The birthday problem and its application to breaking cryptographic hash functions

David Jay

What is a Hash Function?

What is a Hash Function?

$$F : \{0,1\}^{\infty} \to \{0,1\}^{n}.$$

What is a Hash Function?

“hello world” → 5eb63bbbe01eeed093cb22bb8f5acdc3
“hello worle” → 18c5650581f01f1a52c87eee5baa754a

using the md5 hashing algorithm

What is a Cryptographic Hash Function?

What is a Cryptographic Hash Function?

- Preimage resistance

What is a Cryptographic Hash Function?

- Preimage resistance
- Second preimage resistance

What is a Cryptographic Hash Function?

- Preimage resistance
- Second preimage resistance
- Collision resistance

What is a Cryptographic Hash Function?

- Preimage resistance
- Second preimage resistance
- Collision resistance
- Uniformly distributed

What are Hash Functions used for?

Cryptography

Validation of message integrity

Hash tables

Breaking hash functions.

Types of attack:

Preimage attack

Second preimage attack

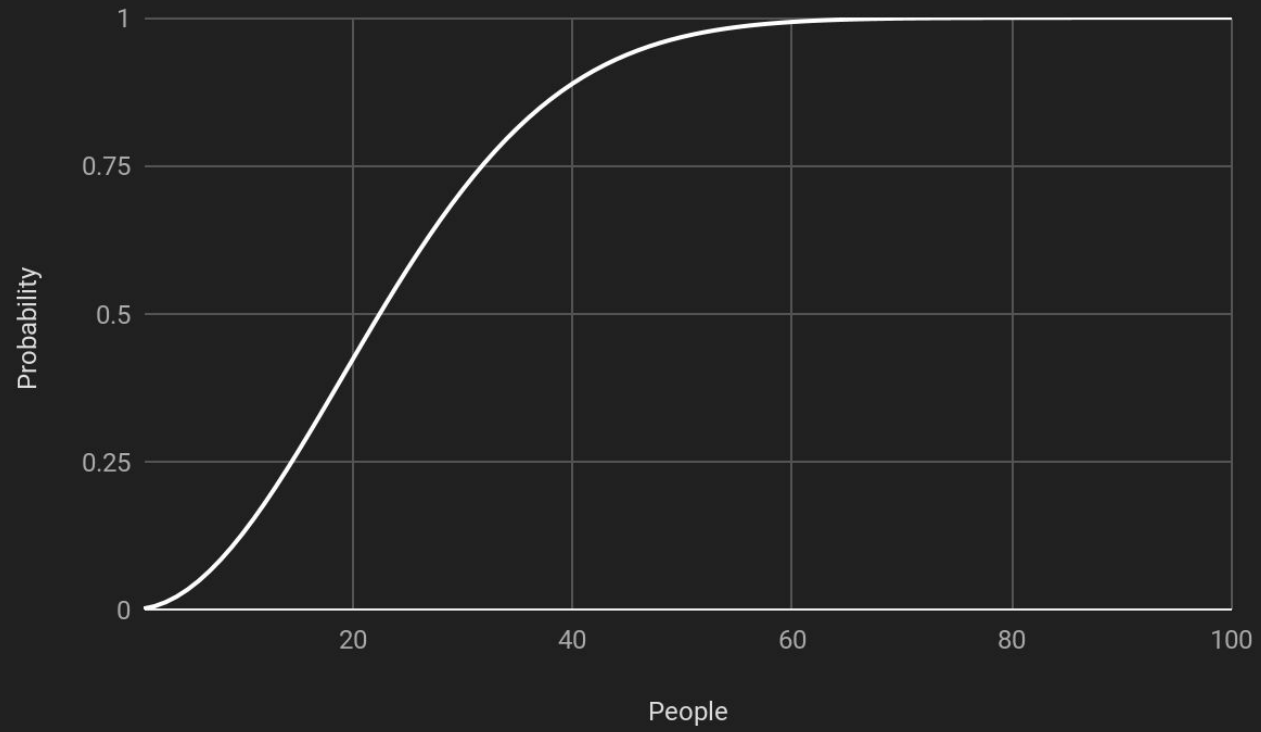
Collision attack

What is the Birthday Party Problem?

Let’s do some maths!

$$\mathrm{P}(\text{no collisions}) = \prod_{i=o}^{k-1}(1 - \frac{i}{m})$$

$$\begin{aligned} \mathrm{P}(\text{collision}) &= 1 - \mathrm{P}(\text{no collision}) \\ &= 1 - e^{-\frac{k^2}{2m}} \end{aligned}$$

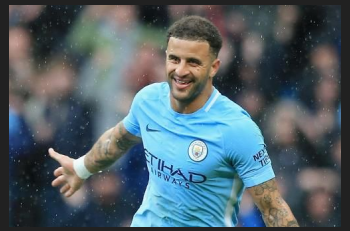

1
0.75
0.5
0.25
0
Probability
20
40
60
80
100
People

Football?

Australia
Brazil
Costa Rica
Croatia
England
France
Germany
IR Iran

Korea Republic
Morocco
Nigeria
Peru
Poland
Portugal
Russia
Spain

John Stones



Kyle Walker

Breaking hash functions with a birthday attack.

$$k = \sqrt{-2m \ln(1-p)}$$

		Probability of random collision (p)				
Bits	**Possible outputs (m)**	0.10%	1%	25%	50%	75%
16	6.55E+04	11	36	190	300	430
32	4.29E+09	2.90E+03	9.30E+03	5.00E+04	7.70E+04	1.10E+05
64	1.84E+19	1.90E+08	6.10E+08	3.30E+09	5.10E+09	7.20E+09
128	3.40E+38	8.30E+17	2.60E+18	1.40E+19	2.20E+19	3.10E+19
256	1.16E+77	1.50E+37	4.80E+37	2.60E+38	4.00E+38	5.70E+38
512	1.34E+154	5.20E+75	1.60E+76	8.80E+76	1.40E+77	1.90E+77

How can combat this attack?

Thanks, any questions?

Refs:
http://math.sun.ac.za/wp-content/uploads/2011/10/mmile_writeup.pdf
http://www.winlab.rutgers.edu/comnet2/Reading/documents/Birthday_attack.pdf
http://wdsinet.org/Annual_Meetings/2017_Proceedings/CR%20PDF/cr88.pdf
http://www.pumj.org/docs/Issue1/Article_3.pdf
https://blockgeeks.com/guides/cryptographic-hash-functions/