CIS 3362 – 11/22/21

1. Birthday Paradox
2. Relationship to forging a message signature.

If you have 23 or more people in a row, there's > 50% chance that some pair share a birthday.

n boxes

Randomly throw k balls into the n boxes s.t. each ball has a $\frac{1}{n}$ chance of landing in any particular box. What is the probability that at least 1 box has more than 1 ball?

What's probability all different?

$$\frac{n}{n} \times \frac{n-1}{n} \times \frac{n-2}{n} \times \cdots \frac{n-k+1}{n}$$

At least 1 box ≥ 2 balls:

$$\boxed{1 - \frac{n!}{n^k (n-k)!}}$$

How to use this idea to get a fake sign.

1. Get a message Person A is willing to sign.

2. Make many different versions of the message by creating words where a synonym could be used, repeating this k times so that there are 2^k roughly equivalent msgs.

3. For each of these calc hash func.

Choices	Hash Val
0110101000	1111010..1
⋮	
	⋮

2^k entries

one match!

4. Create your nefarious msg. (One they wouldn't sign but you want to pretend it's from them!) Create 2^k versions in the same way.

5. See if <u>any</u> of these versons has a hash value equal to <u>ANYTHING</u> on this constructed table.

6. Get Person A to sign the specific version that matches one of my nefarious messages! But then change the message since hash val is the same!

On average, we need $k = \frac{n}{2}$ for us to expect this technique to work, where $n =$ # bits output of the hash function.

We need $\mathcal{O}(2^{n/2})$ memory and $\mathcal{O}(2^{n/2})$ time for this technique.