

Forum:[Hack Forums](#)

Thread: [How I won \\$200 CRACK THE SEED Contest](#)

RangoWorld - April 10, 2025, 6:51 am

For those who are not aware [7](#) ran a unique contest giving away \$200 SOL to the winner. He dropped a riddle every single day for 12 days. Each riddle revealed a unique mnemonic seed to the \$200 Trust wallet.

All it was needed was to find the 12 right seed words. The person to crack the mnemonic seeds and transfer the money wins.

[Contest Thread](#)

Now here's how I did it.

The riddle came in daily to participants via PMs. The first riddle was;

Quote:I'm not just good, I go beyond,
With cape or strength, I break the bond.
A comic favorite, admired and bright —
What am I, with extraordinary might?

Answer: super. Pretty easy right?

Except that not all riddles were this easy and you didn't know what your answer for a riddle was until you had all the 12 correct seed words with you. This increased the probability exponentially with every new word introduced.

After the first few riddles I started researching on cryptography, wallet addresses and how wallets work with seeds exactly. I learned that Trust Wallet uses [BIP39 Wordlist](#) (A group of 2048 unique words) that make up the said 12 or 24 words seed for the wallet.

This is the case with every wallet. This wallet was protected with 12 seed words.

The BIP39 seed word list contains 2,048 words, so a 12 word seed has about $2048^{12} = 2^{132}$ possible combinations. You are probably better off buying a lottery ticket than trying to crack a random wallet, let alone with the prize money in it. Because the world is more likely to end than two people generating the same seed for their wallet.

Anyways, I started getting cracking. After Day 10. I started working on my script in an effort to try and crack the last riddle word even before the riddle is revealed. For that the probability was in around few thousands. But the problem was that you could not know the right word for a single seed. You had to click right on all 12 seed words together. So the probability actually still was in millions.

Here you need to use a bit of ingenuity and try to work things through in your own problem solving style.

I tried solving the 12 riddles again and again and again. Narrowed some down to one or two right answers. Still there was some wiggle room. That's what I thought and I was right. I gave the BIP39 list to ChatGPT and asked it to find me synonyms for each of the seed word that I had narrowed it down.

Then came the last day. I was prepared with my scripts. One of my first scripts was to run through these specified and narrowed down seed combos and try to find wallets with non zero balance on the Sol network. Unfortunately that didn't worked out as the script was passing by wallets without really checking in for balance. I found that out later.

I had tried over a million combinations and none worked.

Though luckily even after the 12 riddles were revealed that wallet was still not cracked but I was about to give up. Until an idea sparked and I quickly designed another script to generate me all valid seed combinations for Sol addresses. Which is not every combo, since not every seed combination translates into a valid address. I was left with 30 odd seeds.

30 odd seeds were in valid_seeds.txt file. You can see 3 scripts here ending with .py

Then I manually tried pasting it and one of them worked!

Riddle 5 and Riddle 10 were the hardest for me. Riddle 5's right answer was "Lumber" and I was stuck on being "Wood" for too long. That's where ChatGPT helped me find synonym for it and I think that did the deal for me at the end as I had gotten the other words pretty much right on.

I'm not a pro "hacker" or anything like that. People here maybe more skilled in coding and various tasks than me. But problem solving skills matters more than anything else. That's what I learned through this contest and that's what I want to say to you all.

It doesn't matter what approach or method you take for solving anything, as long as it works!

Lastly I want to Thank [7](#) again for running this contest. It was a truly unique contest. One of a kind and I have told him, "HackForums" fitting contest. I implore all of you to checkout the original thread. He has hinted on running these kind of contests in the near future as well. I definitely had a good time.

Thanks for reading! ?

_VOX - April 10, 2025, 6:54 am

Congratulations! I currently didn't have the headspace or time to compete. So hopefully theres another one soon!

Trust - April 10, 2025, 7:31 am

My brain hurt reading this, but I'm glad somebody managed to crack the code.
Congratulations!

plops - April 10, 2025, 7:38 am

Congrats man,
Cryptography and riddles are very frustrating imo. Good on you for your paitence and persistence.

blackhat314 - April 10, 2025, 8:54 am

There is 0 chance I would have gotten this but congrats on winning!

Jamika - April 10, 2025, 9:43 am

(Apr 10, 2025 06:51 AM)RangoWorld Wrote: [\[CITE\]](#) For those who are not aware [7](#) ran a unique contest giving away \$200 SOL to the winner. He dropped a riddle every single day for 12 days. Each riddle revealed a unique mnemonic seed to the \$200 Trust wallet.

All it was needed was to find the 12 right seed words. The person to crack the mnemonic seeds and transfer the money wins.

[Contest Thread](#)

Now here's how I did it.

The riddle came in daily to participants via PMs. The first riddle was;

Answer: super. Pretty easy right?

Except that not all riddles were this easy and you didn't know what your answer for a riddle was until you had all the 12 correct seed words with you. This increased the probability exponentially with every new word introduced.

After the first few riddles I started researching on cryptography, wallet addresses and how wallets work with seeds exactly. I learned that Trust Wallet uses [BIP39 Wordlist](#) (A group of 2048 unique words) that make up the said 12 or 24 words seed for the wallet.

This is the case with every wallet. This wallet was protected with 12 seed words.

The BIP39 seed word list contains 2,048 words, so a 12 word seed has about $2048^{12} = 2^{132}$ possible combinations. You are probably better off buying a lottery ticket than trying to crack a random wallet, let alone with the prize money in it. Because the world is more likely to end than two people generating the same seed for their wallet.

Anyways, I started getting cracking. After Day 10. I started working on my script in an effort to try and crack the last riddle word even before the riddle is revealed. For that the probability was in around few thousands. But the problem was that you could not know the right word for a single seed. You had to click right on all 12 seed words together. So the probability actually still was in millions.

Here you need to use a bit of ingenuity and try to work things through in your own problem solving style.

I tried solving the 12 riddles again and again and again. Narrowed some down to one or two right answers. Still there was some wiggle room. That's what I thought and I was right. I gave the BIP39 list to ChatGPT and asked it to find me synonyms for each of the seed word that I had narrowed it down.

Then came the last day. I was prepared with my scripts. One of my first scripts was to run through these specified and narrowed down seed combos and try to find wallets with non zero balance on

the Sol network. Unfortunately that didn't work out as the script was passing by wallets without really checking in for balance. I found that out later.

I had tried over a million combinations and none worked.

Though luckily even after the 12 riddles were revealed that wallet was still not cracked but I was about to give up. Until an idea sparked and I quickly designed another script to generate me all valid seed combinations for Sol addresses. Which is not every combo, since not every seed combination translates into a valid address. I was left with 30 odd seeds.

30 odd seeds were in valid_seeds.txt file. You can see 3 scripts here ending with .py

Then I manually tried pasting it and one of them worked!

Riddle 5 and Riddle 10 were the hardest for me. Riddle 5's right answer was "Lumber" and I was stuck on being "Wood" for too long. That's where ChatGPT helped me find synonym for it and I think that did the deal for me at the end as I had gotten the other words pretty much right on.

I'm not a pro "hacker" or anything like that. People here maybe more skilled in coding and various tasks than me. But problem solving skills matters more than anything else. That's what I learned through this contest and that's what I want to say to you all.

It doesn't matter what approach or method you take for solving anything, as long as it works!

Lastly I want to Thank [7](#) again for running this contest. It was a truly unique contest. One of a kind and I have told him, "HackForums" fitting contest. I implore all of you to checkout the original thread. He has hinted on running these kind of contests in the near future as well. I definitely had a good time.

Thanks for reading! ?

Nice work , congrats bro , now send me some lol

Regulus - April 10, 2025, 9:46 am

(Apr 10, 2025 07:31 AM)Trust Wrote: [\[CITE\]](#) My brain hurt reading this, but I'm glad somebody managed to crack the code.

Congratulations!

Vouch for this, didn't even get the first phrases here.

But congrats to OP, well deserved!

Pr0m3th3us - April 10, 2025, 10:28 am

What program did you use to read the scripts and try the combinations?

RangoWorld - April 10, 2025, 10:30 am

(Apr 10, 2025 10:28 AM)Rustoleum Wrote: [\[CITE\]](#) What program did you use to read the scripts and try the combinations?

Python.

There are also plenty of resources available online on wallet recovery, wordlist, and combinatorics.

7 - April 10, 2025, 10:32 am

Great initiative.

I like how you did your research and also explained to others.
Congratulations on winning but more congratulations on your thought process.

Pr0m3th3us - April 10, 2025, 10:34 am

(Apr 10, 2025 10:30 AM)RangoWorld Wrote: [\[CITE\]](#) Python.

There are also plenty of resources available online on wallet recovery, wordlist, and combinatorics.
Ahh ok got it. Really legit work your did, must have been super satisfying hitting that transfer SOL button. You earned it man.

RangoWorld - April 10, 2025, 10:37 am

(Apr 10, 2025 10:34 AM)Rustoleum Wrote: [\[CITE\]](#) Ahh ok got it. Really legit work your did, must have been super satisfying hitting that transfer SOL button. You earned it man.

I was a little nervous when I pressed the button as time was running out virtually. Lol

Pr0m3th3us - April 10, 2025, 10:40 am

(Apr 10, 2025 10:37 AM)RangoWorld Wrote: [\[CITE\]](#) I was a little nervous when I pressed the button as time was running out virtually. Lol

Something I was wondering also, what if 30 seconds after you recovered the wallet with the seed someone else was trying to do it also. Would it have allowed them?

7 - April 10, 2025, 11:54 am

(Apr 10, 2025 10:40 AM)Rustoleum Wrote: [\[CITE\]](#) Something I was wondering also, what if 30 seconds after you recovered the wallet with the seed someone else was trying to do it also. Would it have allowed them?

Yes it would allow both I believe... just whoever withdrew the money first won

Omniscient - April 10, 2025, 11:57 am

(Apr 10, 2025 10:32 AM)7 Wrote: [\[CITE\]](#) Great initiative.

I like how you did your research and also explained to others.
Congratulations on winning but more congratulations on your thought process.
More of items like that would attract some new members imho.

7 - April 10, 2025, 11:59 am

(Apr 10, 2025 11:57 AM)Omniscient Wrote: [\[CITE\]](#) More of items like that would attract some new members imho.

Glad you think so.

I am going to run something like this every other week and the hopefully when I manage to process the new competition there will be an OSint competition in the weeks between.

It will not only encourage engagement but also educate users by doing so.

BTW. you owe me 13\$ lol haha

Just joking. I wondered if the person would take it all or just the prize money

Dredd - April 10, 2025, 3:17 pm

Awesome thread, well deserved win as well by the looks of it.

Congrats bro.

Rsynced - April 10, 2025, 5:01 pm

Congrats, I didn't even know where to begin with this.

Money- - April 11, 2025, 12:37 am

I think I saw 7 posted in fallen. Damn it. This seems fun honestly. Guessing/bruting the seed phrases.

Maybe I'll play around next challenge. See if I have the time.

gwiz - April 11, 2025, 9:42 am

Hell yeah man, you did great!

Love the approach you took and that you learned along the way.

TrackPro+ - April 11, 2025, 10:30 am

Congratulations! I love the idea of this type of contest and I would love to see more of these from [7](#) awesome ?!!!

Syndicate - April 11, 2025, 10:32 am

Congratulations on your win brother. I wouldn't have been able to win it myself. Thank you again, [7](#) for hosting this contest :) It was wonderful.

7 - April 11, 2025, 10:40 am

(Apr 11, 2025 12:37 AM)Money- Wrote: [\[CITE\]](#) I think I saw 7 posted in fallen. Damn it. This seems fun honestly. Guessing/bruting the seed phrases.

Maybe I'll play around next challenge. See if I have the time.

The thread was stickied in contests.

I will try and make a bigger announcement next time I run it, it's quite a full time job not just a cost.

(Apr 11, 2025 10:30 AM)Vizionware.app Wrote: [\[CITE\]](#) Congratulations! I love the idea of this type of contest and I would love to see more of these from [7](#) awesome ?!!!

Glad you think so. I also believe it's engaging and educational

Djangoo - April 11, 2025, 7:20 pm

(Apr 10, 2025 06:51 AM)RangoWorld Wrote: [\[CITE\]](#) For those who are not aware [7](#) ran a unique contest giving away \$200 SOL to the winner. He dropped a riddle every single day for 12 days. Each riddle revealed a unique mnemonic seed to the \$200 Trust wallet.

All it was needed was to find the 12 right seed words. The person to crack the mnemonic seeds and transfer the money wins.

[Contest Thread](#)

Now here's how I did it.

The riddle came in daily to participants via PMs. The first riddle was;

Answer: super. Pretty easy right?

Except that not all riddles were this easy and you didn't know what your answer for a riddle was until you had all the 12 correct seed words with you. This increased the probability exponentially with every new word introduced.

After the first few riddles I started researching on cryptography, wallet addresses and how wallets work with seeds exactly. I learned that Trust Wallet uses [BIP39 Wordlist](#) (A group of 2048 unique words) that make up the said 12 or 24 words seed for the wallet.

This is the case with every wallet. This wallet was protected with 12 seed words.

The BIP39 seed word list contains 2,048 words, so a 12 word seed has about $2048^{12} = 2^{132}$ possible combinations. You are probably better off buying a lottery ticket than trying to crack a random wallet, let alone with the prize money in it. Because the world is more likely to end than two people generating the same seed for their wallet.

Anyways, I started getting cracking. After Day 10. I started working on my script in an effort to try and crack the last riddle word even before the riddle is revealed. For that the probability was in around few thousands. But the problem was that you could not know the right word for a single seed. You had to click right on all 12 seed words together. So the probability actually still was in millions.

Here you need to use a bit of ingenuity and try to work things through in your own problem solving style.

I tried solving the 12 riddles again and again and again. Narrowed some down to one or two right answers. Still there was some wiggle room. That's what I thought and I was right. I gave the BIP39 list to ChatGPT and asked it to find me synonyms for each of the seed word that I had narrowed it down.

Then came the last day. I was prepared with my scripts. One of my first scripts was to run through these specified and narrowed down seed combos and try to find wallets with non zero balance on the Sol network. Unfortunately that didn't worked out as the script was passing by wallets without really checking in for balance. I found that out later.

I had tried over a million combinations and none worked.

Though luckily even after the 12 riddles were revealed that wallet was still not cracked but I was about to give up. Until an idea sparked and I quickly designed another script to generate me all valid seed combinations for Sol addresses. Which is not every combo, since not every seed combination translates into a valid address. I was left with 30 odd seeds.

30 odd seeds were in valid_seeds.txt file. You can see 3 scripts here ending with .py

Then I manually tried pasting it and one of them worked!

Riddle 5 and Riddle 10 were the hardest for me. Riddle 5's right answer was "Lumber" and I was stuck on being "Wood" for too long. That's where ChatGPT helped me find synonym for it and I think that did the deal for me at the end as I had gotten the other words pretty much right on.

I'm not a pro "hacker" or anything like that. People here maybe more skilled in coding and various tasks than me. But problem solving skills matters more than anything else. That's what I learned through this contest and that's what I want to say to you all.

It doesn't matter what approach or method you take for solving anything, as long as it works!

Lastly I want to Thank [7](#) again for running this contest. It was a truly unique contest. One of a kind and I have told him, "HackForums" fitting contest. I implore all of you to checkout the original thread. He has hinted on running these kind of contests in the near future as well. I definitely had a good time.

Thanks for reading! ?

Congrats Rango! you deserved it?. In my case I had so many synonyms in mind which were also present in the BIP39 list due to which even the no. of valid solana addresses were too many and the faculty word seriously drove me crazy.

Yanix - April 11, 2025, 11:55 pm

Congratulations! You did it pretty well [RangoWorld](#)

Cooligan - April 12, 2025, 2:03 am

So really for this, you needed solid problem solving skills, rather than actual coding or technical knowledge. Very interesting.

I didn't attempt it as I didn't have the spare time to, but it would've been a lot of fun now that I know how it worked.

[7](#) you should do more contests like these. The community clearly likes them, and they're great for engagement & activity.

7 - April 12, 2025, 2:45 am

(Apr 12, 2025 02:03 AM)Cooligan Wrote: [\[CITE\]](#) So really for this, you needed solid problem solving skills, rather than actual coding or technical knowledge. Very interesting.

I didn't attempt it as I didn't have the spare time to, but it would've been a lot of fun now that I know how it worked.

[7](#) you should do more contests like these. The community clearly likes them, and they're great for engagement & activity.

Thank you mate.

I definately will.

K1. - April 12, 2025, 4:03 am

Congratulations on the solve man

That's a pretty cool way of doing a challenge too [7](#)

rebeecer - April 12, 2025, 5:28 am

very cool, i will to study more

HankiePankie - April 12, 2025, 9:19 am

Congrats!

Thanks for explaining, seems really cool to do it.