MATH 314 Spring 2018 - Class Notes

5/7/2019

Scribe: Alex Buttrum

Summary: Learned about the Birthday attack and setup for Digital Structure Algorithm (DSA)

Notes:

Probability:

- If we have K people what is the probability that at least two share a birthday?
- Compute probability that none share a birthday?
- $K = 2$ $(\frac{365}{366})$ -¿ Probability that 2 people do not share birthday.
- $K = 3$ $(\frac{365}{366}) \times (\frac{364}{366})$ - Probability that 3 people do not share birthday.
- For general K: $\frac{366-K+1}{366} = e^{\frac{-K^2}{2\times 366}}$
- If K things are chosen from N things (with replacement) the probability that no object is drawn is about $e^{\frac{-K^2}{2^N}}$
- Birthday paradox allows us to see probability of collision.

Birthday Attack

- Mallory wants to maliciously make Alice sign a bad contract.
- She going to draft a good contract that Alice would be willing to sign
- She finds 30 places in this contract where she can make small changes (2 possibilities)
- 2^{30}good contracts.
- She also drafts a bad contract with 30 possible changes. So she gets 2^{30}bad contracts.
- Alice uses a weakly collision resistant hash function that produces 50 bit digests.
- Mallory has 2^{31}contracts total, she computes the has of every one of those contracts.
- $N = 2^{50}$ $K = 2^{31}$
- What is the probability of finding a collision? (2 different contracts with the same hash)

- Plug these into $e^{\frac{-K^2}{2^N}} = e^{\frac{-2^{62}}{2^{51}}} = e^{\frac{-2}{11}}$

- - e^{-2048} essentially 0, lots of collisions.

- So there is almost certainty a collision between a good contract and a bad contract.

- So Mallory gives Alice this contract to sign. Good contract = m1, Bad contract = m2. $h(m1) = h(m2)$

- Alice looks over the good contract and signs it $SA(m) = S(h(m1)) = S(h(m2))$ She sends (m1,s)

- Mallory claims Alice signed m2 since h(m2)=h(m1). S is also a valid signature for m2.

- Never sign a message that someone else produced.

- Use digests with more than e + 256 bits.

- Another way to sign messages uses El gamal. (Check book for that)

Digital Structure Algorithm (DSA)

- Uses the same ideas but faster and more secure

- Relies on discrete log problem to be secure.

DSA setup

- Large prime number p (200 digits)

- $p - 1$ has a large factor p

- $q(p-1) => (p-1) \equiv Kq$ Where K is small

- Pick a primitive root $g(modp)$

- Compute $\alpha \equiv g^{\frac{p-1}{q}} \equiv g^K(modp)$

- Note α is not a primitive root $\alpha^q \equiv (g^{\frac{p-1}{q}})^q \equiv 1(modp)$

- What matters in the exponent of α is (mod q)

- Alice picks a secret number with $1 < a < q$, then computes $\beta \equiv \alpha^a(modp)$

- Her public key is (p, q, α, β)

- That's where the lesson ended