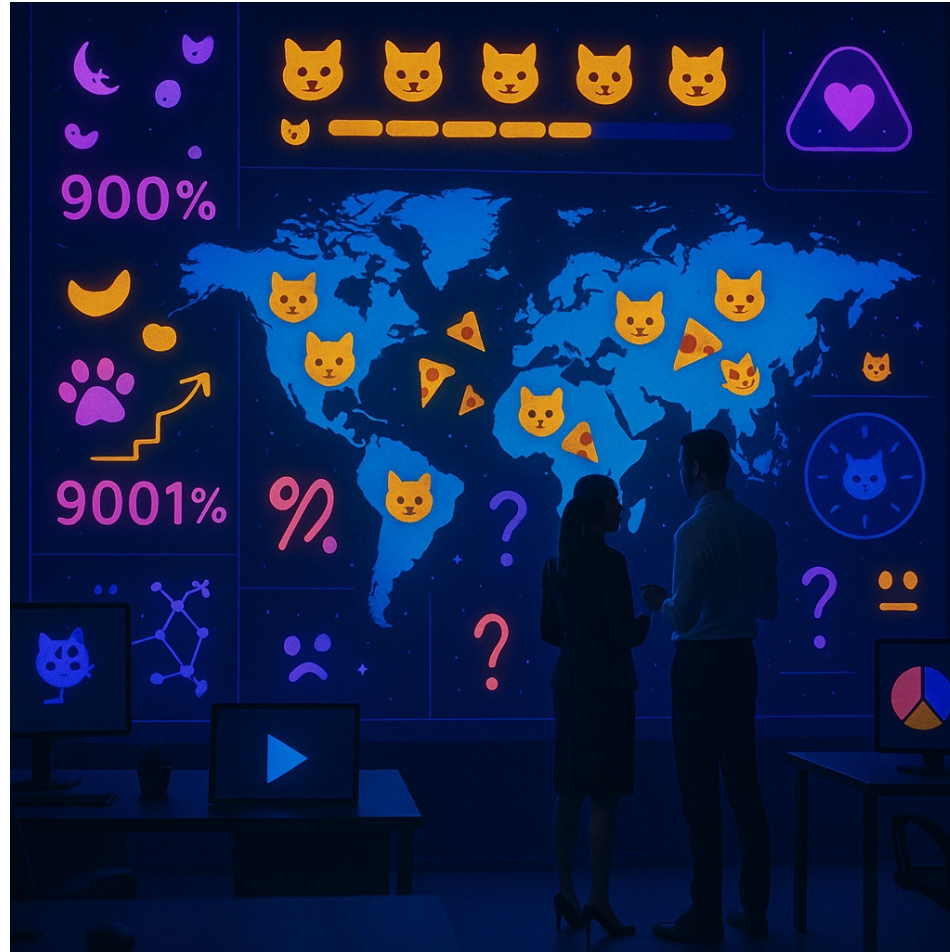


Welcome to Cybersecurity!



Word of the day

NINETY-NINETY RULE n. "The first 90% of the code accounts for the first 90% of the development time. The remaining 10% of the code accounts for the other 90% of the development time."

- PHP readfile(): read a file and write its contents directly to the output

thumbnailer.php?name=kitten.jpeg

- PHP readfile(): read a file and write its contents directly to the output

...

```
readfile($name);
```

...

thumbnailer.php?name=kitten.jpeg

- PHP `readfile()`: read a file and write its contents directly to the output

...

```
readfile('images/' . $name);
```

...

Questions

- What files should we look for?

Questions

- How can we tell if an API is vulnerable?
- <http://165.227.36.197:8080/cool.php>

Users

- Stored in /etc/passwd
- What files can I access?
- What processes can I modify?
- What hardware can I access?

Groups

- Stored in /etc/group
- Every user has at least one
 - E.g., jeffrey in “jeffrey” group
- File and hardware access control
- Examples: cdrom, wireshark, sudo

UIDs/GIDs

- Unix system calls reference users/groups by ID
- Convention:
 - Lower numbers → services
 - Higher numbers → people

root

- Superuser
- `uid == gid == 0`
- Different concept than /

Files

- /etc/passwd → accounts
- /etc/shadow → passwords (hashed)
- /etc/group → group membership

Real vs. effective ID

- Effective → used to determine access
- Real → used to determine what you can set your ID to
- You can only set your effective ID to either your real ID or your effective ID
 - Exception: ?

Real vs. effective ID

- Effective → used to determine access
- Real → used to determine what you can set your ID to
- You can only set your effective ID to either your real ID or your effective ID
 - Exception: root

When are they different?

- Temporarily dropping privileges (e.g., FTP server)
- Temporarily elevating privileges (e.g., setuid root binary)

Important commands

- whoami
- groups
- su
- sudo

Important commands

- `id -u -r` → real UID
- `id -u` → effective UID
- `id -g -r` → real GID
- `id -g` → effective GID

File permissions

```
$ ls -l
```

drwx-----	18	jeffrey jeffrey	4096	Aug 21	2024	moreimages
drwxr-xr-x	12	jeffrey jeffrey	4096	Aug 22	2024	public_html
-rw-----	1	jeffrey jeffrey	14341	Aug 23	2024	kitten.jpeg
-rwx-----	1	jeffrey jeffrey	21312	Aug 24	2024	exploit

Important commands

- `chmod` → change file permissions
- `chown` → change file ownership
- `ls -l` → show file permissions and ownership

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
-rw-----  18 jeffrey jeffrey    4096 Aug 21  2024 kitten.jpeg
```

```
$ cat kitten.jpeg
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
-rw-----  18 jeffrey jeffrey    4096 Aug 21  2024 kitten.jpeg
```

```
$ cat kitten.jpeg 
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
-rw-----  18 root  jeffrey    4096 Aug 21  2024  kitten.jpeg
```

```
$ cat kitten.jpeg
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
-rw-----  18 root  jeffrey  4096 Aug 21  2024 kitten.jpeg
```

```
$ cat kitten.jpeg ❌
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
-rw-rw----  18 root  jeffrey  4096 Aug 21  2024  kitten.jpeg
```

```
$ cat kitten.jpeg
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
-rw-rw----  18 root    jeffrey    4096 Aug 21  2024 kitten.jpeg
```

```
$ cat kitten.jpeg 
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
-rw-rw----  18 root  student    4096 Aug 21  2024  kitten.jpeg
```

```
$ cat kitten.jpeg
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
-rw-rw----  18 root  student      4096 Aug 21  2024  kitten.jpeg
```

```
$ cat kitten.jpeg 
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
-rw-rw----  18 root    root      4096 Aug 21  2024 kitten.jpeg
```

```
$ cat kitten.jpeg
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
-rw-rw----  18 root    root      4096 Aug 21  2024 kitten.jpeg
```

```
$ cat kitten.jpeg ❌
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
-rw-rw-rw-  18 root    root    4096 Aug 21  2024 kitten.jpeg
```

```
$ cat kitten.jpeg
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
-rw-rw-rw-  18 root    root    4096 Aug 21  2024 kitten.jpeg
```

```
$ cat kitten.jpeg 
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
-rw-rw----  18 jeffrey jeffrey    4096 Aug 21  2024 exploit
```

```
$ cat exploit
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
-rw-rw----  18 jeffrey jeffrey    4096 Aug 21  2024 exploit
```

```
$ cat exploit 
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
-rw-rw-rw-  18 jeffrey jeffrey  4096 Aug 21  2024 exploit
```

```
$ ./exploit
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
-rw-rw-rw-  18 jeffrey jeffrey  4096 Aug 21  2024 exploit
```

```
$ ./exploit 
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
d--x----- 18 jeffrey jeffrey 4096 Aug 21 2024 moreimages
```

```
$ ls -l moreimages
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
d--x----- 18 jeffrey jeffrey 4096 Aug 21 2024 moreimages
```

```
$ ls -l moreimages ❌
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
dr-x----- 18 jeffrey jeffrey 4096 Aug 21 2024 moreimages
```

```
$ ls -l moreimages
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
dr-x-----  18 jeffrey jeffrey    4096 Aug 21  2024 moreimages
```

```
$ ls -l moreimages 
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
dr----- 18 jeffrey jeffrey 4096 Aug 21 2024 moreimages
```

```
$ ls -l moreimages
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
dr----- 18 jeffrey jeffrey 4096 Aug 21 2024 moreimages
```

```
$ ls -l moreimages 
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
dr----- 18 jeffrey jeffrey 4096 Aug 21 2024 moreimages
```

```
$ ls -l moreimages
```

```
-r----- 18 jeffrey jeffrey 4096 Aug 21 2024 barf
```

```
$ cat moreimages/barf
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
dr----- 18 jeffrey jeffrey 4096 Aug 21 2024 moreimages
```

```
$ ls -l moreimages
```

```
-r----- 18 jeffrey jeffrey 4096 Aug 21 2024 barf
```

```
$ cat moreimages/barf ❌
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
d--x----- 18 jeffrey jeffrey 4096 Aug 21 2024 moreimages
```

```
$ ls -l moreimages/barf
```

```
-r----- 18 jeffrey jeffrey 4096 Aug 21 2024 barf
```

```
$ cat moreimages/barf
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
d--x----- 18 jeffrey jeffrey 4096 Aug 21 2024 moreimages
```

```
$ ls -l moreimages/barf
```

```
-r----- 18 jeffrey jeffrey 4096 Aug 21 2024 barf
```

```
$ cat moreimages/barf 
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
---rwxrwx  18 jeffrey jeffrey    4096 Aug 21  2024 kitten.jpeg
```

```
$ cat kitten.jpeg
```

Can I do it?

```
$ whoami
```

```
jeffrey
```

```
$ groups
```

```
jeffrey student
```

```
$ ls -l
```

```
---rwxrwx  18 jeffrey jeffrey    4096 Aug 21  2024 kitten.jpeg
```

```
$ cat kitten.jpeg  !?!
```

Back to passwords...

- How can we measure the strength of a password generator?
- ***Entropy***

Information theory



Information theory

- An event's information: the amount of “surprise” we have from learning that outcome
 - It's sunny today in Phoenix → low information
 - It's raining today in Phoenix → high information

Information theory

- If I roll a 6-sided die, do I learn more information than if I flip a coin?
- What about if I learn an 8 letter alphabetic password (a...z) vs. a 6 character alphanumeric (a...z, 0...9)?
- Entropy: ***expected*** information

Probability theory

- A random variable X is a function mapping events to numbers
- Consider rolling a die...
- Events: $\{1, 2, 3, 4, 5, 6\}$
- Let X = the outcome of rolling a six-sided die
- $\Pr(X = 4) = 1/6$, $\Pr(X \text{ is even}) = 1/2$

$$E(X) = \sum_i p(x_i)x_i$$

So for a die roll...

$$E(X) = \sum_i p(x_i)x_i$$

$$= \sum_{i=1}^6 p(i)i$$

$$= \frac{1}{6} \sum_{i=1}^6 i$$

$$= 3.5$$

Information (in bits)

$$I(x_i) = -\log_2(p(x_i))$$

So for a roll of a die...

$$I(1) = \dots = I(6) = -\log_2(1/6).$$

Coin flip?

- More or less information than a roll of the die?

← Undo

Programming ▼



$-\log_2(1 \div 6)$

=

2.584962501

2.584962501|

Decimal ▼

0₈ = 0₁₆

63 0000 0000 0000 0000 48
47 0000 0000 0000 0000 32
31 0000 0000 0000 0000 16
15 0000 0000 0000 0000 0

C

(

)

mod

n

↓n

↑n

<< ▼

>> ▼

XOR

C

D

E

F

÷

√

ones

twos

NOT

AND

OR

8

9

A

B

×

.

x^y

x^{-1}

int

$\log_2$

log

4

5

6

7

-

=

$x!$

$|x|$

frac

á

0

1

2

3

+

x ▼

fact

64-bit ▼

Coin flip?

- Hint: we measure information in bits.

← Undo

Programming ▼



$-\log_2(1 \div 2)$

=

1

1|

Decimal ▼

1₈ = 1₁₆

63	0000	0000	0000	0000	48
47	0000	0000	0000	0000	32
31	0000	0000	0000	0000	16
15	0000	0000	0000	0001	0

C

(

)

mod

n

↓n

↑n

<< ▼

>> ▼

XOR

C

D

E

F

÷

√

ones

twos

NOT

AND

OR

8

9

A

B

×

.

x^y

x^{-1}

int

$\log_2$

log

4

5

6

7

-

=

$x!$

$|x|$

frac

á

0

1

2

3

+

x ▼

fact

64-bit ▼

Weather in Seattle

- $p(\text{rainy}) = 9/10$
- $p(\text{sunny}) = 1/10$
- Which outcome (rainy / sunny) would give us more information?

← Undo

Programming ▼



$-\log_2(9 \div 10)$

=

0.152003093

0.152003093|

Decimal ▼

0₈ = 0₁₆

63 0000 0000 0000 0000 48
47 0000 0000 0000 0000 32
31 0000 0000 0000 0000 16
15 0000 0000 0000 0000 0

C

(

)

mod

n

↓n

↑n

<< ▼

>> ▼

XOR

C

D

E

F

÷

√

ones

twos

NOT

AND

OR

8

9

A

B

x

.

x^y

x^{-1}

int

$\log_2$

log

4

5

6

7

-

=

x!

|x|

frac

á

0

1

2

3

+

x ▼

fact

64-bit ▼

← Undo

Programming ▼



$-\log_2(1 \div 10)$

=

3.321928095

3.321928095|

Decimal ▼

0₈ = 0₁₆

63 0000 0000 0000 0000 48
47 0000 0000 0000 0000 32
31 0000 0000 0000 0000 16
15 0000 0000 0000 0000 0

C

(

)

mod

n

↓n

↑n

<< ▼

>> ▼

XOR

C

D

E

F

÷

√

ones

twos

NOT

AND

OR

8

9

A

B

x

.

x^y

x^{-1}

int

$\log_2$

log

4

5

6

7

-

=

$x!$

$|x|$

frac

á

0

1

2

3

+

x ▼

fact

64-bit ▼

Entropy (in bits)

$$\begin{aligned} H(X) &= E(I(X)) \\ &= E(-\log_2 p(X)) \\ &= -\sum_i p(x_i) \log_2 p(x_i) \end{aligned}$$

Entropy of a coin flip

$$\begin{aligned} H(X) &= E(I(X)) \\ &= E(-\log_2 p(X)) \\ &= -\sum_i p(x_i) \log_2 p(x_i) \\ &= -\frac{1}{2} \log_2 \frac{1}{2} - \frac{1}{2} \log_2 \frac{1}{2} \\ &= 2\left(-\frac{1}{2} \log_2 \frac{1}{2}\right) \\ &= 1. \end{aligned}$$

Entropy of a die roll

$$\begin{aligned} H(X) &= E(I(X)) \\ &= E(-\log_2 p(X)) \\ &= -\sum_i p(x_i) \log_2 p(x_i) \\ &= 6\left(-\frac{1}{6} \log_2 \frac{1}{6}\right) \\ &\approx 2.58. \end{aligned}$$

Shortcut!

- When the probability of each outcome is equal, then we have that, for all x_i ,

$$I(x_i) = H(X).$$

Why called entropy?

- John von Neumann: “Call it entropy for two reasons: (1) the same function is already used in statistical mechanics under that name; and (2) nobody really knows what entropy is, so in a debate you’ll always have the advantage.”
- (Apocryphal...)

Why called entropy?

$$\begin{aligned} H(X) &= E(I(X)) \\ &= E(-\log_2 p(X)) \\ &= -\sum_i p(x_i) \log_2 p(x_i) \end{aligned}$$

In physics, Gibbs–Boltzmann entropy

$$S = -k \sum_i p(x_i) \log_e p(x_i).$$

Passwords

- Same as coin flips / die rolls but larger numbers
- We can calculate the entropy of password generators
- 8 random lowercase letters?
- 6 random, lowercase alphanumerics?



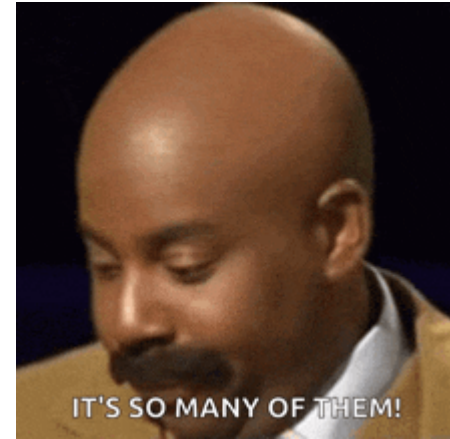
Only a fool asks what is the entropy of a password.

Entropy of a password?

- Passwords have *information content*
- Password generators have *entropy*

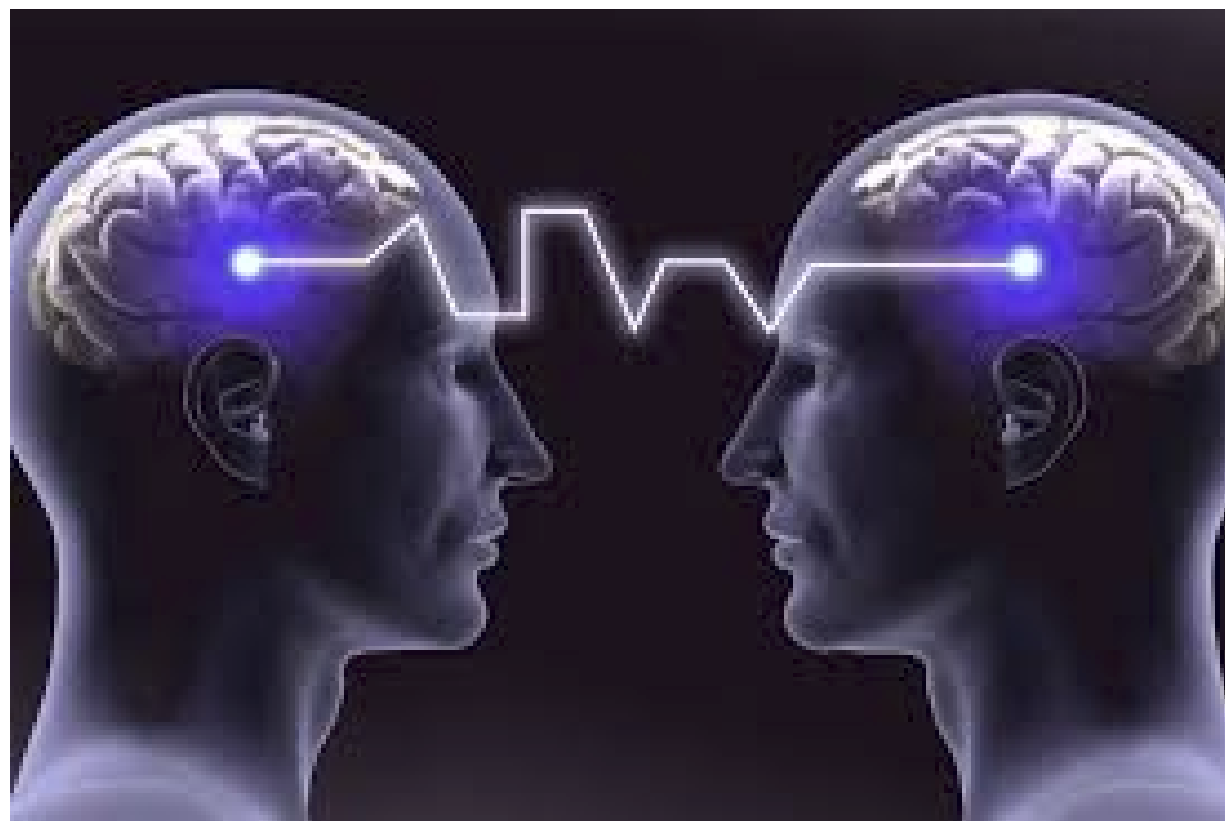
Generating phrases?

- YesterdayInTodayGreaterGood
- So long! Super secure?



Kerckhoffs's principle

- A security system should be secure, even if everything about the system, except the key (or password), is public knowledge.
- In other words: your secret should not be the algorithm

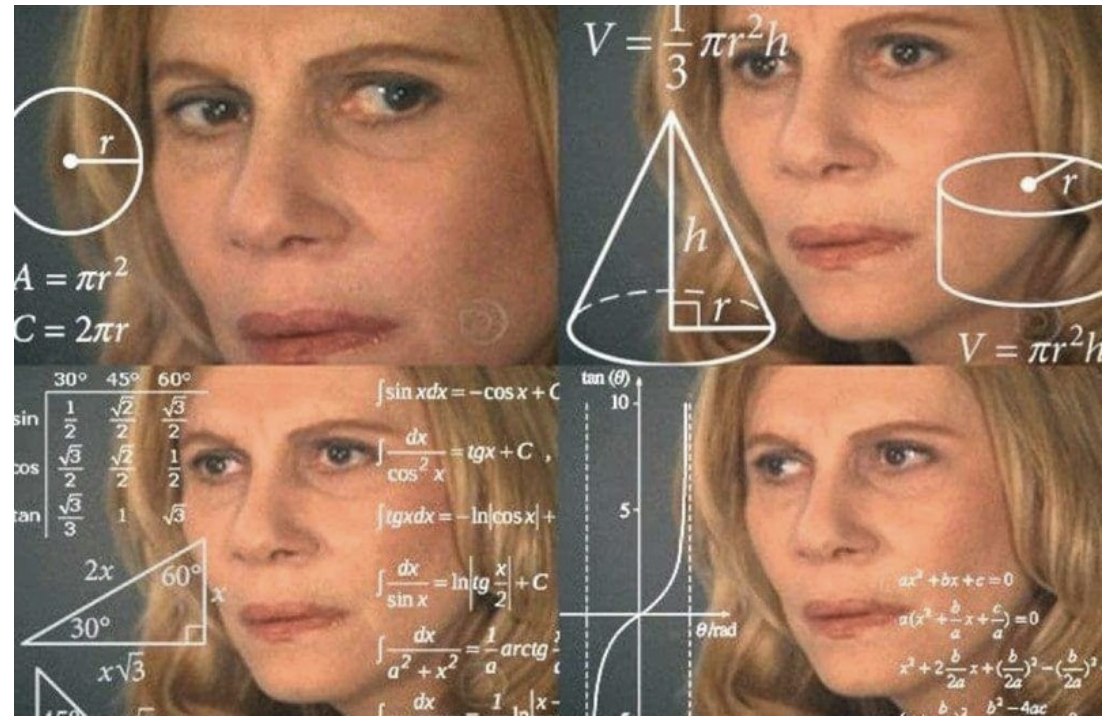


Entropy of a password?

- Assume each word is chosen from dictionary of 2000.
- And there are 5 words in the phrase.
- What is the entropy of this generator?

Entropy vs. memorability

- Entropy unfortunately corresponds roughly to memorability



Assignment 0

- Deadline: September 9, 2025, 10:00pm
- Set up Slack, read Syllabus, etc.
- <https://tildesites.bowdoin.edu/~j.knockel/csci3330f25/assignment0.pdf>