2/8/23 Security & Security

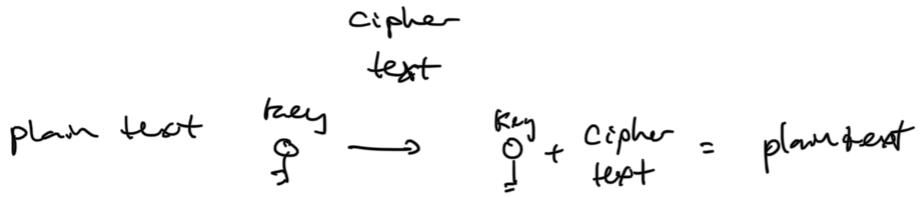
Schwartz schmo

gpz

rsa

German Enigma

Japanese Purple



<u>Key</u> is important, not algorithm

Sci.crypt - upload algorithm

let smart people break it, don't keep it secret

encryption & decryption key, could be the same

read Gallic Wars book

Cesear Cipher - shift letters down

the bit player - movie good

- information theory
- stg sally
- xor random noise w/ message
- undo random later to decode
- need to carry key w/ message

Unbreakable

Modern algorithms

- DES (data encryption standard)
  - 56 bit key
  - old, not great
- AES (Advanced encryption standard)
  - 10 billion years to crack w/ brute force

- 128 bit key

Can Quantum Computer beat AES?
- would require power of USA for a year
- bc bit flipping still requires energy

Simon
- made by NSA — run a certain # of times
- group of block ciphers — undo certain # of times
- not linear

Network protocol
- critical for encryption

Kirchoff's principle

Public key cryptography
- 2 keys, public & private
- digital signatures = private key
- slow, small data good
- uses big #s - multiplication
- RSA

I know friends public key, but only they can decrypt it

Diffie Hellman key exchange
- securely exchange key over insecure channel
- creating a shared key by mixing private keys w/ message

RSA
- pick 2 random prime p & q
- product $n = p \times q$

public is excel

- log en
- random 3rd prime e
- GCD checks conditions of q_0 q_0 & e
- d mod ular inverse of e
- decryption
- encryption

$\varphi(n) = (p-1)(q-1)$

choose e such that $\gcd(e, \varphi(n)) = 1$

private key :: n & d

RFCs for RSA

you have to factor
- public key
- big composite
- very hard

noel brooks history of the world

what makes this difficult is a lot of pieces & unknowns to the code breaker. You need all the pieces to decrypt

prime #s are very important to cryptography
- probabilistic test - fast
- AKS test - slow but accurate - polynomial
- Euler-Witness - probabilistic
- Miller Rabin - probabilistic

power mod (Modular exponentiation)
- repeated squares

Modular Inverse
- by Euclid

GMP (GNU multiprecision package)
- fast, precise
- annoying to use
- line by line substitution of normal operators

- comment actual equation
- everything is an array, all pass by ref, choose nots to arrays

How to break modern cryptography

- cheat
- guess bits of RSA encryption using microphone on phone