IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IMPLEMENTATION OF THE AES ENCRYPTION ALGORITHM 256 BITS IN CRYPTOGRAPHY

ASE algorithm in cryptography 256 bits

[1]Dr. Balaji k, [2]Mohammed Tauqir Ali T.M, [3]Satyajit Mohanty, [4]N.V. Rakesh, [5]Viswa .M

[1]Professor, Department of MCA, Cambridge Institute of Technology CITech, Bengaluru, India, [2,3,4,5] Student, Department of MCA, CITech, Bengaluru, India

Abstract:

In today's corporate world, network and data security is a major concern. Many different types of businesses, such as financial institutions, law firms, schools, healthcare, telecommunications, mining, and government organizations, have a strong demand for strategic data management techniques. Businesses lose sensitive data, such as biometric and financial information, to competitors and other parties as a result of hackers' activity. Businesses are losing millions of dollars as a result of malicious people gaining access to unprotected data. Businesses now place a great value on data security. Protection is required to guarantee information security. Using encryption algorithms to protect communications in these kinds of threads is one of the most important and practical solutions available. Performance and security are two factors that the developer must take into account while creating an extremely secure Android application. Android-based applications must perform better because Android smartphones have constrained resources. The most widely used secure encryption algorithms Rijndael, Serpent, and Two fish will be evaluated in this study to see which works best in order to overcome the issues.

Keywords: telecommunications, android, encryption algorithms.

1. Introduction

Applications that need minimal power consumption, like smart cards, wireless LANs, wireless sensor networks, and personal area networks, frequently use cryptographic techniques for security. Hardware is preferred over software in order to run such algorithms with optimal performance and power usage. The Advanced Encryption Standard (AES) was created and shown to be secure before becoming the default choice in most applications. IEEE802.15.4 [2], ZigBee [3], and WPA2 (IEEE 802.11i) [1], wireless standard technologies were used in these applications. Applications requiring low power and low cost will benefit greatly from our FPGA-based AES encryption core. Data security is becoming increasingly critical in a variety of embedded applications. One of an encryption algorithm's most important properties is its ability to withstand known attacks. To ensure data security, the encryption mechanism must be updated each time a new attack is proven successful. Advanced Encryption Standard (AES) is presently the most widely used encryption technology in many security applications, surpassing its predecessor, Double Encryption Standard (DES) [4]. "Performance, security, efficiency, implement ability, and flexibility" are effectively combined [5]. This work covers AES encryption hardware implementations that use a modular memory method and Lookup tables for keys with lengths of 128,

192, and 256 bits. The ciphered data is more safe the greater the key size, but this requires more rounds. To evaluate the three various AES key sizes' hardware implementations' throughput and area (128, 192, and 256).

2. AES stands for asymmetric encryption

Grover's approach [7, 8] can be used to illustrate the quantum resistance of AES. Grover's algorithm is a quantum algorithm that uses only the $O(\sqrt{N})$ function evaluation—where N is the size of the function domain—to determine the exact output value in a black box function that has a high probability for a given input value. Since the worst-case calculation always returns the N^{th} member's answer, A general calculation can never be faster than O(N) in solving a problem. As shown by [7], Grover's method is asymptotically optimal, and there is no quantum solution to the problem of evaluating the function in less than $O(\sqrt{N})$ time. Instead of producing exponential speedup, Grover's method results in quadratic speedup. Grover's method takes roughly 2^{64} iterations to generate a 128-bit cryptographic key and 2^{128} iterations to generate a 256-bit.

2.1. This makes 256-bit AES keys impervious to quantum assaults

The preceding reasoning clearly demonstrates that AES, Rijndael's symmetric key approach based on block ciphers, is entirely quantum secure Preparation of Material.

3. AES's Comparative Analysis with Other Cryptographic Systems

It is now obvious that the AES encryption method provides quantum security. Table 1 [6], displays how safe AES is at the quantum level.

Table 1. compares the security levels of conventional and quantum cryptography systems with AES.

Algorithm	**Key Length**	**Key Strength/ Security Level**	
		Classical Computing (bits)	**Quantum Computing (bits)**
AES-128	128 bits	128	64
AES-256	256 bits	256	128
RSA-1024	1024 bits	80	0
RSA-2048	2048 bits	112	0
ECC-256	256 bits	128	0
ECC-384	384 bits	256	0

The following four processes are necessary for every AES round

Sub bytes:

It is a nonlinear byte substitution transformation that uses the S-box substitution table to carry out byte-by-byte substitution. All byte values between 0 and 255 are mapped one to one using a S box. The ciphertext is created by S-box from the original plaintext in bytes. Since the encryption only uses one S-box, it needs to be constructed properly. Hexadecimal notation is used to express all values. The S-box result is converted to decimal format.

Shift rows:

The state's rows are shifted using a transposition step. Where N is the row number, N bytes are shifted to the left. This means that there will be no shift in row 0, but the first, second, and third rows will all be shifted left by one, two, and three bytes, respectively. Each row is shifted cyclically. For $0 \leq i \leq 3$, row i is shifted by i bytes.

Mix columns:

The mix column action is used to combine each array column after the shift and substitute processes have been used. The final matrix is created by pre-multiplying the (4×4) GF (2^8) constant matrix M by the defined column, which is a (4×1) column vector of entries in GF (2^8). A (4×1) column vector of elements in GF (2^8) will be the output, replacing the processed column.

Add round key:

The last AES operation yields a round key for the state matrix via the XOR technique. The subkey array is p0 …p15, while the current state of the byte array is k_0 … k_{15}. Add Round Key is used to link the two arrays byte-by-byte, creating the array q_0. . q_{15}, where $q_i = k_i \oplus p_i$ for $0 \le i \le 15$.

3.1. One Time Pad

OTP, which uses a cipher box to process data, is one important security cipher.

Traditional encryption algorithms are not as secure as randomly generated keys. Both encryption and decryption use the same key, which yields the original plaintext when applied to the ciphertext. Because of its XOR operations, OTP performs better in terms of security than other algorithms. To ensure that they cannot be used again, the sender and receiver's keys are automatically erased after usage. In the event that a nonrecurring, random key is used to create the message, the theoretically unsolvable impact of a one-time pad will be shown. The process of OTP encryption is shown in Figu

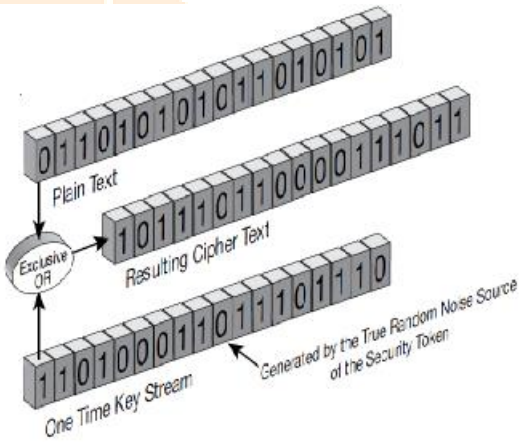

Figure 1. OTP encryption process

4. Conclusion

The methods of quantum resistance for AES-256 are examined in this work. RSA and ECC, two well-known public key cryptography algorithms, can be cracked using quantum computing thanks to Shor's method. Grover's method implies that it may be possible to defeat some well-known cryptographic algorithms with quantum computing, such as AES-128 and IDEA. To put it briefly, AES-256 will never be compromised in the post-quantum computing age.

References

[1] Ernst, Young (2011) Data loss prevention: Keeping your sensitive data out of the public domain. Ernst & Young Global Limited, United Kingdom.

[2] Ibrahim (2015) FPGA-based hardware implementation of compact aes encryption hardware core. WSEAS transactions on circuits and systems.

[3] A. Madhuri, N.M. Suresh (2016) Implementation of advanced encryption standard algorithm for communication security using FPGA. International. Research Journal of Engineering and Technology 3: 1176-1179.

[4] National Institute of Standards and Technology (U.S.), Data Encryption Standard (DES), FIPS Publication 46-3, NIST, 1999. Available at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf.

[5] A. Rudra, P.K. Dubey, C.S. Jutla, V. Kumar, J.R. Rao, P. Rohatgi, (2001) Efficient Rijndael encryption implementation with composite field arithmetic," Lecture Notes in Computer Science 2162 171–184.

[6] http://www.etsi.org/images/files/ETSIWhitePapers/ QuantumSafeWhitepaper.pdf.

[7] C.H. Bennett, E. Bernstein, G. Brassard, U. Vazirani, (1997) The strengths and weaknesses of quantum computation. SIAM Journal on Computing. 26(5): 1510–1523.

[8] L. K. Grover, (2001) From Schrödinger's equation to the quantum search algorithm. American Journal of Physics 69.7: 769-777.