RSA

Rivest**S**hamir**A**dleman

RSA Secure?

- What makes RSA difficult?

RSA Secure?

- What makes RSA difficult?
  - Factoring is hard!
    - Well at least for large integers

History

- Was developed independently by Clifford Cocks in 1973
  - However, it was classified as secret and RSA guys never knew about it.
  - It was declassified in 1998
  - More about the patents stuff on Wikipedia

Encipher

$$c = m^e \bmod n$$

Decipher

$$m = c^d \bmod n$$

Variables

- $n = pq$, where p and q are prime numbers
- $e : \gcd(e, \varphi(n)) = 1$
  - $\varphi(n) = (p-1)(q-1)$
- $d = e^{(-1)} \bmod \varphi(n)$

Example code

- n = 77
- d = 53
- e = 17
- Encode the message then decode the message. Use the weird print function (wprint) to see if you got it right.

Quantum Stuff

- Qubit
  - Has 3 states (sort of)
    - 0
    - 1
    - Superposition of the two states

Quantum Stuff

- Qubit can be in states described previously, but when read must be 0 or 1.
  - Measuring the system changes it

Quantum Stuff

- Quantum Entanglement
  - Two objects interact and become entangled
  - Anything affecting either side causes the other to be changed
    - This holds even if the entangled objects are separated over long distances

Quantum Key Exchange

- How would this be helpful for exchanging keys secretly?

Quantum Key Exchange

- How would this be helpful for exchanging keys secretly?
  - If we can tell someone is eavesdropping on the conversation then we know when the key is compromised

Quantum Key Exchange

- How would this be helpful for exchanging keys secretly?
  - If we can tell someone is eavesdropping on the conversation then we know when the key is compromised
  - Is it just theoretical?

Shores Algorithm

- An algorithm that runs in polynomial time that factors a number N.

Shores Algorithm

- An algorithm that runs in polynomial time that factors a number N.
  - So what can we do with that?

Shores Algorithm

- An algorithm that runs in polynomial time that factors a number N.(1994)
  - So what can we do with that?
  - BREAK RSA! $O((\log n)^3)$
  - Its been done on a 7 qubit quantum computer

Grovers Algorithm

- Grovers search algorithm
  - Searching in unsorted database
  - Quantum algorithm that runs on O(sqrt(N))
  - Traditionally O(N)

Grovers Algorithm

- Cuts the complexity by the square root
  - So what? Are there any implications to symmetric crypto?

Grovers Algorithm

- Cuts the complexity by the square root
  - So what? Are there any implications to symmetric crypto?
  - NO. Just double the key and you are back to where you started on classical computers

Take Away

- Asymmetric crypto?
- Symmetric crypto?

Take Away

- Asymmetric crypto: is dead in the face of quantum computers when/if they arrive
- Symmetric crypto: lives in the face of quantum computers
  - How to exchange keys though?

Take Away

- Asymmetric crypto: is dead in the face of quantum computers when/if they arrive
- Symmetric crypto: lives in the face of quantum computers
  - How to exchange keys though?
    - Quantum Key distribution!