RSA vs AES Encryptions

Introduction:

As a Data Engineer, data security, data privacy and data governance are part of a successful data pipelines. Data Security involves steps to ensure that the data is protected like RSA and AES encryptions. Data Privacy involved steps to make sure that access/store of the data is following the privacy standard like FERPA, HIPAA and etc. Data governance is a good procedure to practice at any organizations to ensure that the data was used appropriately by people in the organization since the weakest link in security and privacy is us. This paper focuses on the data security with RSA and AES encryptions and explains the pros and cons of each encryption type.

Overview of RSA and AES encryptions:

RSA is an asymmetric encryption that requires both public and private keys. It uses the public key to encrypt the data and the private key to decrypt the data. This will ensure that the cipher data can only be decrypted with users who have access to private key.

AES is a symmetric encryption that using the same key to encrypt and decrypt the data. The methods of encryption mainly consist of four steps which are substitution, shifting, mixing and further encryption. The decrypt process is just the reverse of the encryption process.

Below are the common characteristics of each encryption type:

Characteristics	RSA	AES
Full Name	Rivest-Shamir-Adleman	Advanced Encryption Standard
Year Invented/Developed	1977	1997
Key	Asymmetric	Symmetric
Key Sizes	1024/2048 bits	128/192/256 bits
Encryption Method	Whole Content at once	By Block

Below are pros and cons of RSA:

Pros	Cons
Security	Complexity
Widely used	Key Size
Key Exchange/Digital Signatures	Speed
	Vulnerability to Quantum Computing

RSA is highly secured due to the algorithm using the properties of large prime numbers to make it difficult to crack the code but at the same time it is a very complex algorithm with

large key size. Due to large key size, it can sometime affect the performance when encrypting large amount of data. RSA is also very popular and utilized by many industries and applications like online banking, e-commerce, and secure communications. Digital Signatures is also a good feature of RSA for verifying documents. RSA 1024 bit key is also not recommended due to recent development in quantum computing that can be vulnerable to brute force attacks.

Below are pros and cons of AES:

Pros	Cons
Robust Security Protocol (Easy to implement)	Too simple algebraic structure
Higher lengths Key sizes	Hard to implement with software
Widely used	Every block is always encrypted the same way
Speed	Key Management

AES encryption process are easy to learn and implement. It usually has a faster encryption and decryption times while consuming less resources. It is also widely used in a variety of applications like wireless security, file encryption and web https protocol.

Compare and Contrast RSA and AES encryption methods:

RSA is considered to be more secured than AES due to its algorithm complexity but AES is easier to manage and requires less computational power than RSA which make it faster in encryption/decryption performance. The minimum key length of 128 bits for AES is also recommended by many experts which yield the best performance, and it is still no evidence that it can be hacked as of date. In contrast the RSA minimum key length of 1024 bits is not recommended due to recent development in quantum computing that can potentially crack the code at this key length. Therefore, 2048 bits key length is recommended for RSA.

Due to RSA complexity it is best suited to encrypt small amount of data like small data files, SSH protocols and etc. AES is suitable to encrypt large amount of data which are the main method for encryption for many organizations like governments and financial institutions.

One of the weaknesses of AES is that it is using the same key for encryption and decryption. By distributing the key to many recipients, it is running a risk of key falling to the wrong hand while RSA uses two separate keys for encryption (public key) and decryption (private key). So only public key is distributed to the recipients for RSA.

By using these encryptions not only they ensure the data security but also help organizations to follow data privacy and data governance regulations.

Impact of RSA and AES encryption methods with data governance regulations:

In many situations, data sharing between organizations is needed in order to provide effective data insight. For example, universities and colleges might need wages data from Department of Labor in order to determine the social mobility of their students after graduation. To establish trust and accountability with the department of labor, universities and DOL need to ensure that the data is protected and this is where RSA or AES encryption can

come into play and help build trust and also follow regulations standard like FERPA to protect these students data. These encryptions not only protect the data but also can be used to establish secure connections between organizations.

Conclusion:

As you can see, RSA and AES encryptions can be utilized to protect organization data assets in many ways. They can be used to ensure data security (data encryption), data privacy (i.e. FERPA) and data governance (FERPA and data quality). RSA is suitable for securing smaller data files/connections (password) while AES is suitable for large data volume encryption due to its simplicity and speed. One of the AES encryption weaknesses is the key management since it's using the same key for both encryption and decryption. One way to deal with this weakness is by using both encryptions for their strengths. For example, we can use AES to encrypt the data while using RSA to encrypt the AES key. This will ensure the effective performance of data encryption/decryption while protecting the key.

There are many ways to protect organization data assets and RSA/AES encryption are ones that highly effective and widely used in many industries. It is imperative that as a data engineer, security awareness is one of the key duties in dealing with data.

References:

(2022, December 16). *What Is the Advanced Encryption Standard (AES)?* Usnews.com. Retrieved May 1, 2023, from https://www.usnews.com/360-reviews/privacy/what-is-advanced-encryption-standard

(n.d.). *RSA algorithm (Rivest-Shamir-Adleman)*. Techtarget.com. Retrieved May 1, 2023, from (2022, December 16). What Is the Advanced Encryption Standard (AES)? Usnews.com. Retrieved May 1, 2023, from https://www.usnews.com/360-reviews/privacy/what-is-advanced-encryption-standard

(n.d.). *Advantages and Disadvantages of RSA Algorithm*. Aspiringyouths.com. Retrieved May 1, 2023, from https://aspiringyouths.com/advantages-disadvantages/rsa-algorithm/

(n.d.). *What is the Advanced Encryption Standard (AES)?* Sunnyvalley.io/. Retrieved May 1, 2023, from https://www.sunnyvalley.io/docs/network-security-tutorials/what-is-advanced-encryption-standard-aes

(2022, November 14). *AES vs. RSA Encryption: What Are the Differences?* Precisely.com. Retrieved May 1, 2023, from https://www.precisely.com/blog/data-security/aes-vs-rsa-encryption-differences

Reis, J., & Housely, M. (2022). *Fundamentals of Data Engineering* (1st ed.). O'Reilly Media, Inc.