CSCI 530: Security Systems
Lab Assignment 2: Submission Due 27th September 2024
Name: Anne Sai Venkata Naga Saketh
USC Email: annes@usc.edu
USC ID: 3725520208

Question 1:

Imagine a "file-based/static/pre-computed" type dictionary attack for cracking all the words in a language of 100,000 words. Suppose, when utilized as passwords, these are hashed as-is (unsalted), and the result then stored. ("Hashed" here means processed as the passwd command does.) To attack this, the cracker creates his dictionary in advance by 1) hashing all 100,000 words from first to last, then 2) re-sorting his dictionary on the hashes. Then, given a hashed password to crack, he simply looks it up and there he finds the original, plaintext password.

Without salt:
a) Number of different ways a single password can come out if hashed using no salt, is ***1.***

Reason*: For a given plan text(password), a hash function will produce the same hash, how many times it is executed, so there will only be 1 outcome if used with no salt.*

b) The number of entries there will be in the dictionary the cracker must create is ***100,000.***

Reason: *Since there are 100,000 different (unique) words in the dictionary, each word will have a different hash value when unsalted, so the total number of entries in the dictionary is 100,000*

Now imagine that a 2-byte salt is introduced, randomly chosen then prefixed to each word before it is hashed and stored for use as a password.

With salt:

c) The number of different ways a single password could come out if hashed when prefixed with a random 2-byte salt is ***65,536***.

Reason: *Since a 2-byte salt is used, each byte can take 256 different values. Therefore, the 2-byte salt can take up to 216 values, i.e., 256 * 256 = 65,536. With 216 possible salt values, each value producing a unique hash value, the total number of resulting values will be 65,536.*

d) The number of entries will there be in the dictionary the cracker must create is ***6,553,600,000.***

Reason: *There are 100,000 words in the dictionary, and for each word, the cracker will produce 65,536 different possibilities, so the total number of outcomes will be 6,553,600,000.*

e) If all the words in the language are 8 characters long and resolve to hashes 86 bytes long, thus

requiring 94 bytes to store each mapped pair (dictionary entry), then the number of gigabytes the cracker's dictionary must occupy is ***573.74 GB***

Reason: *Each password and hash pair will take up to 94bytes, and there are 6,553,600,000 different pairs, so the total number of bytes is 6,553,600,000 * 94 = 616,038,400,000 bytes*

*Converting this to bytes: 616,038,400,000 / (1024 * 1024 * 1024) ~= 573.73 GB*

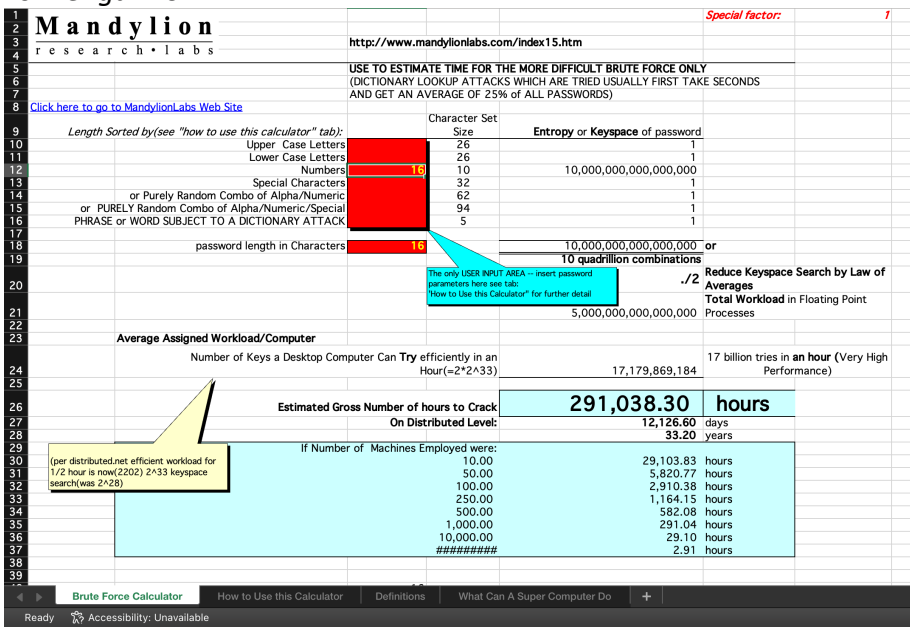
Question 2:

Use the Mandylion "Brute Force Attack Estimator" Excel spreadsheet (a slightly modified version). Suppose you want a password that requires the rest of your life for a PC to crack. You have 50 years to live. How many days (live each to the fullest) is that? In the spreadsheet, consider passwords consisting of numerals ("Numbers") only.

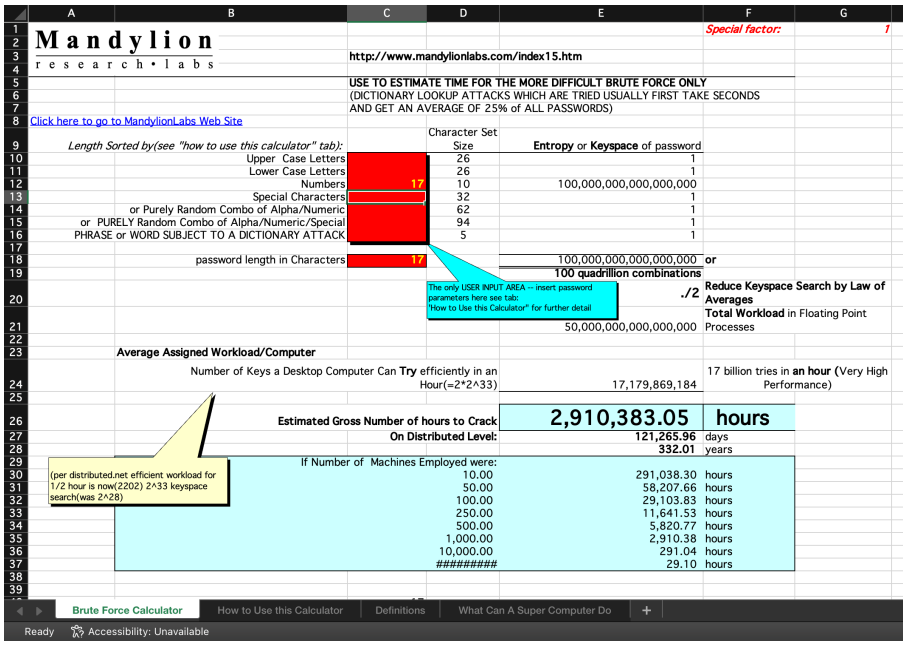
a) The length of the numbers-only password that requires at least 50 years to crack, according to the spreadsheet, is ***17*** characters.

Reason: *As shown in the pictures below, for a password containing a numerical only of length 16, it takes around 33.20 Years to creak, and for a length of 17, it takes around 332.01 Years to crack.*

*For Length **16**:*



*For length **17**:*



Mandylion research • labs

Special factor: 1

http://www.mandylionlabs.com/index15.htm

USE TO ESTIMATE TIME FOR THE MORE DIFFICULT BRUTE FORCE ONLY
(DICTIONARY LOOKUP ATTACKS WHICH ARE TRIED USUALLY FIRST TAKE SECONDS AND GET AN AVERAGE OF 25% of ALL PASSWORDS)

Click here to go to MandylionLabs Web Site

Length Sorted by(see "how to use this calculator" tab):		Character Set Size	Entropy or Keyspace of password
Upper Case Letters		26	1
Lower Case Letters		26	1
Numbers	17	10	100,000,000,000,000,000
Special Characters		32	1
or Purely Random Combo of Alpha/Numeric		62	1
or PURELY Random Combo of Alpha/Numeric/Special		94	1
PHRASE or WORD SUBJECT TO A DICTIONARY ATTACK		5	1
password length in Characters	17		100,000,000,000,000,000 or 100 quadrillion combinations

The only USER INPUT AREA -- insert password parameters here see tab: "How to Use this Calculator" for further detail

./2 Reduce Keyspace Search by Law of Averages

Total Workload in Floating Point Processes: 50,000,000,000,000,000

Average Assigned Workload/Computer

Number of Keys a Desktop Computer Can Try efficiently in an Hour(=2*2^33): 17,179,869,184 (17 billion tries in an hour (Very High Performance))

(per distributed.net efficient workload for 1/2 hour is now(2202) 2^33 keyspace search(was 2^28))

Estimated Gross Number of hours to Crack	2,910,383.05	hours
On Distributed Level:	121,265.96	days
	332.01	years

If Number of Machines Employed were:		
10.00	291,038.30	hours
50.00	58,207.66	hours
100.00	29,103.83	hours
250.00	11,641.53	hours
500.00	5,820.77	hours
1,000.00	2,910.38	hours
10,000.00	291.04	hours
#########	29.10	hours

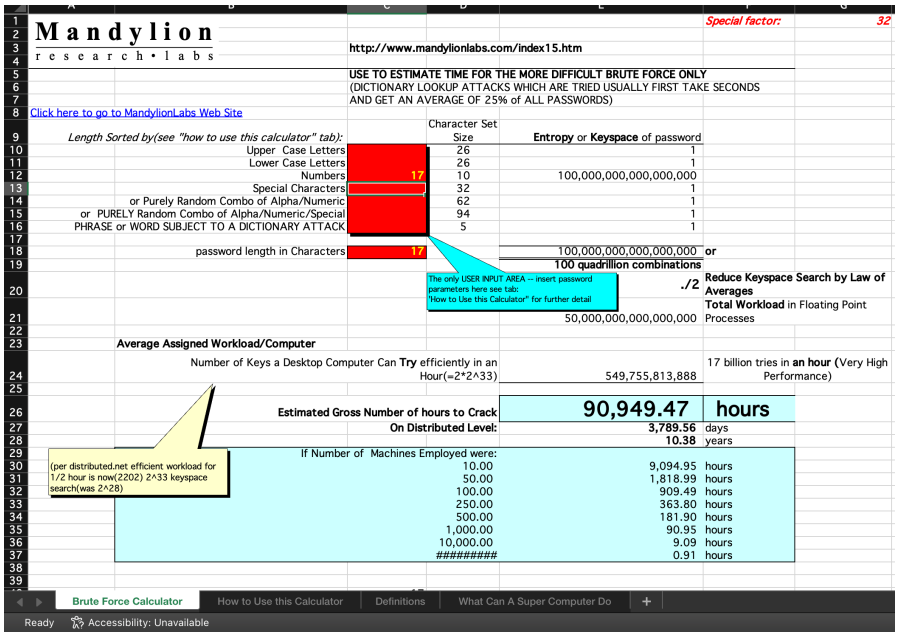
Brute Force Calculator | How to Use this Calculator | Definitions | What Can A Super Computer Do | +

Ready Accessibility: Unavailable

b) Account for Moore's law. It says computing power doubles every 2 years. The spreadsheet is dated. It reflects the computing power of 10 years ago. For today, you need to increase its computing power assumptions by a factor of 32 (having doubled 5 times over the 10 years). Do so by entering 32 as the "Special factor" in cell G1 (which is applied in the "computing power" cell, E24, as a multiplier). Thus, with *today's* computing power, the length of the numerals-only password that requires at least the rest of your life to crack is ***18*** characters.

Reason: *As shown in the pictures below, for a password containing a numerical only of length 17, it takes around 10.38 Years to creak, and for a length of 18, it takes around 103.75 Years to crack.*

*For Length **17**:*



Mandylion research • labs

Special factor: 32

http://www.mandylionlabs.com/index15.htm

USE TO ESTIMATE TIME FOR THE MORE DIFFICULT BRUTE FORCE ONLY
(DICTIONARY LOOKUP ATTACKS WHICH ARE TRIED USUALLY FIRST TAKE SECONDS
AND GET AN AVERAGE OF 25% of ALL PASSWORDS)

Click here to go to MandylionLabs Web Site

Length Sorted by(see "how to use this calculator" tab):		Character Set Size	Entropy or Keyspace of password
Upper Case Letters		26	1
Lower Case Letters		26	1
Numbers	17	10	100,000,000,000,000,000
Special Characters		32	1
or Purely Random Combo of Alpha/Numeric		62	1
or PURELY Random Combo of Alpha/Numeric/Special		94	1
PHRASE or WORD SUBJECT TO A DICTIONARY ATTACK		5	1
password length in Characters	17		100,000,000,000,000,000 or 100 quadrillion combinations

The only USER INPUT AREA -- insert password parameters here see tab: "How to Use this Calculator" for further detail

./2 Reduce Keyspace Search by Law of Averages

Total Workload in Floating Point Processes: 50,000,000,000,000,000

Average Assigned Workload/Computer

Number of Keys a Desktop Computer Can Try efficiently in an Hour(=2*2^33): 549,755,813,888

17 billion tries in an hour (Very High Performance)

Estimated Gross Number of hours to Crack: 90,949.47 hours

On Distributed Level: 3,789.56 days / 10.38 years

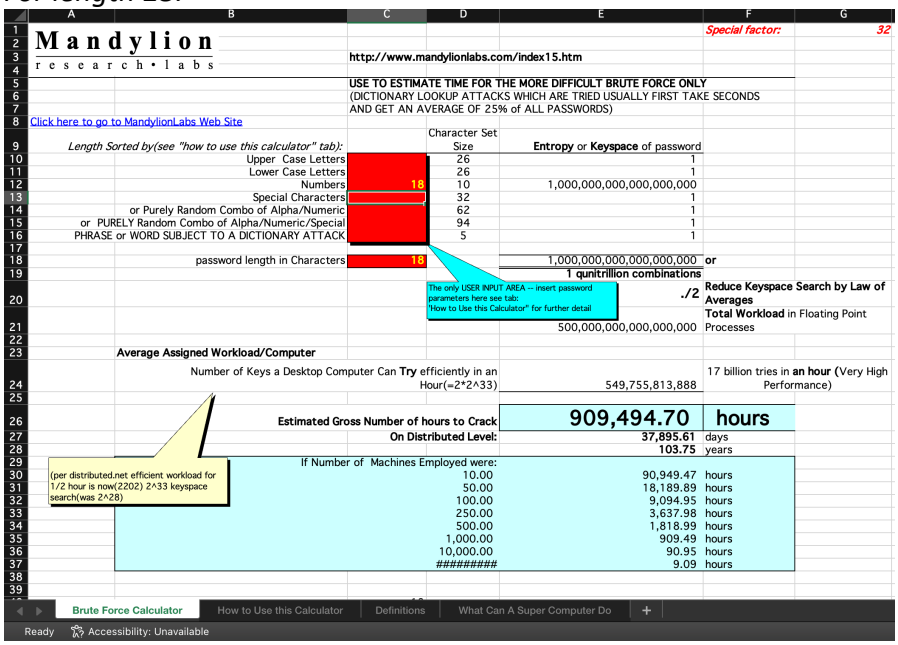
(per distributed.net efficient workload for 1/2 hour is now(2202) 2^33 keyspace search(was 2^28)

If Number of Machines Employed were:	
10.00	9,094.95 hours
50.00	1,818.99 hours
100.00	909.49 hours
250.00	363.80 hours
500.00	181.90 hours
1,000.00	90.95 hours
10,000.00	9.09 hours
##########	0.91 hours

Brute Force Calculator | How to Use this Calculator | Definitions | What Can A Super Computer Do | +

Ready Accessibility: Unavailable

*For length **18**:*



Mandylion research • labs

Special factor: 32

http://www.mandylionlabs.com/index15.htm

USE TO ESTIMATE TIME FOR THE MORE DIFFICULT BRUTE FORCE ONLY
(DICTIONARY LOOKUP ATTACKS WHICH ARE TRIED USUALLY FIRST TAKE SECONDS
AND GET AN AVERAGE OF 25% of ALL PASSWORDS)

Click here to go to MandylionLabs Web Site

Length Sorted by(see "how to use this calculator" tab):		Character Set Size	Entropy or Keyspace of password
Upper Case Letters		26	1
Lower Case Letters		26	1
Numbers	18	10	1,000,000,000,000,000,000
Special Characters		32	1
or Purely Random Combo of Alpha/Numeric		62	1
or PURELY Random Combo of Alpha/Numeric/Special		94	1
PHRASE or WORD SUBJECT TO A DICTIONARY ATTACK		5	1
password length in Characters	18		1,000,000,000,000,000,000 or 1 quintrillion combinations

The only USER INPUT AREA -- insert password parameters here see tab: "How to Use this Calculator" for further detail

./2 Reduce Keyspace Search by Law of Averages

Total Workload in Floating Point Processes: 500,000,000,000,000,000

Average Assigned Workload/Computer

Number of Keys a Desktop Computer Can Try efficiently in an Hour(=2*2^33): 549,755,813,888

17 billion tries in an hour (Very High Performance)

Estimated Gross Number of hours to Crack: 909,494.70 hours

On Distributed Level: 37,895.61 days / 103.75 years

(per distributed.net efficient workload for 1/2 hour is now(2202) 2^33 keyspace search(was 2^28)

If Number of Machines Employed were:	
10.00	90,949.47 hours
50.00	18,189.89 hours
100.00	9,094.95 hours
250.00	3,637.98 hours
500.00	1,818.99 hours
1,000.00	909.49 hours
10,000.00	90.95 hours
##########	9.09 hours

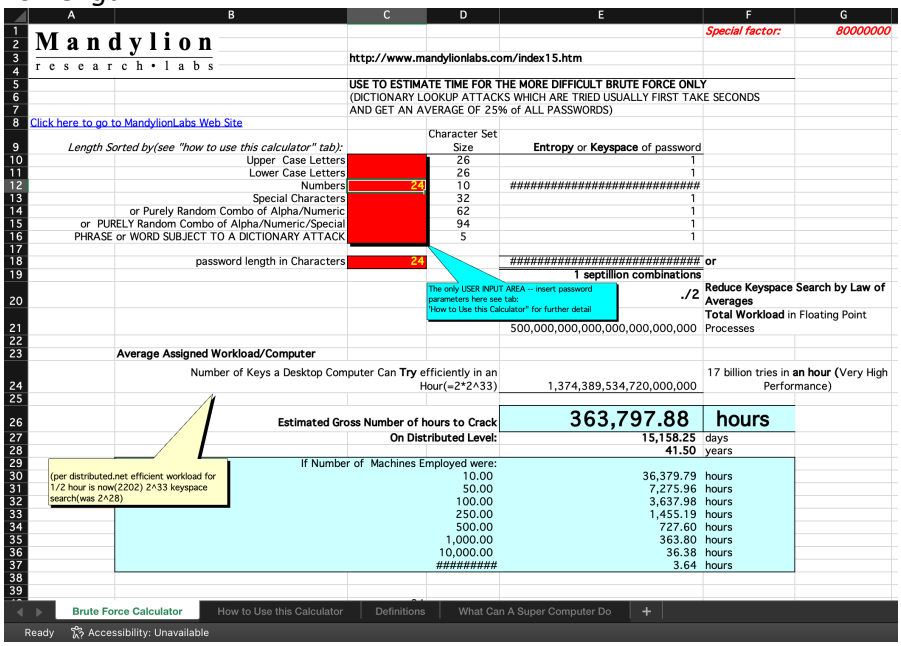
Brute Force Calculator | How to Use this Calculator | Definitions | What Can A Super Computer Do | +

Ready Accessibility: Unavailable

c) Account for Moore's law's continued operation. Let's assume Moore's law doesn't stop. (There's debate about that. But let's set it aside because if Moore's law's potential to continue raising cracking power is blunted, GPU advances or specialized cracking silicon may more than fill the gap.) Then today's isn't the right computing power for the upcoming 50 years' calculations. I say that on average (less near term, more far term) the upcoming power is 2.5 million times today's (approximately). Using 2.5 million as your future computing power, the length of the password that requires at least 50 years to crack becomes ***25*** characters. (Multipy the current special factor by yet a further 2.5x10^6)

Reason: *As shown in the pictures below, for a password containing numerical only of length 24, it takes around 41.50 Years to creak, and for a length of 25, it takes around 415.01 Years to crack.*

*For length **24**:*



Mandylion research • labs

http://www.mandylionlabs.com/index15.htm

Special factor: 80000000

USE TO ESTIMATE TIME FOR THE MORE DIFFICULT BRUTE FORCE ONLY
(DICTIONARY LOOKUP ATTACKS WHICH ARE TRIED USUALLY FIRST TAKE SECONDS AND GET AN AVERAGE OF 25% of ALL PASSWORDS)

Click here to go to MandylionLabs Web Site

Length Sorted by(see "how to use this calculator" tab):		Character Set Size	Entropy or Keyspace of password
Upper Case Letters		26	1
Lower Case Letters		26	1
Numbers	24	10	############################
Special Characters		32	1
or Purely Random Combo of Alpha/Numeric		62	1
or PURELY Random Combo of Alpha/Numeric/Special		94	1
PHRASE or WORD SUBJECT TO A DICTIONARY ATTACK		5	1
password length in Characters	24		############################ or 1 septillion combinations

The only USER INPUT AREA -- insert password parameters here see tab: 'How to Use this Calculator" for further detail

./2 **Reduce Keyspace Search by Law of Averages**

500,000,000,000,000,000,000,000 **Total Workload** in Floating Point Processes

Average Assigned Workload/Computer

Number of Keys a Desktop Computer Can **Try** efficiently in an Hour(=2*2^33): 1,374,389,534,720,000,000 — 17 billion tries in **an hour** (Very High Performance)

(per distributed.net efficient workload for 1/2 hour is now(2202) 2^33 keyspace search(was 2^28))

Estimated Gross Number of hours to Crack: **363,797.88 hours**

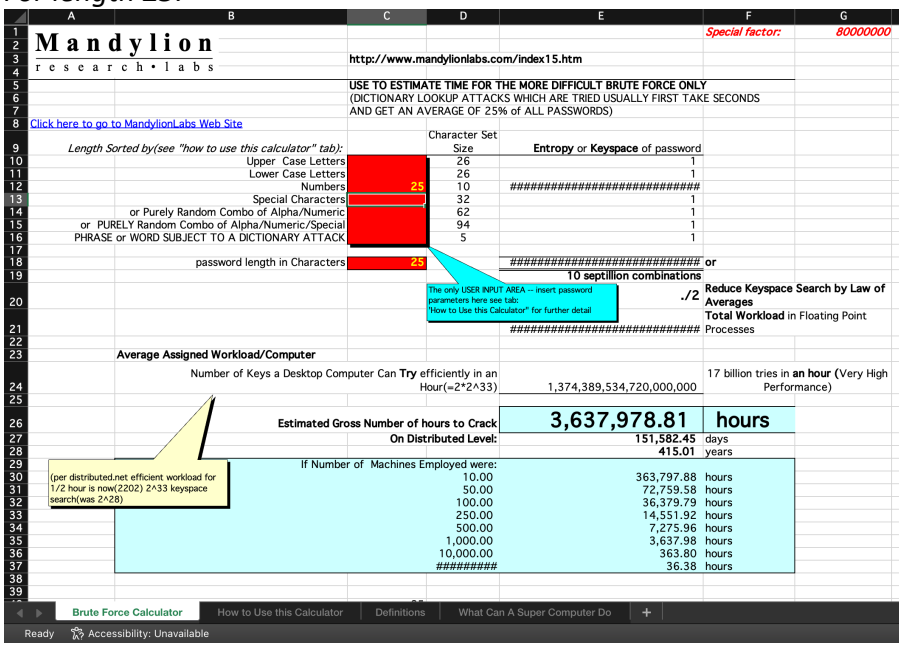
On Distributed Level: **15,158.25** days / **41.50** years

If Number of Machines Employed were:	
10.00	36,379.79 hours
50.00	7,275.96 hours
100.00	3,637.98 hours
250.00	1,455.19 hours
500.00	727.60 hours
1,000.00	363.80 hours
10,000.00	36.38 hours
#########	3.64 hours

Brute Force Calculator | How to Use this Calculator | Definitions | What Can A Super Computer Do | +

Ready | Accessibility: Unavailable

*For length **25**:*



Mandylion research • labs

http://www.mandylionlabs.com/index15.htm

Special factor: 80000000

USE TO ESTIMATE TIME FOR THE MORE DIFFICULT BRUTE FORCE ONLY
(DICTIONARY LOOKUP ATTACKS WHICH ARE TRIED USUALLY FIRST TAKE SECONDS AND GET AN AVERAGE OF 25% of ALL PASSWORDS)

Click here to go to MandylionLabs Web Site

Length Sorted by(see "how to use this calculator" tab):		Character Set Size	Entropy or Keyspace of password
Upper Case Letters		26	1
Lower Case Letters		26	1
Numbers	25	10	############################
Special Characters		32	1
or Purely Random Combo of Alpha/Numeric		62	1
or PURELY Random Combo of Alpha/Numeric/Special		94	1
PHRASE or WORD SUBJECT TO A DICTIONARY ATTACK		5	1
password length in Characters	25		############################ or 10 septillion combinations

The only USER INPUT AREA -- insert password parameters here see tab: 'How to Use this Calculator" for further detail

./2 **Reduce Keyspace Search by Law of Averages**

############################ **Total Workload** in Floating Point Processes

Average Assigned Workload/Computer

Number of Keys a Desktop Computer Can **Try** efficiently in an Hour(=2*2^33): 1,374,389,534,720,000,000 — 17 billion tries in **an hour** (Very High Performance)

(per distributed.net efficient workload for 1/2 hour is now(2202) 2^33 keyspace search(was 2^28))

Estimated Gross Number of hours to Crack: **3,637,978.81 hours**

On Distributed Level: **151,582.45** days / **415.01** years

If Number of Machines Employed were:	
10.00	363,797.88 hours
50.00	72,759.58 hours
100.00	36,379.79 hours
250.00	14,551.92 hours
500.00	7,275.96 hours
1,000.00	3,637.98 hours
10,000.00	363.80 hours
#########	36.38 hours

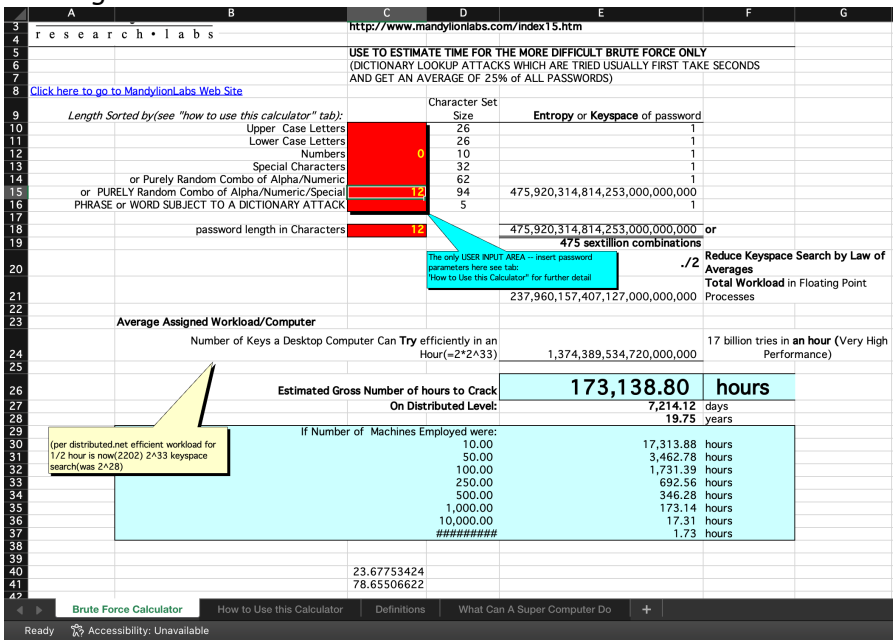
Brute Force Calculator | How to Use this Calculator | Definitions | What Can A Super Computer Do | +

Ready | Accessibility: Unavailable

d) If you then made the one change of allowing mixed random characters (spreadsheet's "PURELY Random Combo of Alpha/Numeric/Special") instead of confining your password to numerals only you should be able to use a shorter password with equal effect. The shortest "mixed character" password that'll last 50 years is ***13*** characters.

Reason: *As shown in the pictures below, for a password containing numerical only of length 12, it takes around 19.75 Years to creak, and for a length of 13, it takes around 1856.61 Years to crack.*

*For length **12**:*



r e s e a r c h • l a b s

http://www.mandylionlabs.com/index15.htm

USE TO ESTIMATE TIME FOR THE MORE DIFFICULT BRUTE FORCE ONLY
(DICTIONARY LOOKUP ATTACKS WHICH ARE TRIED USUALLY FIRST TAKE SECONDS AND GET AN AVERAGE OF 25% of ALL PASSWORDS)

Click here to go to MandylionLabs Web Site

Length Sorted by(see "how to use this calculator" tab):		Character Set Size	**Entropy** or **Keyspace** of password
Upper Case Letters		26	1
Lower Case Letters		26	1
Numbers	0	10	1
Special Characters		32	1
or Purely Random Combo of Alpha/Numeric		62	1
or PURELY Random Combo of Alpha/Numeric/Special	12	94	475,920,314,814,253,000,000,000
PHRASE or WORD SUBJECT TO A DICTIONARY ATTACK		5	1
password length in Characters	12		475,920,314,814,253,000,000,000 **or**
			475 sextillion combinations
			./2 **Reduce Keyspace Search by Law of Averages**
			Total Workload in Floating Point Processes
			237,960,157,407,127,000,000,000

The only USER INPUT AREA -- insert password parameters here see tab: "How to Use this Calculator" for further detail

Average Assigned Workload/Computer

Number of Keys a Desktop Computer Can **Try** efficiently in an Hour(=2*2^33)	1,374,389,534,720,000,000	17 billion tries in **an hour** (Very High Performance)
Estimated Gross Number of hours to Crack	**173,138.80**	**hours**
On Distributed Level:	**7,214.12**	days
	19.75	years

(per distributed.net efficient workload for 1/2 hour is now(2202) 2^33 keyspace search(was 2^28)

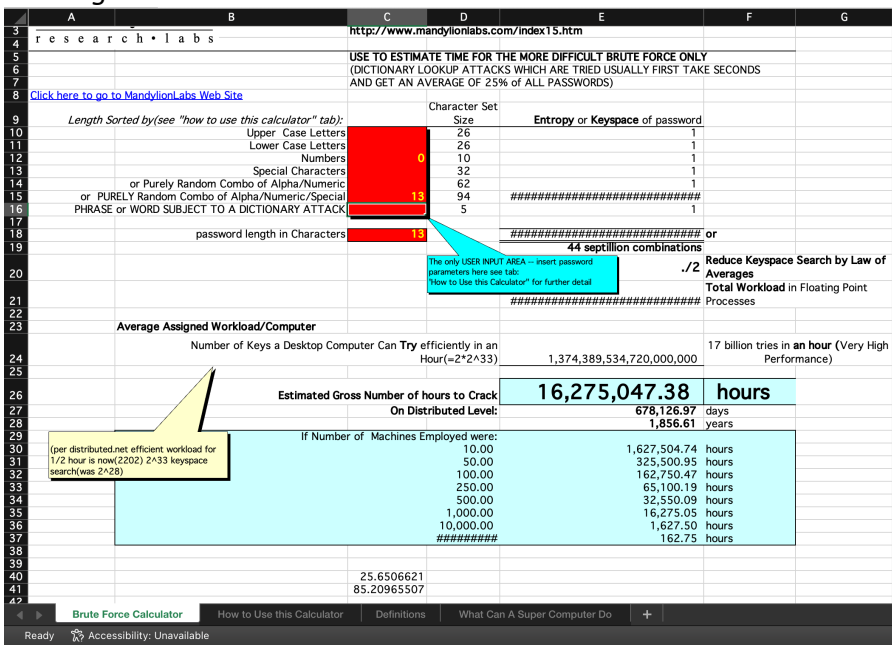
If Number of Machines Employed were:		
10.00	17,313.88	hours
50.00	3,462.78	hours
100.00	1,731.39	hours
250.00	692.56	hours
500.00	346.28	hours
1,000.00	173.14	hours
10,000.00	17.31	hours
##########	1.73	hours

23.67753424
78.65506622

Brute Force Calculator | How to Use this Calculator | Definitions | What Can A Super Computer Do | +

Ready Accessibility: Unavailable

*For length **13**:*



r e s e a r c h • l a b s

http://www.mandylionlabs.com/index15.htm

USE TO ESTIMATE TIME FOR THE MORE DIFFICULT BRUTE FORCE ONLY
(DICTIONARY LOOKUP ATTACKS WHICH ARE TRIED USUALLY FIRST TAKE SECONDS AND GET AN AVERAGE OF 25% of ALL PASSWORDS)

Click here to go to MandylionLabs Web Site

Length Sorted by(see "how to use this calculator" tab):		Character Set Size	**Entropy** or **Keyspace** of password
Upper Case Letters		26	1
Lower Case Letters		26	1
Numbers	0	10	1
Special Characters		32	1
or Purely Random Combo of Alpha/Numeric		62	1
or PURELY Random Combo of Alpha/Numeric/Special	13	94	############################
PHRASE or WORD SUBJECT TO A DICTIONARY ATTACK		5	1
password length in Characters	13		############################ **or**
			44 septillion combinations
			./2 **Reduce Keyspace Search by Law of Averages**
			Total Workload in Floating Point Processes
			############################

The only USER INPUT AREA -- insert password parameters here see tab: "How to Use this Calculator" for further detail

Average Assigned Workload/Computer

Number of Keys a Desktop Computer Can **Try** efficiently in an Hour(=2*2^33)	1,374,389,534,720,000,000	17 billion tries in **an hour** (Very High Performance)
Estimated Gross Number of hours to Crack	**16,275,047.38**	**hours**
On Distributed Level:	**678,126.97**	days
	1,856.61	years

(per distributed.net efficient workload for 1/2 hour is now(2202) 2^33 keyspace search(was 2^28)

If Number of Machines Employed were:		
10.00	1,627,504.74	hours
50.00	325,500.95	hours
100.00	162,750.47	hours
250.00	65,100.19	hours
500.00	32,550.09	hours
1,000.00	16,275.05	hours
10,000.00	1,627.50	hours
##########	162.75	hours

25.6506621
85.20965507

Brute Force Calculator | How to Use this Calculator | Definitions | What Can A Super Computer Do | +

Ready Accessibility: Unavailable