

Forum:[Hack Forums](#)

Thread: [What is the best algorithm to encrypt a file ?](#)

Danny65 - July 18, 2025, 11:14 am

What is the best algorithm to encrypt a file ?

DramaKing - July 18, 2025, 11:26 am

(Jul 18, 2025 11:14 AM)Danny65 Wrote: [\[CITE\]](#) What is the best algorithm to encrypt a file ?
You're asking like it matters. One member suggested that stream ciphers are better than block ciphers, but I can't say that any cipher can't be decrypted by AV, which I assume is the point of the question.

Danny65 - July 18, 2025, 11:32 pm

(Jul 18, 2025 11:26 AM)DramaKing Wrote: [\[CITE\]](#) You're asking like it matters. One member suggested that stream ciphers are better than block ciphers, but I can't say that any cipher can't be decrypted by AV, which I assume is the point of the question.
Thanks a lot !

???????????? - July 19, 2025, 4:08 am

(Jul 18, 2025 11:32 PM)Danny65 Wrote: [\[CITE\]](#) Thanks a lot !
I think the best algorithm to encrypt a file is AES-256 (Advanced Encryption Standard with a 256-bit key), especially using the GCM mode for both encryption and integrity. It's fast, highly secure, and widely supported across systems. For extra safety, combine it with a strong password-based key derivation like PBKDF2 or Argon2. AES-256-GCM is the go-to choice for securely encrypting files of any size.

Danny65 - July 19, 2025, 8:23 am

(Jul 19, 2025 04:08 AM)???????? Wrote: [\[CITE\]](#) I think the best algorithm to encrypt a file is AES-256 (Advanced Encryption Standard with a 256-bit key), especially using the GCM mode for both encryption and integrity. It's fast, highly secure, and widely supported across systems. For extra safety, combine it with a strong password-based key derivation like PBKDF2 or Argon2.
AES-256-GCM is the go-to choice for securely encrypting files of any size.
Nice thanks a lot man !

tanooki - July 31, 2025, 10:51 pm

(Jul 19, 2025 04:08 AM)???????? Wrote: [\[CITE\]](#) I think the best algorithm to encrypt a file is AES-256 (Advanced Encryption Standard with a 256-bit key), especially using the GCM mode for both encryption and integrity. It's fast, highly secure, and widely supported across systems. For extra safety, combine it with a strong password-based key derivation like PBKDF2 or Argon2.
AES-256-GCM is the go-to choice for securely encrypting files of any size.
Agreed.

Use this with Picocrypt, a lightweight file encryption tool.

(If you had to choose one, just use AES-256-GCM).

(Jul 18, 2025 11:26 AM)DramaKing Wrote: [\[CITE\]](#) You're asking like it matters. One member suggested that stream ciphers are better than block ciphers, but I can't say that any cipher can't be decrypted by AV, which I assume is the point of the question.
To put it simply:

Block ciphers are better "secure encryption". What I mean by that is that block ciphers use more complex operations, leading to more complex encryption. Better for secure data storage and bulk. Stream ciphers are quicker. Faster operations, albeit simpler. Better for real-time data transmission.

Each one has their own time and place to be used.

LOVESOSA098997 - *August 19, 2025, 8:20 am*

AES-256