**An Improved RSA Algorithm for Enhanced Security (2022)**

**Proposed Solution** The document proposes an improved RSA algorithm to enhance security by introducing two algorithmic variations that conceal critical components during public key exchanges. Algorithm 1 hides the encryption key (e) while revealing the modulus (n), whereas Algorithm 2 hides the modulus and sends the encryption key publicly. To decide between these algorithms, a true random number generator (e.g., /dev/random or /dev/urandom in Linux) is used, ensuring unpredictability and making the system more resistant to attacks. The implementation also incorporates optimized modular exponentiation techniques to improve the efficiency of encryption and decryption operations, enhancing the overall performance of the cryptosystem.

**Limitations** The proposed algorithm has certain limitations. The random number used for algorithm selection is transmitted unencrypted, which makes it vulnerable to interception or manipulation by a third party. Although encrypting the random number using a pre-shared key could mitigate this risk, it introduces additional complexity to the system. Additionally, the algorithm may remain susceptible to side-channel attacks, such as timing attacks, depending on the specifics of its implementation. Moreover, the added computational overhead due to the inclusion of randomization and the use of dual algorithms could negatively impact performance, particularly in large-scale or real-time systems.

**New RSA Scheme For Improved Security (2021)**

### **Proposed Solution:**

The proposed modification replaces n with a derived value t to enhance security. This transformation obscures the original modulus n and its factors, making it harder for attackers to perform factorization or derive private keys.

### **Limitations:**

RSA remains susceptible to brute-force attacks if keys are poorly chosen. Additionally, the algorithm can be computationally intensive, particularly as key sizes increase to counteract more sophisticated attack methods​

**An improved random bit-stuffing technique with a modified RSA algorithm for resisting attacks in information security (RBMRSA) (2022)**

### **Proposed Solution:**

This research study provides encryption algorithms that bring confidentiality and integrity based on two algorithms. The encryption algorithms include a well-known RSA algorithm (1024 key length) with an enhanced bit insertion algorithm to enhance the security of RSA against different attacks.

### **Limitations:**

The limitation of this approach is that more encryption and decryption time is required due to less processing speed and it does not provide or increase the security of RSA against common RSA attacks.

**An Effective and enhanced RSA based Public Key Encryption Scheme (XRSA) (2022)**

### **Proposed Solution:**

The XRSA encryption scheme enhances the standard RSA algorithm by introducing several improvements. It utilizes four random prime numbers instead of the traditional two, significantly increasing the complexity of factorization. Additionally, XOR operations and intermediate variables are incorporated during key generation, encryption, and decryption, adding an extra layer of security. The use of intermediate keys, such as E1, E2, and E', further complicates the relationship between the public and private keys, making it more time-consuming to break the cipher. As a result, XRSA demonstrates enhanced resistance to brute-force attacks compared to standard RSA, ESRKGS, and MRSA.

### **Limitations:**

Despite its advancements, XRSA has certain limitations. The use of four primes and XOR operations leads to increased computational costs, resulting in longer encryption, decryption, and key generation times compared to standard RSA. The added layers of computation also make the algorithm more complex to implement and maintain, especially in resource-constrained environments. Scalability is another concern, as the additional computational overhead may not perform well in large-scale applications or high-frequency cryptographic operations. Moreover, the current version of XRSA does not support parallel computing, which could alleviate some of these computational challenges. While XRSA is efficient for key sizes up to 1024 bits, its performance declines with higher bit sizes, such as 2048 or 4096 bits. Furthermore, the algorithm lacks real-world validation, with most analyses being theoretical or simulated, leaving its practicality in real-world applications uncertain. Although XRSA increases resistance to brute-force attacks, it does not explicitly address other threats, such as side-channel attacks or the potential risks posed by quantum computing.

**Improved RSA security using Chinese Remainder Theorem and Multiple Keys (2019)**

**Proposed Solution:**The problem with traditional RSA is its vulnerability to performance inefficiencies during decryption and susceptibility to certain attacks due to the reliance on a single public and private key pair. To address these concerns, an advanced RSA model is proposed, incorporating the Chinese Remainder Theorem (CRT) and multiple key pairs. The CRT is utilized to reduce the computational complexity during decryption, enhancing the decryption speed by operating on smaller modular sizes. Additionally, the advanced RSA algorithm generates two public keys and two private keys derived from four prime numbers, making it more resistant to brute-force attacks and ensuring stronger security compared to standard RSA.

**Limitations:**While the advanced RSA model increases security and improves performance during decryption, it introduces additional computational overhead during encryption due to the use of multiple key pairs. This results in slower encryption times compared to both standard RSA and RSA-CRT. Moreover, the complexity of key management increases, as it involves generating and securely storing multiple keys. These limitations might hinder its practicality in time-critical applications or environments with constrained computational resources.

**References:**

Abdulkader, Hatem; Samir, Rasha; and Hussien, Reda (2019) "Improved RSA security using Chinese Remainder Theorem and Multiple Keys," Future Computing and Informatics Journal: Vol. 4 : Iss. 1 , Article 1. Available at: <https://digitalcommons.aaru.edu.jo/fcij/vol4/iss1/1>

Balasubramanian, Dr & Arun, M. & Sekar, Dr K R. (2022). An Improved RSA Algorithm for Enhanced Security. Indian Journal of Cryptography and Network Security. 2. 1-4. 10.54105/ijcns.B1421.112222. Retrieved from: <https://www.researchgate.net/publication/365874002_An_Improved_RSA_Algorithm_for_Enhanced_Security>

Imam, R., Anwer, F. & Nadeem, M. An Effective and enhanced RSA based Public Key Encryption Scheme (XRSA). Int. j. inf. tecnol. 14, 2645–2656 (2022). <https://doi.org/10.1007/s41870-022-00993-y>

Mojisola, F. O., Misra, S., Febisola, C. F., Abayomi-Alli, O., & Sengul, G. (2022). An improved random bit-stuffing technique with a modified RSA algorithm for resisting attacks in information security (RBMRSA). *Egyptian Informatics Journal*, *23*(2), 291–301. <https://doi.org/10.1016/j.eij.2022.02.001>

O. Sarjiyus, B.Y Baha and E.J Garba (2021). New RSA Scheme For Improved Security. International Journal of Science and Innovative Research. Retrieved from: <https://ijesir.org/wp-content/uploads/2021/10/0100069IJESIRnew.pdf>