Jurassic Passwords

No Thesaurus Necessary

davie @ LayerOne 2023

https://www.textstudio.com/logo/jurassic-park-logo-873

Who, me?

Network Engineer

Infosec Adjacent

ShellCon

Reverse Shell Corp

WRCCDC

3D Printing & LEGO Technic Addict

Twitter: @daschu117

@ me on the LayerOne Discord: @davie#0001

ShellCon.io
Hack. Share. Include. Grow.

https://shellcon.io/

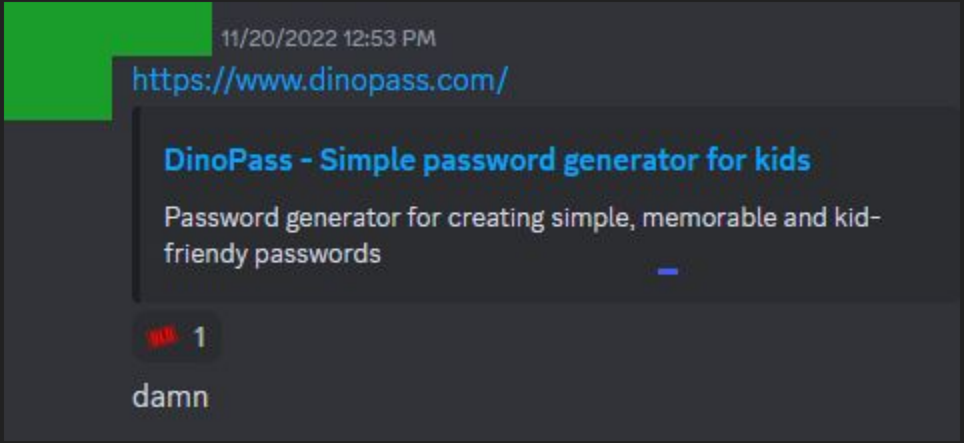
RSC

https://revshellcorp.org/

WESTERN REGIONAL COLLEGIATE CYBER DEFENSE COMPETITION

https://wrccdc.org/

Just hanging out on Discord



[redacted] 11/20/2022 12:53 PM

https://www.dinopass.com/

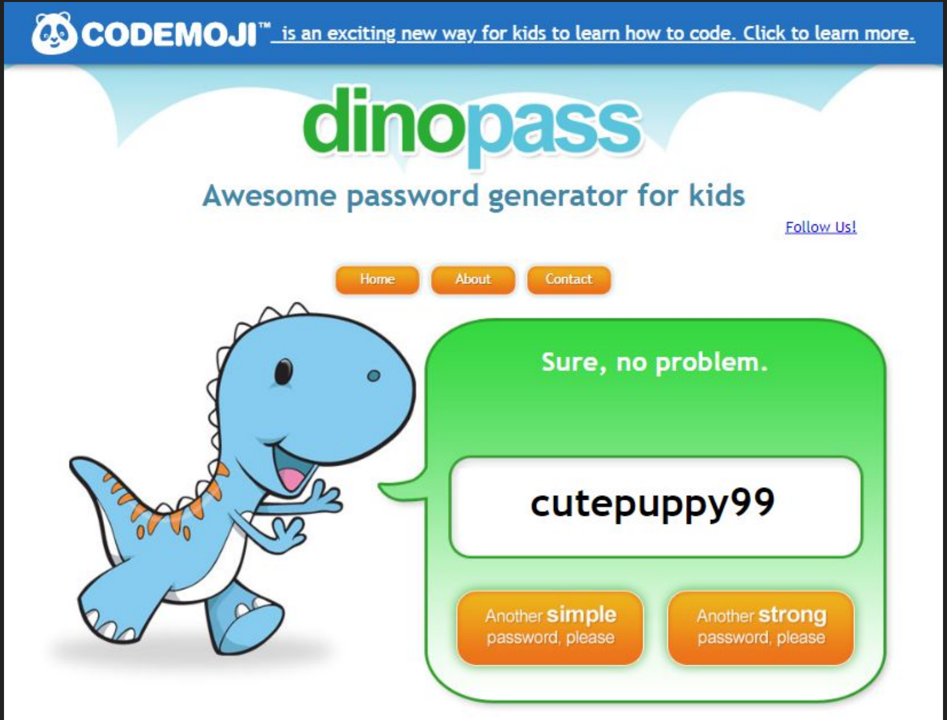
DinoPass - Simple password generator for kids

Password generator for creating simple, memorable and kid-friendy passwords

1

damn

Welcome to Jurassic Pa….. sswords



CODEMOJI™ is an exciting new way for kids to learn how to code. Click to learn more.

dinopass

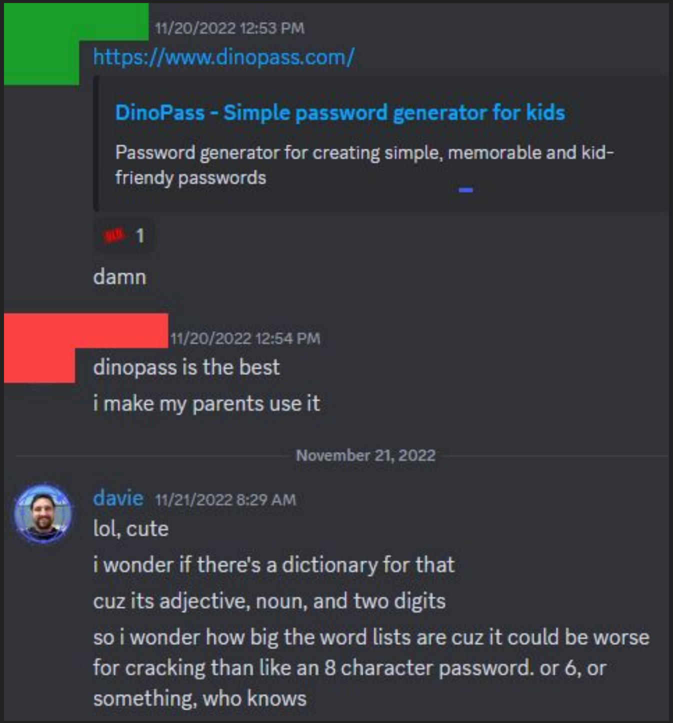
Awesome password generator for kids

Sure, no problem.

cutepuppy99

Follow Us!
Home
About
Contact
Another simple password, please
Another strong password, please

"I make my parents use it"



[redacted] 11/20/2022 12:53 PM

https://www.dinopass.com/

DinoPass - Simple password generator for kids

Password generator for creating simple, memorable and kid-friendy passwords

1

damn

[redacted] 11/20/2022 12:54 PM

dinopass is the best

i make my parents use it

November 21, 2022

davie 11/21/2022 8:29 AM

lol, cute

i wonder if there's a dictionary for that

cuz its adjective, noun, and two digits

so i wonder how big the word lists are cuz it could be worse for cracking than like an 8 character password. or 6, or something, who knows

Disclaimers

I have no affiliation with Dinopass.

Dinopass doesn’t claim to generate secure passwords.

Use a password manager to generate and store good random passwords.

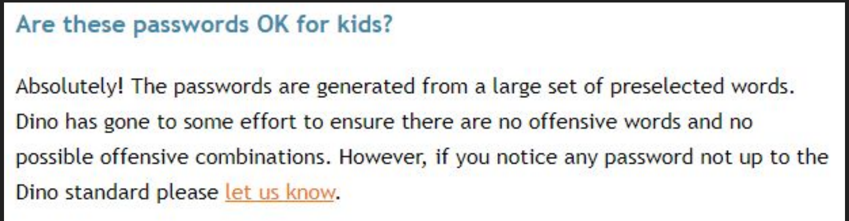
Don’t reuse passwords across services.

Use 2FA everywhere you can.

Prioritize longer and random passwords on email, banking, social media, and password managers.

Welcome to Jurassic Pa….. sswords

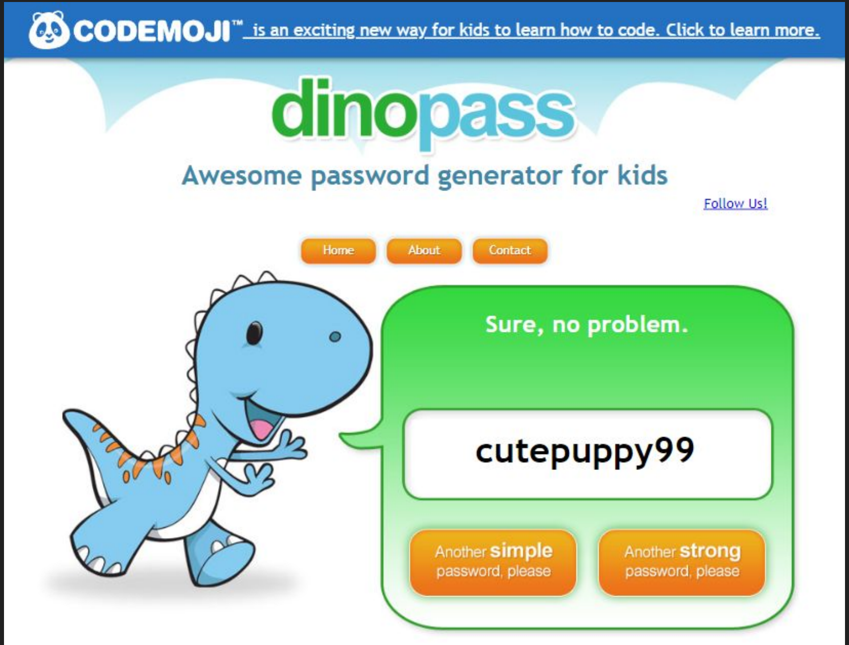
- Generates a simple password just for visiting the site
- Easily get more simple passwords
- Can ask for a strong password, but it’s not the default
- Rate limit of ~35, but clears on page refresh



Are these passwords OK for kids?

Absolutely! The passwords are generated from a large set of preselected words. Dino has gone to some effort to ensure there are no offensive words and no possible offensive combinations. However, if you notice any password not up to the Dino standard please let us know.

https://dinopass.com/



CODEMOJI™ is an exciting new way for kids to learn how to code. Click to learn more.

dinopass

Awesome password generator for kids

Sure, no problem.

cutepuppy99

Follow Us!
Home
About
Contact
Another simple password, please
Another strong password, please

https://dinopass.com/

Some Dinopasswords

itchyanimal70
palejaguar16
ivoryriver82
poorseal73
poorgiraffe53
fuzzyfinch77
braveiguana38
wisecircle59
bigseal48
superowl46
luckyrhino25
meganumber78
mushybaboon61
slowapple26
fancyhorse66
noisyearth87
bigsea60
cutepencil67
wackymetal35
fancycoral72

emptytest39
olivelight45
dizzyhorn17
superboo18
whiteyak52
thinweasel80
wildwhale47
greensoda35
superrat99
heavyhair63
loudlynx73
luckyjam25
flatbean56
blackmoney43
limeearth45
wisemark88
windywolf10
funnygopher15
luckyglass99
lazynose41

lushsnake21
cuteedge50
firsterror19
emptyjam45
quickchalk61
longbike93
messyice47
goldraccoon28
goldbeam48
weirdcircle65
quickblob34
busyram62
wackypotato26
keengoat52
angryjelly22
richwheel25
roundgate97
busystar27
uglygame61
tallferret58

slimyclass48
slowgoat10
nicebat23
busyiron77
freshferret28
mushymuskrat92
blueboot28
angrydrum13
bestwax23
happyllama48
smallname70
thintooth12
blackengine44
supergorilla14
bluerose98
mushysoup80
happyedge78
heavypatch83
hotsalt97
smallpark28

cutewombat57
sadboot81
tinyivory26
smartwing99
jumpycow88
newbuffalo25
giantmist23
jollyball92
jadefang13
poorlake15
weirdwax51
palepony13
oddwalrus98
messyraccoon92
spicypet30
braveplay36
mistybrown55
calmeye40
tallchalk61
jadefish18

scarywheel96
brownline95
emptypanda91
swiftcard28
keenhamster23
superbeam11
smallfly89
jumpyamber41
longtiger95
crazywing74
jollysheep73
bestcoyote66
smallmoon26
heavyfire12
itchybrick57
lushsea86
jadefact37
sweetpanda78
olivelunch53
shortcheetah15

greencanary38
quickcamp22
redbike80
crazydirt22
firsthouse28
weirdlight65
busyhouse21
amberink41
bumpycopper74
mushyisland65
heavydoor12
brownox30
smalllizard64
scarymatch39
fuzzystory12
ivorycamel77
cutekey24
busysoda20
bluesummer73
goodforce77

Anatomy of a Dinopass

- 1x Adjective
  - amber, brown, busy, cute, ivory
- 1x Noun
  - camel, puppy, chess, rose, muskrat
- 2x Digits
  - 00-99

cute puppy 99

adjective noun digits

https://www.rawpixel.com/image/6259252/png-sticker-vintage

It's a UNIX System! I know this!

- All the following code and snippets are written in Bash script
- Python might be better, but Bash was faster for me to write
- The CLI programs I used:
  - **`sed`**: for removing and replacing characters
  - **`grep`**: for finding matching lines
  - **`sort`**: sorting alphabetically
  - **`sort -u`**: sorting and removing duplicates
  - **`sort -h`**: sorting by human readable numbers
  - **`uniq -c`**: counting the number of duplicates
  - **`wc -l`**: counting the number of lines
  - **`curl`**: connecting to the Dinopass API
  - **`openssl passwd -apr1 -stdin`**: create a password hash from the input
  - **`john`**: a password cracking tool
  - **`hashcat`**: a password cracking tool

Session Show Display Directory File
Help
fsn: a 3D File System Navigator
festival.rgb
peach-scr2.rgb

Spielberg, Steven. *Jurassic Park*. Universal Pictures, 1993

Digging up bones

```
while true; do
     curl -s https://www.dinopass.com/password/simple
     echo
done | tee -a dinopass.txt
```

- Not rate-limited, but is slow
- ~400ms per response
- Let that run for like 2 weeks
- 3.5 million passwords generated
- 41MB

https://commons.wikimedia.org/wiki/File:Spinophorosaurus_digsite.jpg

They spared no expense!

- 3.5 million generated passwords
- Only 2.2 million uniques
- 7 exact passwords showed up 10 times

```
calmsystem33
cutekite86
cutemuskrat99
limesystem99
longreptile99
supersand99
zanyscale97
```

- 4 end with "99"?
- 2 start with "cute"?

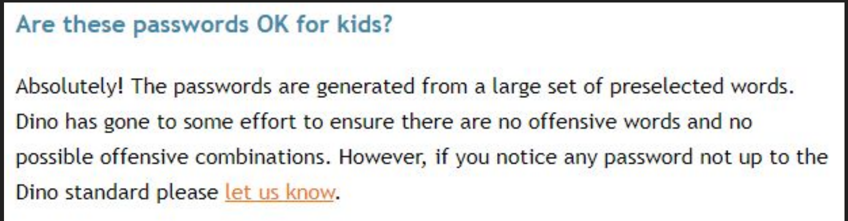
- What happens if we ignore the digits?:
  - `sed -e 's/[[:digit:]]//g' | sort -u | wc -l`
  - Only 37960 unique combinations of adjectives and nouns
  - The most frequent duplicates start with "cute"
  - Actually, the 365 most duplicated words all start with "cute"

Spielberg, Steven. *Jurassic Park*. Universal Pictures, 1993

Well that's cute…

```
152 cutewool
153 cutebrick
153 cuteship
157 cutenumber
158 cuteapple
158 cutebrown
158 cutegrape
158 cutestory
159 cutesign
160 cutedirt
160 cutegopher
160 cutesea
161 cutebear
161 cutequeen
163 cutecoyote
163 cutedrum
163 cutehyena
163 cutenest
164 cuteerror
164 cutefarm
164 cuteice
164 cutelamb
164 cutestone
164 cutewind
165 cutelook
166 cuteend
166 cuteleaf
167 cuteday
167 cuteiron
167 cuteox
168 cutecoal
168 cutegame
168 cutenail
168 cuteraccoon
168 cutered
168 cutetwist
169 cuteclam
169 cutemask
169 cutenight
170 cutedeer
170 cutefood
170 cutefrog
170 cutelake
170 cutelime
170 cutemustang
170 cutepet
170 cuteskunk
171 cutedonkey
171 cuteearth
171 cuteland
171 cutelemur
171 cutemice
171 cutenewt
171 cutepart
171 cutesnake
172 cutecheese
172 cutegiraffe
172 cutegnu
172 cutejaguar
172 cutekick
172 cutespring
173 cutechain
173 cutehat
173 cutemilk
173 cutenose
173 cutesteam
173 cutewar
173 cutewish
173 cuteyak
174 cuteant
174 cutebaboon
174 cutebike
174 cutebook
174 cutefeast
174 cuteferret
174 cutehamster
174 cutespark
174 cutewarthog
175 cutebell
175 cutedime
175 cutehelp
175 cutehen
175 cuteink
175 cutelamp
175 cutemist
175 cuteotter
175 cutestick
176 cutecougar
176 cutedust
176 cutepage
176 cutesand
176 cuteseed
176 cutesloth
177 cutecircle
177 cutedog
177 cutehook
177 cutejam
177 cutepanther
177 cutepatch
177 cutesneeze
177 cutewax
177 cutewhite
177 cuteworm
178 cuteblob
178 cutefeet
178 cutegrip
178 cuteleopard
178 cutelift
178 cuteram
178 cuterose
178 cutesnail
178 cutesquare
179 cuteboat
179 cuteface
179 cutefinch
179 cuteglass
179 cutelynx
179 cutemonster
179 cutepark
179 cuterain
179 cuteroll
179 cuteweasel
180 cuteamber
180 cutegrain
180 cutegrass
180 cutejeans
180 cuterabbit
180 cutevoice
181 cutecard
181 cutecoral
181 cutefawn
181 cutefoot
181 cuteisland
181 cutemass
181 cutenorth
182 cuteart
182 cutebone
182 cutebrain
182 cutebulb
182 cutebull
182 cutecave
182 cuteclass
182 cutefog
182 cutekoala
182 cutemonkey
182 cutemoon
182 cutenoise
182 cutereptile
183 cuteanimal
183 cutechalk
183 cutecheetah
183 cutedoor
183 cuteegg
183 cutefang
183 cuteflame
183 cutefruit
183 cuteheat
183 cutematch
183 cutemetal
183 cuteriver
183 cutesalmon
183 cutesugar
183 cutesystem
183 cutewalrus
184 cuteball
184 cutebutter
184 cutegoat
184 cutesmile
184 cutezebra
185 cuteberry
185 cutecap
185 cutecopper
185 cutefox
185 cuteknot
185 cutemint
185 cutemouse
185 cutepaste
185 cutepuma
185 cuteray
185 cutestamp
186 cuteboot
186 cutefork
186 cuteheart
186 cutescarf
186 cutesoup
186 cutetest
186 cutewood
187 cutehair
187 cutejoke
187 cutemagic
187 cutepaint
187 cutepotato
187 cutesmoke
187 cutesound
188 cutecloud
188 cuteeye
188 cuteflag
188 cutehoney
188 cutejuice
188 cutekitten
188 cutelunch
188 cutemonth
188 cutepig
188 cuterat
188 cuterobin
188 cutesheep
188 cuteturtle
189 cutegoose
189 cuteseal
189 cutesoda
190 cutebread
190 cutebutton
190 cutecow
190 cutehog
190 cutehouse
190 cutelace
190 cutepoint
190 cutesilver
190 cutetown
191 cuteangle
191 cutecake
191 cutedress
191 cutepaper
191 cutepuppy
191 cuterhino
191 cutespoon
191 cutestar
191 cutewire
191 cutewolf
192 cutecar
192 cuteghost
192 cutehall
192 cutejelly
192 cutellama
192 cutelock
192 cutemoose
192 cutemuskrat
192 cuteplay
192 cuterice
193 cutebean
193 cutecamp
193 cutecart
193 cutegorilla
193 cuteliquid
193 cutering
193 cuterock
193 cutewater
193 cutewombat
194 cutebuffalo
194 cuteglue
194 cutehill
194 cuteiguana
194 cutemark
194 cutepencil
194 cuteroad
194 cutesleep
194 cutetooth
194 cutewhale
195 cutebeam
195 cutebox
195 cuteclub
195 cutefish
195 cuteflock
195 cutehome
195 cuteindigo
195 cutejump
195 cutekey
195 cuteolive
195 cutescale
195 cuteshow
195 cutesoap
195 cutesun
195 cutewave
196 cuteewe
196 cutehorn
196 cutejewel
196 cutemind
196 cutename
196 cuteocean
196 cutepeach
196 cutepear
196 cutepie
196 cutepump
196 cuterule
196 cutetime
197 cutedingo
197 cutejade
197 cutepanda
197 cutestart
198 cutecorn
198 cuteengine
199 cutecat
199 cutecurve
199 cutedoe
199 cutehand
199 cutepurple
199 cuteview
200 cutecanary
200 cutefire
200 cuteflower
200 cutehorse
200 cutelead
200 cuteplant
200 cutesmash
200 cutetiger
201 cutebee
201 cutebird
201 cuteboo
201 cutefly
201 cutehare
201 cutelight
201 cuteowl
201 cuteshoe
202 cuteedge
202 cutekite
202 cutelizard
202 cutepail
202 cuteshape
202 cutespace
203 cuteivory
203 cutelion
203 cutesteel
203 cuteviolet
203 cutewing
204 cutemoney
205 cutebrass
205 cutechess
205 cuteloaf
205 cutemusic
205 cuteparrot
205 cutesnow
205 cutewinter
207 cutememory
207 cutesummer
207 cuteyear
208 cuteforce
209 cuteactor
209 cutealarm
209 cutebat
209 cutegeese
209 cutemusk
209 cutesky
210 cutespy
211 cutesong
211 cutetree
212 cutedugong
212 cutefact
212 cutegate
212 cutegazelle
212 cutejackal
212 cuteline
212 cutesalt
213 cutestop
214 cutecamel
214 cutesilk
215 cutething
216 cutewheel
217 cutebunny
217 cutehippo
218 cutepony
219 cutecrow
220 cuteroom
224 cuteplane
230 cutecrown
231 cutepink
```

Won't Somebody Please Think of the Children!

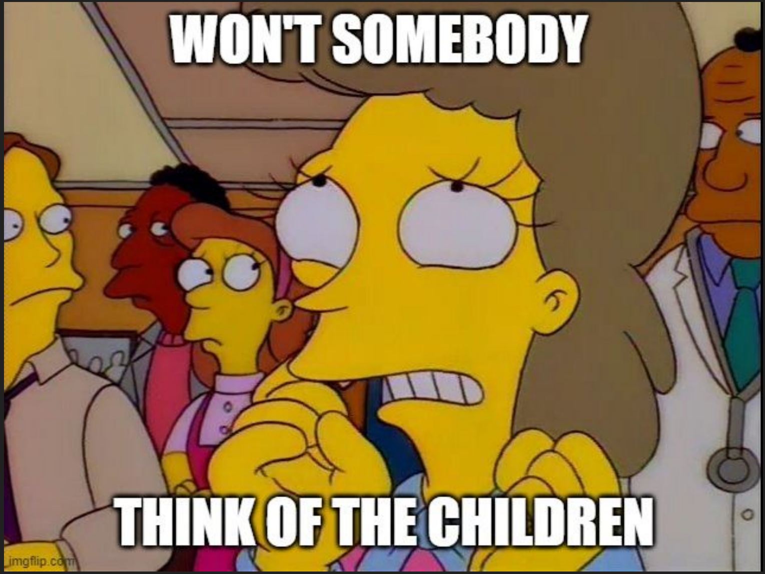


Are these passwords OK for kids?

Absolutely! The passwords are generated from a large set of preselected words. Dino has gone to some effort to ensure there are no offensive words and no possible offensive combinations. However, if you notice any password not up to the Dino standard please let us know.

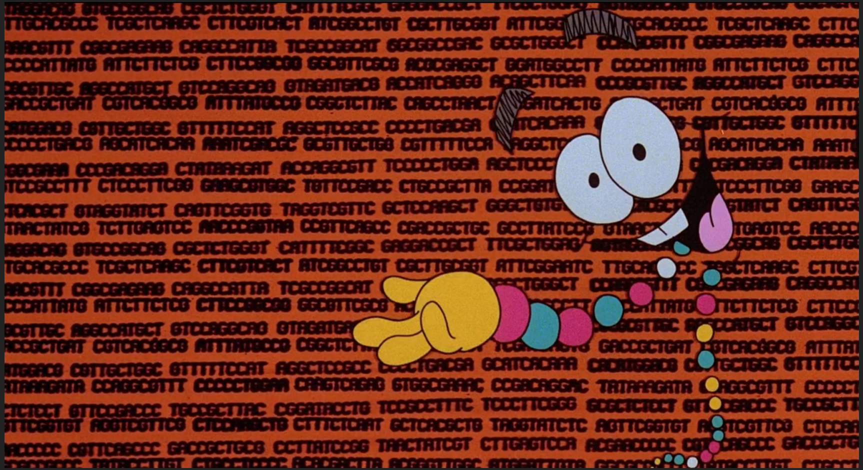
https://dinopass.com/

The dictionary probably isn't fully randomized in order to "ensure there are no offensive words and no possible offensive combinations."



https://imgflip.com/memegenerator/235699747/Wont-Somebody-Please-Think-of-the-Children

Finding the Numbers



Spielberg, Steven. *Jurassic Park*. Universal Pictures, 1993

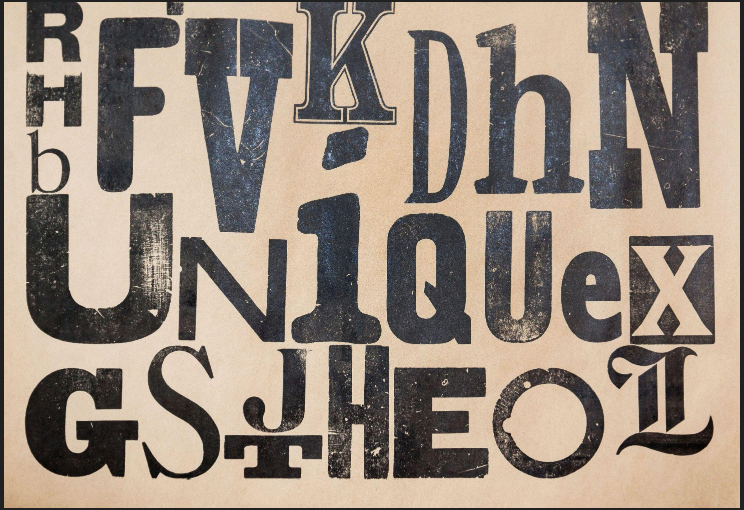
- Remove all alphabet characters from the passwords:
  - `sed -e 's/[[:alpha:]]//g' | sort -u | wc -l`
- Returns 89 combinations
- Save it in a file
  - `sed -e 's/[[:alpha:]]//g' | sort > numbers_only.txt`
- Analyze the entries:
  - `cat numbers.txt | uniq -c`

Numbers (89)

```
39532 10    39321 23    39129 36    39296 49    39775 62    39329 76    39539 89
39445 11    39708 24    39451 37    39858 50    39360 63    39480 77    39098 90
39075 12    39510 25    39245 38    39694 51    39059 64    39633 78    39689 91
39669 13    39292 26    39397 39    39317 52    39278 65    39357 79    39453 92
39525 14    39198 27    39441 40    39336 53    39214 66    39782 80    39314 93
39504 15    39593 28    39319 41    39486 54    39398 67    39775 81    39405 94
39448 16    39443 29    39273 42    39048 55    39236 68    39436 82    39522 95
39447 17    39619 30    39472 43    39435 56    39574 70    39305 83    39321 96
39680 18    39717 31    39097 44    39524 57    39466 71    39677 84    39212 97
39440 19    39609 32    39810 45    39549 58    39546 72    39475 85    39600 98
39387 20    39462 33    39737 46    39351 59    39857 73    39833 86    78708 99
39459 21    39441 34    39591 47    39512 60    39753 74    39298 87
39496 22    39587 35    39421 48    39464 61    39348 75    39492 88
```

- 99: appears twice as often
- 00-09: Missing
- 69: Missing

Finding the Nouns



https://www.rawpixel.com/image/5920980/photo-image-public-domain-art-wood

1. "cute" is the most duplicated adjective
2. Let’s find all adjective-noun pairs that start with cute:
   ```
   grep '^cute' | sort -u | wc -l
   ```
3. Returns 365 combinations
4. Remove "^cute" to keep only nouns:
   ```
   grep '^cute' | sort -u | sed 's/^cute//'
   ```
5. Now we have 365 bare nouns
6. Save it in a file:
   ```
   grep '^cute' | sort -u | sed 's/^cute//'> nouns.txt
   ```

Nouns (365)

actor
alarm
amber
angle
animal
ant
apple
art
baboon
ball
bat
beam
bean
bear
bee
bell
berry
bike
bird
blob
boat
bone
boo
book
boot
box
brain
brass
bread
brick
brown
buffalo
bulb
bull
bunny
butter
button
cake
camel
camp
canary
cap
car
card
cart
cat
cave
chain
chalk
cheese
cheetah
chess
circle
clam
class
cloud
club
coal
copper
coral
corn
cougar
cow
coyote
crow
crown
curve
day
deer
dime
dingo
dirt
doe
dog
donkey
door
dress
drum
dugong
dust
earth
edge
egg
end
engine
error
ewe
eye
face
fact
fang
farm
fawn
feast
feet
ferret
finch
fire
fish
flag
flame
flock
flower
fly
fog
food
foot
force
fork
fox
frog
fruit
game
gate
gazelle
geese
ghost
giraffe
glass
glue
gnu
goat
goose
gopher
gorilla
grain
grape
grass
grip
hair
hall
hamster
hand
hare
hat
heart
heat
help
hen
hill
hippo
hog
home
honey
hook
horn
horse
house
hyena
ice
iguana
indigo
ink
iron
island
ivory
jackal
jade
jaguar
jam
jeans
jelly
jewel
joke
juice
jump
key
kick
kite
kitten
knot
koala
lace
lake
lamb
lamp
land
lead
leaf
lemur
leopard
lift
light
lime
line
lion
liquid
lizard
llama
loaf
lock
look
lunch
lynx
magic
mark
mask
mass
match
memory
metal
mice
milk
mind
mint
mist
money
monkey
monster
month
moon
moose
mouse
music
musk
muskrat
mustang
nail
name
nest
newt
night
noise
north
nose
number
ocean
olive
otter
owl
ox
page
pail
paint
panda
panther
paper
park
parrot
part
paste
patch
peach
pear
pencil
pet
pie
pig
pink
plane
plant
play
point
pony
potato
puma
pump
puppy
purple
queen
rabbit
raccoon
rain
ram
rat
ray
red
reptile
rhino
rice
ring
river
road
robin
rock
roll
room
rose
rule
salmon
salt
sand
scale
scarf
sea
seal
seed
shape
sheep
ship
shoe
show
sign
silk
silver
skunk
sky
sleep
sloth
smash
smile
smoke
snail
snake
sneeze
snow
soap
soda
song
sound
soup
space
spark
spoon
spring
spy
square
stamp
star
start
steam
steel
stick
stone
stop
story
sugar
summer
sun
system
test
thing
tiger
time
tooth
town
tree
turtle
twist
view
violet
voice
walrus
war
warthog
water
wave
wax
weasel
whale
wheel
white
wind
wing
winter
wire
wish
wolf
wombat
wood
wool
worm
yak
year
zebra

Finding the Adjectives

https://commons.wikimedia.org/wiki/File:Alphabet_Soup_-_8485913543.jpg

- Pick a noun like "puppy"
- Find all the adjective-noun pairs that end with "puppy":
  ```
  grep 'puppy$' | sort -u | wc -l
  ```
- Returns 104 combinations
- Remove "puppy$" to keep only adjectives:
  ```
  grep 'puppy$' | sort -u | sed 's/puppy$//'
  ```
- Save it in a file
  ```
  grep 'puppy$' | sort -u | sed 's/puppy$//' > adjectives.txt
  ```

Adjectives (104)

- amber
- angry
- bad
- bent
- best
- big
- black
- blue
- brave
- brown
- bumpy
- busy
- calm
- cold
- cool
- crazy
- curly
- **cute**
- damp
- dark
- dizzy
- empty
- fancy
- fast
- first
- flat
- free
- fresh
- funny
- fuzzy
- giant
- gold
- good
- gray
- great
- green
- happy
- heavy
- hot
- huge
- icy
- itchy
- ivory
- jade
- jazzy
- jolly
- jumpy
- keen
- kind
- lazy
- light
- lime
- long
- loud
- lucky
- lumpy
- lush
- mega
- messy
- misty
- muddy
- murky
- mushy
- new
- nice
- noisy
- odd
- old
- olive
- pale
- pink
- poor
- quick
- quiet
- red
- rich
- rose
- round
- sad
- scary
- shiny
- short
- silly
- slim
- slimy
- slow
- small
- smart
- spicy
- super
- sweet
- swift
- tall
- thin
- tiny
- ugly
- ultra
- wacky
- weird
- white
- wild
- windy
- wise
- zany

- Cute appears twice as likely as any other adjective

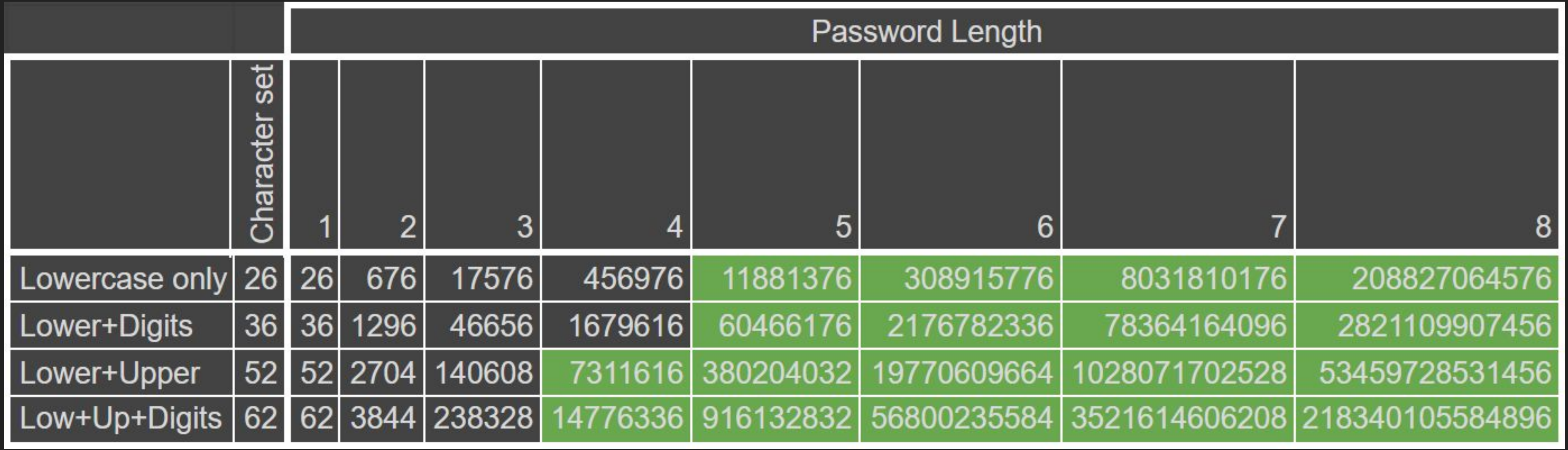
What we know so far

- Nouns: 365
  - All nouns appear about equally often
- Adjectives: 104
  - The adjective "cute" appears twice as often as any other adjective
- Numbers: 89
  - No passwords end in 00-09
  - No passwords end in 69
  - The digits 99 appears twice as often as any other set of digits
- Total adjective+noun combinations: 104*365 = 37960
- Total potential passwords: 104*365*89 = 3,378,440

$V = \frac{1}{3}\pi r^2 \cdot h$
h
r
sin
cos
tan
30°
45°
60°
$y = ax^2 + bx + c$
$(x_1, x_2) = \frac{-b \pm \Delta}{2a}$

https://knowyourmeme.com/memes/math-lady-confused-lady

Comparing password entropy



		Password Length							
	Character set	1	2	3	4	5	6	7	8
Lowercase only	26	26	676	17576	456976	11881376	308915776	8031810176	208827064576
Lower+Digits	36	36	1296	46656	1679616	60466176	2176782336	78364164096	2821109907456
Lower+Upper	52	52	2704	140608	7311616	380204032	19770609664	1028071702528	53459728531456
Low+Up+Digits	62	62	3844	238328	14776336	916132832	56800235584	3521614606208	218340105584896

Scenarios

- Ansible playbook setting user passwords stored in a public Git repo
- System backups that include /etc/shadow
- Application backups or DB dumps that contain user password hashes
- A dump of NTLM hashes
- An Apache .htpasswd file containing usernames and hashed passwords protecting a website with Basic Auth

Generating a .htpasswd file

```
#!/bin/bash
for name in alice bob charlie devon evan frank; do
  pass="$(curl -s https://dinopass.com/password/simple \
    | openssl passwd -stdin -apr1)"
  echo "${name}:${pass}"
done > shadow.txt
```

- The Apache "apr1" hash format is used in .htpasswd files to protect web directories.
- Here, we're generating a file to represent a file that you might accidentally find accessible on a website.

Generating the wordlist

```
#!/bin/bash
while read adjective; do
  while read noun; do
    for i in $(seq -w 10 68) $(seq -w 70 99) ; do
      echo ${adjective}${noun}${i}
    done
  done < nouns.txt
done < adjectives.txt > dinopass.wordlist
```

- This wordlist file contains the full 3,378,440 unique combinations possible

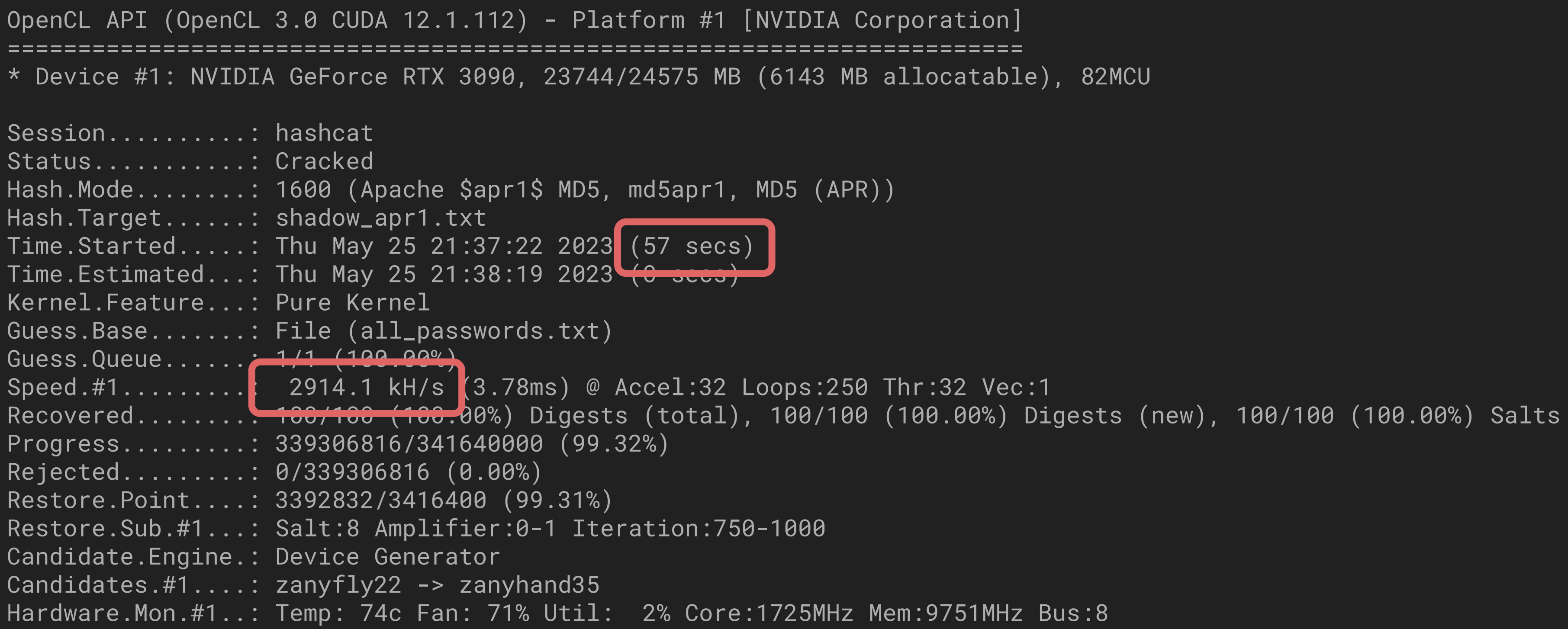
Running John The Ripper

```
john --format=md5crypt --wordlist=dinopass.wordlist shadow.txt
```

- **`md5crypt`**: tells john that the hashes are **`$apr1$`**

Live Demo

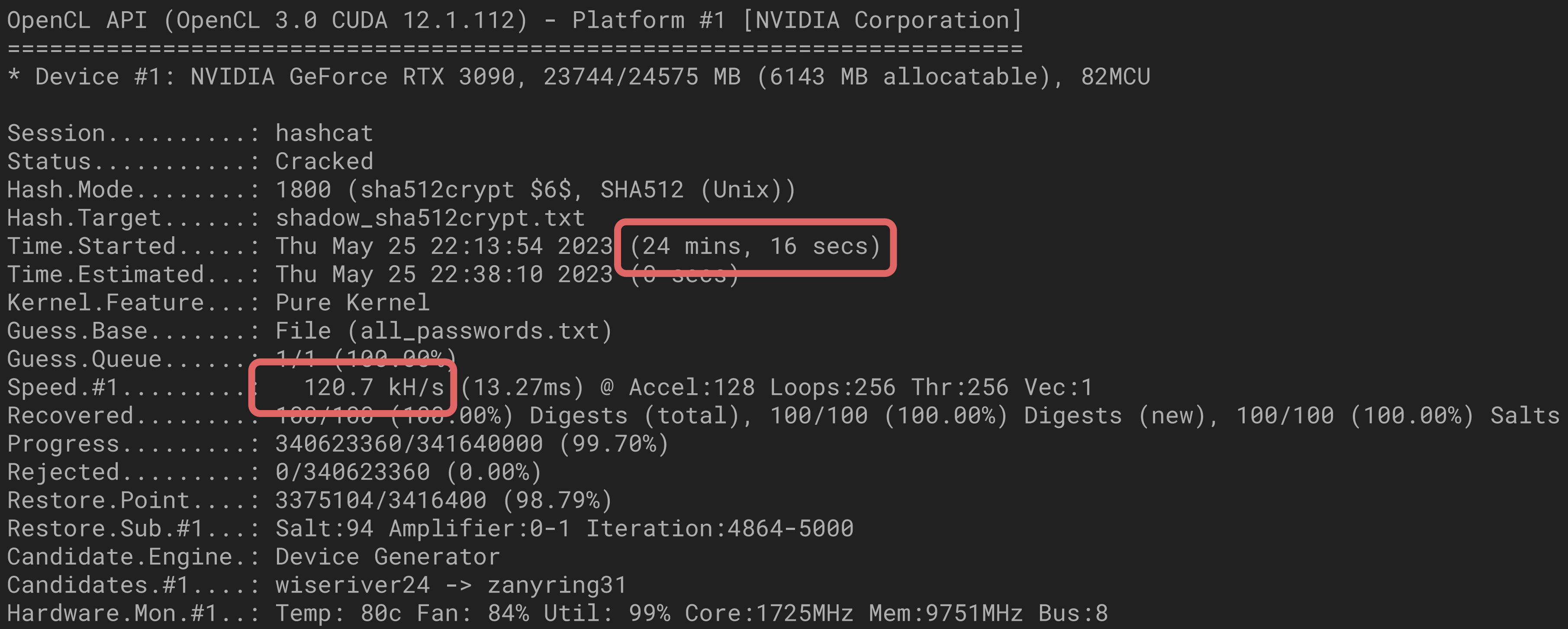
hashcat: apr1, 100 hashes, RTX3090



```
OpenCL API (OpenCL 3.0 CUDA 12.1.112) - Platform #1 [NVIDIA Corporation]
========================================================================
* Device #1: NVIDIA GeForce RTX 3090, 23744/24575 MB (6143 MB allocatable), 82MCU

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1600 (Apache $apr1$ MD5, md5apr1, MD5 (APR))
Hash.Target......: shadow_apr1.txt
Time.Started.....: Thu May 25 21:37:22 2023 (57 secs)
Time.Estimated...: Thu May 25 21:38:19 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (all_passwords.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2914.1 kH/s (3.78ms) @ Accel:32 Loops:250 Thr:32 Vec:1
Recovered........: 100/100 (100.00%) Digests (total), 100/100 (100.00%) Digests (new), 100/100 (100.00%) Salts
Progress.........: 339306816/341640000 (99.32%)
Rejected.........: 0/339306816 (0.00%)
Restore.Point....: 3392832/3416400 (99.31%)
Restore.Sub.#1...: Salt:8 Amplifier:0-1 Iteration:750-1000
Candidate.Engine.: Device Generator
Candidates.#1....: zanyfly22 -> zanyhand35
Hardware.Mon.#1..: Temp: 74c Fan: 71% Util:  2% Core:1725MHz Mem:9751MHz Bus:8
```

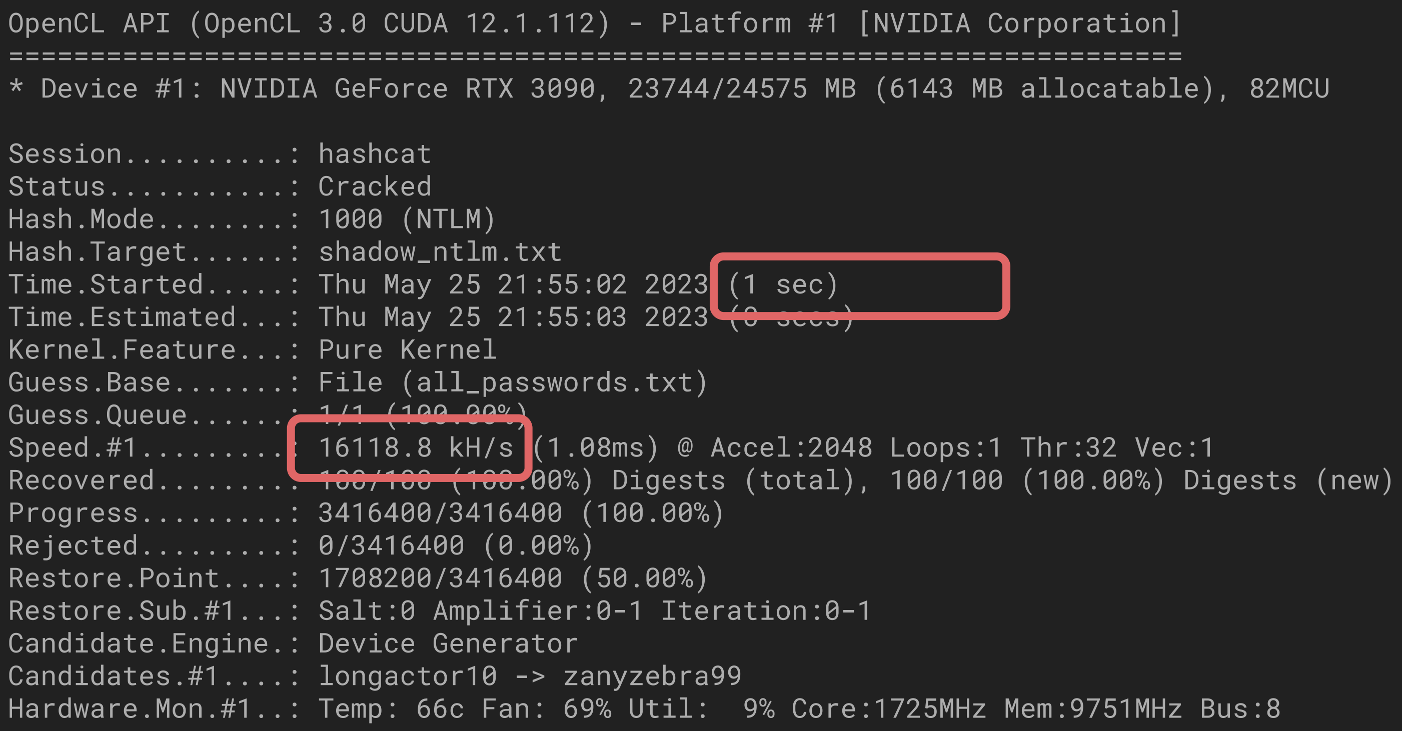
hashcat: sha512crypt, 100 hashes, RTX3090



```
OpenCL API (OpenCL 3.0 CUDA 12.1.112) - Platform #1 [NVIDIA Corporation]
========================================================================
* Device #1: NVIDIA GeForce RTX 3090, 23744/24575 MB (6143 MB allocatable), 82MCU

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: shadow_sha512crypt.txt
Time.Started.....: Thu May 25 22:13:54 2023 (24 mins, 16 secs)
Time.Estimated...: Thu May 25 22:38:10 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (all_passwords.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   120.7 kH/s (13.27ms) @ Accel:128 Loops:256 Thr:256 Vec:1
Recovered........: 100/100 (100.00%) Digests (total), 100/100 (100.00%) Digests (new), 100/100 (100.00%) Salts
Progress.........: 340623360/341640000 (99.70%)
Rejected.........: 0/340623360 (0.00%)
Restore.Point....: 3375104/3416400 (98.79%)
Restore.Sub.#1...: Salt:94 Amplifier:0-1 Iteration:4864-5000
Candidate.Engine.: Device Generator
Candidates.#1....: wiseriver24 -> zanyring31
Hardware.Mon.#1..: Temp: 80c Fan: 84% Util: 99% Core:1725MHz Mem:9751MHz Bus:8
```

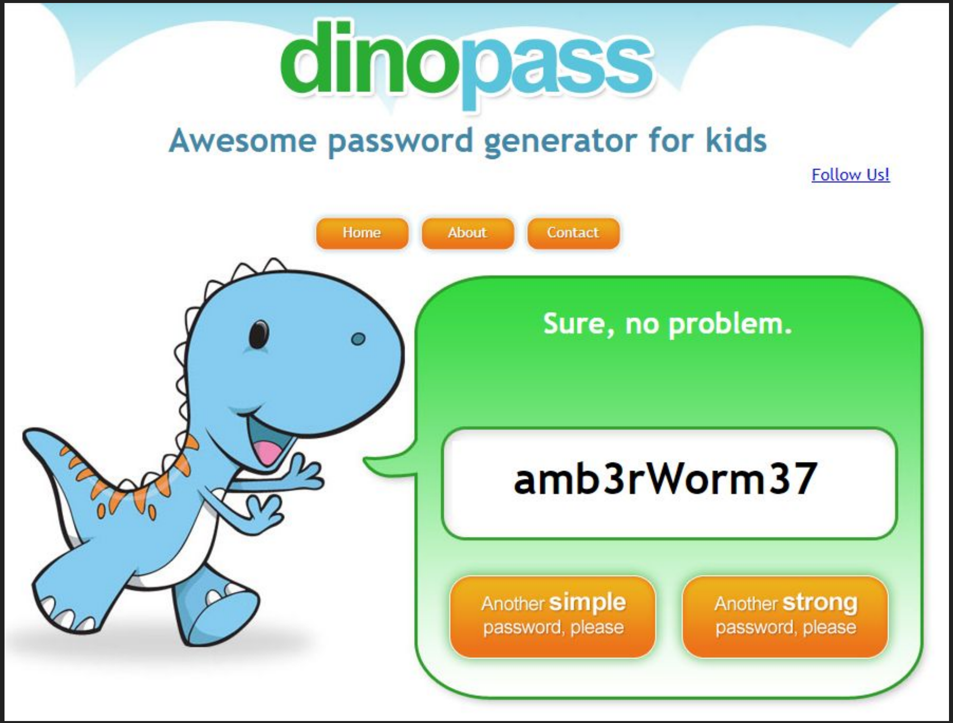
hashcat: NTLM, 100 hashes, RTX3090



```
OpenCL API (OpenCL 3.0 CUDA 12.1.112) - Platform #1 [NVIDIA Corporation]
========================================================================
* Device #1: NVIDIA GeForce RTX 3090, 23744/24575 MB (6143 MB allocatable), 82MCU

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: shadow_ntlm.txt
Time.Started.....: Thu May 25 21:55:02 2023 (1 sec)
Time.Estimated...: Thu May 25 21:55:03 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (all_passwords.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 16118.8 kH/s (1.08ms) @ Accel:2048 Loops:1 Thr:32 Vec:1
Recovered........: 100/100 (100.00%) Digests (total), 100/100 (100.00%) Digests (new)
Progress.........: 3416400/3416400 (100.00%)
Rejected.........: 0/3416400 (0.00%)
Restore.Point....: 1708200/3416400 (50.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: longactor10 -> zanyzebra99
Hardware.Mon.#1..: Temp: 66c Fan: 69% Util:  9% Core:1725MHz Mem:9751MHz Bus:8
```

What about Dinopass "Strong" Passwords?



dinopass
Awesome password generator for kids
Follow Us!
Home
About
Contact
Another simple password, please
Another strong password, please

Sure, no problem.

amb3rWorm37

https://dinopass.com/

Dinopass "Strong" Passwords

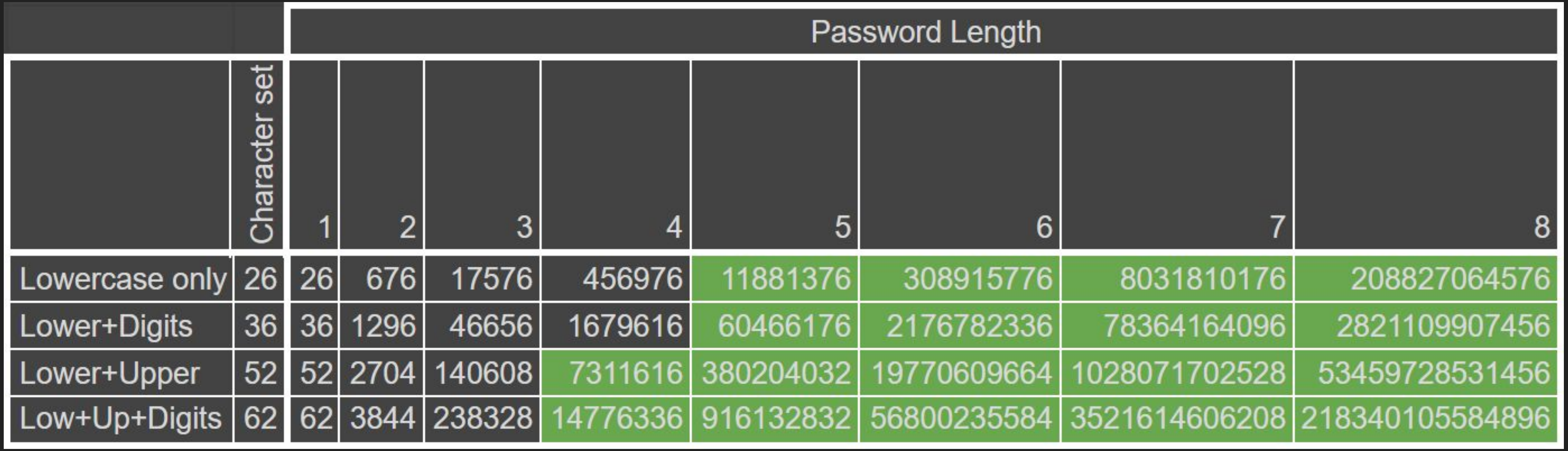
```
wac<yGrain91
3mptyActor52
ol)Spoon16
ol!veDingo98
$adMoon84
bumpyGnu45
dampT!me56
ros3Silver27
mu$hyFly82
ivoryP3ar59
j@zzyTooth37
o)dRoll15
blu3Rule33
coldSnee2e29
+hinPeach94
angryM3mory23
murkyRo$e41
!cyWire95
ho+Page26
)ampNoise94
gr@yCanary71
h3avyRose66
ben+Earth24
fancyP!g74
brownFeas+66
fla+Tooth52
sup3rMoose97
emp+yFlower62
slimNos348
sp!cyApple33
wil)Fog35
grayMe+al97
!cyCow16
qui(kGopher47
wac<yDrum31
ligh+Star79
k3enChain20
blu3Purple74
busySug@r17
roundP3t25
blac<Boo18
fla+Goat28
cut3Name39
h@ppySoda83
b3ntHorse47
goodLac387
swee+Zebra98
fre$hBeam51
gr@yCrown18
hug3View48
roun)Fox85
fl@tNest36
qui3tCrow44
we!rdAnimal88
cra2yWorm39
gi@ntMustang30
cuteH@ir37
noisySqu@re85
loudAr+59
=irstMemory33
goldLa<e63
j@deCoal13
!cyPink14
loudR!ng38
thinS3ed34
d@rkWolf82
w!ldGlue61
gr3atStar14
2anyCheetah36
greenSlo+h74
!tchyWheel65
mu)dyRabbit94
bu$yFork71
l!ghtWish59
whi+eLime11
$wiftIndigo52
gi@ntLamb30
w@ckyCrown53
$caryBrass70
cr@zyLamb12
s!llyCar66
no!syRay79
cu+eIsland31
limeZebr@84
pinkFoo+15
lou)Animal21
bigHoo<49
mushyCopp3r84
limeMil<30
cut3Wing45
h3avyLace22
goldP3ach36
z@nyHen19
s!llyLock49
bumpyShow52
gr3atRock47
goldAppl391
wil)Hog99
ros3Town70
messySm!le32
ri(hMusic99
=latKnot14
(oolPump27
fla+Stamp79
bu$yStar95
zanyLoa=40
$hortGrape30
mushySal+54
lushParro+78
slimyB@boon87
jad3Wave30
lazyIn)igo30
whi+eActor46
l@zyPeach77
sm@llPump61
sup3rCloud54
bu$yEye76
longDre$s82
me$sySummer97
jollyPum@22
w!ndyLine52
goldS<y25
swee+Start94
lushKi+ten42
sl!mPoint92
hug3Horse46
=reeDoe52
jumpyC!rcle64
wil)Fly20
goldY@k36
lu$hIsland57
poorBoo<99
sh!nyPail42
jazzyNa!l83
brownTwis+81
(urlyWorm66
smar+Cart40
badIc399
win)yHelp13
di2zySand51
fr3shSquare79
!voryRiver52
thinGla$s58
p@leHog55
$martButton35
brownB3am91
goodS<unk11
ultr@Chess39
gian+Milk12
richShap396
shinyNigh+63
roundEw350
mushyPan+her15
blackS+one34
```

Dinopass "Strong" Passwords

- Same basic format:
  - adjective + noun + [10-99]
- Same lists of adjectives and nouns
- First character of noun is always capitalized
- One lowercase letter replaced with number or symbol
- One adjective+noun combo has multiple replacement options
  - `windyHar356`
  - `w!ndyHare45`
- Total "strong" wordlist could be 3x-6x larger than "simple"
  - 10-20 Million possible passwords
  - 200-400 MBs
  - Still reasonable for a wordlist

a	→	@
c	→	(
d	→	)
e	→	3
f	→	=
i	→	!
j	→	]
k	→	<
s	→	$
t	→	+
z	→	2

Comparing password entropy



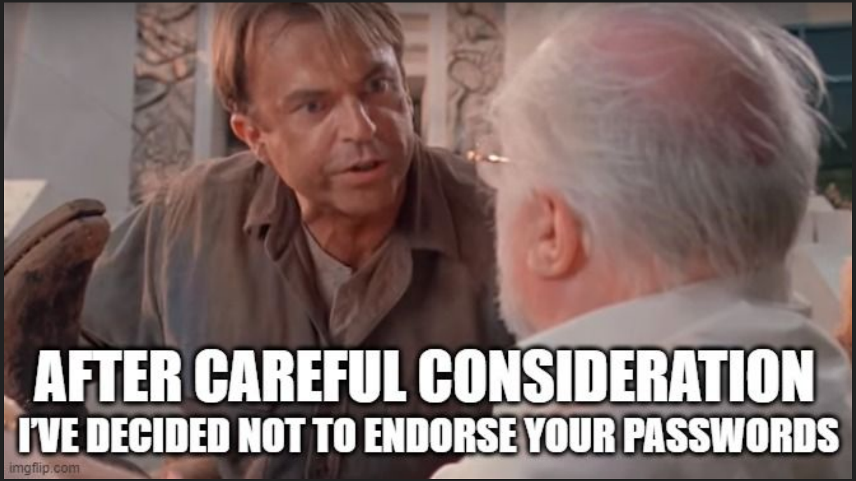
		Password Length							
	Character set	1	2	3	4	5	6	7	8
Lowercase only	26	26	676	17576	456976	11881376	308915776	8031810176	208827064576
Lower+Digits	36	36	1296	46656	1679616	60466176	2176782336	78364164096	2821109907456
Lower+Upper	52	52	2704	140608	7311616	380204032	19770609664	1028071702528	53459728531456
Low+Up+Digits	62	62	3844	238328	14776336	916132832	56800235584	3521614606208	218340105584896

Conclusions

- Wordlist is too small
- Format is too simple
- Susceptible to offline dictionary attacks
- No GPU acceleration needed for weak hash formats
- With GPU acceleration, the small wordlist can still break strong hashes
- No "rules" needed, the dictionary is < 40MBs
- Dinopass "Strong" passwords aren't really better

Who is Dinopass for?

- You?
  - Now you know better.
- Your parents?
  - Also no.
- Your kids?
  - Maybe, if you're comfortable with it.
- Homelab stuff?
  - I wouldn't.
- Work/enterprise?
  - Definitely not.
- CCDC?
  - It'll make the Blue Teams cry.


AFTER CAREFUL CONSIDERATION
I'VE DECIDED NOT TO ENDORSE YOUR PASSWORDS
imgflip.com

Trix are for kids, and so is Dinopass.

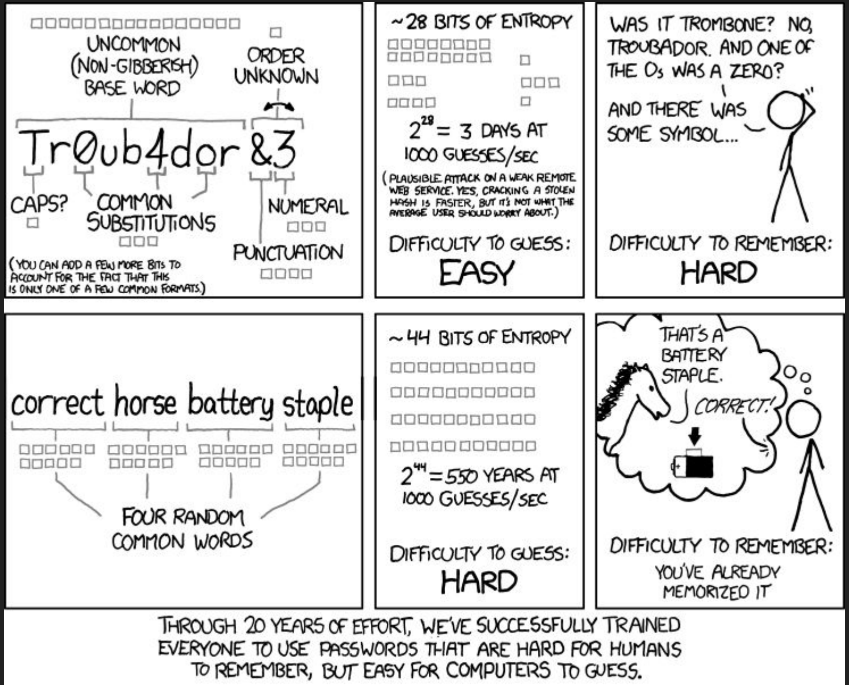
Password Best Practices

Use a password manager to generate and store good random passwords.

Don’t reuse passwords across services.

Use 2FA everywhere you can.

Prioritize longer and random passwords on email, banking, social media, and password managers.


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

https://xkcd.com/936/

Thank you!

Twitter: @daschu117

https://github.com/daschu117/dinopass

@davie#0001 on the LayerOne Discord

https://revshellcorp.org/