

Forum:[Hack Forums](#)

Thread: [Preferred Cryptographic Methods?](#)

Tyr - March 14, 2025, 5:12 pm

I'm curious to know which cryptographic method you rely on most for your security and privacy, and I'd like to get your input through a poll I've set up. I've designed this poll to not only capture your favorite techniques but also to spark a broader discussion on how different cryptographic methods perform in our day-to-day security practices.

In the poll, I'll ask you a straightforward question: Which cryptographic method do you prefer for security and privacy? I've included several options based on popular methods and emerging trends:

- AES (Advanced Encryption Standard)
- RSA (Rivest-Shamir-Adleman)
- ECC (Elliptic Curve Cryptography)
- ChaCha20
- Blowfish/Twofish
- Quantum Cryptography (Post-Quantum Algorithms)
- Other (Comment Below)

I understand that each method comes with its own set of strengths and quirks, which is why I'm giving you the option to select more than one if you apply different techniques in various scenarios. If none of the listed options quite fits your style, the "Other" option allows you to share your unique approach in the comments section. Also unique scenarios call for different algorithms so feel free to include that as well in your reply. If there's more than one (which I speculate is the case), feel free to say.

Look forward to see the replies.

ttbr0 - March 14, 2025, 6:06 pm

im no crypto expert nor do i really read much about it but the basics stay the same. it really depends on your needs because symmetric and asymmetric have their use cases and can be chained to provide guarantees. grouping them all together does not really make any sense.

im not particularly worried about most modern day symmetric algorithms so using the standardized aes is sufficient given a large enough key size, the correct encryption mode (not ecb for example) and obviously correct and proper implementation and usage. i dont believe other close contenders like blowfish and chacha20 have any issues either and i think it doesnt really matter and is up to preference.

asymmetric encryption for things like ssh i think the current recommendation is using ed25519 so i just go with that since it is more efficient and secure compared to rsa. quantum will mainly affect asymmetric algorithms given how shors algorithm trivializes the factorization math behind something like rsa (im unsure about the math behind ecc). i believe any and all tls communications that have been stashed by the nsa will be broken when quantum computing with enough qubits is built regardless of technology like perfect forward secrecy assuming they have stored all of the communication history for each session. once the asymmetric crypto is broken, all the symmetric keys will be leaked and all data can be decrypted. having said that, symmetric crypto seems to be somewhat resistant to quantum attacks so with a large enough key size, you should be fine.

post quantum crypto is slowly being developed but i dont know if any of it has been integrated into everything yet. but im not too worried about it personally. i dont use telegram for anything important and i dont advocate for it either since they break the first rule of crypto: never roll your own crypto. use signal.

putnik1313 - May 22, 2025, 5:22 am

i just noticed you forgot to mention SERPENT cipher, for people who don't know, SERPENT is actually more secure than AES, even if AES is used with a key of 256 bits and GCM mode, SERPENT offer more security if properly implemented, the reason Rijndael was approved and made the standard was actually because the NSA found a way to exploit it but very few people know this today, while they did not find a way in SERPENT, so yeah... if you wanna go for the most secure symmetric cipher, go for SERPENT at the cost of some performance in software implementation

(Mar 14, 2025 06:06 PM)ttbr0 Wrote: [\[CITE\]](#) im no crypto expert nor do i really read much about it but the basics stay the same. it really depends on your needs because symmetric and asymmetric have their use cases and can be chained to provide guarantees. grouping them all together does not really make any sense.

im not particularly worried about most modern day symmetric algorithms so using the standardized aes is sufficient given a large enough key size, the correct encryption mode (not ecb for example) and obviously correct and proper implementation and usage. i dont believe other close contenders like blowfish and chacha20 have any issues either and i think it doesnt really matter and is up to preference.

asymmetric encryption for things like ssh i think the current recommendation is using ed25519 so i just go with that since it is more efficient and secure compared to rsa. quantum will mainly affect asymmetric algorithms given how shors algorithm trivializes the factorization math behind something like rsa (im unsure about the math behind ecc). i believe any and all tls communications that have been stashed by the nsa will be broken when quantum computing with enough qubits is built regardless of technology like perfect forward secrecy assuming they have stored all of the communication history for each session. once the asymmetric crypto is broken, all the symmetric keys will be leaked and all data can be decrypted. having said that, symmetric crypto seems to be somewhat resistant to quantum attacks so with a large enough key size, you should be fine.

post quantum crypto is slowly being developed but i dont know if any of it has been integrated into everything yet. but im not too worried about it personally. i dont use telegram for anything important and i dont advocate for it either since they break the first rule of crypto: never roll your own crypto. use signal.

Regarding the math behind them, if we're talking about just RSA core logic ONLY, then the math you find in symmetric ciphers like AES is bigger and more complex in my own opinion..

Yeww - May 22, 2025, 1:39 pm

can you pm me please Tyr

ZLOY - May 24, 2025, 8:58 am

I really appreciate stream ciphers like ChaCha20 (even Salsa20) when encrypting small sequences of bytes that are smaller than a block, since I don't have to worry about block size or padding.

TemporalAnomaly73946 - May 24, 2025, 10:04 am

SERPENT is definitely what I use everyday.

putnik1313 - May 24, 2025, 10:43 am

(May 24, 2025 10:04 AM)TemporalAnomaly73946 Wrote: [\[CITE\]](#) SERPENT is definitely what I use

everyday.

SERPENT is definitely a better choice than AES, why do you use SERPENT if I may ask? just curiosity :)

socratic - May 24, 2025, 12:40 pm

(May 24, 2025 10:04 AM)TemporalAnomaly73946 Wrote: [\[CITE\]](#) SERPENT is definitely what I use everyday.

That's almost definitely not true. AES is the standard for a reason and you are forced to use it if you want to interact with the internet in a way that is secure.

devnullops - May 25, 2025, 8:14 pm

I've taken a few cryptography classes, which taught me that I'm not as clever as I sometimes like to think, and to stick with the vetted stuff.

(I didn't say "defaults" because it's pretty well-documented that the NSA and others have influenced companies to make shitty defaults, knowing that users don't really mess with them.)

So my typical practice is to google the program/framework/situation plus the string "best practices" and spend a little time reading up on what The Experts do in a given situation, and to understand the various trade-offs, since the answer is always "it depends".

I generally max out key size unless there's some good performance reason not to. I used to use SERPENT with TrueCrypt back in the day, due to the NSA-related allegations above, but I feel like it's usually not an option in day-to-day stuff.

putnik1313 - May 26, 2025, 5:19 am

(May 25, 2025 08:14 PM)devnullops Wrote: [\[CITE\]](#) I've taken a few cryptography classes, which taught me that I'm not as clever as I sometimes like to think, and to stick with the vetted stuff.

(I didn't say "defaults" because it's pretty well-documented that the NSA and others have influenced companies to make shitty defaults, knowing that users don't really mess with them.)

So my typical practice is to google the program/framework/situation plus the string "best practices" and spend a little time reading up on what The Experts do in a given situation, and to understand the various trade-offs, since the answer is always "it depends".

I generally max out key size unless there's some good performance reason not to. I used to use SERPENT with TrueCrypt back in the day, due to the NSA-related allegations above, but I feel like it's usually not an option in day-to-day stuff.

what classes did you take?

devnullops - May 26, 2025, 10:06 am

<https://www.coursera.org/learn/cryptography> and <https://www.coursera.org/learn/crypto> (the old one, before they started charging extra for it). Looks like Cryptography II is available here: <https://www.my-mooc.com/en/mooc/crypto2>, based on their book (<https://toc.cryptobook.us/>)

I also went through a few books, like Practical Cryptography by Ferguson/Schneier and another one that I can't find right now, that was like 'Cryptography Engineering' or something. I thought it was part of that series but I guess not..

I just enrolled in <https://www.coursera.org/specializations/applied-crypto> because I'm getting a little rusty. I try to cycle through basics (going to do Algorithms & Data Structures since I haven't done anything meaningful in that area in a while).

There's also a Beginner-level "Intro to Applied Crypto" by the same folks (U of Colorado)
<https://www.coursera.org/specializations/introduction-applied-cryptography>

TemporalAnomaly73946 - June 4, 2025, 4:38 am

(May 24, 2025 12:40 PM)socratic Wrote: [\[CITE\]](#) That's almost definitely not true. AES is the standard for a reason and you are forced to use it if you want to interact with the internet in a way that is secure.

I said I use SERPENT for privacy and security purposes, but I never said that I used exclusively SERPENT.

(May 24, 2025 10:43 AM)putnik1313 Wrote: [\[CITE\]](#) SERPENT is definitely a better choice then AES, why do use use SERPENT if i may ask? just curiosity :)

I use it primarily for encrypting files on other sort of stuff. I'm not a specialist in cryptography but I needed something very strong because I'm paranoid, and unless you have really, really important files that you REALLY need to keep secret I would recommend you just use AES. (Also there is no BEST encryption, everyone has different needs and different threat models. Actually I don't even need something as strong as SERPENT but it feels satisfying to me to know that my curriculum vitae is encrypted with SERPENT.)

Tyr - June 4, 2025, 10:58 am

(Jun 4, 2025 04:38 AM)TemporalAnomaly73946 Wrote: [\[CITE\]](#) I said I use SERPENT for privacy and security purposes, but I never said that I used exclusively SERPENT.

I use it primarily for encrypting files on other sort of stuff. I'm not a specialist in cryptography but I needed something very strong because I'm paranoid, and unless you have really, really important files that you REALLY need to keep secret I would recommend you just use AES. (Also there is no BEST encryption, everyone has different needs and different threat models. Actually I don't even need something as strong as SERPENT but it feels satisfying to me to know that my curriculum vitae is encrypted with SERPENT.)

No blowfish? That's for the true paranoid type.

TemporalAnomaly73946 - June 4, 2025, 1:11 pm

(Jun 4, 2025 10:58 AM)Tyr Wrote: [\[CITE\]](#) No blowfish? That's for the true paranoid type.

As I said, I'm not an expert in cryptography and I simply have some basic knowledge, so I don't know all of them. But you seem quite right about that, so thanks for the suggestion !

Tyr - June 4, 2025, 4:36 pm

(Jun 4, 2025 01:11 PM)TemporalAnomaly73946 Wrote: [\[CITE\]](#) As I said, I'm not an expert in cryptography and I simply have some basic knowledge, so I don't know all of them. But you seem quite right about that, so thanks for the suggestion !

Only teasing you my friend; best of luck with your learning endeavors!

TemporalAnomaly73946 - June 5, 2025, 10:12 am

(Jun 4, 2025 04:36 PM)Tyr Wrote: [\[CITE\]](#) Only teasing you my friend; best of luck with your learning endeavors!

thank you !

Hunt3rX211111 - June 8, 2025, 3:20 am

My favorite encryption method is the Advanced Encryption Standard (AES). AES is a symmetric encryption algorithm widely regarded as safe, fast, and flexible. It encrypts data in fixed-size blocks (128 bits) and supports multiple key lengths (128, 192, or 256 bits), with longer keys providing stronger security.

Voidlight - June 8, 2025, 9:18 pm

best encryption for malware is some ai generated slop custom algorithm. prompt something like:
Code Generate me a function that takes in raw bytes and outputs encrypted bytes based on a key.
make the encryption method obscure and esoteric, security and being able to crack it are not an issue or the focus, only novelty and obscurity of the algorithm, is should be something completely unique and outside the box.

Tyr - June 8, 2025, 10:59 pm

(Jun 8, 2025 09:18 PM)Voidlight Wrote: [\[CITE\]](#) best encryption for malware is some ai generated slop custom algorithm. prompt something like:

Code Generate me a function that takes in raw bytes and outputs encrypted bytes based on a key.
make the encryption method obscure and esoteric, security and being able to crack it are not an issue or the focus, only novelty and obscurity of the algorithm, is should be something completely unique and outside the box.

interesting i never contemplated this, good addition man