INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 07, July 2024, pp: 1323-1328

THE INTERPLAY BETWEEN RSA KEY LENGTH, SECURITY, AND COMPUTATIONAL EFFICIENCY: A COMPREHENSIVE REVIEW

Divya[1], Upasna Setia[2]

[1,2]Computer Science and Engineering, Ganga Institute of Technology and Management, India.

ABSTRACT

RSA (Rivest-Shamir-Adleman) is one of the Asymmetric key cryptographic algorithm ,which helps to secure data privacy and data confidentiality .This paper will help to understand **the** impact of key size on RSA algorithm security and efficiency, and also the role of randomness for key generation. Through an extensive literature review and simulations we explore how key length influence the difficulty of prime factorization and with that how it is resilience against many attacks. Also this paper discuss about the mathematical complexity of RSA. Additionally we review the impact of emerging technology for example quantum computing like shor's algorithm affect the security of RSA.

Keywords: Cryptography, Asymmetric algorithm, RSA, Key lengths, Security, Efficiency.

1. INTRODUCTION

RSA, one of the oldest cryptographic algorithm designed by Ron Rivest, Adi Shamir and Leonard Adleman. They publicly show this algorithm in 1977 [1]. It Charter in USA on 1983. The significant advancement by RSA is that it is the first algorithm which introduced the concept of two keys (public key and private key), for encryption and decryption RSA use two keys public key and private key respectively.

Before the RSA , cryptography primarily depend on the symmetric key algorithm where we use same key for both encryption and decryption. Symmetric key cryptography face the challenge of secure communication of the keys. At the Massachusetts Institute of Technology (MIT) RSA was invented by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977 by publishing a paper titled "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems."The algorithm was patented in the United States (US Patent 4,405,829) on September 20, 1983, and the patent expired in September 2000

PRIME FACTORIZATION: The idea behind this algorithm was that we can not break the multiplication of prime numbers. But if anyone can break these prime number, one can easily find the private key. So the capability of encryption and decryption is rely upon the length of key sizes**.** If we the key size, the longer the key length, it strength will also increases**.** RSA is widely adopted in various protocols and cryptographic standard, like SSL/TLS which secure internet communication, digital signature for authentication, PGP for email encryption. The security of RSA depends on its computational complexity. RSA is considered as the foundational element of modern cryptographic system, popularly used for securing digital communication. With the large key lengths a problem becomes more complex. We need to understand the relationship between RSA key length, security, and efficiency for maintaining security standards because of computational power advances and cryptographic or quantum attacks.

KEY GENERATION ALGORITHM: The keys are generated by multiplication of two prime numbers larger the prime numbers larger the key lengths), public key is the multiplication of these two prime numbers, and private key is generated from the same prime numbers. RSA key can be of length 1024 or 2048 bits long, but experts believe that 1024 bits keys could easily be broken in the near future it seems as impossible task now.

ALOGORITHM:

Choose any two prime numbers, let p and q such that there product should be larger than the message we want to encrypt [1].

n=p*q where n is called modulus for encryption and decryption

Now choose a number e(integer) such that $1<e<\phi(n)$

Where $\phi(n)=(p-1)*(q-1)$ p, q are integers.

Public key made of n and e. They have no common factor other than one. That means gcd(e,d(n))=1. To find the cipher text from the plain text following formula is used.

$C=m^e \bmod n$ where m is less than n

For private key d we use

$d_e \bmod\{(p-1)*(q-1)\}=1$ the private key is between d and n. to find the plain text m fron the cipher text c following formula is used:

$m=c^d \bmod n$.

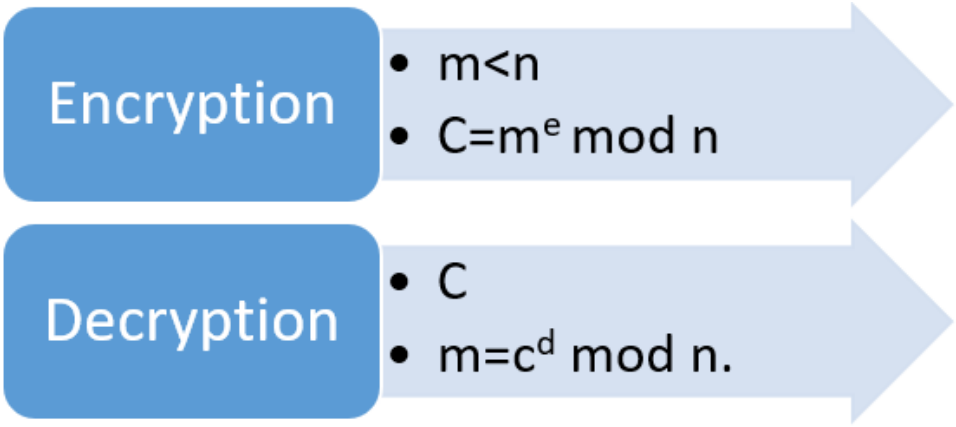
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 07, July 2024, pp: 1323-1328



IMPACT OF KEY SIZE ON RSA ALGORITHM:

RSA worked on different key sizes and they impact the security of message. So the security of RSA depends how large the key lengths are. If we take larger keys then it provides a great security so it will became impossible for attacker to find the private key. For any algorithm secrecy is the main task so they must protect their keys so that no one can read them. If the key size is large enough than its impossible to factorize them. RSA algorithm works on large integers or prime numbers and uses them as its private key and public key. For instance a 2048 bit key is more secure than a 1024bit key. Smaller key can be broken by brute force or factorization. So we need large key sizes for better security. There are some disadvantages of large key size in RSA:

ENCRYPTION /DECRYPTION SPEED:

Larger key affect the speed of encryption/decryption. For larger key we require more computational resources, which leads to slower encryption and decryption process. Larger key impact the performance of the algorithm, especially where many operation performed simultaneously.

Due to the need of finding large prime numbers, generating larger key is more time consuming.

1024 bit considered as insecure because now a days there are many advancement with that attacker can easily factorize the prime numbers

2048 bit considered as secure for many application.

3072 bit or 4096 bit considered for higher security needs ,against advances in computing power.

Use of different key size: Modern web browsers and servers often use 2048 bit keys foe SSL/TLS encryption.

4096 bit or higher keys can be used for data which needs to secure for many decades. Government and financial institution use larger keys like 3072 bit or 4096 bit to ensure higher security levels . Several attacks have influenced the computational power and the key sizes of RSA to ensure its security. Quadric sieve is an algorithm for factoring integer and General number field sieve currently the most efficient algorithm for factoring large integers.

RANDOMNESS IN KEY GENERATION:

We know it is necessary to have larger key size for better security, but randomness in key generation can also affect the security levels. We choose random prime numbers,so it is possible that attacker can factorize these with finding some common integer between them . So it is necessary to choose prime numbers like this that there are no common factor between them.

Alternative technique to RSA:

ECC (elliptical curve cryptography) is an alternative technique of RSA. It is useful and also asymmetric key cryptography method which works as elliptical curve and generates key as mathematical pairs of keys which represent on the curve and works as public and private keys. ECC is based on the algebraic expression of elliptical curve over finite fields. The main advantage of ECC over RSA is that it provides great security while using smaller key sizes

DIFFRENCE BETWEEN RSA (RIVEST-SHAMIR-ADLEMAN) AND ECC(ELLIPTIC CURVE CRYPTOGRAPHY):

	RSA	**ECC**
Memory used	More	Least
Execution time	Slower (because of larger key size)	Faster(key size is less than rsa)
Throughput	Lowest	Higher

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com

editor@ijprems.com

Vol. 04, Issue 07, July 2024, pp: 1323-1328

Energy Consumption	High energy consumption	Low energy consumption
Mathematical Complexity	Based on factoring large integer numbers	Based on algebraic structure of Elliptic Curve

2. LITERATURE REVIEW

The RSA algorithm, named after its inventors Rivest, Shamir, and Adleman, is one of the most widely used cryptographic systems for securing digital communication.

In its early days, RSA used to secure email and digital signature. It quickly gained popularity because of its robustness and the way it provide security. It assure security by providing the difficulty of mathematical problem, the factorization of large integers. RSA became a standard component in many security protocols, including SSL/TLS, which is a fundamental for securing web communications.

The security and efficiency of RSA largely depend on its key lengths. This literature review includes the impact of key length on its security and computational efficiency, examining the trade-offs and considerations involving choosing the appropriate key sizes.

Mathematical Foundation: This study evaluates RSA key lengths of 1024, 2048, 3072, and 4096 bits by evaluating the encryption and decryption times and monitoring CPU and memory usage. Using a combination of C++ for cryptographic operations and Python for resource monitoring, the research reveals a significant trade-off between security and performance. The findings suggest optimal key lengths for various applications, balancing security needs against computational resources. The security of RSA depends on its computational complexity. RSA is considered as the foundational element of modern cryptographic system, popularly used for securing digital communication. With the large key lengths a problem become more complex. We need to understand the relationship between RSA key length, security, and efficiency for maintaining security standards because of computational power advances and cryptographic or quantum attacks.

Implications of Key Length: The power of RSA encryption and decryption is rely upon the key size that used. When the size of keys is longer than these keys provides security which is stronger. For instance, a 1024-bit key was considered secure in the past, but with the advent of more powerful computers and advanced algorithms, it is now considered vulnerable to attack. Research has shown that RSA keys of 2048 bits are currently secure, but for applications requiring longer-term security, 3072-bit or 4096-bit keys are recommended. The Study by Lenstra and Verheul (2001) shows how different key length influence the recommendation for choosing these key lengths [2].

We can combine the two algorithm to enhance the security of RSA. RSA and Diffle-hellman keys can be combined together, we can use Diffle-hellman key for encipher and RSA keys for decipher [3].

Power consumption is an important factor while considering the security. According to study if comparison is done between DES, 3DES, AES, BLOWFISH, ECC, and RSA , the power consumption is higher in RSA over all these cryptographic algorithm[4].

When RSA is used for encryption it provides security so that only concerned user access the key [5].

The comparison is done with parameter like speed and security. In asymmetric cryptography it shows that RSA is better in terms of speed and security [6].

For different input size a single input processor is used, the study is about the performance of different security algorithm. This paper aims to find speed up ratio that benefits for implementation of security algorithm. When symmetric key(AES) and asymmetric key(RSA) used for the commercial purpose to encrypt and decrypt the large amount of data. It shows RSA is most time consuming [7].

The encryption/decryption time processes, the usage of memory and output time are three major parameters for any encryption algorithm. RSA, AES, and DES is compared based on these parameters. RSA has the longest encryption time for larger key length and has high memory use. The output time in RSA [8].

Various technique and algorithm are studied for the security in multimode network. It seems as that the power of the system rely upon the how the key manage, also rely upon the use of cryptography, for example(public or private), how many number of keys, and number of bits are used in a key.

Keys with more bits require longer computation times, indicating that the system will take more time to encrypt the data. While larger keys enhance security, their strength diminishes over time due to advances in computational methods. When we use longer key lengths, they consume more resources and power, leading to increased heat dissipation [9].

The use of network and internet is grown wide, so the need of security increases also. To provide the security for data transmission over different networks, different algorithm and encryption method are used. A survey on different algorithm is done, to sum it all the technique used here are work better for real time encryption. Each algorithm has its pro's and con's, and is unique in their ways, which is suitable according to the application they used [10].

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 07, July 2024, pp: 1323-1328

2.1 Efficiency Considerations

Trade-offs Between Security and Efficiency: By increasing the key length its security enhance but at a cost. Longer keys require more computational power and result in slower encryption and decryption processes. A study by Lim and Lee (2007) showed that while 2048-bit keys are significantly more secure than 1024-bit keys, they also lead to noticeable performance degradation in real-time applications [11]. That is why there is a communication between achieving higher security and maintaining acceptable performance levels.

The research survey the existing encryption algorithm technique like AES, DES, RSA. It uses text file and based on them it shows that which algorithm takes lower time in encryption process and which consume longest encryption time. The Decryption process of symmetric algorithm is better than many cryptography algorithms. The simulation result are applied on them, they evaluate RSA shows trade-offs between security and efficiency [12].

An evaluation comparing performance efficiency and security measures of cryptographic algorithm is done. It shows computational power of symmetric algorithm is least than the asymmetric algorithm. Asymmetric algorithms are considered as slow because of the larger key sizes. But the security because it uses two keys is high. It concluded that the encryption ratio of symmetric key algorithm is high. The tunability is high in asymmetric key algorithms. The length of keys is high in asymmetric algorithms, so it is complex task to break the keys in RSA. In symmetric algorithm the data shows hat AES is better. And in asymmetric the data shows that RSA offers enhanced security due to its reliance on the factorization of large prime numbers for key generation, making it a superior solution in this context. [13].

There are some factors which are used here to measure the performance of various symmetric and asymmetric cryptographic algorithms performance, and these are speed of different algorithm, tenability, etc for finding the better algorithm based on these factors [14].

The distinctive study of different encryption algorithms for wireless network, are evaluated. Also evaluate the comparison based on the techniques is used [15].

It discusses the different rule and regulations used for the wireless transmission for the message after encryption process [16].

It technique that can be used to encrypt different files and provide security so that these fillies remain hidden and while doing that there can be some security issues occur in these files so it keep them in notice[17].

The various parameters which are used to evaluate the strength and efficiency of the algorithms are evaluated while doing the encryption/decryption process [18].

1.2 Performance Metrics

The performance of RSA encryption and decryption depends heavily influenced by key length. Performance metrics include encryption and decryption time, CPU usage, and memory consumption. A study by Boneh and Shacham (2001) demonstrated that doubling the key length approximately quadruples the computational effort required for encryption and decryption [19].

The different types of asymmetric key algorithms are assessed here [20].

The RSA cryptosystem's security is investigated. It tells about that how can attack happen on this algorithm. The crypto analysis of RSA is also talked about here. It shows it is possible to find the key. But if the difficulty is increased it will become impossible [21]

It shows the example for selecting the large integer number with a condition, and use of the generation of encryption key, and generation of decryption key [22].

Notable Attacks on RSA: The factorization of shorter RSA keys has led to increased recommendations for key sizes. For example, NIST recommended transitioning from 1024-bit keys to 2048-bit keys by the year 2010. More recent attacks, such as those leveraging side-channel methods (e.g., timing attacks, power analysis), have further influenced recommendations for secure key lengths and implementation practices [23].

Several attacks have targeted RSA over the years, highlighting vulnerabilities associated with shorter key lengths and poor implementation practices. One of the most famous attacks was the successful factorization of a 512-bit RSA key in 1999 using the General Number Field Sieve (GNFS) algorithm, demonstrating the need for longer keys.

Current standards and recommendations shows organizations such as NIST and ENISA advise a minimum key length of 2048 bits for most applications. For long-term security, especially where data needs to remain secure for several decades, 3072-bit or 4096-bit keys are recommended. These recommendations are based on projections of future computing power and advances in cryptographic attack techniques [24].

The advantages of longer key sizes can eliminate the attacks. One of the most famous attacks was the successful factorization of a 512-bit RSA key in 1999 using the General Number Field Sieve (GNFS) algorithm, demonstrating the need for longer keys.RSA is not easily broken by the brute force attacks [25].

The encryption and decryption time consume by DES is least as compared to RSA algorithm. Its speed is also fast, but the threats which DES can handle, RSA can easily handled [26].

If the attacker can compute the secret key than it can be decrypted using the standard procedure. The known attacks for RSA is factoring algorithms like quantum attacks which are used to factoring the public key [27].

Recommended Key Sizes: Current standards and recommendations shows organizations such as NIST and ENISA advise a minimum key length of 2048 bits for most applications. For long-term security, especially where data needs to remain secure for several decades, 3072-bit or 4096-bit keys are recommended. These recommendations are based on projections of future computing power and advances in cryptographic attack techniques.

A comparison of different RSA key lengths reveals that while 1024-bit keys may still be used in low-security applications, 2048-bit keys are most secure communications today. For higher security needs, especially in scenarios where the data has a long shelf life, 3072-bit and 4096-bit keys are preferred. Studies have shown that while 4096-bit keys provide the highest security, they can significantly impact performance, making them suitable only for applications where performance is less critical.

3. FUTURE SCOPE

RSA is secure for many classical attacks, it is vulnerable to quantum attacks, for example shor's algorithm which can factorize the large number efficiently. Future research can focus on the need to stay ahead of new threats and computational capabilities and by focusing on the quantum resistant algorithm. With the advent of quantum computing, traditional RSA cryptography faces significant challenges due to the potential of quantum algorithms, such as Shor's algorithm, to break large integer factorization problems efficiently. Future research will focus on developing and standardizing post-quantum cryptographic algorithms that can withstand quantum attacks, ensuring long-term security.

4. CONCLUSION

RSA algorithm security depends on its large key sizes, and the affect the speed of encryption/decryption. This paper includes detail study of the impact of these large key sizes and also states these key sizes affects the execution time and energy consumption. RSA is vulnerable to the quantum attacks. So with the improve RSA implementation, developing adaptive key management and by focusing on quantum resistant algorithm ,the cryptographic community can ensure security over future digital communication and data protection.

5. REFERENCES

[1] Rivest, Designers Ron, Adi Shamir, and Leonard Adleman. "RSA (cryptosystem)." Arithmetic Algorithms And Applications (1978): 19.

[2] Lenstra, A. K., & Verheul, E. R. (2001). Selecting cryptographic key sizes. Journal of cryptology, 14, 255-293

[3] R. Kumar, and C. C. Ravindranath, "Analysis of Diffie Hellman Key Exchange Algorithm with proposed Key Exchange Algorithm," Int. J. Emerg. Trends Technol. Comput. Sci., 4(1), 2015, pp. 40-43.

[4] M. Mohan, and J. Prakash, "Analysis of various cryptographic algorithms," International Journal of Engineering Technology, Management and Applied Sciences, 2(3), 201, pp. 51-61

[5] Mahajan, Prerna, and Abhishek Sachdeva. "A study of encryption algorithms AES, DES and RSA for security." Global journal of computer science and technology 13.15 (2013): 15-22.

[6] Bisht, Nivedita, and Sapna Singh. "A comparative study of some symmetric and asymmetric key cryptography algorithms." International Journal of Innovative Research in Science, Engineering and Technology 4.3 (2015): 1028-1031.

[7] Arora, Priyanka, Arun Singh, and Himanshu Tiyagi. "Evaluation and comparison of security issues on cloud computing environment." World of Computer Science and Information Technology Journal (WCSIT) 2.5 (2012): 179-183.

[8] Shashi Mehrota Seth, Rajan Mishra, "Comparative Analysis of Encryption Algorithms for Data Communication", International Journal of Computer Science and Technology, Vol. 2, Issue 2, pp. 292-294, June 2011.

[9] Ajay Kakkar, M.L Singh and P.K. Bansal, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication In Multinode Network", International Journal of Engineering and Technology Volume 2 No. 1, pp. 87-92, January 2012.

[10] Gurpreet Singh , Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications(0975-8887) Volume 67-No. 19, April 2013.

[11] Lim, Meng-Hui, Sanggon Lee, and Sangjae Moon. "Cryptanalysis of Tso et al.'s id-based tripartite authenticated key agreement protocol." International Conference on Information Systems Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007.

[12] Mahajan, Prerna, and Abhishek Sachdeva. "A study of encryption algorithms AES, DES and RSA for security." Global journal of computer science and technology 13.15 (2013): 15-22.

[13] Jeeva, A. L., Dr V. Palanisamy, and K. Kanagaram. "Comparative analysis of performance efficiency and security measures of some encryption algorithms." International Journal of Engineering Research and Applications (IJERA) 2.3 (2012): 3033-3037.

[14] Jolly Shah and Dr. Vikas Saxena," Performance Study on Image Encryption Schemes" In: IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4.

[15] Pranay Meshram,Pratibha Bhaisare, S.J.Karale,",comparative study of selective encryption algorithm for wireless adhoc network" ,IJREAS Volume 2, Issue 2 , in International Journal of Research in Engineering & Nachiketh Potlapally Srivaths Ravi Anand Raghunathan and Ganesh Lakshminarayana_ "Algorithm Exploration for Efficient PublicKey Security Processing on Wireless Handsets", U. S. Department of Commerce, The Emerging Digital Economy II.

[16] Nachiketh Potlapally Srivaths Ravi Anand Raghunathan and Ganesh Lakshminarayana_ "Algorithm Exploration for Efficient PublicKey Security Processing on Wireless Handsets", U. S. Department of Commerce, The Emerging Digital Economy II.

[17] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki," A Modified AES Based Algorithm for Image Encryption" ,in World Academy of Science, Engineering and Technology.

[18] MarwaAbd El-Wahed and Mesbah and Amin shoukry, 2008, "Efficiency and Security of some Image Encryption Algorithms", Proceedings of the world Congress on Engineering 2008 Vol I.

[19] Boneh, Dan, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. "International conference on the theory and application of cryptology and information security." Berlin, Heidelberg: Springer Berlin Heidelberg, 2001.

[20] Zirra Peter Buba & Gregory Maksha Wajiga "Cryptographic Algorithms for Secure Data Communication International "in International Journal of Computer Science and Security IJCSS, Volume no 5, Issue 2.

[21] Chandra M. Kota et al., "Implementation of the RSA algorithm and its cryptanalysis," In proceedings of the 2002 ASEE Gulf-Southwest Annual Conference, March 20 – 22, 2002.

[22] Prasant Singh Yadav et al., "Implementation of RSA algorithm using Elliptic Curve Algorithm for security and performance enhancement," International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012.

[23] Crypto, F. A. Q. "TWIRL and RSA Key Size", May 6 2003.

[24] A. Perrig, J. Stankovic, and D. Wagner, "Security In Wireless Sensor Networks," ACM, Vol. 47, No.653.2004.

[25] Marwaha, M., Bedi, R., Singh, A., & Singh, T. (2013). Comparative analysis of cryptographic algorithms. Int J Adv Engg Tech/IV/III/July-Sept, 16, 18.s

[26] Singh, Sombir, Sunil K. Maakar, and Sudesh Kumar. "A performance analysis of DES and RSA cryptography." International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) 2.3 (2013): 418-423.

[27] Hercigonja, Zoran. "Comparative analysis of cryptographic algorithms." International Journal of Digital Technology & Economy 1.2 (2016): 127-134.