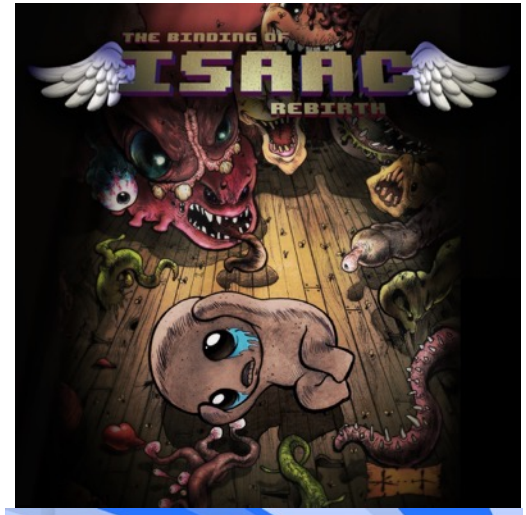
Random Numbers

Games


THE BINDING OF
ISAAC
REBIRTH

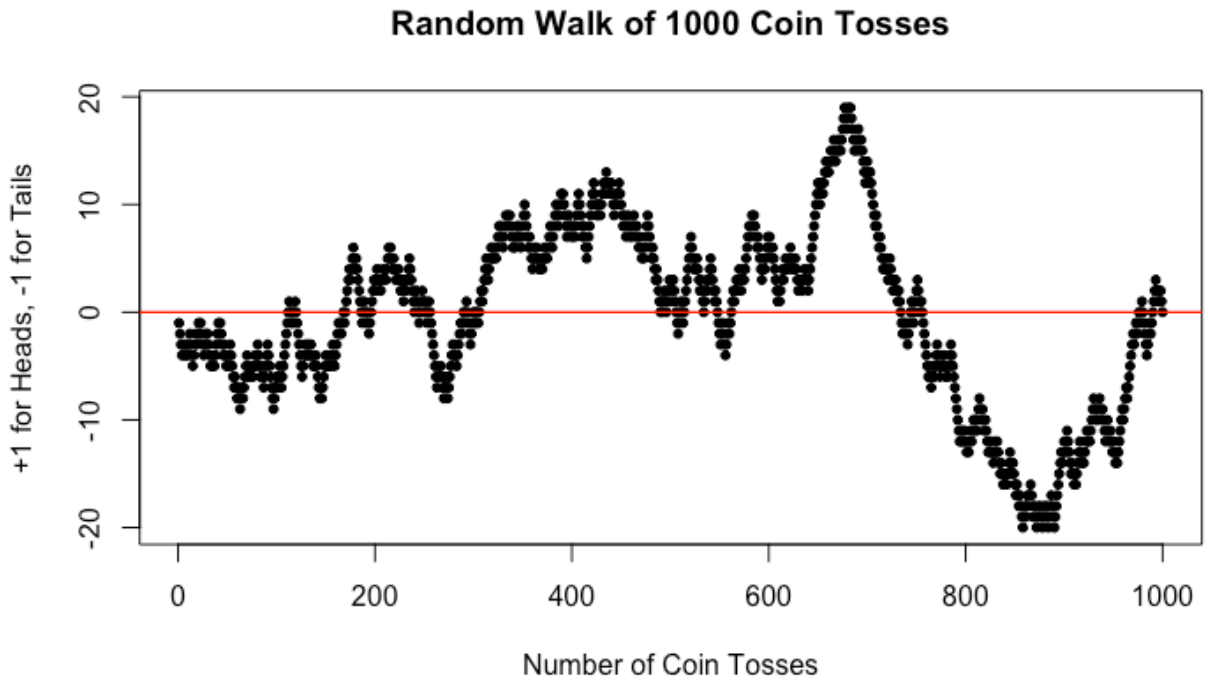

SPELUNKY
2


DEAD CELLS

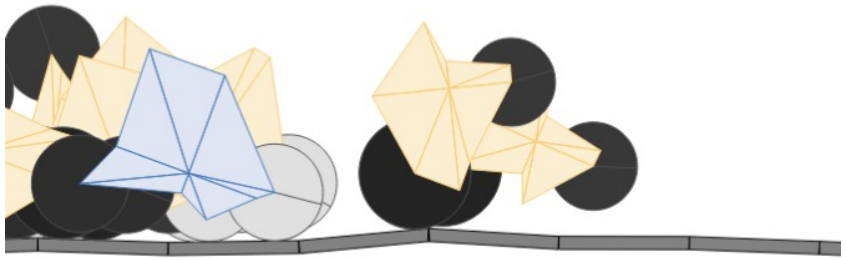

MINECRAFT


HADES

Simulations

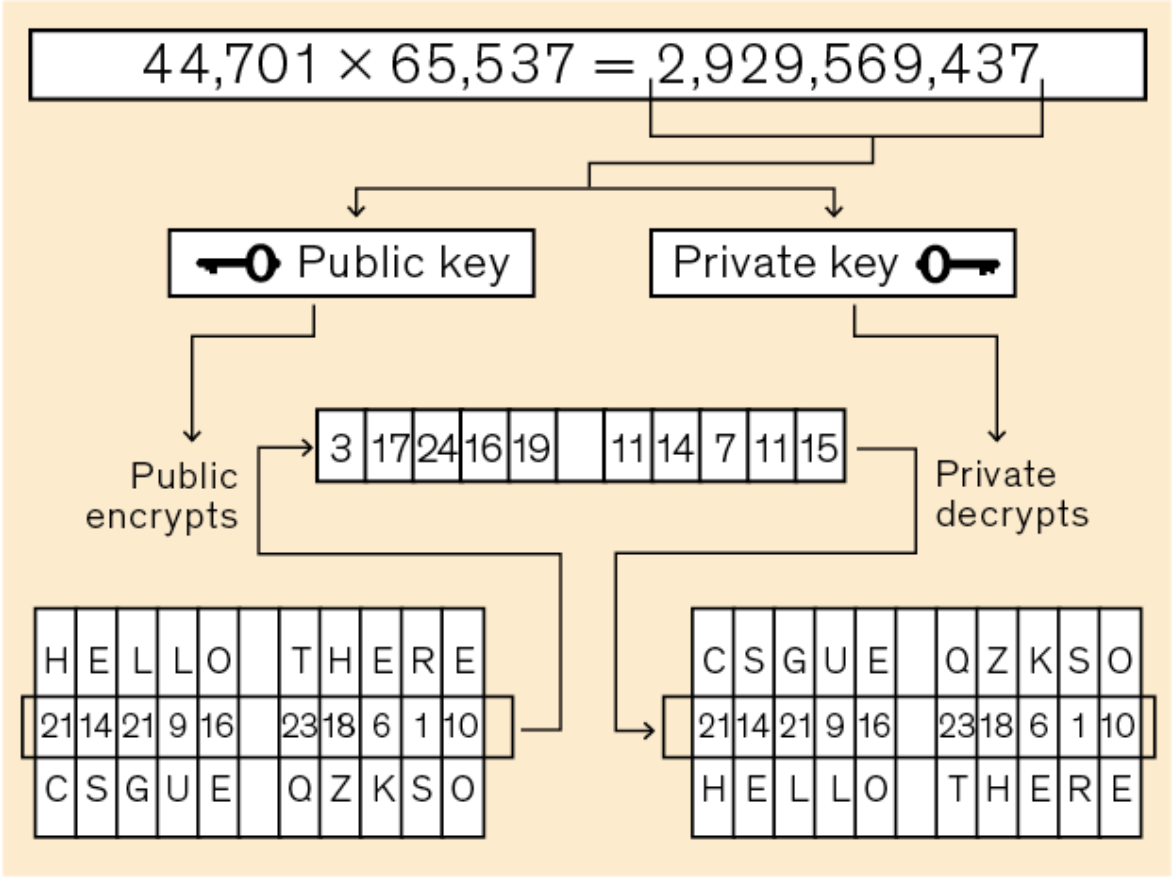


https://rednuht.org/genetic_cars_2/



Cryptography

RSA Encryption Keys



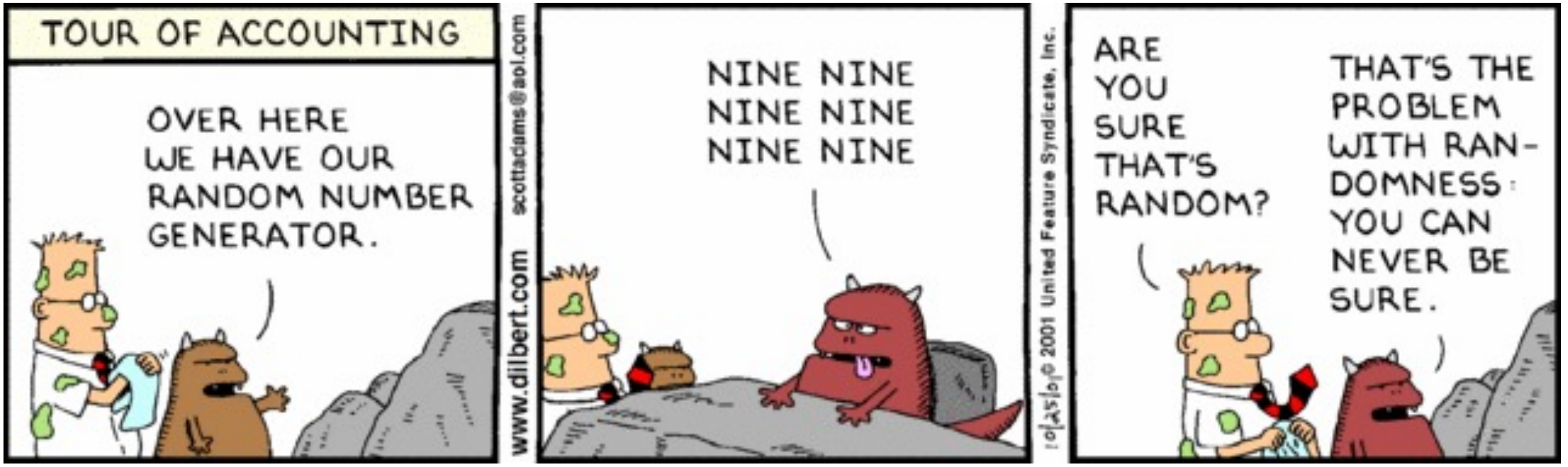
Truly Random Numbers

- Impossible to predict a number
- Aperiodic
  - No repeating sequences
- Difficult for computers
  - Programs are made up of algorithms which have deterministic behavior
    - Cannot use an algorithm alone for true randomness
  - Requires external randomness to create truly random numbers

Pseudo-Random Numbers

- Generated via an algorithm
- Provided a seed value to start the generation
- Only “secure” if you don’t know the algorithm or the seed
  - Also true for very complex algorithms
  - “Security” through obscurity
- Easy to generate them quickly

Pseudo-Random Numbers



A Naive Psuedo-Random Algorithm

```
value = seed
add = 11
repeat forever:
        value = value + add
        value = value % 10
        add = add + 1
```

A Naive Psuedo-Random Algorithm

```
value = seed
add = 11
repeat forever:
        value = value + add
        value = value % 10
        add = add + 1
```

Seed = 4

value	add
4	11
5	12
7	13
0	14
4	15
9	16
5	17
2	18

A Naive Psuedo-Random Algorithm

```
value = seed
add = 11
repeat forever:
        value = value + add
        value = value % 10
        add = add + 1
```

Seed = 4

value	add
4	11
5	12
7	13
0	14
4	15
9	16
5	17
2	18

Seed = 5

value	add
5	11
6	12
8	13
1	14
5	15
0	16
6	17
3	18

A Naive Psuedo-Random Algorithm

```
value = seed
add = 11
repeat forever:
        value = value + add
        value = value % 10
        add = add + 1
```

Only generates numbers between 0 and 9 and repeats after 20 values!

Seed = 4

value	add
4	11
5	12
7	13
0	14
4	15
9	16
5	17
2	18

Seed = 5

value	add
5	11
6	12
8	13
1	14
5	15
0	16
6	17
3	18

Generating Truly Random Numbers

- Requires entropy from the real world
  - Entropy here is a measure of how unpredictable the information is
  - More entropy more random

- We can get entropy from:
  - User Interaction (mouse movements)
  - Atmospheric Noise
  - Radioactive Decay

When to Use

Pseudo-Random Numbers:

- Low Stakes Games
- Simulations that require efficiency

Truly Random Numbers:

- Generating encryption keys
- High stakes games
  - Money or tangible rewards involved
- Simulations that need true randomness