MATH 314 Fall 2018 - Class Notes

12/3/2018

Scribe: Jason Hamilton

Summary: We went over the Birthday Paradox and Birthday Attack when it comes to the DSA Algorithm.

Notes:

- Generalize the Birthday paradox to n "boxes" k "objects"
- Put k objects in n boxes. Randomly ask what is the probability that two objects end up in the same box.
- Call this $P(n,k)$ = Prob k things in n boxes = 2 in the same box.

or **other** formatting *commands.* Make sure to write $e^{qu}a + i \circ \mathbb{N}s$ in math mode.
Examples: $P(365, 23)$ $1 - (365/365)(364/365)(363/365)...(343/365) \approx 0.502$

Approximation of $P(n,k) \approx e^{-k^2/2n}$

- We can think of objects in boxes as being like values of hash functions digest two objects in the same box form a collision
- Birthday Attack: Suppose Alice is using a hash with 50 bit digests. She then signs these digest using her public key.
- 2^{50} possible digests. Alice uses a cyptographically secure hash so it is hard to find a collision with a specific digest.
- Eve wants to trick Alice into signing a bad contract
- She drafts a "good" contract that Alice is willing to sign. Before she gives it to Alice. She finds 30 places in the contract where she can make a small change without effecting the contract.
- She also writes a bad contract. Eve finds 30 places alter the bad contract without changing it.
- **Eve tries hashing all of the contracts.**
- 2^{30} "good" contracts. 2^{30} "bad" contracts. 2^{31} contracts overall.
- Even hashes all 2^{31} contracts looks for collisions k = 2^{31}, n = 2^{50} $k^2/n = 2048$
- Lots of collisions so almost certainly there is a good contract mg and a bad contract mb with $h(mg) = h(mb)$

- She presents mg to Alice. Alice signs it $(mg, s(h(mg)))$
- Eve turns around and claims Alice signed $(mb, s(h(mb)))$
- *What does Alice do if she suspects Eve is trying to trick her?*
- Alice can defend against this by making sure small changes to the contract before signing it.
- *General Principle*: Never digitially sign something created by someone else without introducing a small change first.

Eliptic Curves

- Nothing to do with Ellipses (ovals)
- Generally - An elliptic curve is an equation of the form $y^2 = x^3 + ax + b$ where $4a^2 + 27b^3 \neq 0$
- **Nifty Fact:** Take any two points on a elliptic curve draw a line connecting them. There is always a 3rd point the line also goes through. Use this to define "addition" of points on a curve.
- To add two points on an elliptic curve, draw the line between them. Find the third point on that line reflect across x-axis that points is P+Q