Hy-Com Cryptographic Technique for Efficient Data Transmission

Sindhuja S.

Assistant Professor, Department of Computer Science, Auxilium College, Vellore, India

Abstract— *Hy-Com Cryptographic technique is an acronym for Hybrid Compressive Cryptographic technique. This research uses two main cryptographic techniques like Symmetric key cryptography and Asymmetric key cryptography and with a lossless compression algorithm. The Symmetric Key cryptographic technique uses single key for both encryption and decryption. The Asymmetric key cryptographic technique uses two separate keys for encryption and decryption.*

Advanced Encryption Standards (AES) algorithm is used for imparting Symmetric key cryptographic technique and Rivest-Shamir-Adleman(RSA) algorithm is used for imparting Asymmetric key cryptographic technique.

The compression algorithm is used to compress the encrypted text before sending it. This reduces the size of the encrypted file and abets in fast file transmission. Therefore by compression of the encrypted file increases the efficiency of data transmission. Compression technique is of two types, lossy compression and lossless compression. This research deals with the lossless compression.

The plain text is first encrypted using Symmetric technique. The symmetric key which is used to encrypt the data is encrypted using Asymmetric technique. The encrypted key and the encrypted text are compressed and sent to the receiver. The integrity of the data that is transmitted can be checked by subjecting the plaintext to the MD5 Hash algorithm. The Message Digest obtained by this process is also encrypted using Asymmetric technique.

The public key of the RSA technique is also encrypted before transmitting to the other end. This makes the Hy-Com technique more robust. The key is encrypted using the rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. This increases the security in the key distribution.

Therefore the sender sends the compressed modes of cipher text of the message, cipher text of the key and cipher text of the message digest. The receiver uncompresses the file first and decrypts it. The original file is checked with the digest. If both are equal the message is accepted else rejected.

Keywords— *Hycom, Hybrid compressive technique, Secured data transmission, AES, RSA, LZW, MD5, Rail Fence Technique.*

I. Introduction

The Hy-Com cryptographic technique is the hybrid of Symmetric, Asymmetric, Compressing and authentication techniques. Advanced Encryption Standards (AES) algorithm is used for imparting Symmetric key cryptographic technique and Rivest-Shamir-Adleman (RSA) algorithm is used for imparting Asymmetric key cryptographic technique. For compressing the encrypted text Lossless compression technique is used. Data compression increases the speed of data traversal. This increases the efficiency of the data transmission. Message is authenticated by MD5 Hashing algorithm. Thus formed Message Digest is checked with the original message for its integrity.

The plaintext is first subjected to Hash algorithm to get the message digest. The message digest is encrypted with the RSA algorithm. The plaintext is encrypted to cipher text using AES. The encrypted text and the key which is used for AES are then encrypted using RSA algorithm. The encrypted plaintext, encrypted message digest and along with the encrypted public key is send to the receiver end.

The receiver first decrypts the cipher key using the Transposition technique. Using the obtained public key and with his own private key the receiver decrypts the second cipher text using the RSA algorithm to get the first cipher text and the symmetric key. So obtained cipher text is decrypted with the Symmetric key and AES algorithm.

Cipher message digest is decrypted using RSA algorithm with the public and private key. The message digest is compared with the plain text which was obtained earlier. If both are equal the message is accepted else rejected.

II. Hy-Com Architecture for Encryption

The main issues of cryptographic algorithm are the security and authenticity. The Hy-Com technique uses the combination of both Symmetric and Asymmetric Techniques and its protocol architecture is shown below.

The plain text is first encrypted with the Advanced Encryption Standards, AES to obtain cipher1. This encryption uses Symmetric technique which takes a single key for encryption. The cipher1 and along with its key is again subjected to the second level of encryption with Rivest-Shamir-Adleman (RSA) to obtain cipher2. This encryption uses Asymmetric technique which takes a pair of key named Public (PU) key and Private (PR) key. Thus got cipher2 is compressed with the LZW compression algorithm.

Simultaneously, the Message digest and the encrypted Public (PU) key are created. The Hash value is calculated through MD5 for the same plain text. This Hash value is encrypted with RSA. The public key is encrypted with the Transposition technique to obtain the cipher key. The cipher key and the message digest are compressed with LZW so as to reduce the time for data transmission.

The compressed and the encrypted form of the text, key and message digest is send to the receiver side.

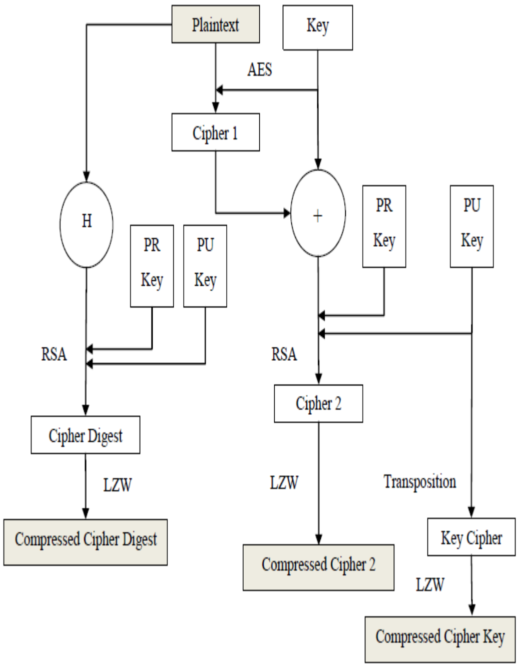
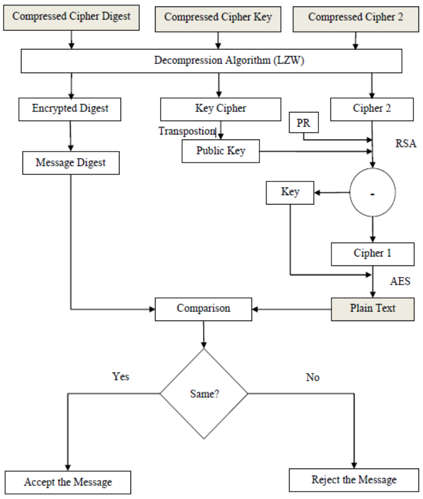
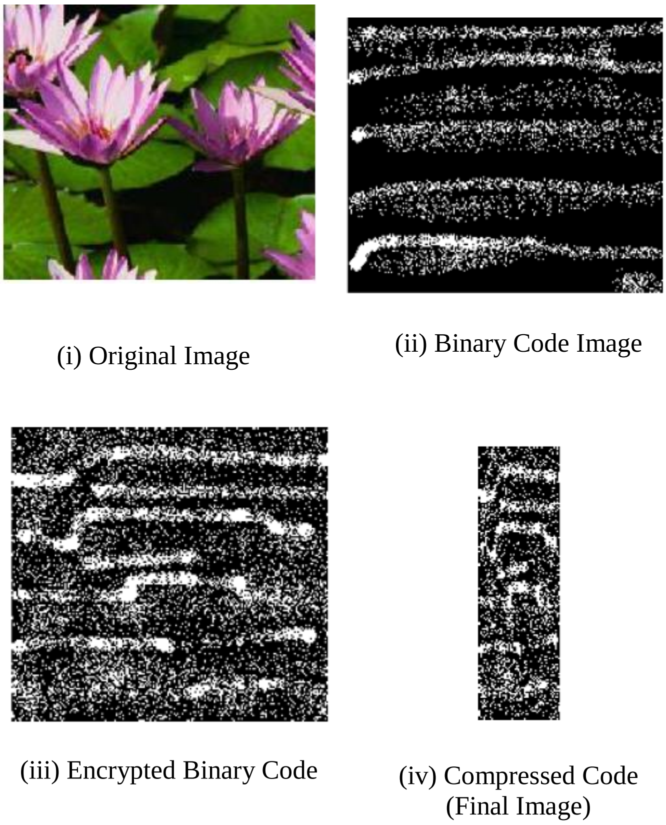


Fig. 1 Hy-Com Architecture for Encryption

III. HY-COM ARCHITECTURE FOR DECRYPTION

The decryption is done in the reverse order on encryption. The receiver receives the compressed and the encrypted form of plain text, the public key of the RSA algorithm and the message digest. First Decompression is done using the LZW algorithm to obtain cipher2. The decompressed cipher text is decrypted first by the RSA algorithm to obtain cipher1. The cipher1 is then decrypted by AES algorithm to obtain the plaintext. The plaintext is compared with message digest. If both are same the message is accepted else rejected.





(i) Original Image

(ii) Binary Code Image

(iii) Encrypted Binary Code

(iv) Compressed Code (Final Image)

Fig. 2 Hy-Com Architecture for Decryption

IV. DIAGRAMMATIC REPRESENTATION OF HY-COM CRYPTOGRAPHY

The diagrammatic representation of the original and the final image is presented here. Figure 3 (i) represents the original image that has to be encrypted and compressed using Hy-Com technique. The original image is then subjected to the converter, to convert each and every pixel to its corresponding Binary Values. The image with binary code is depicted in the Figure 3 (ii). Encryption technique is used to make the Binary code unreadable so as to protect the image from hacking. The Encrypted form of the Binary Code is depicted in the Figure 3 (iii). The encrypted image is the compressed and shown in Figure 3 (iv). Thus formed image is the final image that is to be transferred to the other end on the network.

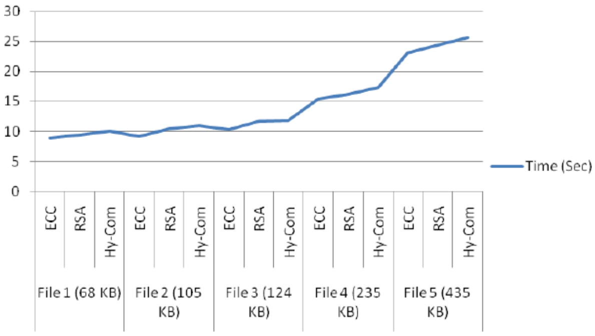


Fig. 3 Diagrammatic Representation of Hy-Com Cryptography

V. RESULT

Performance of encryption algorithm is evaluated considering the following parameters.

i. Computation Time

ii. Memory usage

iii. Output Bytes

The performance of the algorithm comparison this section is the results obtained from the cryptography library Crypto++.

A. *Comparison of Performance on the Aspect of Computational Time*

TABLE I
COMPARISON TABLE ON ENCRYPTION TIME

Data	Algorithm	Time (sec)
File 1 (68 KB)	ECC	8.9
	RSA	9.4
	Hy-Com	10.02
File 2 (105 KB)	ECC	9.2
	RSA	10.5
	Hy-Com	10.98
File 3 (124 KB)	ECC	10.3
	RSA	11.67
	Hy-Com	11.9
File 4 (255 KB)	ECC	15.4
	RSA	16.2
	Hy-Com	17.42
File (435 KB)	ECC	23.12
	RSA	24.4
	Hy-Com	25.72

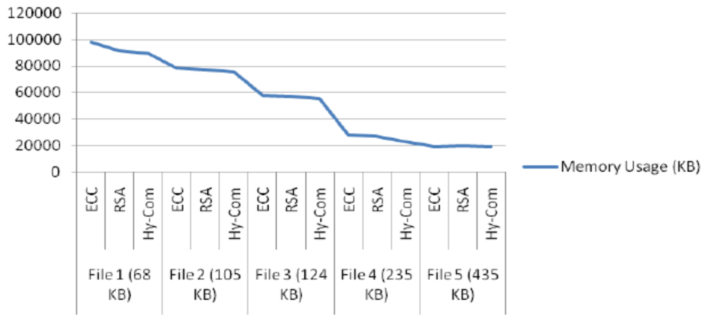


Fig. 4 Comparison Chart on Encryption Time

TABLE II
COMPARISON TABLE ON DATA ENCRYPTION AND TRANSMISSION TIME

Data	Algorithm	Time (sec)
File 1 (68 KB)	ECC	11.2
	RSA	12.3
	Hy-Com	10.52
File 2 (105 KB)	ECC	13.3
	RSA	13.7
	Hy-Com	12.09
File 3 (124 KB)	ECC	14.6
	RSA	15.42
	Hy-Com	12.98
File 4 (255 KB)	ECC	22.3
	RSA	23.5
	Hy-Com	20.5
File (435 KB)	ECC	34.47
	RSA	36.03
	Hy-Com	29.2

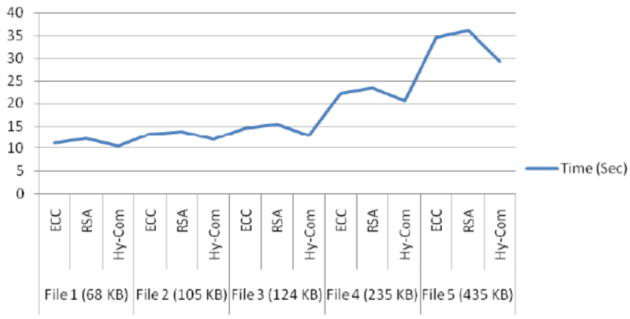


Fig. 5 Comparison Chart on Data Encryption and Transmission Time

B. *Comparison of Performance on the Aspect of Memory Usage*

TABLE III
COMPARISON TABLE ON MEMORY USAGE

Data	Algorithm	Memory Usage (KB)
File 1 (68 KB)	ECC	98113
	RSA	91814
	Hy-Com	89671
File 2 (105 KB)	ECC	78490
	RSA	77117
	Hy-Com	75372
File 3 (124 KB)	ECC	58012
	RSA	57178
	Hy-Com	55173
File 4 (255 KB)	ECC	27912
	RSA	26891
	Hy-Com	23006
File (435 KB)	ECC	19239
	RSA	19802
	Hy-Com	19511

Fig. 6 Comparison Chart on Memory Usage

C. *Comparison of Performance on the Aspect of Memory Bytes*

TABLE IV
COMPARISON TABLE ON MEMORY BYTES

Data	Algorithm	Output (Bytes)
File 1 (68 KB)	ECC	14336
	RSA	65536
	Hy-Com	1280
File 2 (105 KB)	ECC	14336
	RSA	65536
	Hy-Com	1280
File 3 (124 KB)	ECC	14336
	RSA	65536
	Hy-Com	1280
File 4 (255 KB)	ECC	14336
	RSA	65536
	Hy-Com	1280
File (435 KB)	ECC	14336
	RSA	65536
	Hy-Com	1280

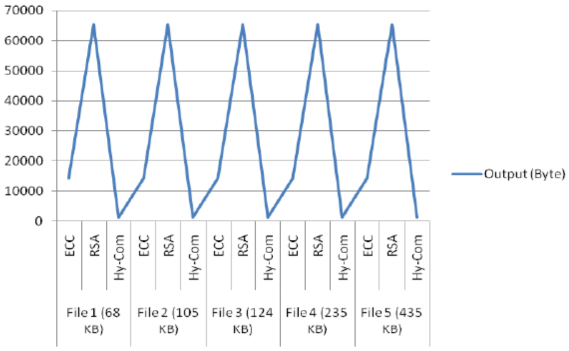


Fig. 7 Comparison Chart on Output Bytes

VI. CONCLUSIONS

At present, Internet and network applications are growing very fast, so the need to protect such applications has increased. Encryption algorithms play an immense role in information security systems. This research has presented the optimization of attacks for text encryption and its performance analysis. All essential and collateral parameters are systematically determined to satisfy the specific cryptographic security requirements. This technique solves at least some of the drawbacks suffered by existing cryptographic algorithms such as AES and RSA. In this research, the Hy-Com cryptographic technique is fully described and validated with functional and load tests. Then, appropriate metrics for performance measurements are identified; the performance of the algorithm was measured and compared with such existing cryptographic algorithms as RSA and ECC. The test results show that the designed algorithm works as required, that is, the data enciphered and compressed by the Hy-Com process is fully recovered by the deciphering and uncompressing process. The test and security analysis prove that the cipher is not prone to threat or statistical attack, and the key is secure. The performance of the Hy-Com cryptographic technique is by far better than the ECC and RSA. It has less encryption time, less power consumption, and higher throughput than ECC and RSA. The RSA cipher is longer than the Hy-Com cipher causing more resource consumptions and congestion in memory and bandwidth. Comparing Hy-Com with AES, AES has better performance only for relatively smaller data sizes. Hy-Com encryption has another advantage over RSA and AES in that it's key.

Thus the Hy-Com technique ensures the confidentiality, effectiveness, integrity and authentication. The AES and RSA algorithm provides confidentiality, the hash function provides the integrity, LZW algorithm provides effectiveness and RSA will ensure the authentication.

REFERENCES

[1] Willaim Stallings, "Cryptography and network Security Principles and Practices", Prentice Hall, 2005.

[2] J. Daemen and V. Rijmen, "AES Proposal: Rijndae"l, AES Algorithm Submission, September 3, 1999.

[3] Menezes, P. van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, New York, 1997.

[4] D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key d less than N ", IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1339–1349, Jul. 2000.

[5] B. den Boer and A. Bosselaers, "Collisions for the compression function of MD5", Advances in Cryptology, Eurocrypt „07, pages 293-304, Springer-Verlag, 2007.

[6] J. Ziv and A. Lempel, "Compression of Individual Sequences via Variable-Rate Coding", IEEE Transactions on Information Theory, Sept. 1978.

[7] National institute of standards and technology, "Digital signature standard", FIPS Publication, February 2000.

[8] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, 1978.

[9] T. El Gamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory.

[10] Sayood K., "Introduction to Data Compression", Academic Press, San Diego, 1996.

[11] Ravindra Kumar Chahar, "Design of a new Security Protocol", IEEE International Conference on Computational Intelligence and Multimedia Applications, pp 132 – 134, 2007.

[12] Kamana Singh, Ankur Goyal, "Implementation of Modified CRT Algorithm for Packet Routing Evaluation to Improved Energy Saving and Reliability in Wireless Sensor Networks, IJCOT, Volume 12, pp 35, Sept. 2014.