

Forum:[Hack Forums](#)

Thread: [Coding an AES encryptor || Need help to code](#)

Nanga - March 27, 2018, 9:04 pm

Hello guys,
It's been quite a while since i have started this project.

I need a little help, i basically have no idea where to start coding for an AES encryptor i have developed certain algorithms to further improve the current scenario in AES and basically want to implement it. (preferably in C or C++ lang even java will do) .

INFO ABOUT AES and MY FIX

The AES currently uses the Rijndael algo to generate the ciphertext, but the use of this algorithm allows error propagation in the cipher text as it goes through several rounds(ultimately resulting in a huge difference from the original plaintext when the ciphertext is decrypted), well i have theoretically devised an algorithm which will help in warding off this error propagation in the ciphertext. I have the Block diagram also ready with me, but the problem is that i am very bad at coding, i had coding for 3 years and i didnt even attend a single lecture , but i know the basics of coding, and if someone can direct me on how to start with the coding process and what all to do i will be very grateful to him/her. ?

Please help me in my endeavour.

Thank you for reading. ?

Annabelle Lee - March 29, 2018, 2:05 am

Well, if you don't know how to code at all, I suggest learning that first. If you do, I suggest finding an implementation of the current AES algorithms and reading that, and understanding how it works. From there you can edit the existing code or reference it when writing your own version. Regardless, cryptography isn't that simple a subject and you might find it useful to do a basic version of your algorithm on paper; that way you can see how it works and iron out any further issues. Hopefully my advice was sound, but perhaps someone with more cryptography experience can weigh in as well.

Nanga - March 29, 2018, 4:21 am

(Mar 29, 2018 02:05 AM)Annabelle Lee Wrote: [\[CITE\]](#) Well, if you don't know how to code at all, I suggest learning that first. If you do, I suggest finding an implementation of the current AES algorithms and reading that, and understanding how it works. From there you can edit the existing code or reference it when writing your own version. Regardless, cryptography isn't that simple a subject and you might find it useful to do a basic version of your algorithm on paper; that way you can see how it works and iron out any further issues. Hopefully my advice was sound, but perhaps someone with more cryptography experience can weigh in as well.
Yes indeed.

But i know coding basics and all the loops but the problems i face are with classes and objects.

Annabelle Lee - March 29, 2018, 5:05 am

Then what part are you stuck with, exactly? What have you tried so far?

un4gott3n - March 29, 2018, 8:41 am

I would personally recommend that you start out with easier encryption algorithms such as XOR and RSA before you move on to more advanced algorithms.

Check out these links for more information on how to build simple encryption/decryption projects;

Click me Spoiler ([Click to View](#))

<http://www.trytoprogram.com/cpp-examples/cplusplus-program-encrypt-decrypt-string/>

<http://www.cplusplus.com/forum/articles/38516/>

Get familiar with these types of algorithms and then you will have some knowledge going into the more difficult things.

Good luck.

webdev77 - March 30, 2018, 11:01 am

(Mar 29, 2018 04:21 AM)Nanga Wrote: [\[CITE\]](#) Yes indeed.

But i know coding basics and all the loops but the problems i face are with classes and objects. Show us the outline of what your classes and objects should look like. If you don't know, post what you do know about them.

Sajuuk - March 31, 2018, 12:53 am

(Mar 29, 2018 04:21 AM)Nanga Wrote: [\[CITE\]](#) Yes indeed.

But i know coding basics and all the loops but the problems i face are with classes and objects. For anyone to be able to assist you, they'd need to see what they're working with. Otherwise, they can only assume they're blabbering about something relevant to your issue.