Birthday Attack

Objective

Objective

Identify proper password handling practices

What is the Birthday Problem?

Assumptions

Given a room with *n* people in it. We assume that everyone has a month and day for a birthday. We ignore leap years and assume that the distribution of birthdays is uniform or random.

Assumptions, cont'd

Event *A*

- At least one person in the room has a birthday on July 14th.

Event *B*

- At least two people in the room have the same birthday.

Probability Calculation

Probability Table

n	P(A)	P(B)
1	0.0028	0.0000
2	0.0055	0.0028
3	0.0082	0.0082
5	0.0136	0.0271
10	0.02771	0.1169
23	0.0612	0.5073

Conclusion

We see that *P(B)* can be quite large for relatively few people.

Application to Security Considerations

Let *H(x)* represent a hash function. Then the birthday problem applies to these two problems involving *H(x)*.

Pre-image Attack

Given a hash value *h* find x so that *H(x)* = *h*

Collision Attack

Find *x* and *x'* such that *H(x)* = *H(x')*

Brute Force Solutions

If *H(x)* has an 8 byte output:

Brute Force Pre-image

1.27×10^{19} attempts
12.7 Exahashes

Brute Force Collision

5.1×10^{9} attempts
5.1 Gigahashes

Here we expect an event if it has probability over 50%.

Application to Bitcoin

- Xthin block propagation uses “cheap hashes” which are eight bytes.