Data Security Optimization Using Hybrid Cryptography -An Empirical Study of Hybrid Encryption Using Symmetric, Asymmetric and Hashing Algorithms

Sivananda Lahari Reddy. Elicherla[1] Dr. Raghunatha Reddy. Vandavagula[2]
[1]Research Scholar [2]Assisitant Professor
[1,2]Department of Computer Science & Technology
[1,2]S.K.University, Anantapur, A.P. India

Abstract— This research study proposes Hybrid Encryption System using public key, private key and hashing algorithms in unison. Hybrid encryption is a mode of encryption that amalgamates two or more encryption systems. It integrates a combination of symmetric, asymmetric and hashing encryption to benefit from the strengths of each form of encryption. This paper presents a provably three way secured data encryption system, which addresses the concerns of users privacy, security, and integrity. In the proposed system, three different encryption algorithms have been used in the encryption sequence. One is private key cryptography based on the simple symmetric algorithm and another one is public-key cryptography based on a linear block cipher and a hashing function algorithm (Message-Digest). This cryptography algorithm provides more security and makes the encryption further robust compared to the existing hybrid algorithms.

Keywords: Cryptography, Hybrid Encryption, Security, Symmetric, Asymmetric, Hashing Algorithms, Hybrid Cryptography

I. INTRODUCTION

In today's world, insecure data are growing used in communication over the internet. Thus security of data is a major interest of internet users. The best solution is to use some of the cryptographic algorithms which encrypt the data in some cipher and transmit it over the Net and again decrypted to genuine data. The field of cryptography deals with the strategy for transmitting the information securely. The goal is to allow the intended recipients of a message to receive the message properly while interrupting eaves-droppers from understanding the Message.

Cryptography is a popular way of sending vital information covertly as it includes techniques derived from mathematical concepts and a set of rule-based calculations called algorithms to transform messages in ways that are hard to decipher. In current computer systems, cryptography provides a strong basis for keeping data classified and also validating the data integrity aspect. Therefore it becomes very important to consider data security, as it is one of the most necessary factors that need attention during the process of data transfer.

The importance of information and communication systems for society and the global economy is intensifying with the increasing value and quantity of data that is transmitted and stored on those systems. At the same time, those systems and data are also increasingly vulnerable to a variety of threats, such as unauthorized access and use, misappropriation, alteration, and destruction.

The hiding of information is called encryption, and when the information is unhidden, it is called decryption. A cipher is used to accomplish the encryption and decryption. Merriam-Webster's Collegiate Dictionary defines cipher as a method of transforming a text to conceal its meaning. The information that is being hidden is called plaintext; once it has been encrypted, it is called cipher text.

Hybrid encryption is a mode of encryption that merges two or more encryption systems. It incorporates a combination of asymmetric, asymmetric and hashing encryption to benefit from the strengths of each form of encryption. This journal presents an empirical study on various cryptographic algorithms such as symmetric, asymmetric, and hashing and combination of symmetric, asymmetric and hashing algorithms to explore the potential cryptographic solutions that make the encryption process more robust, secure and cumbersome to access the data by unintended recipients'.

By using cryptography several goals can be achieved, the solution that is being proposed in this paper aims at achieving two major goals of the data security aspect i.e. Confidentiality and Data Integrity. Confidentiality ensures that nobody can understand the received message except the one who has the decipher key whereas the Data Integrity ensures that the received message has not been changed in any way from its original form.

II. DATA ENCRYPTION

Data encryption is a random string of bits created explicitly for scrambling and unscrambling data. Data encryption is designed with algorithms intended to ensure that every key is unpredictable and unique.

Cryptography uses two types of keys: symmetric and asymmetric. Symmetric keys have been around the longest; they utilize a single key for both the encryption and decryption of the cipher text. This type of key is called a secret key. Secret-key ciphers generally fall into one of two categories: stream ciphers or block ciphers. A block cipher applies a private key and algorithm to a block of data simultaneously, whereas a stream cipher applies the key and algorithm one bit at a time.

Most cryptographic processes use symmetric encryption to encrypt data transmissions but use asymmetric encryption to encrypt and exchange the secret key. Symmetric encryption, also known as private key encryption, uses the same private key for both encryption and decryption. The risk in this system is that if either party loses the key or the key is intercepted, the system is broken and messages cannot be exchanged securely.

As this research prime objective is to compare the effectiveness of hybrid cryptosystems, it's important to know how symmetric, asymmetric and hashing algorithms work in reality.

A. Symmetric Key Cryptography

In symmetric-key cryptography is also known as private-key cryptography, a secret key may be held by one person or exchanged between the sender and the receiver of a message. If private key cryptography is used to send secret messages between two parties, both the sender and receiver must have a copy of the secret key.

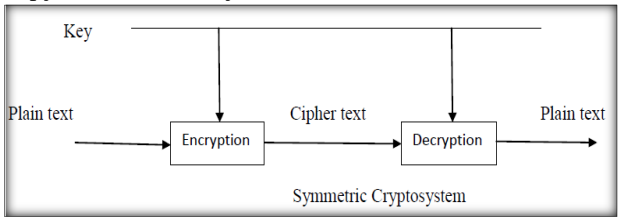

Fig. 1: Flow diagram of symmetric cryptography

B. Asymmetric Key Cryptography

In the two-key system is also known as the public key system, one key encrypts the information and another, mathematically related key decrypts it. The computer sending an encrypted message uses a chosen private key that is never shared and so is known only to the sender. If a sending computer first encrypts the message with the intended receiver's public key and again with the sender's secret, private key, then the receiving computer may decrypt the message, first using its secret key and then the sender's public key. Using this public-key cryptographic method, the sender and receiver can authenticate one another as well as protect the secrecy of the message.

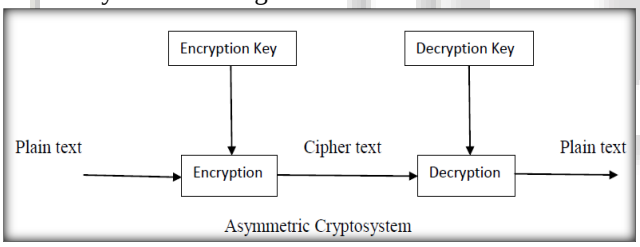

Fig. 2: Flow diagram of Asymmetric cryptography

C. Cryptographic Hash Function (CHF)

A cryptographic hash function (CHF) is a hash function that is suitable for use in cryptography. It is a mathematical algorithm that maps data of arbitrary size (often called the "message") to a bit string of a fixed size (the "hash value", "hash", or "message digest") and is a one-way function, that is, a function which is practically infeasible to invert. The input to the hash function is of arbitrary length but the output is always of fixed length.

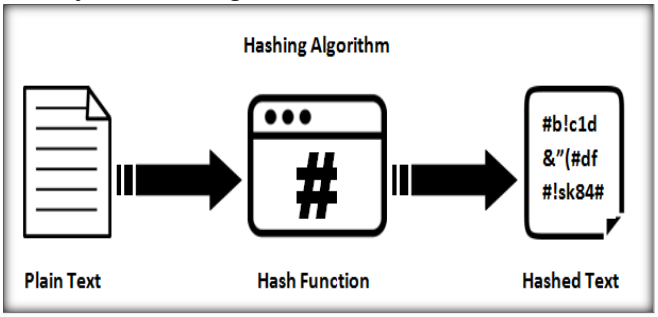

Fig. 3: Flow diagram of hash function

III. Cryptographic Algorithms Considered for Research

A. Advanced Encryption Standard (AES)

The Advanced Encryption Standard, AES, is a symmetric encryption algorithm and one of the most secure. This method uses a block cipher, which encrypts data one fixed-size block at a time, unlike other types of encryption, such as stream ciphers, which encrypt data bit by bit. AES is comprised of AES-128, AES-192, and AES-256.

Since AES is symmetric key encryption, you must share the key with other individuals for them to access the encrypted data. Furthermore, if you don't have a secure way to share that key and unauthorized individuals gain access to it, they can decrypt everything encrypted with that specific key. It is a symmetric-key algorithm, meaning each recipient must receive the key through a different channel than the message.

The major drawbacks of AES algorithm are as follows:

1) Slow performance due to the key size, the time it will take to encrypt and decrypt the message hinders efficient communication.
2) It has been proven to be a weak cipher; therefore, should not be trusted to protect sensitive data

B. Rivest-Shamir-Adleman (RSA)

This asymmetric algorithm is named after Ron Rivest, Adi Shamir, and Len Adelman. It uses public-key cryptography to share data over an insecure network. There are two keys: one public and one private. The public key is just as the name suggests: public. Anyone can access it. However, the private key must be confidential. When using RSA cryptography, you need both keys to encrypt and decrypt a message. You use one key to encrypt your data and the other to decrypt it.

According to Search Security, RSA is secure because it factors large integers that are the product of two large prime numbers. Additionally, the key size is large, which increases security. Most RSA keys are 1024-bits and 2048-bits long. However, the longer key size does mean it's slower than other encryption methods.

The advantages include; it's safe and secure for its users through the use of complex mathematics. It's hard to crack since it involves the factorization of prime numbers which are difficult to factorize. Moreover, the RSA algorithm uses the public key to encrypt data and the key is known to everyone, therefore, it is easy to share the public key.

The disadvantages include:

- It can be very slow in cases where large data needs to be encrypted
- It requires a third party to verify the reliability of public keys
- Data transferred through RSA algorithm could be compromised through middlemen who might tamper with the public key system

C. Message-Digest 5 (MD5)

In cryptography, MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function with a 128-bit hash value. As an Internet standard (RFC 1321), MD5 has been employed in a wide variety of security applications and is also commonly used to check the integrity of files. An MD5 hash

is typically expressed as a 32 digit hexadecimal number. The advantages of MD5 include; fast computation, collision resistance and Provides a one-way hash which is irreversible if we use it diligently.

One of the major disadvantages of MD5 is its known security flaws and vulnerabilities.

IV. PROPOSED SOLUTION FRAMEWORK

In cryptography, a hybrid cryptosystem is one that combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem. As discussed above Symmetric, Asymmetric and hash functions have their advantages and disadvantages which make these systems vulnerable to the security threats when they are used or implemented independently. For instance, MD5 encryption key can be easily broken and decipher by the hackers when it's used separately. Hence, there is a need for a better cryptosystem which generates a more robust encryption key to make sensitive data more secure and intact.

To make a robust cryptosystem, we have conducted a study by implementing below three combinations making use of their unique features and advantages. Particularly we have used MD5 hashing function in these combinations to make the encryption more robust and indissoluble.

- Symmetric Hashing Encryption (AES + MD5)
- Asymmetric Hashing Encryption (RSA + MD5)
- Hybrid or Multi-Level Hashing Encryption (AES + RSA + MD5)

Let's look at each of these crypto systems briefly to know the benefit of using these algorithms in combination.

A. Symmetric Hashing Encryption (AES + MD5)

In symmetric hashing, both AES and MD5 algorithms have combined to develop a new cryptosystem. Though AES is one of the good encryption algorithms, it's considered as a weak cipher which makes this algorithm unreliable. For that reason, to make the encryption more robust we have applied the hashing (MD5) function at the end of AES encryption. Here is the block diagram of the symmetric hashing function.

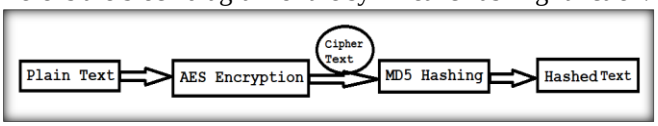

Fig. 4: Flow diagram of symmetric hashing cryptosystem

Having combined the two algorithms, as shown in the graph (Fig.5) it's very evident that Encrypted Key Length is increased (32) and Encryption Elapsed Time (Fig.6) has come down (11436) significantly in symmetric hashing when compared with AES encryption algorithm performance (Key length is 24 and elapsed time is 55295) in its independence.

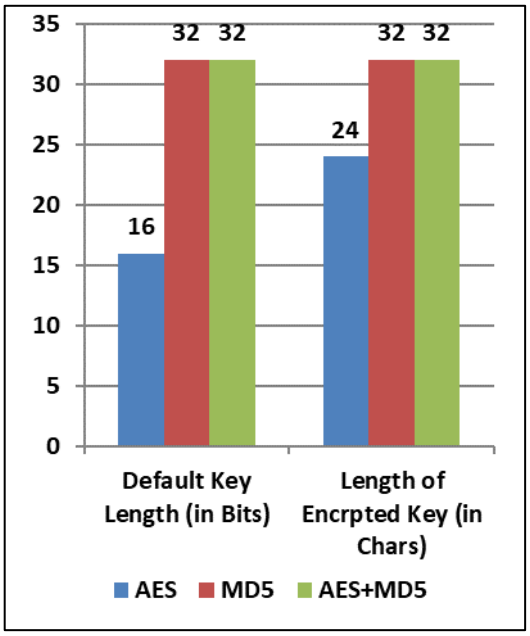

Fig. 5: Hybrid Symmetric Hashing Encryption graph (Default Key Vs Encrypted key)

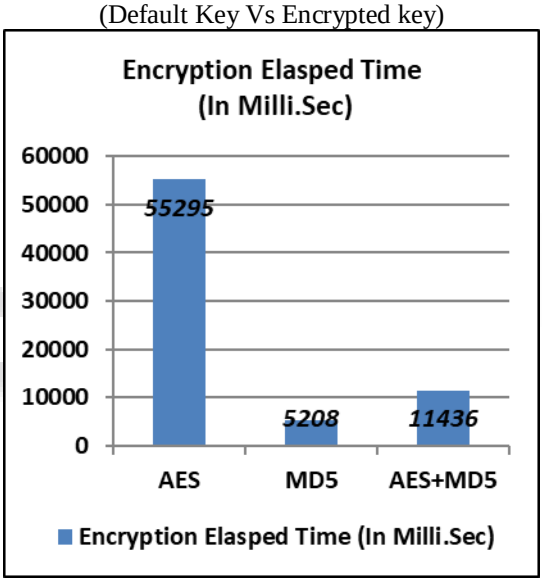

Fig. 6: Hybrid Symmetric Hashing Encryption graph (Encryption Elapsed Time)

B. Asymmetric Hashing Encryption (RSA + MD5)

In asymmetric hashing, both RSA and MD5 algorithms have been combined to develop a new cryptosystem. Though RSA encryption is secure and difficult to crack, one of its disadvantages is that data transferred using the RSA algorithm could be compromised through middlemen who might tamper with the public key system. Therefore, to make the encryption more robust we have applied the hashing (MD5) function at the end of RSA encryption. Here is the block diagram of the symmetric hashing function.

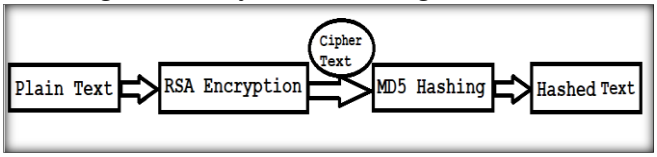

Fig. 7: Flow diagram of asymmetric hashing cryptosystem

Having combined the two algorithms, as shown below its very evident that Encrypted Key Length is decreased significantly (32) in asymmetric hashing when compared with RSA encryption key length (684) in its independence. Also, the hash text generated post RSA encryption is very robust.

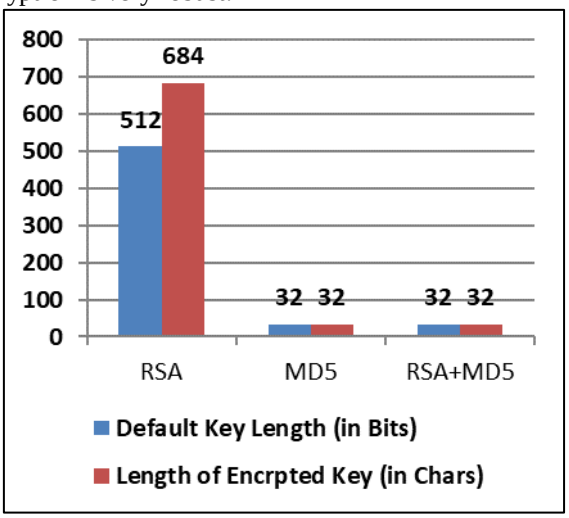

Fig. 8: Hybrid Asymmetric Hashing Encryption graph (Default Key Vs Encrypted key)

One more observation is that Encryption Elapsed Time is slightly higher (13826) when compared with RSA encryption elapsed time (10654), the reason being RSA encryption takes a longer time due to its larger key length and applying hash function on top of it would take little longer time as evidenced in the below graph.

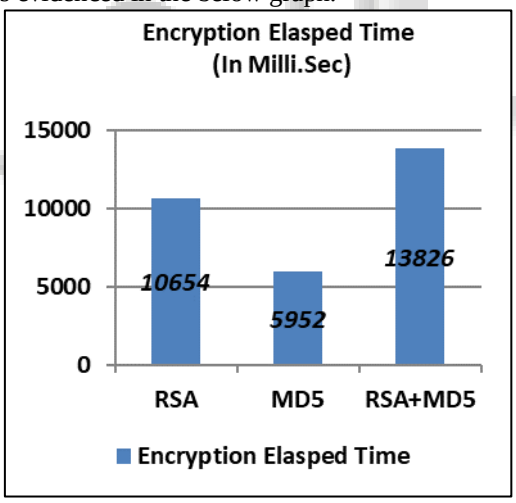

Fig. 9: Hybrid Asymmetric Hashing Encryption graph (Encryption Elapsed Time)

C. Hybrid or Multi-Level Hashing Encryption (AES + RSA + MD5)

In hybrid hashing, both symmetric (AES), asymmetric (RSA) algorithms along with hashing function (MD5) have been combined to make the encryption more robust and reliable. In this solution, multi-level encryption happens which makes the encryption more composite and cumbersome to crack by the hackers. Here is the block diagram of the Hybrid hashing algorithm.

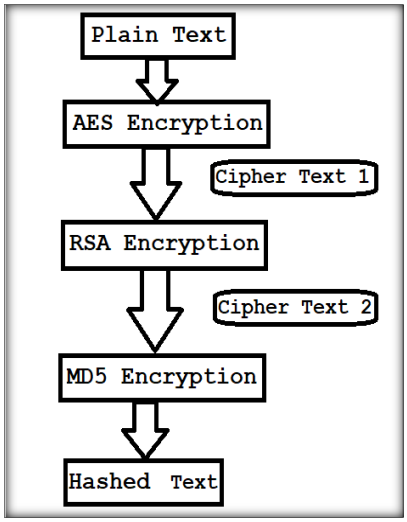

Fig. 10: Flow diagram of Hybrid hashing cryptosystem

Having combined all three algorithms as shown below (Fig.11) it's very evident that Encrypted Key Length is decreased significantly (32) in hybrid hashing when compared with asymmetric hashing encryption key length (684) in its independence. Also, the hash text generated post-RSA encryption is very robust as encryption happening at multi-level and key is generated multiple times.

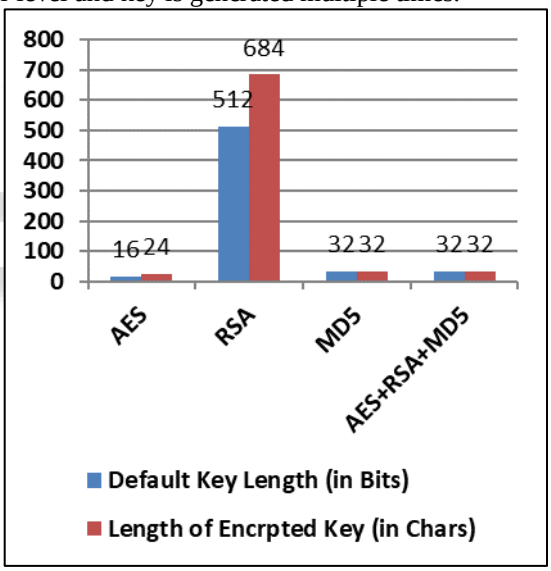

Fig.11. Hybrid Hashing Encryption graph (Default Key Vs Encrypted key)

One more observation is that Encryption Elapsed Time has significantly reduced (8139) when compared with symmetric and asymmetric encryption elapsed times (11436 and 13826 respectively).

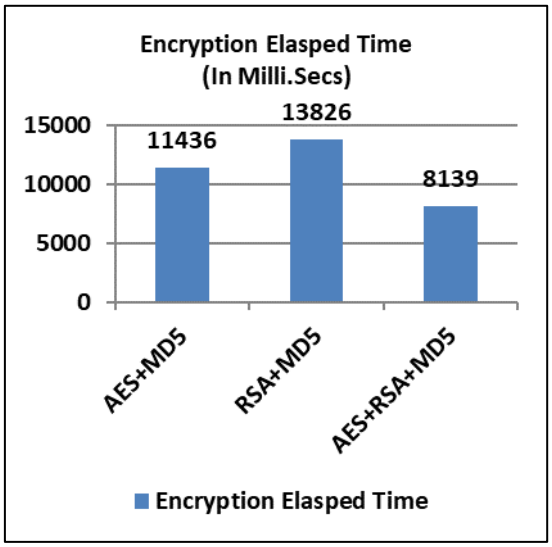

Fig. 12: Hybrid Hashing Encryption graph (Encryption Elapsed Time)

V. Conclusion

To optimize the data security using asymmetric, asymmetric or hashing algorithms may not be the right choice as these algorithms have their pros and cons. Instead, if these algorithms are combined in such a way that the sensitive data can be protected much efficient way by making the encryption process more robust and cumbersome to break it by the unauthorized personnel.

Out of three proposed hybrid cryptosystems, it's very evident that Hybrid Hashing or Multi Level encryption seemed to be more proficient and effective due to the following rationale

- Multilevel encryption makes the encrypted key complex in nature
- Elapsed time to encrypt the key is lesser than the other two hashing algorithms
- Generation of encryption key is dynamic

Thus the proposed hybrid hashing or multi-level encryption is more efficient in optimizing the data security with respect to confidentiality and integrity of the data.

Acknowledgement

I would like to thank Dr. Raghunatha Reddy for his invaluable support and guidance as a research guide to help me prepare and publish this paper. I would also like to extend my heartfelt thanks to Mr. E. Mahendranath Reddy (B.Tech. pursuant, REVA University, Bangalore) who helped me with implementation and testing of the proposed solution. Last but not the least, I would like to thank my spouse Parimala Devi and super Kids Dharani and Niyati for their understanding and unconditional support to complete this paper on time.

References

[1] Sarita Kumari (Research Scholar) - A research Paper on Cryptography Encryption and Compression Techniques
[2] Prof. Swapnil Chaudhari - A Research Paper on New Hybrid Cryptography Algorithm
[3] Prakash Kuppuswamy, Saeed Q.Y.Al-Khalidi - Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm
[4] https://en.wikipedia.org/wiki/Cryptographic_hash_function
[5] https://medium.com/bugbountywriteup/breaking-down-sha-1-algorithm-c152ed353de2
[6] http://practicalcryptography.com/hashes/md5-hash/

