g. a hard key)

Authentication - Forms

Inherence Factor - What you **are** (e.g. finger print)



Cryptographic Hashing

- Don't want to store passwords in databases as-is
  - But still need to know if user has right password
- Solution is cryptographic hash functions
- Like normal hash functions, but with special properties
  - Should be very hard to undo
  - Should have few collisions
  - Should have the "avalanche effect"
- Still susceptible to attack, like brute force and rainbow tables
  - Can use salt to help
- MD5 was big, now people use SHA-2

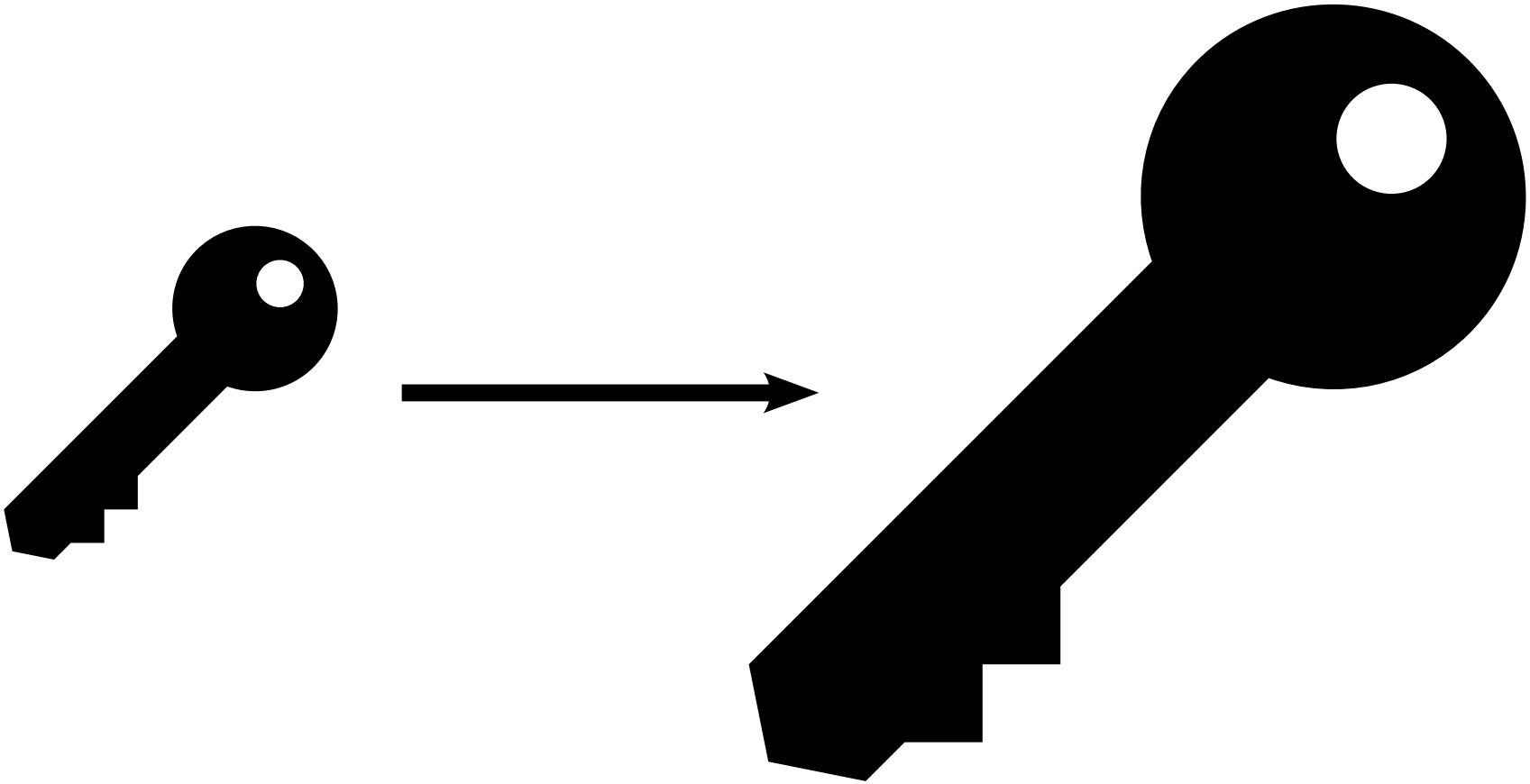
Future of Cryptography

Future of Cryptography

- Computers are going to keep getting faster, the brute force attack will keep getting stronger
- Moore's Law might be running out, but parallelism on the rise
- Quantum computing could mess up a lot of things

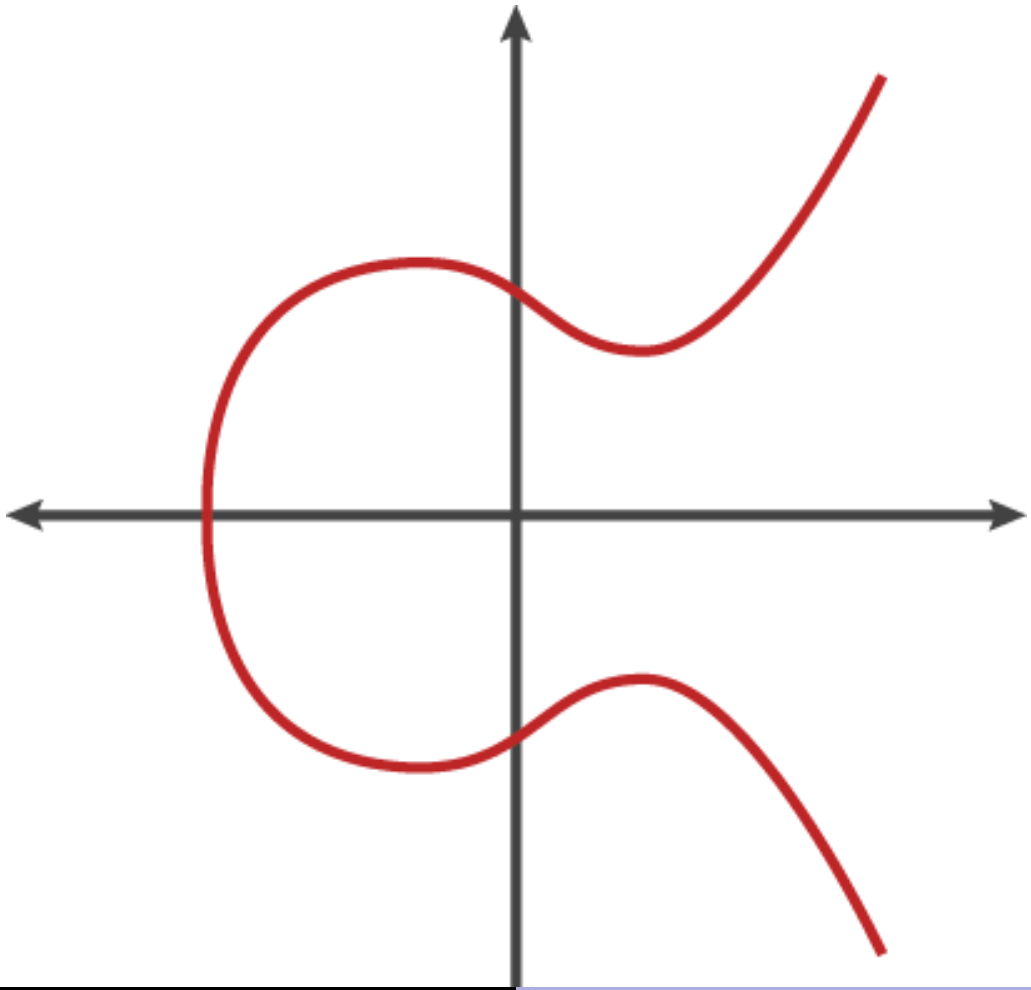
Future of Cryptography

Symmetric Key - Keys will keep getting bigger



Future of Cryptography

Asymmetric Key - RSA's factoring problem may get replaced by something else. Current crowd favorite is elliptic curves ($y^2 = x^3 + ax + b$)



Quantum Cryptography

- Utilize quantum physics to aid in ciphers or cryptanalysis
- Still very young, not actually used yet
- Quantum computers could be able to factor quickly and break RSA
- Can use properties to distribute keys without eavesdropping
  - Observing a particle can change it
  - Sometimes it is impossible to "unchange" it
  - It can be noticed that someone saw that particle

Theoretical Cryptography

- Is it even possible, in theory, to have an unbreakable cipher?

One Time Pad

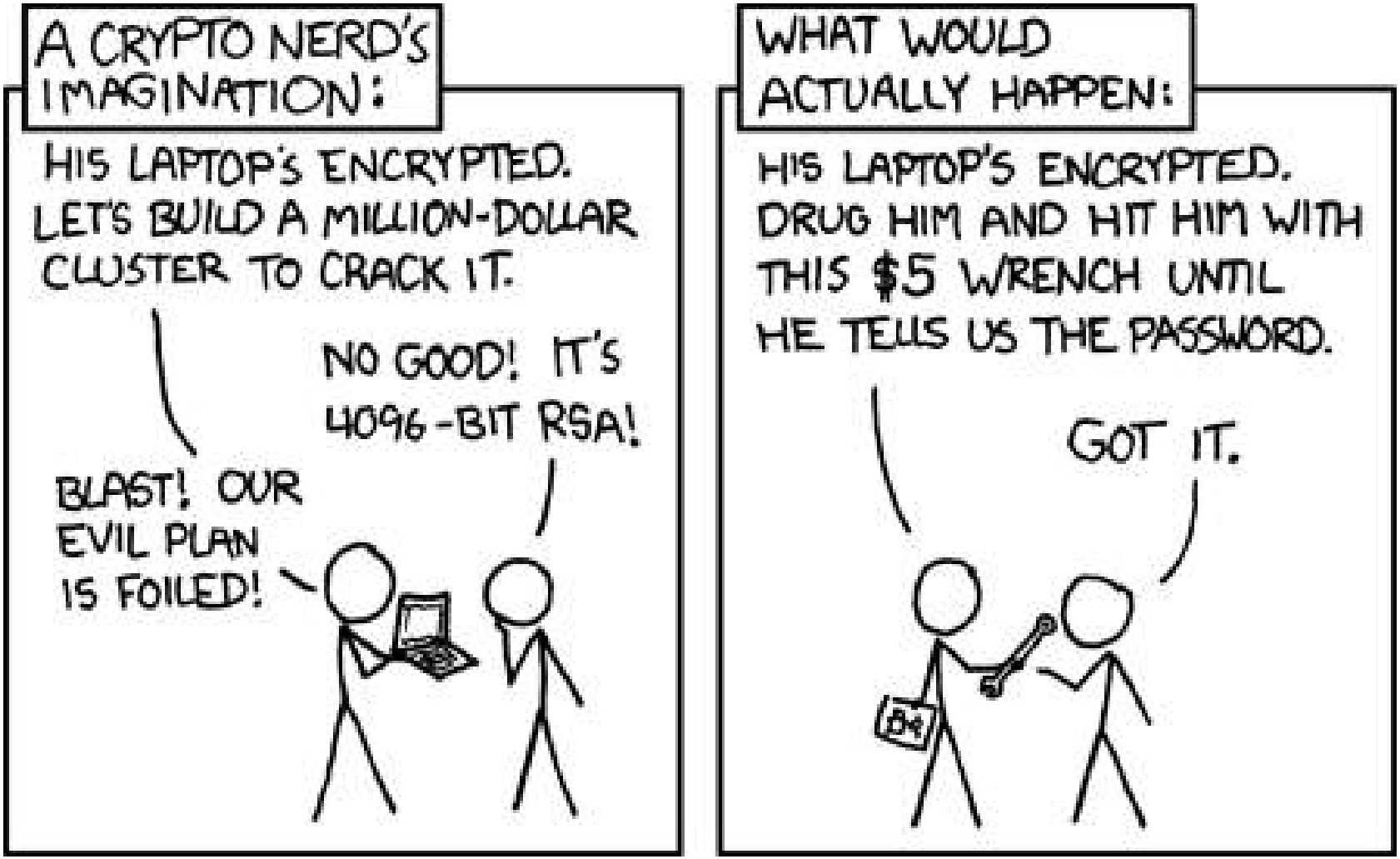
- A provable unbreakable cipher which is remarkable simple
- Encryption and decryption is just XORing with the key
- Used during the Cold War occasionally by field agents
- In most cases, impractical because the key must be as big as the message
- Issues with random key generation

Final Remarks

Why does Cryptography Matter?

- It's cool (reason enough)
- It's the reason computers exists
- It's the information age; the idea of securing information should be obvious
- With so much data easily accessible, security is a clear issue
- Cryptography, while establish in some places, is still legal murky ground
  - Use AES or RSA in the wrong country and you could be arrested
  - Others have key disclosure laws

Do people really break codes?



Want More On Cryptography?

- Today was focused on a survey of cryptography's evolution with a bias to encryption
- There is lots of neat cryptanalysis techniques for breaking moderate ciphers
- Cryptography lies in-between computer science and mathematics (number theory usually)
- Cryptography is related but not the same as computer security or information security or privacy
  - Most studies in those areas are regarding human factors
- Want a job in crypto? NSA is your best bet... maybe only bet...

End Note

- Slides from lecture delivered by Jordan Zink for 15-112 on April 23rd, 2015 at Carnegie Mellon University
- Quite a bit of this talk is based on a research paper written by myself (Jordan Zink) in 2010. The information should be (mostly) correct
- Besides a few simple figures, all drawings and pictures are from various online sources, mostly Wikipedia
- Opinions presented in this lecture are the opinions of Jordan Zink and may or may not coincide with the opinions of Carnegie Mellon University