Birthday attack

If there are $N$ numbers and
have a chance of colliding,

\[ P > \frac{1}{\sqrt{N}} \]
Your same hand,

2 feet at a ft²
\[-L = 1.2 \int_2^n \frac{\partial}{\partial n} \frac{n}{2} n^{1/2} \]

\[
R = 1 \\
\text{Reconstr} \]

\[
C_n = \# F_1 \text{ blocks in layer} \]
As January ends, look forward

If not now, when? in 6-8 months have a bit differently
$\text{Secret Communication over a public channel} \rightarrow \text{key exchange and symmetric encryption}$
Problem word solution ≈ Identity = easy

Hardware - Oracle P2232

Difference of domain key exchange < Difference of domain key exchange

Known key exchange step
Create a lot of puzzles

\[ \text{Encrypt } x \rightarrow \text{ to produce } y \]

\[ \text{with key } k \]

\[ \text{Puzzle } \rightarrow \text{ given } x, y, \text{ find } k \]

\[ \text{Verify } \rightarrow \text{ given } x, y, k \text{ easy to verify} \]
Alice creates a new puzzle

Bob solves Alice's puzzle

E \text{ (winner)}

\text{puzzle 1}

Solution

Each \rightarrow

Bob picks a puzzle & solves it = solution

\text{puzzleindex/puzzles to Bob}
- Others do not know... why?

- Solution 

- Use solution is key for common problem. Bob picked

Here comes the solution to the
index puzzle solution Enc(index)

\[
\text{sln} = \text{key}
\]

Bob

Secret key
No other kitchen
Linear time to brake force
Diffie–Helman key exchange (1976)

Alice & Bob agree on 2 numbers: $p$ and $g$

Choose random numbers $x_A$ for Alice and $x_B$ for Bob.

Compute:

- $A = g^{x_A} \mod p$
- $B = g^{x_B} \mod p$

Exchange $A$ and $B$.

Alice's key: $B^{x_A} = (g^{x_B})^{x_A} = g^{x_B \cdot x_A} \mod p$

Bob's key: $A^{x_B} = (g^{x_A})^{x_B} = g^{x_A \cdot x_B} \mod p$

Their keys are equal: $g^{x_B \cdot x_A} \mod p = g^{x_A \cdot x_B} \mod p$
Secret key

Bob: Compute \((g^y)^x = g^{xy}\) mod \(p\)

The communique \((g^x)^y = g^{xy}\) mod \(p\)

Alice picks \(x\) (secret)
First, discuss log base e. Then all numbers are mapped in:

\[ x = \log_b (y) \]

Log is non-linear, but in linear:

\[ x_n \rightarrow y_n \]
\[ g = 4, \quad \frac{1}{2} = 4, \quad \frac{1}{3} = 4, \quad \frac{1}{4} = 4 \]

\[ g = 4 \]

\[ \log_2 4 = 2 \]

\[ g = 2, \quad g = 4, \quad \frac{1}{2} = 2, \quad \frac{1}{4} = 1 \]

\[ b = 3, \quad g = 4, \quad \frac{1}{3} = 2, \quad \frac{1}{4} = 1 \]

\[ g = 3 < i \Rightarrow \text{a generator} \]

\[ n = 5 \]
\[ \theta = \frac{1}{2} \text{ mod } n \]

There is no integer such that

\[ L \text{ for all } L \text{ because } 4 \text{ is not a prime number except} \]
a. Hence true, key is larger set

(b) is incorrect (as expected)

In short, if it is, the range of

be traversed

I.e., 9 does not have to

by a secret key

x, y ← 2 random keys

\langle y, x \rangle \leftarrow \text{prove key}

\langle y, x \rangle \to \text{prove secret key}

\text{now be friends/choose a}
Public key algo $\rightarrow$ 2 keys
$\rightarrow$ better than DHT