DTTF/NB479: Dszquphsbqiz Day 33

- Remaining course content
  - Remote, fair coin flipping
  - Presentations: Protocols, Elliptic curves, Info Theory, Quantum Crypto, Bitcoin, Error-correcting codes, Digital Cash
- Announcements:
  - See schedule for weeks 9 and 10
  - Project workdays, exam
  - Projects: Look at rubrics, example of past project
  - Early paper submissions are encouraged!
- Questions?

You can't trust someone to flip a coin remotely if they *really* want to win the flip

- Alice and Bob each want to win a coin flip
- Why can't they do this over the phone?

- Let's see…

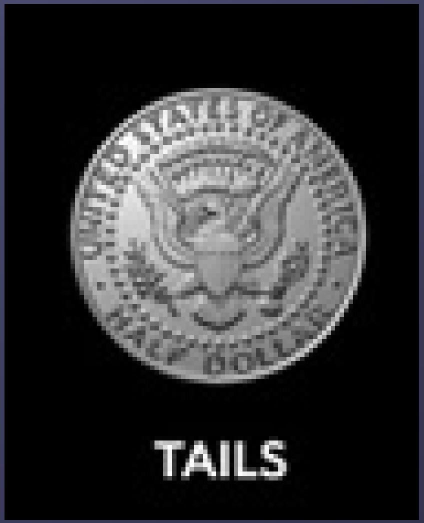
What if Bob flips?

Alice

- Heads!

Bob

- I’ll flip a coin. You call it.
- Looks and sees tails.
- Sorry Alice, it was tails…

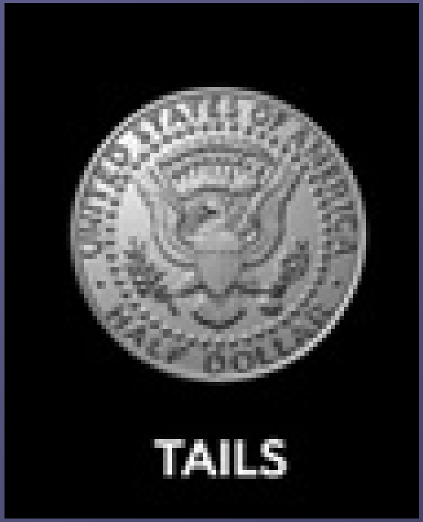


http://g-ecx.images-amazon.com/images/G/01/oreilly/CoinFlip2._V230746768_.jpg

What if Alice flips?

Alice

- I'll flip a coin. You call it.
- Sorry Bob, it was heads. (silent snicker)



Bob

- Tails!

We can use related secrets to guarantee a fair flip

Alice

- Knows something Bob doesn't. Gives him a hint.
- Uses her secret and Bob's hint to calculate 2 guesses for Bob's secret; she can only guess it right ½ the time.

Bob

- Knows something Alice doesn't, gives her a hint
- Alice guesses and dares Bob to prove she's wrong

- If she's right, Bob can't argue.

- If she's wrong, Bob can prove it by calc'ing her secret!

Her secret is so secret, the only way Bob could figure it out is using Alice's *wrong* guess!

What's Alice's secret?
The 2 large prime factors of a huge composite!

- And now for something completely different…
- You can find square roots easily if the base p is "special", a prime congruent to 3 (mod 4)
  - There are many such primes:

    3, 5, **7**, **11**, 13, 17, **19**, **23**, 29, **31**, 37, **43**, …
  - Proof

We can use related secrets to guarantee a fair flip

Alice

- Knows secret primes
  $p \equiv 3 \pmod{4}$ & $q \equiv 3 \pmod{4}$
  Tells Bob hint: $n = pq$
- Finds $a^2 \equiv b^2 \equiv y \pmod{n}$
  using p, q, and ChRT.
  Guesses one of a or b, say b.

Bob

- Knows random x, tells Alice
  $y \equiv x^2 \pmod{n}$
- If $b \equiv \pm x$, Alice won
  and Bob can't argue
- If $b \neq \pm x$, Bob can calculate
  p and q using the SRCT

Her secret is so secret, the only way Bob could figure it out is using Alice's *wrong* guess!

This MATLAB demo ties together many concepts from our number theory work

- Fermat's theorem
- GCD
- Chinese Remainder Theorem
  - Finding the 4 solutions to $y \equiv x^2 \pmod{n}$ is as hard as factoring n
- Square Root Compositeness Theorem
- Modular exponentiation
- Modular inverse
- Miller-Rabin*