Performance Assessment and Hypothesis Validation of Symmetric, Asymmetric & Multi-Level Hybrid Crypto Systems

Sivananda Lahari Reddy. Elicherla[1] Dr. Raghunatha Reddy. Vandavagula[2]
[1]Research Scholar [2]Assistant Professor
[1,2]Department of Computer Science & Technology
[1,2]S.K.University, Anantapur, A.P. -515003, India

Abstract— Hybrid encryption is a mode of encryption that integrates two or more encryption systems. It amalgamates a combination of symmetric, asymmetric and hashing encryption to gain from the strengths of each form of encryption. The objective of this article is to present the performance assessment of the three hybrid crypto systems namely symmetric hashing, asymmetric hashing and multi-level hashing crypto systems through hypothesis validation. These cryptographic algorithms are being evaluated to devise a potential robust cryptographic system which provides more security and makes the encryption further tough compared to the existing hybrid algorithms to protect the data integrity and maintain the confidentiality.

Keywords: Cryptography, Hybrid Encryption, Security, Symmetric, Asymmetric, Hashing Algorithms, Hybrid Cryptography, Data Integrity and confidentiality

I. INTRODUCTION

At present, insecure data is on the rise used in communication over the internet. Consequently security of data is a foremost interest of internet users. The greatest solution is to use some of the cryptographic algorithms which encrypt the data in cipher format and transmit it over the Net and again decrypted to unadulterated data. The field of cryptography deals with the strategy for transmitting the information securely. The purpose is to allow the intended recipients of a message to receive the message properly while disrupting the unintended users from understanding the message.

Cryptography is a popular way of sending vital information secretly. 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. Therefore data security has become one of the most necessary factors that need attention during the process of data transfer.

The significance of information and communication systems for society and for global market is escalating with the growing value and quantity of data that is transmitted and stored on those systems.

The hiding of information is called encryption, and when the information is unhidden, it is called decryption. A cipher is used to achieve the encryption and decryption. 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 assessment various cryptographic systems such as symmetric, asymmetric, and hashing and combination of symmetric, asymmetric and hashing algorithms to discover the probable cryptographic solutions that make the encryption process more robust, secure and cumbersome.

This piece of work is being performed as a part of the research work - “Data Security Optimization through Hybrid Cryptography Using Symmetric (AES), Asymmetric (RSA) & Hashing (MD5) Algorithms”

II. CRYPTOGRAPHY

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. The prefix "crypt-" means "hidden" or "vault" -- and the suffix "-graphy" stands for "writing.

Cryptography uses two types of keys: symmetric and asymmetric. Symmetric keys have been found the longest; they make use of a single key for both the encryption and decryption of the cipher text. This type of key is called a secret key. Most cryptographic processes use symmetric encryption to encrypt data transmission 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. Whereas Asymmetric Encryption uses two distinct, yet related keys. One key, the Public Key, is used for encryption and the other, the Private Key, is for decryption. As implied in the name, the Private Key is intended to be private so that only the authenticated recipient can decrypt the message.

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

A. Symmetric Key Cryptography

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.

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.

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.

III. Cryptographic Algorithms

There are three algorithms considered for the research as follows to discover the potential robust crypto system by combining the strengths of each algorithm.

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.

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.

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.

IV. Hypothesis

As the research major objective is to optimize the data security using hybrid crypto systems, the following hypothesis has been considered to be validated against the standard parameters such as default key length, length of encryption key (in chars) and encryption elapsed time of three proposed hybrid algorithms namely symmetric, asymmetric and multi-level hybrid crypto systems.

1) HYP-1: Hybrid crypto systems (i.e. symmetric hashing, asymmetric hashing and hybrid hashing) generates more complex encryption keys when compared to private (AES), Public (RSA) key or Hash Function (MD5) algorithms
2) HYP-2: Encryption key complexity doesn't depend on its length or size
3) HYP-3: Encryption elapsed time is lesser in multi-level or hybrid hashing crypto system than the symmetric and asymmetric hashing algorithms
4) HYP-4: Cryptographic systems doesn't generate dynamic keys, hence it's easy to decipher

V. Performance Assessment

In order to figure out which hybrid crypto system perform better, all algorithms were tested using a sample input data (i.e. Encrypt!0n) and performance is evaluated against the three parameters- default key length, length of encryption key (in chars) and encryption elapsed time. The results have been depicted in the following tables.

Symmetric Hashing Crypto System Perforamnce			
Standard Parameter	**AES**	**MD5**	**AES+MD5**
Default Key Length (in Bits)	**16**	**32**	**32**
Length of Encrpted Key (in Chars)	**24**	**32**	**32**
Encryption Elasped Time	**55295**	**5208**	**11436**

Fig. 1: Symmetric Hashing Crypto System (AES+MD5) performance

When performances of the independent crypto systems (i.e. AES & MD5) have been compared with symmetric hashing hybrid crypto system, the latter found to be more robust because of the following reasons:

– The final encryption key is compressed to 32 bits
– Two level encryption makes the process complex
– Encryption key is dynamic

Asymmetric Hashing Crypto System Performance			
Standard Parameter	**RSA**	**MD5**	**RSA+MD5**
Default Key Length (in Bits)	**512**	**32**	**32**
Length of Encrpted Key (in Chars)	**684**	**32**	**32**
Encryption Elasped Time	**10654**	**5952**	**13826**

Fig. 2: Asymmetric Hashing Crypto System (RSA+MD5) performance

Whilst performances of the independent crypto systems (i.e. RSA & MD5) have been compared with asymmetric hashing hybrid crypto system, the latter found to be more robust because of the following reasons:

– The final encryption key is compressed to 32 bits
– Two level encryption makes the process complex
– Encryption key is dynamic

Hybrid Hashing or Multi-level Crypto System Performance				
Standard Parameter	**AES**	**RSA**	**MD5**	**AES+RSA+MD5**
Default Key Length (in Bits)	16	512	32	32
Length of Encrpted Key (in Chars)	24	684	32	32
Encryption Elasped Time	8608	5952	6066	8139

Fig. 3: Hybrid Crypto System (AES+RSA+MD5) performance

When performances of the independent crypto systems (i.e. RSA & MD5) have been compared with asymmetric hashing hybrid crypto system, the latter found to be more robust because of the following reasons:

- The final encryption key is compressed to 32 bits
- Two level encryption makes the process complex
- Encryption key is dynamic

Finally, three hybrid crypto systems performances have been assessed as depicted below.

Symmetric Vs Asymmetric Vs Hybrid Hashing Crypto System Performance			
Standard Parameter	**AES+MD5**	**RSA+MD5**	**AES+RSA+MD5**
Default Key Length (in Bits)	32	32	32
Length of Encrpted Key (in Chars)	32	32	32
Encryption Elasped Time	11436	13826	8139

Fig. 4: Comparison b/n Symmetric Vs Asymmetric Vs Hybrid Hashing Crypto Systems

As shown above (Fig.1 through 4), in all three proposed models the below two standard parameters remains constant as hash function is applied at the end of the encryption, length of encrypted key is compressed to 32 bits.

- Default Key Length (in bits)
- Length of Encrypted Key (in Chars)

However, with respect to Encryption Elapsed Time, there is a significant difference has been observed. As shown in Fig-4, asymmetric hashing has taken more time (13286 milli.secs) to generate the encryption key when compared to symmetric hashing (11436 milli.secs) and hybrid hashing (8139 milli.secs) crypto system whereas Hybrid hashing crypto system has taken less time to generate the encryption key. Therefore, it's evident that Hybrid crypto system robust and effective when compared with other two hybrid crypto systems.

VI. Hypothesis Validation

As the research leading objective is to optimize the data security using hybrid crypto systems, the hypothesis mentioned in section IV has been validated against the standard parameters such as default key length, length of encryption key (in chars) and encryption elapsed time. Here is the validation summary.

HYP-1: Hybrid crypto systems (i.e. symmetric hashing, asymmetric hashing and hybrid hashing) generates more complex encryption keys when compared to private (AES), Public (RSA) key or Hash Function (MD5) algorithms

Validation Summary: It's observed that the above hypothesis has been proven as true, reason being all three proposed crypto systems such as symmetric, asymmetric and hybrid hashing crypto systems have generated more complex encryption key when compared to the independent crypto systems such as private (AES), Public (RSA) key or Hash Function (MD5) algorithms (As shown in Fig: 1 through 3). The reason being, in all three proposed crypto systems encryption is performed at multiple levels and at the end of each crypto system, hash function is performed (MD5) which generates very complex key. Hence proved that, Hybrid crypto systems (i.e. symmetric hashing, asymmetric hashing and hybrid hashing) generates more complex encryption keys when compared to private (AES), Public (RSA) key or Hash Function (MD5) algorithms

HYP-2: Encryption key complexity doesn't depend on its length or size

Validation Summary: It's observed that the above hypothesis has been proven as true, reason being encryption key generated by all three proposed crypto systems is compressed into 32 bits as hash function applied at the end of each crypto system which makes the encryption process more complex that results in optimization of data security w.r.t confidentiality and integrity of the data. Hence proved, encryption key complexity doesn't depend on its length.

HYP-3: Encryption elapsed time is lesser in multi-level or hybrid hashing crypto system than the symmetric and asymmetric hashing algorithms

Validation Summary: It's observed that the above hypothesis has been proven as true, reason being elapsed time for multilevel crypto system is lesser than (8139 milli.secs) the other two crypto systems (Symmetric:11436 milli.secs and Asymmetric:13826 milli.secs). Hence proved that encryption elapsed time is lesser in multi-level or hybrid hashing crypto system than the symmetric and asymmetric hashing algorithms.

HYP-4: Cryptographic systems doesn't generate dynamic keys, hence it's easy to decipher

Validation Summary: It's observed that the above hypothesis has been proven as false, reason being algorithms that have been used in the proposed systems have generated different encryption keys instead of similar keys when its executed multiple times. For instance, AES algorithm has generated two unique encryption keys when the same plain text used as an input as shown below.

Algorithm Type	Input Data	Generated Encrypted Key
AES (First Instance)	Encrypt!0n	NWcWPw2WZFhQ50dDmfAGg==
AES (Second Instance)	Encrypt!0n	F9/JANxnxk77s16q8nazcQ==

Fig. 5: AES Algorithm Encryption Key Generation

VII. Conclusion

Having looked at the performance assessment and hypothesis validation, it's evident that in order to optimize the data security using asymmetric, asymmetric or hashing algorithms may not be the right choices as these algorithms have their pros and cons. As an alternative, if these algorithms are united in such a way that the susceptible data can be protected much efficient way by making the encryption process more robust and arduous to break it by the unauthorized personnel.

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] https://searchsecurity.techtarget.com/definition/cryptography
[2] https://cheapsslsecurity.com/blog/what-is-asymmetric-encryption-understand-with-simple-examples/
[3] Data Security Optimization Using Hybrid Cryptography -http://ijsrd.com/Article.php?manuscript=IJSRDV7I120315
[4] https://www.ijser.org/researchpaper/A-Comparative-Analysis-of-AES-and-RSA-Algorithms.pdf
[5] http://practicalcryptography.com/hashes/md5-hash/

