

Forum:[Hack Forums](#)

Thread: [What type of encryption is the strongest?](#)

Hatjorn - April 13, 2024, 4:30 am

I have spending some time to figure out witch encryption is best for Windows. As i understand its VeraCrypt.

Any other suggestions?

JohnFitzgeraldKennedy - April 13, 2024, 10:59 am

For encrypted volumes on Windows I think bitlocker is probably the "best" option. But if you're worried about the secrecy of the information on your machine to that extent you should probably not be using Windows as your host OS in the first place, just saying ?

Hatjorn - April 13, 2024, 11:03 am

(Apr 13, 2024 10:59 AM)JohnFitzgeraldKennedy Wrote: [\[CITE\]](#) For encrypted volumes on Windows I think bitlocker is probably the "best" option. But if you're worried about the secrecy of the information on your machine to that extent you should probably not be using Windows as your host OS in the first place, just saying ?

I just hear bitlocker is easy to decrypt. What type of OS do you prefer? Linux?

I appriciate your input

JohnFitzgeraldKennedy - April 13, 2024, 11:16 am

(Apr 13, 2024 11:03 AM)Hatjorn Wrote: [\[CITE\]](#) I just hear bitlocker is easy to decrypt. What type of OS do you prefer? Linux?

I appriciate your input

Yes some Linux distro is probably the best option, or maybe GrapheneOS, as Windows is basically spyware in itself at this point. I just assume anything done on a Windows machine is logged in a Microsoft/NSA database.

Something like Debian 12 with Gnome would probably be a good starting distro if you're not very experienced with Linux. If you're super paranoid use Tails.

You can set up an encrypted partition with LUKS:

https://en.m.wikipedia.org/wiki/Linux_Unified_Key_Setup

DramaKing - April 13, 2024, 1:37 pm

(Apr 13, 2024 11:03 AM)Hatjorn Wrote: [\[CITE\]](#) I just hear bitlocker is easy to decrypt. What type of OS do you prefer? Linux?

I appriciate your input

BitLocker is so easy to decrypt. With a powerful GPU, you could have a 50% chance of cracking the recovery key in about 11 undecillion years.

Hatjorn - April 15, 2024, 5:21 pm

(Apr 13, 2024 01:37 PM)DramaKing Wrote: [\[CITE\]](#) BitLocker is so easy to decrypt. With a powerful GPU, you could have a 50% chance of cracking the recovery key in about 11 undecillion years.

I guess you think I should go with Bitlocker then

(Apr 13, 2024 11:16 AM)JohnFitzgeraldKennedy Wrote: [\[CITE\]](#) Yes some Linux distro is probably the best option, or maybe GrapheneOS, as Windows is basically spyware in itself at this point. I just assume anything done on a Windows machine is logged in a Microsoft/NSA database.

Something like Debian 12 with Gnome would probably be a good starting distro if you're not very experienced with Linux. If you're super paranoid use Tails.

You can set up an encrypted partition with LUKS:
https://en.m.wikipedia.org/wiki/Linux_Unified_Key_Setup
Thank you for your info JohnFitz. I will be looking into it

DramaKing - April 15, 2024, 6:04 pm

(Apr 15, 2024 05:21 PM)Hatjorn Wrote: [\[CITE\]](#) I guess you think I should go with Bitlocker then

Point is that all FDE software probably uses AES for encryption. I'd never worry about a brute force attack unless you set up a simple password or something.

I also meant to add that BitLocker has the added bonus of not bricking Windows 10/11 computers.

Hatjorn - April 15, 2024, 6:14 pm

(Apr 15, 2024 06:04 PM)DramaKing Wrote: [\[CITE\]](#) Point is that all FDE software probably uses AES for encryption. I'd never worry about a brute force attack unless you set up a simple password or something.

I also meant to add that BitLocker has the added bonus of not bricking Windows 10/11 computers. Great answer. It's nice to get information I can learn from. I guess some people would have wrote redicules answers to a noob question

7 - April 15, 2024, 6:20 pm

Well personally I use veracrypt and encrypt hidden partitions rather than focus so much on full disk encryption.

If I use full disk encryption I use luks

"The default cipher used for LUKS is aes-xts-plain64 . The default key size for LUKS is 512 bits."

But for veracrypt I use

(Serpent(Twofish(AES)) with SHA-512

"Three ciphers in a cascade operating in XTS mode. Each block is first encrypted with AES (256-bit key), then with Twofish (256-bit key), and finally with Serpent (256-bit key). Each cipher uses its own key. All keys are mutually independent.""

Hatjorn - April 15, 2024, 6:30 pm

(Apr 15, 2024 06:20 PM)NullDB Wrote: [\[CITE\]](#) Well personally I use veracrypt and encrypt hidden partitions rather than focus so much on full disk encryption.

If I use full disk encryption I use luks

"The default cipher used for LUKS is aes-xts-plain64 . The default key size for LUKS is 512 bits."

But for veracrypt I use

(Serpent(Twofish(AES)) with SHA-512

"Three ciphers in a cascade operating in XTS mode. Each block is first encrypted with AES (256-bit key), then with Twofish (256-bit key), and finally with Serpent (256-bit key). Each cipher uses its own key. All keys are mutually independent.""

This one is a more advanced. I will have to dig into it later today when I have time

Hackers - April 16, 2024, 10:04 pm

(Apr 15, 2024 06:20 PM)NulldB Wrote: [\[CITE\]](#) encrypt hidden partitions rather than focus so much on full disk encryption.

I'm a fan of partitions, or external drives, or other storage that is encrypted > full encrypted OS. Yes, data can be cached, yes, there may be tmp files, so full disk encryption has a use case, but for most people this level of protection isn't needed. but obviously depends on what people are up to.

7 - April 17, 2024, 12:42 am

(Apr 16, 2024 10:04 PM)nodes Wrote: [\[CITE\]](#) I'm a fan of partitions, or external drives, or other storage that is encrypted > full encrypted OS. Yes, data can be cached, yes, there may be tmp files, so full disk encryption has a use case, but for most people this level of protection isn't needed. but obviously depends on what people are up to.

This is true. I actually have disk encryption on with everything but overall its not the winner for me as most of my work is done on remote servers anyway. But encrypted hidden volumes are what make my life much more simple.

Personally, I say if you don't hide everything they stop looking. I don't want to not login to my laptop if stopped or checked, I don't want my computer to appear to have nothing on it. Just the stuff I need to keep private is very well protected.

But, yes depends on who's doing what, where and how

slezer - April 27, 2024, 6:44 am

ChaCha20 Poly is probably one of the best options out there next to AES256.

nucleo_type09 - April 27, 2024, 1:00 pm

(Apr 27, 2024 06:44 AM)slezer Wrote: [\[CITE\]](#) ChaCha20 Poly is probably one of the best options out there next to AES256.

well why not use sha[x] or other e-funcs from crypto++? is agood library, cross platform and versatile, but is not that good for partition/volume encryption tho, but.... but... the nsa also uses a sha256 for they security crap btw, i would not recommend bitlocker unless u r ok with compatibility issues as bitlocker is a microsoft proprietary software, and i've heard is not even compatible with all it's windows versions as well, let alone the fact that microsoft itself is spying on you so you might also have to be concerned about potential backdoors in your system you might not be aware of, there are a couple of other reasons not to pick bitlocker, go for AES (Advanced Encryption Standard) or RSA, but you didn't specify if u're looking for asymmetric or symmetric encryption, sha doesn't provide asymmetry while RSA does, SHA[X] supports a wide range of encryption algorithms as well, i would go for SHA if i were you. Also some SHA variants, such as SHA-1, are vulnerable to length extension attacks, where an attacker can appendd additional data to a hash without knowing the original input, so be careful with that one, go for SHA3 and over, for example, in SHA-256, which has a block size of 512 bits, the input message is padded with a '1' bit followed by '0' bits until the length is 448 bits less than a multiple of 512, then, the original message length is appended as a 64-bit binary :).

If you're not familiar with padding, padding prevents certain attacks, such as *length extension attacks*, then you have salts, used for protection against hash collision attacks which is another good point for sha functions.

Hatjorn - April 27, 2024, 2:43 pm

(Apr 27, 2024 01:00 PM)nucleo_type09 Wrote: [\[CITE\]](#) well why not use sha[x] or other e-funcs from crypto++? is agood library, cross platform and versatile, but is not that good for partition/volume

encryption tho, but.... but... the nsa also uses a sha256 for they security crap btw, i would not recommend bitlocker unless u r ok with compatibility issues as bitlocker is a microsoft proprietary software, and i've heard is not even compatible with all it's windows versions as well, let alone the fact that microsoft itself is spying on you so you might also have to be concerned about potential backdoors in your system you might not be aware of, there are a couple of other reasons not to pick bitlocker, go for AES (Advanced Encryption Standard) or RSA, but you didn't specify if u're looking for asymmetric or symmetric encryption, sha doesn't provide asymmetry while RSA does, SHA[X] supports a wide range of encryption algorithms as well, i would go for SHA if i were you. Also some SHA variants, such as SHA-1, are vulnerable to length extension attacks, where an attacker can append additional data to a hash without knowing the original input, so be careful with that one, go for SHA3 and over, for example, in SHA-256, which has a block size of 512 bits, the input message is padded with a '1' bit followed by '0' bits until the length is 448 bits less than a multiple of 512, then, the original message length is appended as a 64-bit binary :).

If you're not familiar with padding, padding prevents certain attacks, such as *length extension attacks*, then you have salts, used for protection against hash collision attacks which is another good point for sha functions.

This sounds so technical bro. Im a complete newbie in this field. Would Vera crypt alone be enough to encrypt my who pc's harddrive?

nucleo_type09 - April 27, 2024, 2:57 pm

(Apr 27, 2024 02:43 PM)Hatjorn Wrote: [\[CITE\]](#) This sounds so technical bro. Im a complete newbie in this field. Would Vera crypt alone be enough to encrypt my who pc's harddrive? would be but i'll not suggest it tho...

Hatjorn - April 27, 2024, 11:34 pm

(Apr 27, 2024 02:57 PM)nucleo_type09 Wrote: [\[CITE\]](#) would be but i'll not suggest it tho...

First you suggest Sha-x and then you wrote Sha-x is vulnerable. Im a bit confused so can you tell me what you suggest

nucleo_type09 - April 28, 2024, 4:10 am

(Apr 27, 2024 11:34 PM)Hatjorn Wrote: [\[CITE\]](#) First you suggest Sha-x and then you wrote Sha-x is vulnerable. Im a bit confused so can you tell me what you suggest

i wrote x is just an incognito, it can be whatever version of sha to use, i said sha1 is vulnerable not sha x, if wrote sha-x then my fault :), sha1 is vulnerable to length attacks but other sha versions r ok, like sha3, sha224,sha256, etc..., yes, you should use any sha except SHA 1, r u familiar with SHA algos? sha 1 is not the same as SHA3 the same as SHA224 is not the same as SHA256.

Compared to newer algorithms like SHA-256 or SHA-3, SHA-1 is less secure due to its shorter hash length and susceptibility to collision attacks. Its structure is less complex, making it more vulnerable to sophisticated attack methods.

Hatjorn - April 28, 2024, 4:11 am

(Apr 28, 2024 04:10 AM)nucleo_type09 Wrote: [\[CITE\]](#) i wrote x is just an incognito, it can be whatever version of sha to use, i said sha1 is vulnerable not sha x, if wrote sha-x then my fault :), sha1 is vulnerable to length attacks but other sha versions r ok, like sha3, sha224,sha256, etc..., yes, you should use any sha except SHA 1

Okay thank you for the explanation mate

nucleo_type09 - April 28, 2024, 4:27 am

(Apr 28, 2024 04:11 AM)Hatjorn Wrote: [\[CITE\]](#) Okay thank you for the explanation mate

im trying to share an image but ending up with image broken url for some reason haha, but did u get it at least why u should NOT use sha 1 ?

SHA 1:

512 bits Block Size

160 bits (i.e., 20 bytes), or 40 hexadecimal digits Hash Digest Size

80 (4 groups of 20 rounds) Rounds of ops

SHA-2 (224 & 256/384 & 512):

512/1024 bits Block Size

256 bits (i.e., 32 bytes), or 64 hexadecimal digits/512 bits (i.e., 64 bytes), or 128 hexadecimal digits

64 (for SHA-224 and SHA-256)/80 (SHA-384/SHA-512) Rounds of operations

SHA-3 (224/256/384/512):

32/576 bits (this is referred to as a Rate [R] for SHA-3 algorithms) Block Size

224/256/384/512 bits (i.e., 28/32/48/64 bytes), or 56/64/96/128 hexadecimal digits hash digest size and 24 rounds of Ops.

now you should understand why sha-1 is to be avoided...

Hatjorn - April 28, 2024, 4:30 am

(Apr 28, 2024 04:27 AM)nucleo_type09 Wrote: [\[CITE\]](#) im trying to share an image but ending up with image broken url for some reason haha, but did u get it at least why u should NOT use sha 1 ?

Yea i understand the point but I dont understand what "length attacks" means.

nucleo_type09 - April 28, 2024, 4:34 am

(Apr 28, 2024 04:30 AM)Hatjorn Wrote: [\[CITE\]](#) Yea i understand the point but I dont understand what "length attacks" means.

my fault, what i wanted to write was length extension not length, in a length extension attack, an attacker who knows the output hash of a secret message and its length can append additional data to the message without knowing the original message content. This is possible because hash functions like SHA-1 process messages in fixed-size blocks and append padding to the end of the message to reach the next block boundary, this is a length ext attack. To mitigate LEA, it's crucial to use hash functions that are not vulnerable to this type of attack, such as the SHA-3 family or HMAC constructions that use secure hash functions in combination with secret keys.

Py_Dev - May 1, 2024, 5:55 pm

(Apr 27, 2024 06:44 AM)slezer Wrote: [\[CITE\]](#) ChaCha20 Poly is probably one of the best options out there next to AES256.

I agree with this. If you are building your own application I suggest bouncy castle. They have CHACHA 20 poly. Very strong algorithm. I believe it is also 256 bit encryption with a 128 nonce.

Hatjorn - May 1, 2024, 6:33 pm

(May 1, 2024 05:55 PM)GTAF Wrote: [\[CITE\]](#) I agree with this. If you are building your own application I suggest bouncy castle. They have CHACHA 20 poly. Very strong algorithm. I believe it is also 256 bit encryption with a 128 nonce.

Its for a full disk encryption for my pc bro

Py_Dev - May 2, 2024, 4:27 am

(May 1, 2024 06:33 PM)Hatjorn Wrote: [\[CITE\]](#) Its for a full disk encryption for my pc bro Use Parrot OS. When installing use LUKS.