Introduction to cryptology

Samuel Ranellucci
samuel@umd.edu

Doing online Banking

1. How do you know you are connecting with the bank's website
2. How do you exchange a secret key with your bank
3. How does your password stay secret
    1. Even if the hacker accesses the database of passwords
4. How does the bank hide the information it sends you
5. When you make a transfer, how can we verify
    1. amount
    2. recipient

Ethymology

- Kryptos ⇒ Hidden, concealed, secret
- -graphy ⇒ writing
- -ology ⇒ branch of learning, rel

Why cryptology and not cryptography

- A cryptosystem uses cryptography to protect either
  - Confidentiality
  - Integrity
- Cryptography is the art of making cryptosystems
- Cryptology is the science (math) of making cryptosystems

How is it science?

- Clear definitions of security
- Formal protocol descritptions
- Proofs of security
- Why a science?
  - Crypto is hard

Bad things can happen when crypto is bad

- Millions of bitcoins stolen
- Fake windows updates
- Adobe leaked password database

Historical perspective on computational encryption scheme

- Caesar cipher

- Enigma

- Lessons from historical perspective

Perfect security

- Encryption: When you want to completely hide your message.
  - Used to hide your bank account information
- Message authentication code: What to do to make sure the right person sent the message.
  - Ensures that your bank transfers don’t get modified

Perfect security

- One-time pad
  - How to perfectly encrypt a message
- One-time mac
  - How to perfectly authenticate a message

Private-key encryption

- Definition of indistinguishability
- Pseudo-random generator
- Chosen-plaintext security
- Pseudo-random function
- Secure encryption from PRG and PRF

Private-key encryption

- Block ciphers
- Modes of encryption
- Construction of block ciphers

Hash function

- Map a long string to a shorter string
- Collision-resistance
  - Hard to find (x, y) such that $h(x) = h(y)$
- Useful to protect integrity of systems

Public-key encryption

- Public (encryption) key
  - Anyone can encrypt a message

- Private (decryption) key
  - Only the creator can decrypt a ciphertext

- Allows client to send a secret key to the bank

Public-key encryption

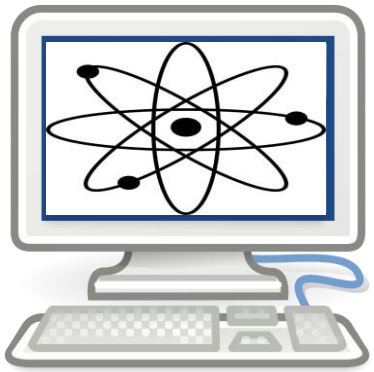
- RSA
- DDH
- LWE
- Etc.

Digital signature

- Signing (private) key
  - Sign a message
- Verification (Public) key
  - Everyone can verify signature
- Enables us to verify that we are connecting to the right website

Post-quantum cryptography

- Bad news
  - quantum computers break security of the internet
  - factoring made easy
  - Discrete logarithm
- Good news
  - Quantum computers are really hard to build
  - Exists assumption (we think) are hard



Quantum Cryptography

- Fun facts of quantum mechanics
  - No cloning
  - Reading a quantum state disturbs the quantum state

- Result
  - Perfect encryption using quantum mechanics

Modern cryptology

- Zero-knowledge
- Secure computation
- Fully-homorphic encryption