What is AES Encryption?

- 2022-08-10 - Encryption

The AES cipher is part of a family known as block ciphers, which are algorithms that encrypt data on a per-block basis.

These “blocks” which are measured in bits determine the input of plaintext and output of ciphertext. So for example, since AES is 128 bits long, for every 128 bits of plaintext, 128 bits of ciphertext are produced.

Like nearly all encryption algorithms, AES relies on the use of keys during the encryption and decryption process. Since the

AES algorithm is symmetric, the same key is used for both encryption and decryption (I will talk more about what this means in a moment).

AES operates on what is known as a 4 x 4 column major order matrix of bytes. If that seems like too much of a mouthful to you, the cryptography community agrees and termed this process the *state*.

The key size used for this cipher specifies the number of repetitions or “rounds” required to put the plaintext through the cipher and convert it into ciphertext.

Here’s how the cycles break down.

- 10 rounds are required for a 128-bit key
- 12 Rounds are required for a 192-bit key
- 14 Rounds are required for a 256-bit key

While longer keys provide the users with stronger encryptions, the strength comes at the cost of performance, meaning that they will take longer to encrypt.

Conversely, while the shorter keys aren't as strong as the longer ones, they provide much faster encryption times for the user.

Aren't Symmetric Ciphers Easier to Break than Asymmetric?

Now before we move on, I want to briefly touch on a topic that has sparked a significant amount of controversy within the cryptographic community.

As I noted earlier, AES relies on a symmetric algorithm, meaning that the key used to encrypt information is the same one used to decrypt it. When compared to an asymmetric algorithm, which relies on a private key for decryption and a separate public key for file encryption, symmetric algorithms are often said to be less secure.

And while it is true that asymmetric encryptions do have an added layer of security because they do not require the distribution of your private key, this does not necessarily mean that they are better in every scenario.

Symmetric algorithms do not require the same computational power as asymmetric keys, making them significantly faster than their counterparts.

However, where symmetric keys fall short is within the realm of file transferring. Because they rely on the same key for encryption and decryption, symmetric algorithms require you to find a secure method of transferring the key to the desired recipient.

With asymmetric algorithms, you can safely distribute your public key to anyone and everyone without worry, because only your private key can decrypt encrypted files.

So while asymmetric algorithms are certainly better for file transfers, I wanted to point out that AES is not necessarily less secure because it relies on symmetric cryptography, it is simply limited in its application.

Attacks and Security Breaches Related to AES

AES has yet to be broken in the same way that DES was back in 1999, and the largest successful brute-force attack against *any* block cipher was only against a 64-bit encryption

(at least to public knowledge).

The majority of cryptographers agree that, with current hardware, successfully attacking the AES algorithm, even on a 128-bit key would take billions of years and is, therefore, highly improbable.

At the present moment, there isn't a single known method that would allow someone to attack and decrypt data encrypted by AES so long as the algorithm was properly implemented.

However, many of the documents leaked by Edward Snowden show that the NSA is researching whether or not something known as the tau statistic could be used to break AES.

Side Channel Attacks

Despite all of the evidence pointing to the impracticality of an AES attack with current hardware, this doesn't mean that AES is completely secure.

Side channel attacks, which are an attack based on information gained from the physical implementation of a cryptosystem, can still be exploited to attack a system encrypted with AES. These attacks are not based on weaknesses in the algorithm, but rather physical indications of a potential weakness that can be exploited to breach the system.

Here are a few common examples.

- **Timing Attack**: These attacks are based on attackers measuring how much time various computations need to perform.
- **Power-monitoring Attack**: These attacks rely on the variability of power consumption by hardware during computation
- **Electromagnetic Attacks**: These attacks, which are based on leaked electromagnetic radiation, can directly provide attackers with plaintext and other information. This information can be used to surmise the cryptographic keys by using methods similar to those used by the NSA with TEMPEST.

The Anthem Hacking: How AES Could Have Saved 80 Million People's Personal

Data

During February of 2015, the database for the Anthem insurance company was hacked, compromising the personal data of over 80 million Americans.

The personal data in question included everything from the names, addresses, and social security numbers of the victims.

And while the CEO of Anthem reassured the public by stating the credit card information of their clients was not compromised, any hacker worth his salt can easily commit financial fraud with the stolen information.

While the company's spokesperson claimed that the attack was unpreventable and that they had taken every measure to ensure the security of their client's information, nearly every major data security company in the world disputed this claim, pointing out that the breach was, in fact, *completely* preventable.

While Anthem encrypted data *in transit,* they did *not* encrypt that same data while it was at rest. Meaning that their entire database.

So even though the attack itself might have been unpreventable, by applying a simple AES encryption to the data at rest, Anthem could have prevented the hackers from viewing their customer's data.

Conclusion

With the increasing prevalence of cyber-attacks and the growing concerns surrounding information security, it is more important now than ever before to have a strong understanding of the systems that keep you and your personal information safe.

And hopefully, this guide has helped you gain a general understanding of one of the most important security algorithms currently in use today.

AES is here to stay and understanding not only how it works, but how you can make it

work *for* you will help you to maximize your digital security and mitigate your vulnerability to online attacks.

If you really want to dig into AES, I consider watching the video below by *Christof Paar* (it goes in-depth and it's interesting, too):

https://www.youtube.com/watch?v=NHuibtoL_qk#action=share

Tags

AES

encryption