Ben Murphy & Coleman Pagac

Professor Urness

CYB 010: Introduction to Cybersecurity

October 11th 2023

A Comparative Analysis of RSA and AES Encryption Algorithms

In the field of modern cryptography, the RSA and AES algorithms stand out as the cornerstones of digital security. While AES illustrates symmetric encryption at its best and excels in data confidentiality, RSA is an asymmetric encryption algorithm recognized for its secure communication and digital signature capabilities. Together, these industry heavyweights in cryptography serve crucial roles in protecting confidential data, guaranteeing privacy, and preserving the integrity of digital data in diverse applications. This investigation will define RSA and AES, highlight their distinctive qualities, and clarify the various functions they perform in the dynamic field of cybersecurity. The success of each depends on the particular security requirements and scenarios in which it is used; while each has unique strengths and areas of applicability, there isn't one that is fundamentally better.

RSA is an essential cryptographic technique that has greatly influenced the field of digital security. Asymmetric encryption, such as RSA, is a ground-breaking idea that significantly altered how we protect digital data. RSA relies on a pair of distinct keys: a public key for encryption and a private key for decryption, in contrast to standard symmetric encryption, which uses a single shared key for encryption and decryption. This development improved the safety of digital communication and opened the door for a wide range of uses in secure messaging, digital signatures, and data security.

AES, which stands for Advanced Encryption Standard. AES is a symmetric block cipher encryption method. Unlike RSA, AES is a symmetric encryption method, which means that there is no public or private key; there is one single key that encrypts and decrypts the information. Due to this, RSA is often used to encrypt the key used for AES. AES was created for use by the US government, specifically by contracts for the US government. The US government wanted to create an impenetrable encryption method to replace the previous encryption standard, DES or Data Encryption Standard, published in 1977. They landed on using the Rijndael cipher as the proposed algorithm for AES in late 2000, and on November 26th, 2001, AES was established as the primary encryption method for the US Government and is still used today. AES is used in many more places besides the government. Some examples are cyber security, electronic data protection, protecting storage data on hard drives, and generally just any form of high-strength security encryption. Overall, AES-256 is exceptionally secure and is the most secure encryption algorithm available today. It is used extensively worldwide to protect the world's most valuable information. It's so secure that the lowest security of AES (AES-128) would take about 200 times longer than the universe has existed to crack, all while also assuming the attacker has a quantum computer with around 2,953 logical qubits. In conclusion, AES is unmatched in encrypting user's data and is in a league of its own compared to other leading encryption methods.

Though it may appear complex at first, RSA encryption works simply by employing two keys: a public key for locking data and a private key for unlocking it. The mystery surrounding RSA encryption can be removed by understanding this basic idea. The fundamental building block of RSA is the choice of two enormous prime numbers. The foundation of security consists of these prime integers. These prime numbers are multiplied and create the beginning of a

challenging security system. Both the public and private keys depend on this number. Another significant number is the total between the two prime numbers. The next step is to choose a smaller integer, which serves as the public key. In this case, the requirement must be less than the total of the two prime numbers being multiplied. A public key is created as a result of this selection and is then used to lock the data.

On the other hand, the data can only be unlocked with the private key consisting of two numbers. The public key encrypts data when it needs to be safeguarded. This procedure changes the data into a format called "ciphertext." What is safely stored or communicated over networks is the ciphertext. It's important to note that this ciphertext may only be restored to its original form with the private key. The mathematical difficulty of determining the private key from the public key is the cornerstone of RSA's security. The larger the prime numbers involved are, the more difficult this issue becomes.

In conclusion, RSA encryption effectively functions as a locking and unlocking system for data. The data is kept secure during transmission thanks to the use of two keys—public and private—and can only be unlocked by the intended receiver. Although the mathematics underlying RSA are complex, at its core, it is a dependable technique for data security in the digital age.

AES functions quite differently than most other encryption methods due to it being built as a symmetric block cipher with a key schedule. When encrypting the information, the algorithm will divide the plain text into 4x4 16-byte blocks. AES functions on a system of SPN or substitution-permutation network; this means when encrypting data, AES will substitute the bytes for letters, integers, or symbols in place of the plain text characters. AES also uses permutation; when executing permutation, it shuffles the plain text into an unrecognizable order.

To begin encrypting with AES, the user will choose to encrypt the data with a 128,192 or 256-bit key. This will also determine how many rounds the encryption algorithm will cycle through. AES also functions with a key schedule to make different round keys. This means that when encrypting data and cycling through the rounds, AES will create a different key for every round or building on top of the existing key. A 128-bit key will cycle through 10 rounds, with 12 for a 192-bit key and 14 for a 256-bit. The next step is to add the key of choice to begin encrypting. Once added, the program will begin the SPN aspect of AES. AES substitutes the 16 bytes using the Rijndael S-Box. The Rijndael S-Box might seem insecure as it's a known public cipher, but it is incredibly random and has been built so that it's resistant to linear and differential cryptanalysis. The main criteria of the S-Box is that it's one-to-one, meaning that every aspect inputted will output a separate unrepeated output to replace the initial byte.

The second step of the SPN aspect is the permutation factor. AES now shifts the rows and mixes the columns in every block of information given. Interestingly, it shifts each round in the same order. Row one is left alone and is not shifted; in row two, everything is shifted to the left by one. Row three is shifted to the left by two, and it ends with row four moving three to the left. This does an incredibly excellent job of making the once-organized bites appear incredibly random while still being able to decrypt by simply reversing each row and how much it's been shifted. In the next step, the algorithm will alter every column and row by using a form of matrix multiplication. This functions by multiplying each column by each row. Overall, this is a much more complicated system for humans, but it's a simple task for computers. The time complexity is also exponential as it is O(n^2.371552), meaning the more extensive the matrix is, the longer it will take. The Matrix uses a four-by-four grid to prevent long encryption times instead of a larger one, like a 50 by 50. To finish the encryption, the algorithm adds the final round key and will

repeat this process up to 14 times. The only difference between each encryption round is the final round skips mixing columns as it adds little to no encryption. All of this can be done on the hard drive or CPU of the computer. These aspects culminate in creating a vastly dominant encryption method in the cyber security space.

There are numerous reasons for the continued usage of RSA, such as how the core of RSA's strength is built from outstanding security. Imagine it as a complex lock with a nearly impossible-to-crack code. The foundation of its security is a challenging mathematical problem that involves factoring the product of two enormous prime numbers. These prime integers serve as the key, and the longer the key, the more secure the encryption. Furthermore, RSA encryption is incredibly adaptable. It extends its usefulness beyond simple message protection to several different cryptographic tasks. RSA can be used for crucial functions like securely exchanging secret keys and generating digital certificates in addition to message encryption and safe transmission. Due to its versatility, RSA is an essential tool in digital security. It can protect various applications, from email and online banking security to maintaining the integrity of digital identities.

However, like anything else, RSA also has a few minor drawbacks. One of the primary problems with RSA encryption is the length of the key. Longer keys slow down the encryption and decryption processes while improving security. This can be an issue when sending large files quickly or in other circumstances when swift data transfer is necessary. One of the most urgent issues with RSA encryption is that it's also vulnerable to attacks from quantum computer systems. Cryptologists have deciphered that methods like Shor's algorithm have figured out how quantum computers have the potential to factor enormous numbers far more effectively than conventional computers. This advancement in computer technology poses a severe risk to RSA's

security because it might drastically cut the time needed to decrypt data. Post-quantum cryptography techniques have been created as a result of the vulnerability being addressed as quantum computer technology develops.

AES, like most encryption methods, has immense advantages while having minor drawbacks, some of which are how AES can strive in combating Brute Force encryption attacks and their inability to break through and steal encrypted information. This is once again due to Brute Force attacks taking trillions of years to break through the lowest level of AES encryption. Overall, AES is incredibly secure against Brute Force attacks, Linear cryptanalysis, and Algebraic attacks. AES also allows users to choose the key length they want to encrypt with. With this being the case, users are able to select how fast and secure they desire their plain text to be encrypted. Due to AES also being originally sponsored by the US government, it is an open-source solution and is royalty-free. This means that anybody can use it for anything they want. AES also replaced DES, and with that, it set a new standard of high-speed, secure encryption. AES also has high-speed encryption and decryption speeds. Overall, AES is one of the most secure encryption methods, if not the most secure.

Like most encryption methods, AES also has minor flaws. One major drawback is that it is a symmetrical encryption method, with which the same key is used to encrypt and decrypt, opening up a massive flaw in how both parties will keep the key secure in transit and storage. In order to transport the master key for your encryption, most encrypt the AES key with RSA encryption; this means that your AES encryption is only as good as your RSA encryption. AES can also sometimes be vulnerable to padding Oracle attacks where they specifically Target Cipher block chaining decryption methods in exploiting the error of “invalid padding” instead of

“decryption failed.” However, to prevent this effect, which many believe works, is to pad the information before authenticating and encrypting.

RSA and AES are two of the strongest ways to encrypt data, as both are great options at this moment; there really isn't a stronger encryption method, as both have flaws that hinder them from reaching the top spot in every category, but overall AES is the better encryption method for various reasons specifically that it dies certain things better than RSA. AES is incredibly secure like RSA, but in the near future, RSA will be cracked in a physical manner, proving the theorized flaw it has with quantum computers. When AES was created, it was built with quantum computers in mind and was designed in a way that quantum computers in the far future would still struggle to decrypt lower-tier AES encryption. Overall, AES has become the gold standard in cyber security and is widely used in every aspect of our lives. AES won’t be replacing RSA’s sheer speed for encryption for small items, but as the world gets more advanced, companies will turn to AES more and more.

References

"Advantages and Disadvantages of RSA Algorithm." *Aspiring Youths*, https://aspiringyouths.com/advantages-disadvantages/rsa-algorithm/. Accessed 11 Oct. 2023.

"AES 256 Encryption: What Is AES 256 Encryption." *Kiteworks | Your Private Content Network*, https://www.facebook.com/KiteworksCGCP, https://www.kiteworks.com/risk-compliance-glossary/aes-256-encryption/#:~:text=AES%2D256%20encryption%20is%20virtually,or%20system%20is%20completely%20secure. Accessed 11 Oct. 2023.

Cobb, Michael. "What Is the RSA Algorithm? Definition from SearchSecurity." *Security*, TechTarget, 4 Nov. 2021, https://www.techtarget.com/searchsecurity/definition/RSA?Offer=abMeterCharCount_var2.

Computerphile. *AES Explained (Advanced Encryption Standard) - Computerphile*. YouTube, 22 Nov. 2019, https://www.youtube.com/watch?v=O4xNJsjtN6E.

Dr. Mike Pound is a "Lecturer and researcher in Computer Science at Nottingham University."

"Matrix Multiplication Algorithm Time Complexity Explained | Saturn Cloud Blog." *Saturn Cloud | Your Data Science Cloud Environment*, 18 July 2023, https://saturncloud.io/blog/matrix-multiplication-algorithm-time-complexity-explained/.

"RSA Full Form - GeeksforGeeks." *GeeksforGeeks*, GeeksforGeeks, 10 Apr. 2020, https://www.geeksforgeeks.org/rsa-full-form/.

silver badges66 bronze badges, Lachezar BalevLachezar Balev 22522. “Encryption - Is the ‘Padding Oracle Attack’ Deterministic? - Cryptography Stack Exchange.” *Cryptography Stack Exchange*, https://crypto.stackexchange.com/q/40800.

Tree, Spanning. *AES: How to Design Secure Encryption*. YouTube, 22 Aug. 2023, https://www.youtube.com/watch?v=C4ATDMIz5wc. https://brianyu.me/ Brian Yu the creator of Spanning Tree, teaches at Harvard University and has created and taught courses about artificial intelligence and web programming.

Vaudenay, Serge. *Security Flaws Induced by CBC Padding Applications to SSL, IPSEC, WTLS...* Swiss Federal Institute of Technology (EPFL), https://www.iacr.org/cryptodb/archive/2002/EUROCRYPT/2850/2850.pdf. Accessed 11 Oct. 2023.

“What Is RSA? How Does an RSA Work? | Encryption Consulting.” *Encryption Consulting*, 23 Sept. 2020, https://www.encryptionconsulting.com/education-center/what-is-rsa/.

“What Is the Advanced Encryption Standard (AES)? - Zenarmor.Com.” *Zenarmor - Agile Service Edge Security*, https://www.zenarmor.com/docs/network-security-tutorials/what-is-advanced-encryption-standard-aes. Accessed 11 Oct. 2023.