

# CS 329E Final Presentation

## # Birthday Problem

Presented by: Jun Seo Park

Instructor: Dr. Warnow



# Birthday Problem : Definition

- The probability that at least two people in a group of  $N$  people share a birthday
- Ex: there are 30 people, and at least two of them share a birthday.



# Birthday Problem

- How to solve the problem.
  1. Greedy algorithm
  2. Simulation
  3. Using Exclusion.

# Greedy algorithm to solve.

1. When  $N = 1$

Only 1 person => it's not possible to share a birthday.

→  $P(1) = 0$

# Greedy algorithm to solve.

2. When  $N = 2$

2 people => Only possible when the second person has the same birthday as the first one's birthday.

→  $P(2) = 1/366$  (There are 366 possible birthdays)

# Greedy algorithm to solve.

3. When  $N = 3$

3 people => two possible situation

- a. 2<sup>nd</sup> person has the same birthday with 1<sup>st</sup> person.
- b. 2<sup>nd</sup> person does not have the same birthday as the 1<sup>st</sup> person ( $365/366$ )

AND

3<sup>rd</sup> person has the same birthday either with the 1<sup>st</sup> person, or the 2<sup>nd</sup> person. ( $2/366$ )

$$\rightarrow P(3) = 1/366 + 365/366 * 2/366$$

# Greedy algorithm to solve.

3. When  $N = 4$  people
  - a. 2<sup>nd</sup> person has the same birthday with 1<sup>st</sup> person. ( $1/366$ )
  - b. 2<sup>nd</sup> person does not share the birthday with 1<sup>st</sup> person, but 3<sup>rd</sup> person has the same birthday with the previous 2. ( $365/366 * 2/366$ )
  - c. 3<sup>rd</sup> person does not share the birthday with the previous 2, but the 4<sup>th</sup> person share the birthday with either of previous 3. ( $365/366 * 364/366 * 3/366$ )

$$\rightarrow P(4) = 1/366 + 365/366 * 2/366 + 365/366 * 364/366 * 3/366$$

# Simulation to solve.

```
#!/usr/bin/perl
use POSIX qw(ceil floor);
for ($n = 0; $n < 367; $n++)
{
    while($count < 10000)
    {
        for ($i=0; $i < $n; $i++)
        {
            $b = 366*rand();
            $b = floor($b);
            $birth[$i] = $b;
            for ($j=0; $j < $i; $j++)
            {
                if ($birth[$j] == $b)
                {
                    $true--;
                    $false++;
                }
            }
        }
    }
}
```

```
$j = $i;
        $i = 20;
    }
}
}
}
$true++;
$count++;
}
print "when N is $n, \n";
print "$n \t true \t false \n";
print "\t".$true."\t".$false."\n";
$count = 0;
$true = 0;
>false = 0;
}
```



# Simulation to solve.

For each N value, 10000 calculations were done.

UT-CS public unix machine 'explosion' was used, it took  
9:24.38

Result: [Birthday Problem.xls](#)



# Using Exclusion

- Trick: Calculate  $1 -$  (the probability of ‘not happening of the incident’)
- The probability that at least two people in a group of  $N$  people share a birthday
  - $1$  minus (probability that no one in a group of  $N$  people share a birthday)
- Gives you much simpler calculation.

# Exclusion

- $N = 2$

$$1 - \frac{365}{366} = \frac{1}{366}$$

- $N = 3$

$$1 - \frac{365}{366} * \frac{364}{366}$$

- $N = 4$

$$1 - \frac{365}{366} * \frac{364}{366} * \frac{363}{366}$$

- $N = 5$

$$1 - \frac{365}{366} * \frac{364}{366} * \frac{363}{366} * \frac{362}{366}$$

# Check with the previous methods

- Greedy algorithm

$$P(4) = (1 / 366) + (((365 / 366) * 2) / 366) + (((((365 / 366) * 364) / 366) * 3) / 366)$$

$$= 0.0163114485$$

- Simulation

$$P(4) = 0.0165$$

- Exclusion

$$P(4) = 1 - (365 / 366) * (364 / 366) * (363 / 366)$$

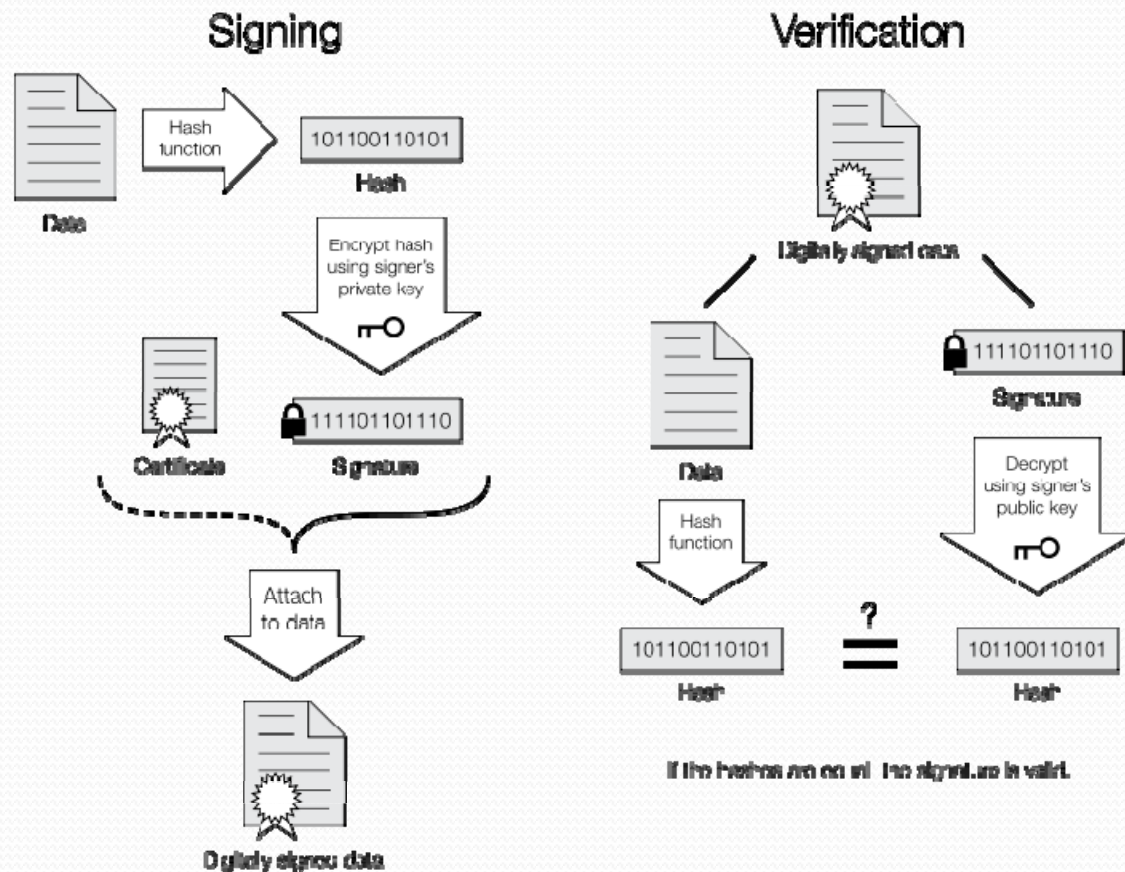
$$= 0.0163114485$$



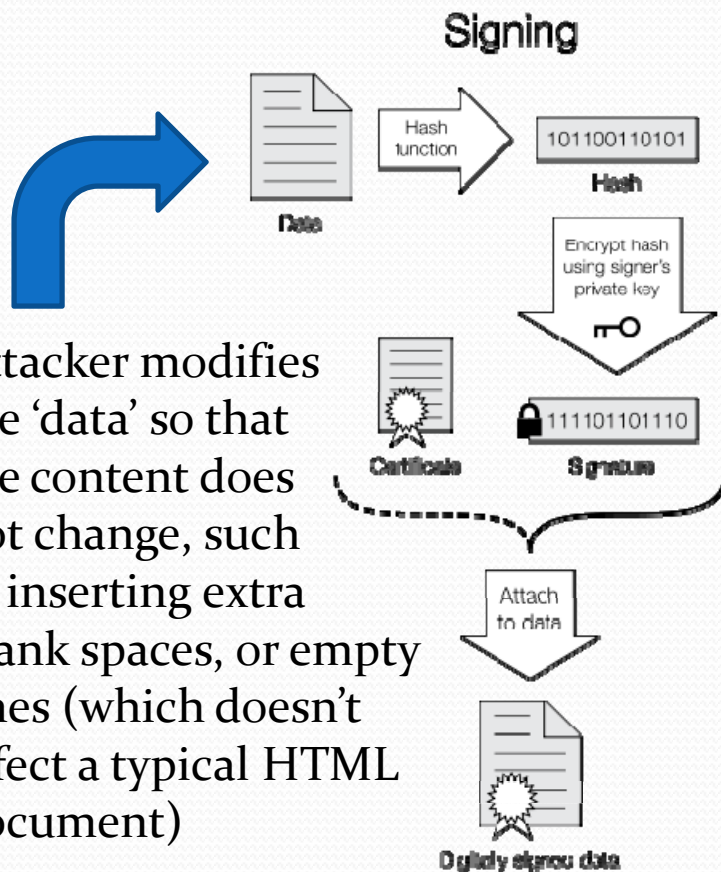
# Application: Birthday Attack

- What Birthday Problem illustrates:
  1. You don't need 183 people to achieve 50%, you need only 23 people.
  2. This Birthday Attack is especially efficient on providing a false digital signature.

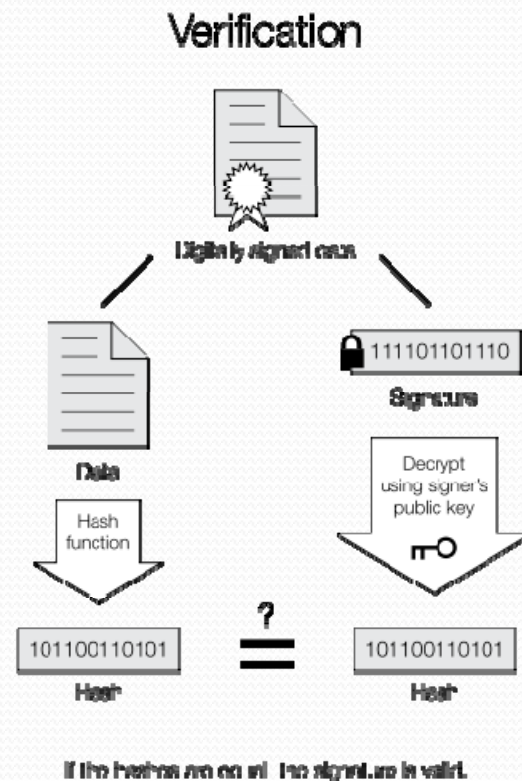
# Application: Birthday Attack



# Application: Birthday Attack



Attacker modifies the 'data' so that the content does not change, such as inserting extra blank spaces, or empty lines (which doesn't affect a typical HTML document)



# Application: Birthday Attack

Bits	Possible outputs (H)	Desired probability of random collision (p)									
		$10^{-18}$	$10^{-15}$	$10^{-12}$	$10^{-9}$	$10^{-6}$	0.1%	1%	25%	50%	75%
32	$4.3 \times 10^9$	2	2	2	2.9	93	$2.9 \times 10^3$	$9.3 \times 10^3$	$5.0 \times 10^4$	$7.7 \times 10^4$	$1.1 \times 10^5$
64	$1.8 \times 10^{19}$	6.1	$1.9 \times 10^2$	$6.1 \times 10^3$	$1.9 \times 10^5$	$6.1 \times 10^6$	$1.9 \times 10^8$	$6.1 \times 10^8$	$3.3 \times 10^9$	$5.1 \times 10^9$	$7.2 \times 10^9$
128	$3.4 \times 10^{38}$	$2.6 \times 10^{10}$	$8.2 \times 10^{11}$	$2.6 \times 10^{13}$	$8.2 \times 10^{14}$	$2.6 \times 10^{16}$	$8.3 \times 10^{17}$	$2.6 \times 10^{18}$	$1.4 \times 10^{19}$	$2.2 \times 10^{19}$	$3.1 \times 10^{19}$
256	$1.2 \times 10^{77}$	$4.8 \times 10^{29}$	$1.5 \times 10^{31}$	$4.8 \times 10^{32}$	$1.5 \times 10^{34}$	$4.8 \times 10^{35}$	$1.5 \times 10^{37}$	$4.8 \times 10^{37}$	$2.6 \times 10^{38}$	$4.0 \times 10^{38}$	$5.7 \times 10^{38}$
384	$3.9 \times 10^{115}$	$8.9 \times 10^{48}$	$2.8 \times 10^{50}$	$8.9 \times 10^{51}$	$2.8 \times 10^{53}$	$8.9 \times 10^{54}$	$2.8 \times 10^{56}$	$8.9 \times 10^{56}$	$4.8 \times 10^{57}$	$7.4 \times 10^{57}$	$1.0 \times 10^{58}$
512	$1.3 \times 10^{154}$	$1.6 \times 10^{68}$	$5.2 \times 10^{69}$	$1.6 \times 10^{71}$	$5.2 \times 10^{72}$	$1.6 \times 10^{74}$	$5.2 \times 10^{75}$	$1.6 \times 10^{76}$	$8.8 \times 10^{76}$	$1.4 \times 10^{77}$	$1.9 \times 10^{77}$

It only takes  $1.25 \cdot \sqrt{H}$  trials to achieve 50% chance



# Application: Birthday Attack

- How to prevent:

Use sufficiently a large hash set (128 bits or more) so the brute force attack would be impossible to break.

# Reference

- Birthday Problem

[http://en.wikipedia.org/wiki/Birthday\\_paradox](http://en.wikipedia.org/wiki/Birthday_paradox)

- Birthday Attack

[http://en.wikipedia.org/wiki/Birthday\\_attack](http://en.wikipedia.org/wiki/Birthday_attack)

Simulation code is available at:

- <http://webpace.utexas.edu/jsp435/cs329e/Birthday.pl>