Maluki Muthusi Maluki
P15/81741/2017

AES, Rajndael Algorithm

Advanced Encryption Standard is an encryption specification that was standardized by the U.S NIST in 2001. It is a variant of the Rajndael block cipher that was developed by Vincent Rijmen and and Joan Daemen, who submitted their proposal to NIST during AES selection process, (Daemen & Rijmen 2002). AES with 10 rounds was the fastest algorithm among the five choice that made it to the finalist, (Schneier et al. 2000, p. 9). The algorithm was chosen because of its speed and security strength.

AES uses a symmetric key algorithm. It is a superset of DES algorithm, performs six times faster. AES does not suffer from an algebraic attach, (Ferguson et al. 2001). AES uses 10, 12, 14 rounds of encreption for key sizes 128, 192 and 256 bits. This enables flexibility in its implementation, adopting to the different use cases.

A system that uses AES bases its security on the hardness of breaking the cipher blocks. The larger the cipher block the harder the problem, hence the more secure the system is. The data is guranteed to be secure over a certain period of time, due to computational power limitations required to break the algorithm, (Ou 2006).

We cannot say that AES is a perfect cryptographic algorithm, since it can theoretically be broken, (Schneier et al. 2000). We can feel safe using AES because it can protect data for the next 50 years, or over our lifetime period. For example, when used to protect data in transaction, that data becomes obsolete very quickly. Hence even if the algorithm was to be broken after 10 years since it was used to protect that data, the information would be less relevant.

AES has been used to protect data in the WEB. SSL/TLS specifies AES in its standard. It is used in Wi-Fi as part of WPA2, VPN implementations, operating system file systems and in mobile applications, among many other use cases. So far there has been not a single incident reported of the algorithm compromised, or hacked.

References

Daemen, J. & Rijmen, V. (2002), *The design of Rijndael : AES–the Advanced Encryption Standard*, Springer.

Ferguson, N., Schroeppel, R. & Whiting, D. (2001), ‘A simple algebraic representation of rijndael’, *Encryption, security* .

Ou, G. (2006), ‘Is encryption really crackable?’. https://www.zdnet.com/article/is-encryption-really-crackable/.

Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., Ferguson, N. & Kohno, T. (2000), ‘The twofish team’s final comments on aes selection’, *Security* .