CHANDIGARH UNIVERSITY

Discover. Learn. Empower.

HYBRID CRYPTOGRAPHY

**BACHELOR OF ENGINEERING IN
COMPUTER SCIENCE & ENGINEERING**

Submittedto:

SHIKHA ATWAL

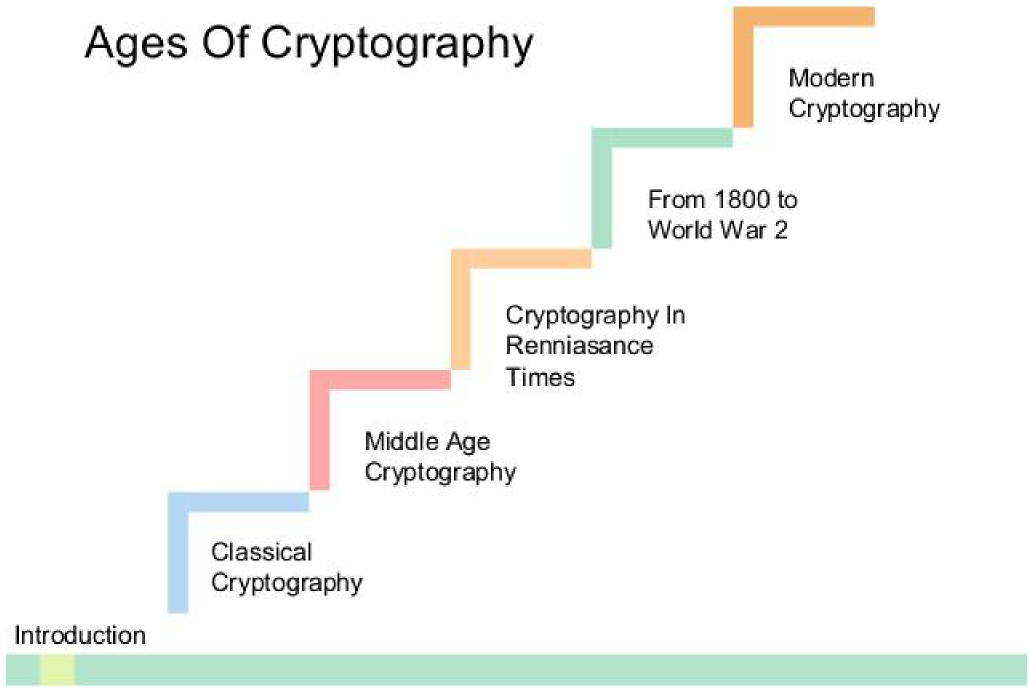
SubmittedBy:

YUKTI GOYAL	18BCS1838
SHUBHAM SHUKLA	18BCS1848
PRADIPTA SARKAR	18BCS1854
MIRTUNJAY GUPTA	18BCS1843

CONTENT:-

- PROJECT DESIGN
- PROPOSED METHODOLOGY
- INTRODUCTION
- HISTORY
- TYPE OF CRYPTOGRAPHY
- ISSUE OF CRYPTOGRAPHY
- IMPLEMENTATION
- RESULT AND DISCUSSION
- CONCLUSION
- REFERENCE

HISTORY OF CRYPTOGRAPHY



Ages Of Cryptography

Modern Cryptography

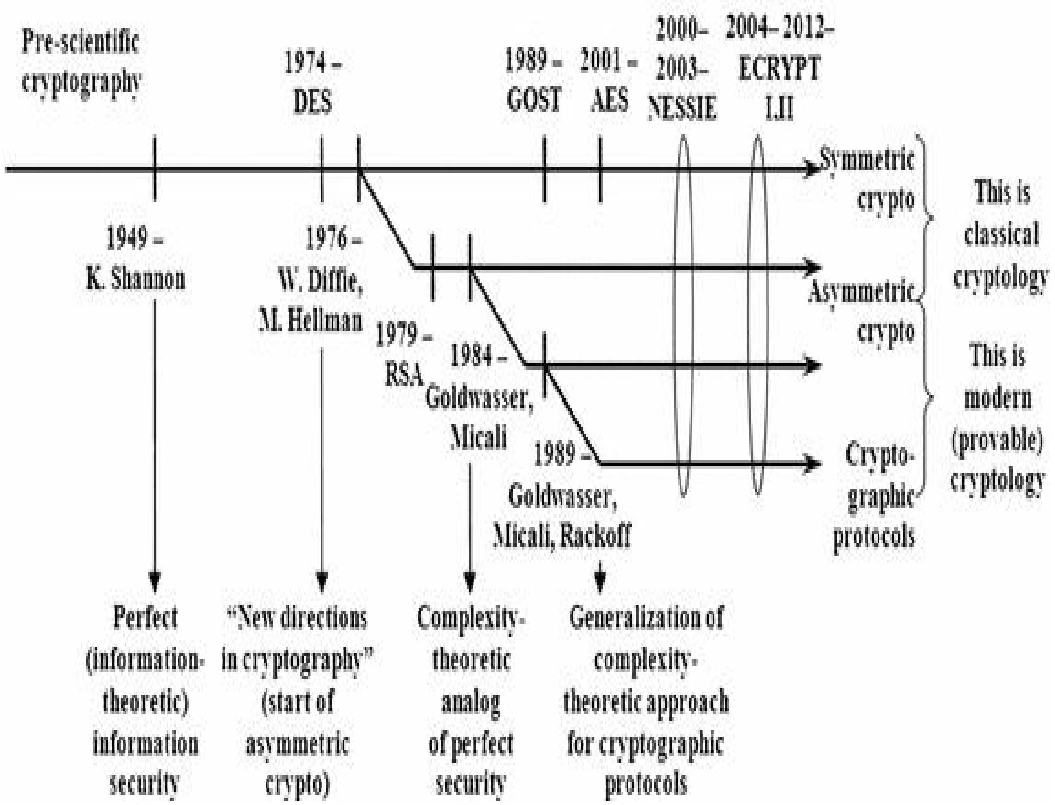
From 1800 to World War 2

Cryptography In Renniasance Times

Middle Age Cryptography

Classical Cryptography

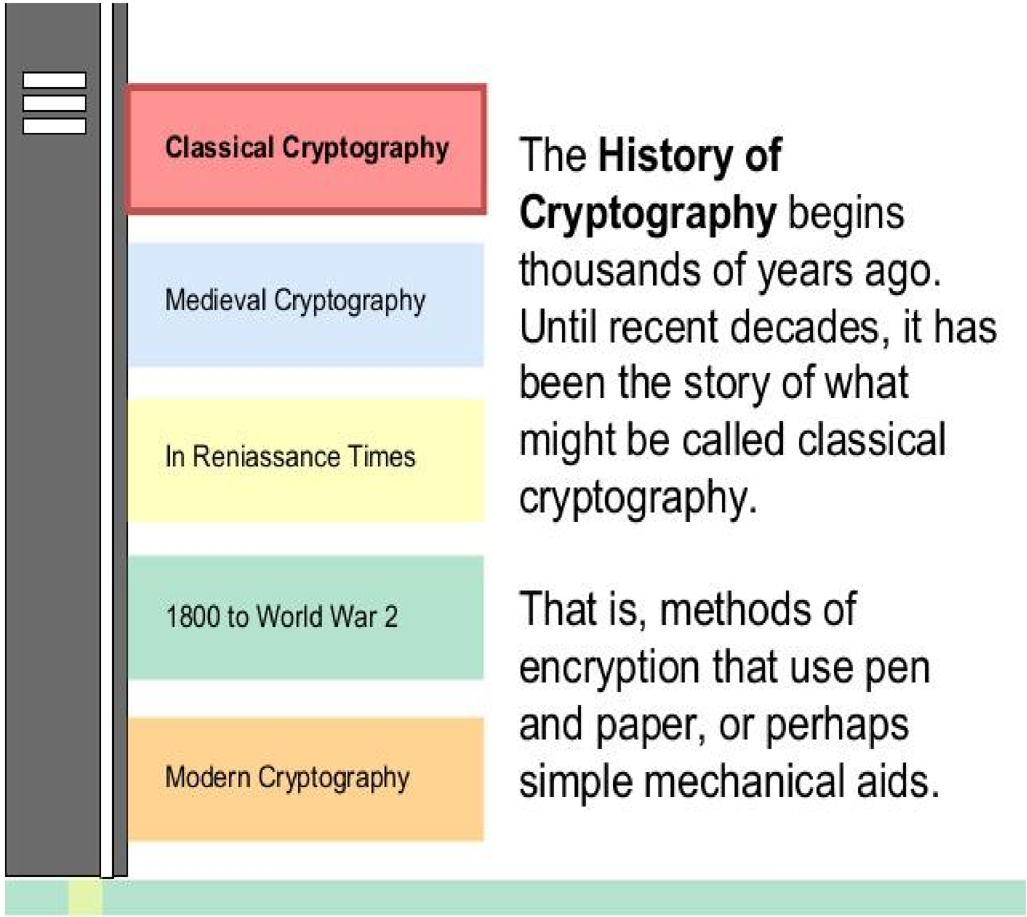
Introduction



Pre-scientific cryptography
1974 – DES
1989 – GOST
2001 – AES
2000–2003– NESSIE
2004–2012– ECRYPT I,II
Symmetric crypto
This is classical cryptology
1949 – K. Shannon
1976 – W. Diffie, M. Hellman
1979 – RSA
1984 – Goldwasser, Micali
Asymmetric crypto
This is modern (provable) cryptology
1989 – Goldwasser, Micali, Rackoff
Crypto-graphic protocols
Perfect (information-theoretic) information security
"New directions in cryptography" (start of asymmetric crypto)
Complexity-theoretic analog of perfect security
Generalization of complexity-theoretic approach for cryptographic protocols

HYSTORY

Cryptography, the use of codes and ciphers to protect secrets, began thousands of years ago. Until recent decades, it has been the story of what might be called classic cryptography — that is, of methods of encryption that use pen and paper, or perhaps simple mechanical aids. In the early 20th century, the invention of complex mechanical and electromechanical machines, such as the Enigma rotor machine, provided more sophisticated and efficient means of encryption



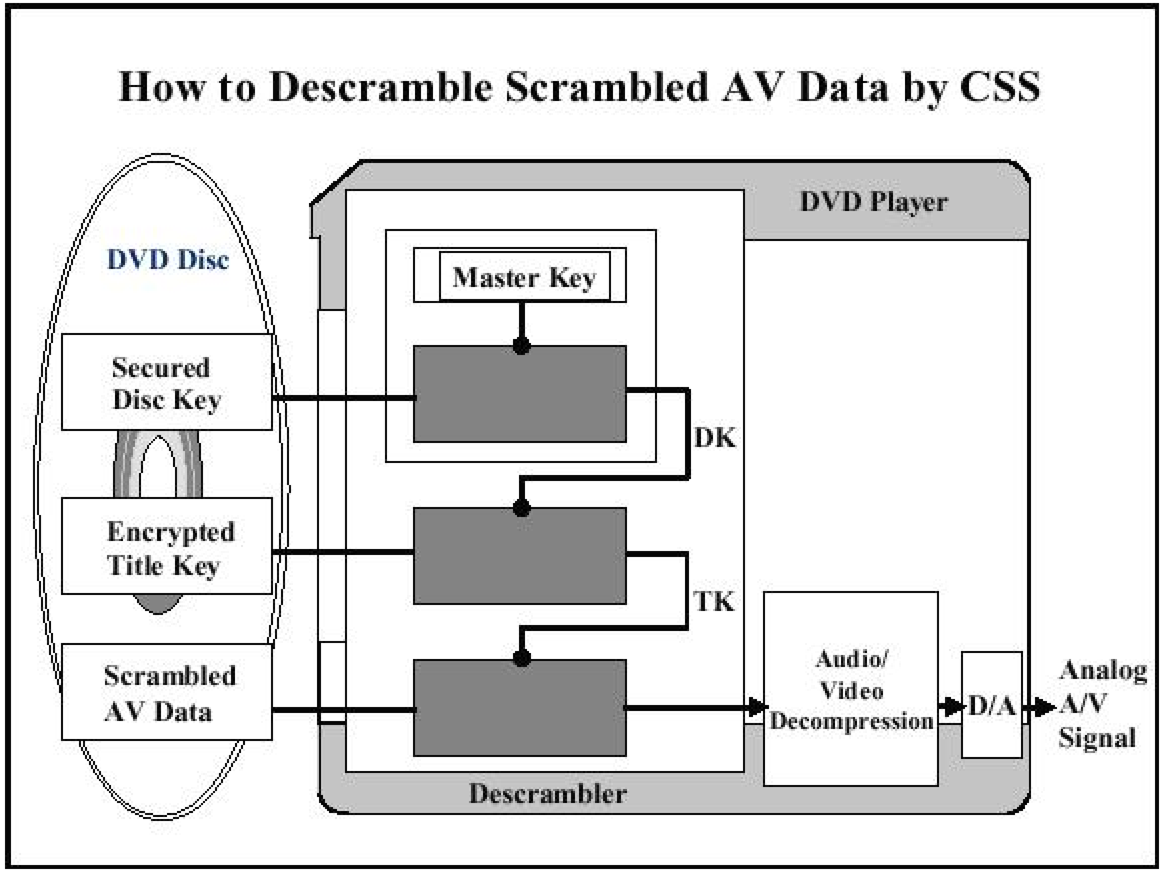
The **History of Cryptography** begins thousands of years ago. Until recent decades, it has been the story of what might be called classical cryptography.

That is, methods of encryption that use pen and paper, or perhaps simple mechanical aids.

PROJECT DESIGN

- The proposed system is a cryptographic algorithm which accepts any kind of data for processing. In addition of that the simulation of the proposed methodology enables a user to send and receive data using the application. The proposed simulation first accepts the data from the user and then compresses it in order to reduce the data size. After doing that it uses the proposed cryptographic algorithm data to manipulate the data into cipher text. The generated cipher text is compressed again and using file splitter utility and then it is transmitted much efficiently on network. On the other end the receiver follows the same procedure in reverse direction to decrypt it.

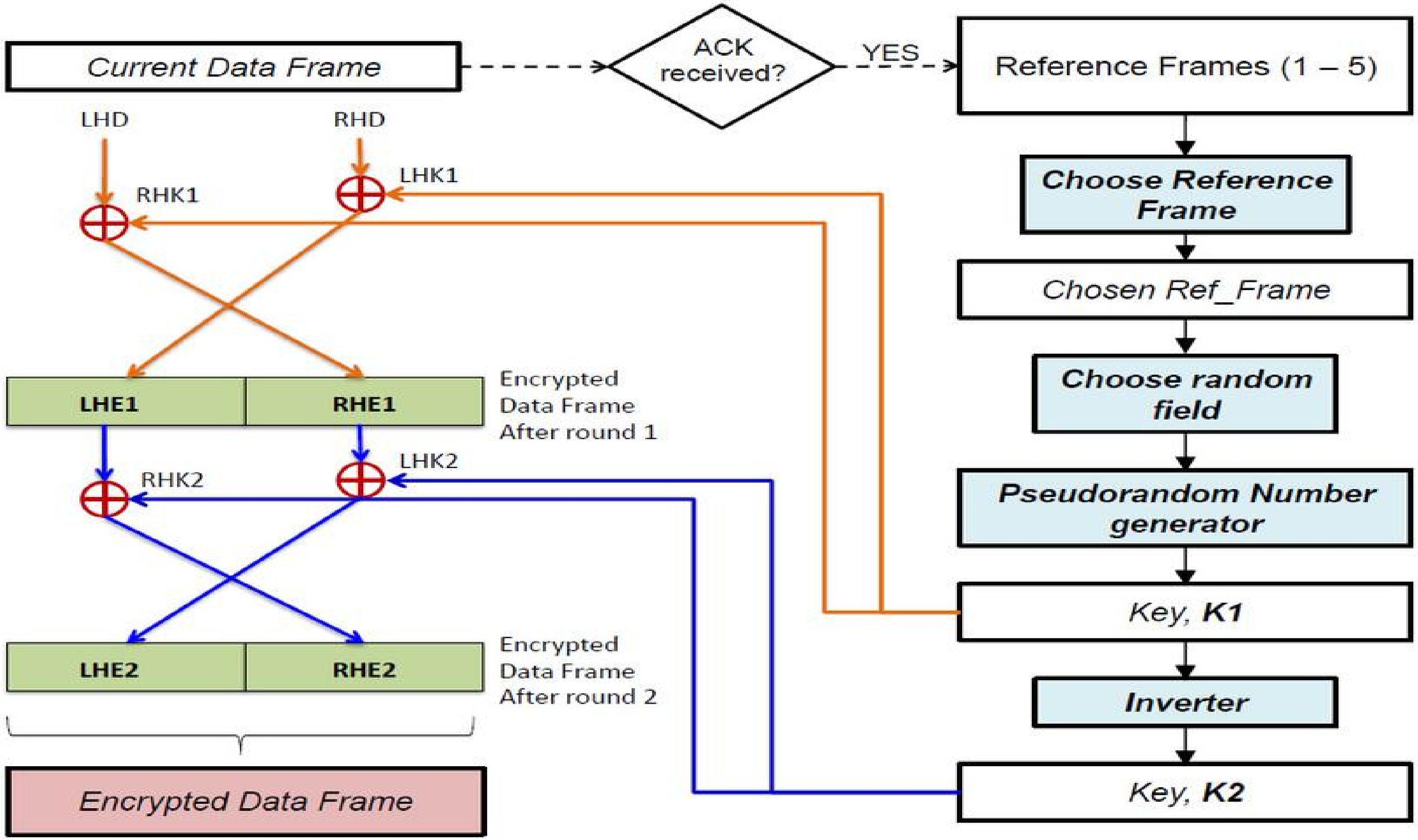
PROPOSED METHODOLOGY



.

- Input file: This is the input file to be sent over the network. SHA1: The compressed zip file is produced before the SHA1 algorithm to generate 128 bit hash. This hash is used to check the data validity at the receiver end. If the sender generated hash matched with the receiver end hash than the data is valid otherwise data is corrupt.
- Key (16 bytes): This is SHA1 generated hash which is separately treated as key form encryption. Over the produced 128 bit hash key the bit discarding process is taken place, in this process the 128 bit hash code is converted into 16 blocks of the 8 bit data. In each block of data the first bit is removed and placed separately for further processing

Encrypted and Decryption



INTRODUCTION

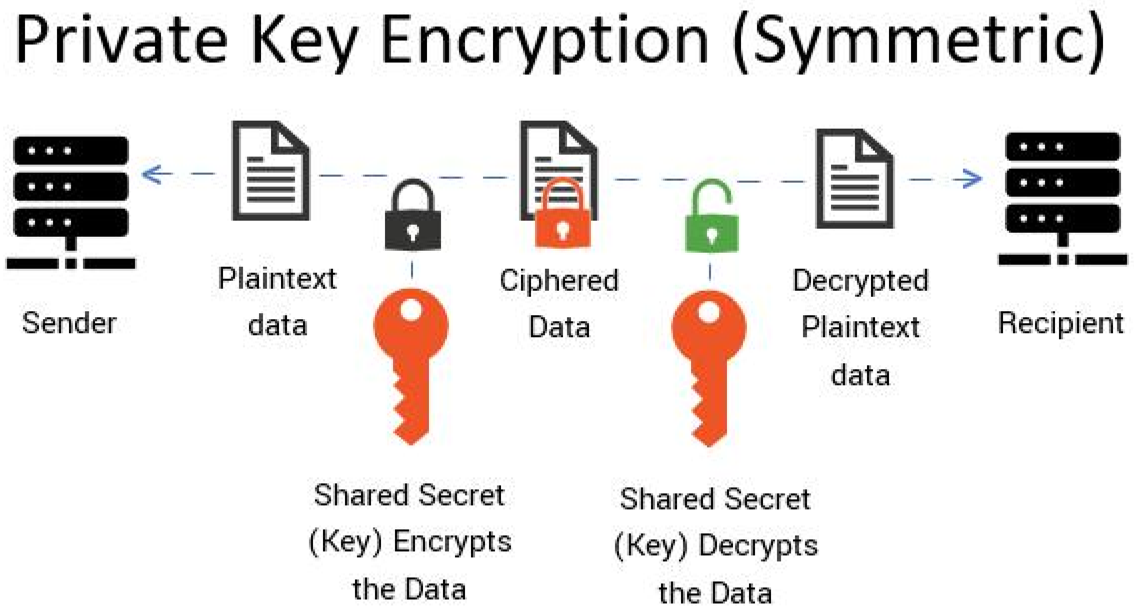
Cryptography enables the user to transmit confidential information across any insecure network so that it cannot be used by an intruder. A cryptographic algorithm is a mathematical function that can be used in the process of encryption and decryption. Encryption is the process of converting the plain text into an unreadable form called a cipher text.. Decryption is the process of converting this unreadable form back into its original form, so that it can be easily understood by the intended recipient. In symmetric-key cryptography, also called conventional cryptography or secret-key encryption, one key is used both for encryption and decryption. Examples include DES and AES. But symmetric-key cryptography has some limitations.

PRIVATE KEY ENCRYPTION

- It is also referred to as conventional encryption or single-key encryption, was the only type of encryption in use prior to the development of public key

- It is also referred to as conventional encryption or single-key encryption, was the only type of encryption in use prior to the development of public key

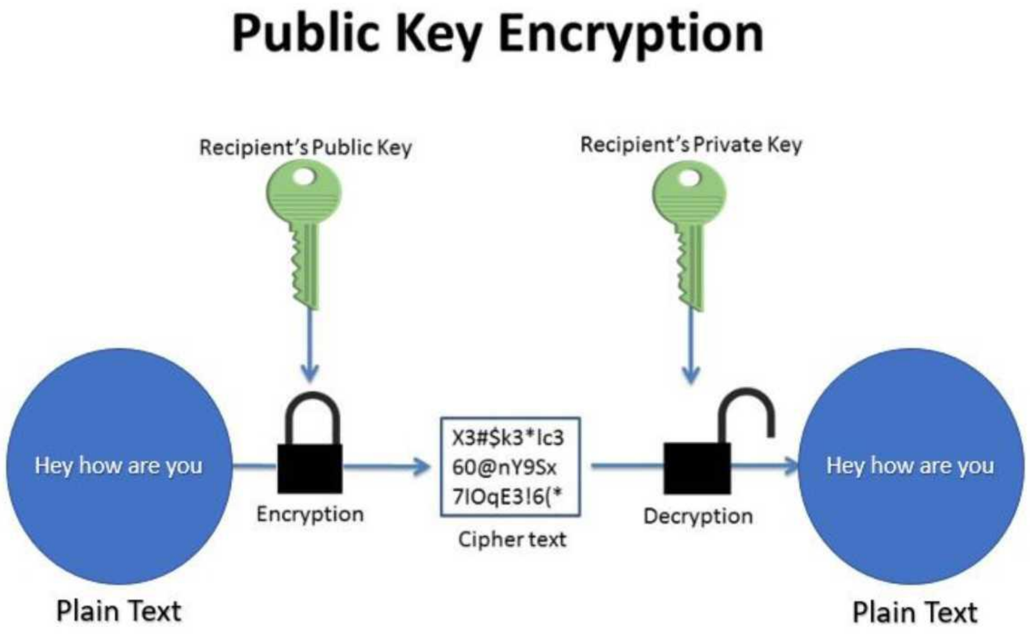
PRIVATE KEY ENCRYPTION

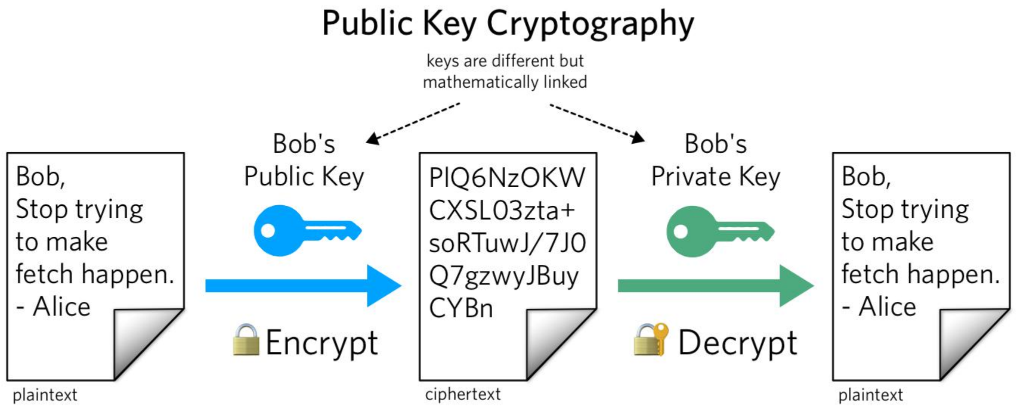

Private Key Encryption (Symmetric)
Sender
Plaintext data
Shared Secret (Key) Encrypts the Data
Ciphered Data
Shared Secret (Key) Decrypts the Data
Decrypted Plaintext data
Recipient

Public Key Encryption:

- The development of public-key cryptography is the greatest and perhaps the only true revolution in the entire history of cryptography [10].
- The concept of public key cryptography evolved from an attempt to attack the most difficult problem associated with conventional symmetric cryptosystems
- Public-key cryptography provides a radical departure from all that has gone before. For one thing, public-key algorithms are based on mathematical functions rather than on substitution and permutation.

Public Key Encryption:





Issues of Cryptography

- There are several issues related to cryptographic algorithm such as time complexity, space complexity and its resistance to various types of attacks. In order to implement an effective cryptographic algorithm all these aspects needs to be considered in order to make it robust. Let’s discuss these issues:- Time Complexity: It is the amount of time required to encrypt and decrypt the data. The algorithm should be designed in such a way that it should take as less time as possible for its execution. Hence it is necessary to consider its time complexity while implementing a cryptographic algorithm.

Space Complexity

- It is the amount of space consumed by cipher text as compared with plain text. As more and more mobile devices with limited connectivity in terms of data rate are being used nowadays, it is very essential to keep the size of cipher text being produced as small as possible as to deal with variable data rates. Thus it is very important to device a way to reduce the size of cipher text as much as possible to increase data transmission efficiency.

SECURITY:

- The very important purpose of cryptography is to secure the data being transmitted over the network from various types of attacks. The data being transmitted is always vulnerable to various types of attacks such as men in the middle attack, brute force attack etc. Thus in order to prevent the data from being compromised it is necessary to protect the data from unauthorized users.

CHARATERISTICS

1 Most of the cryptographic techniques are time consuming processes

2. Not includes the integrity checks on transmitted data

3. Required security in key exchange

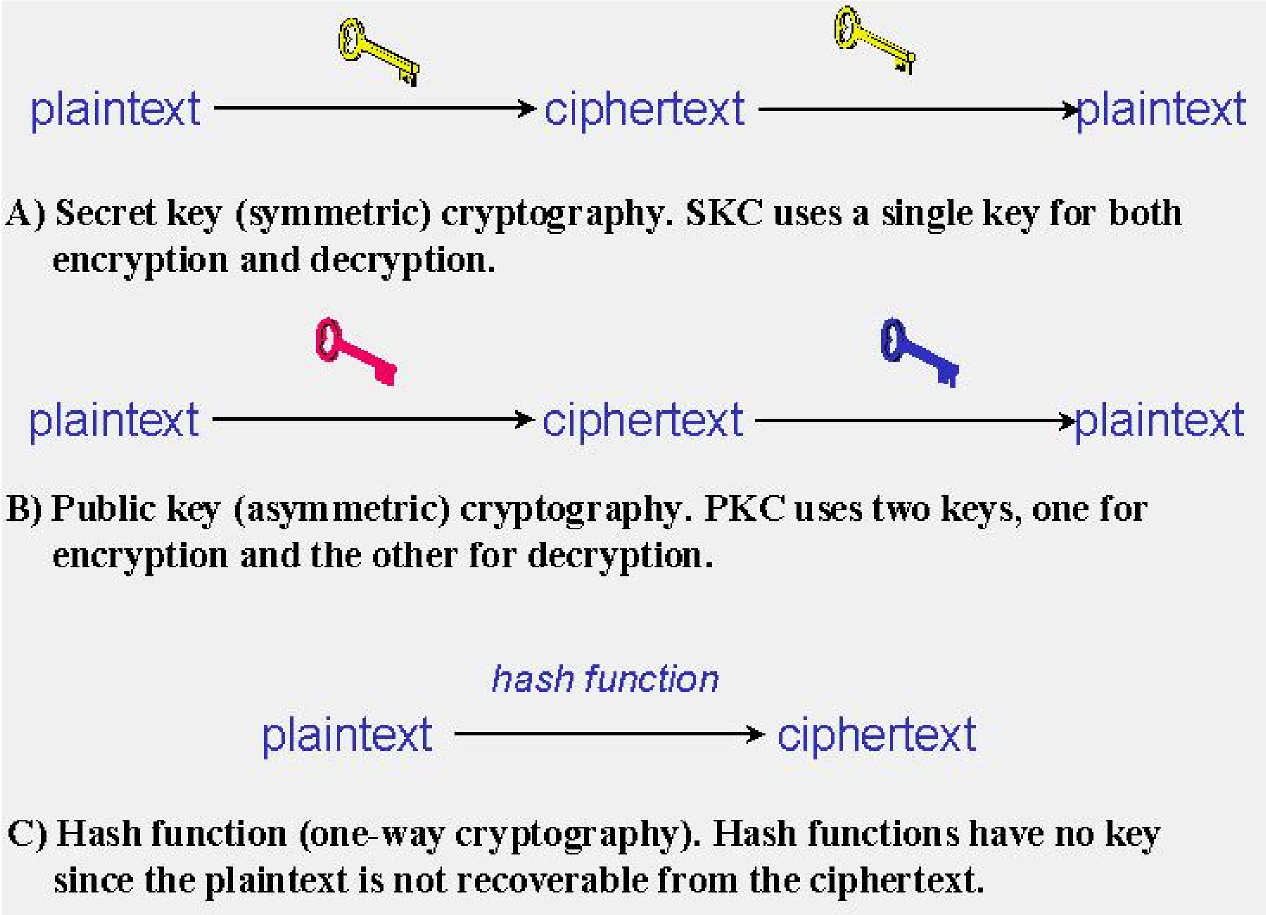
4. The amount of cipher text is higher than the original text

5. During attack the cipher text is easily breakable with Men in the middle kind of attacks. Solution domain In order to find an optimum solution for cryptographic processes the following solutions are suggested to incorporate

Types of Cryptography

- **Secret Key Cryptography (SKC):** Uses a single key for both encryption and decryption; also called symmetric encryption. Primarily used for privacy and confidentiality.
- **Public Key Cryptography (PKC):** Uses one key for encryption and another for decryption; also called asymmetric encryption. Primarily used for authentication, non-repudiation, and key exchange.
- **Hash Functions:** Uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint. Primarily used for message integrity.

CRYPTOGRAPHY FUNCTION



A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

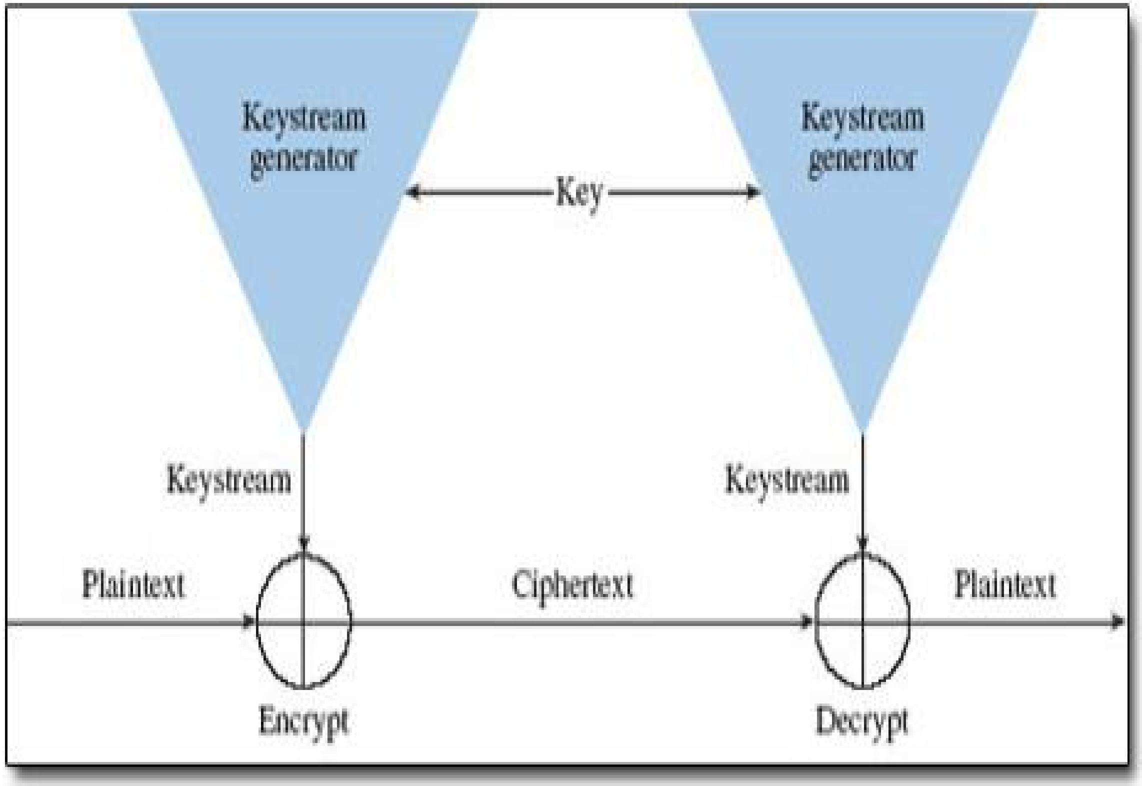
B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

Secret Key Cryptography

Secret key cryptography methods employ a single key for both encryption and decryption. the sender uses the key to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers.



Public Key Cryptography

Public key cryptography has been said to be the most significant new development in cryptography in the last 300-400 years. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key.

.Multiplication vs. Factorization:

Suppose you have two prime numbers, 3 and 7, and you need to calculate the product; it should take almost no time to calculate that value, which is 21. Now suppose, instead, that you have a number that is a product of two primes, 21, and you need to determine those prime factors. You will eventually come up with the solution but whereas calculating the product took milliseconds, factoring will take longer. The problem becomes much harder if we start with primes that have, say, 400 digits or so, because the product will have ~800 digits.

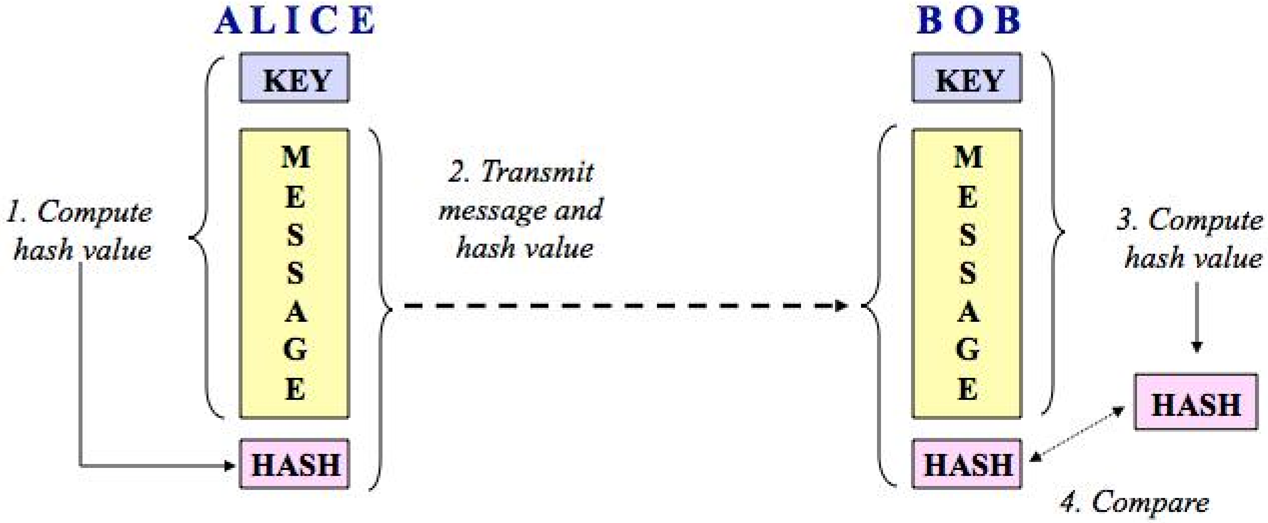
Exponentiation vs. logarithms

Suppose you take the number 3 to the 6th power; again, it is relatively easy to calculate 36 = 729. But if you start with the number 729 and need to determine the two integers, x and y so that logx 729 = y, it will take longer to find the two values.

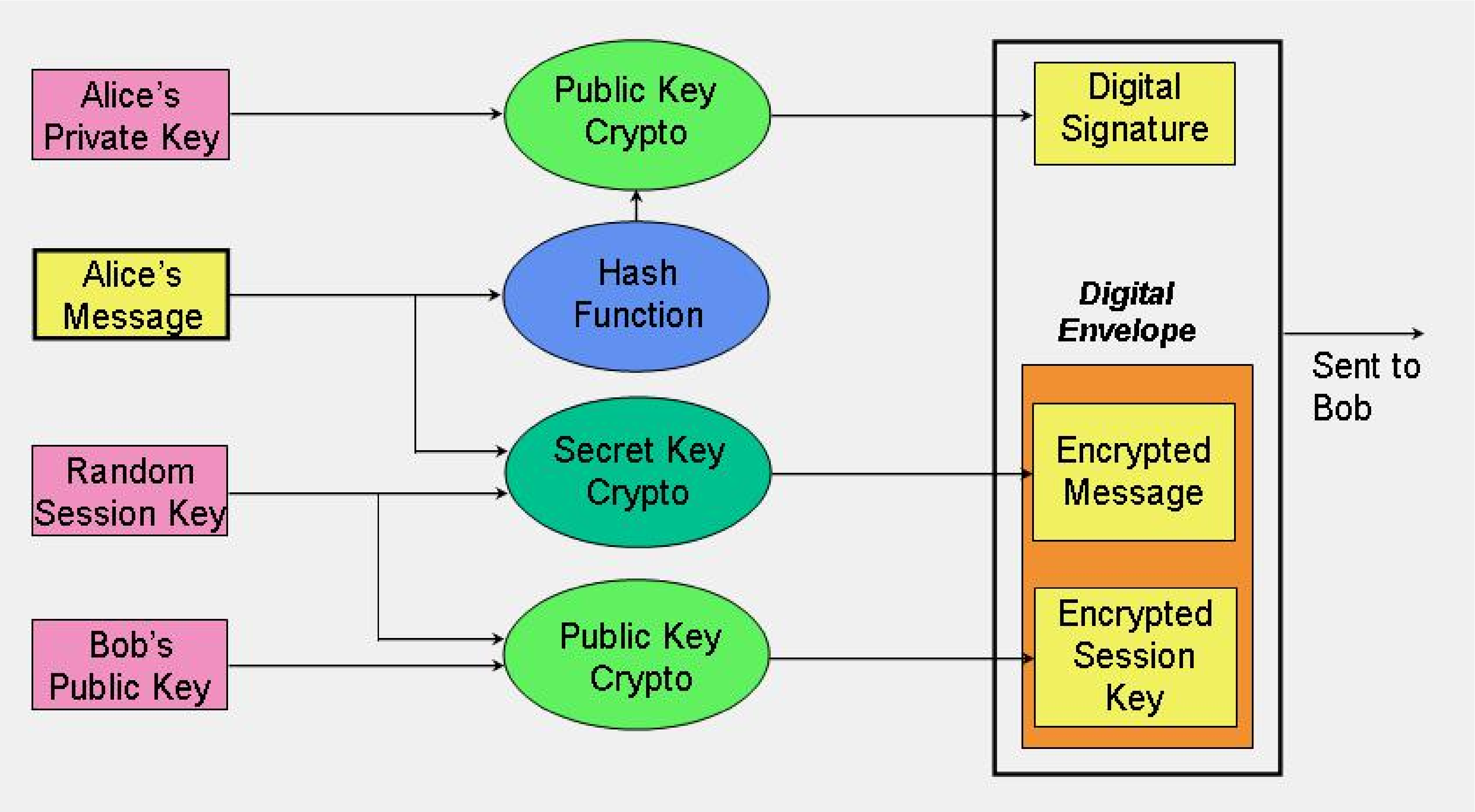
HASH FUNCTIONS

Hash functions, also called message digests and one-way encryption, are algorithms that, in essence, use no key Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents, often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a mechanism to ensure the integrity of a file.

HASH FUNCTION



Three Encryption Techniques



Significance of Key Length

- In a 1998 article in the industry literature, a writer made the claim that 56-bit keys did not provide as adequate protection for DES at that time as they did in 1975 because computers were 1000 times faster in 1998 than in 1975. Therefore, the writer went on, we needed 56,000-bit keys in 1998 instead of 56-bit keys to provide adequate protection. The conclusion was then drawn that because 56,000-bit keys are infeasible (true), we should accept the fact that we have to live with weak cryptography (false!).

IMPLEMENTATION

Proposed algorithm is secure because which encrypt and decrypt message with secretly generated sender key and receiver key which is known to sender and receiver. Two level of security is implemented. Algorithm is based on hybrid cryptography as it uses asymmetric that is sender and receiver key and asymmetric key that is both sender and receiver uses same key pair for both process encryption and decryption.the DES and RSA hybrid cryptographic algorithm is relatively more secure and easier.

IMPLEMENTATION

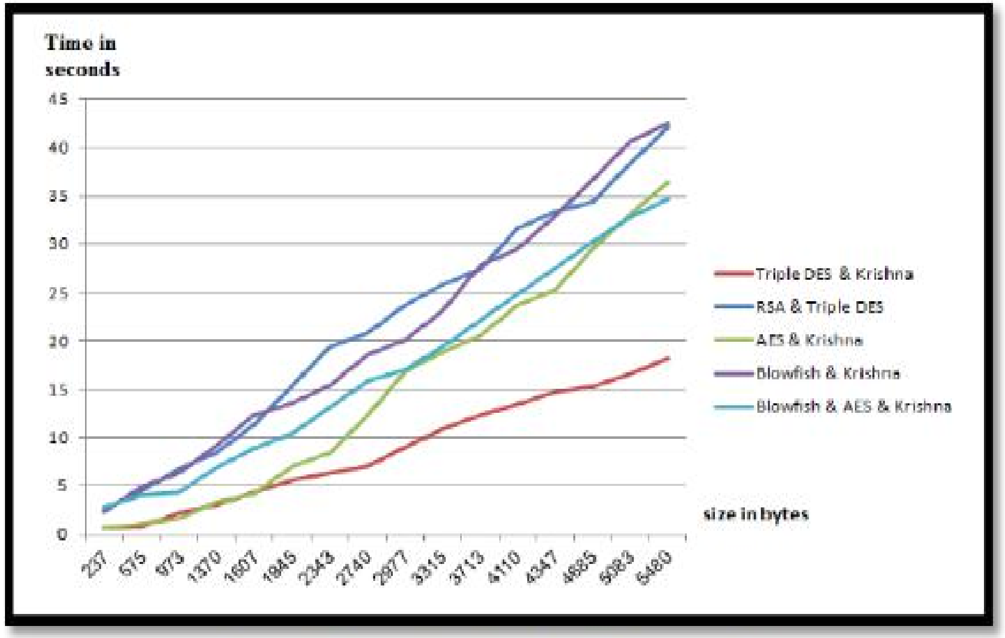


Fig. 7. The time consumed in encrypting data for each algorithm.

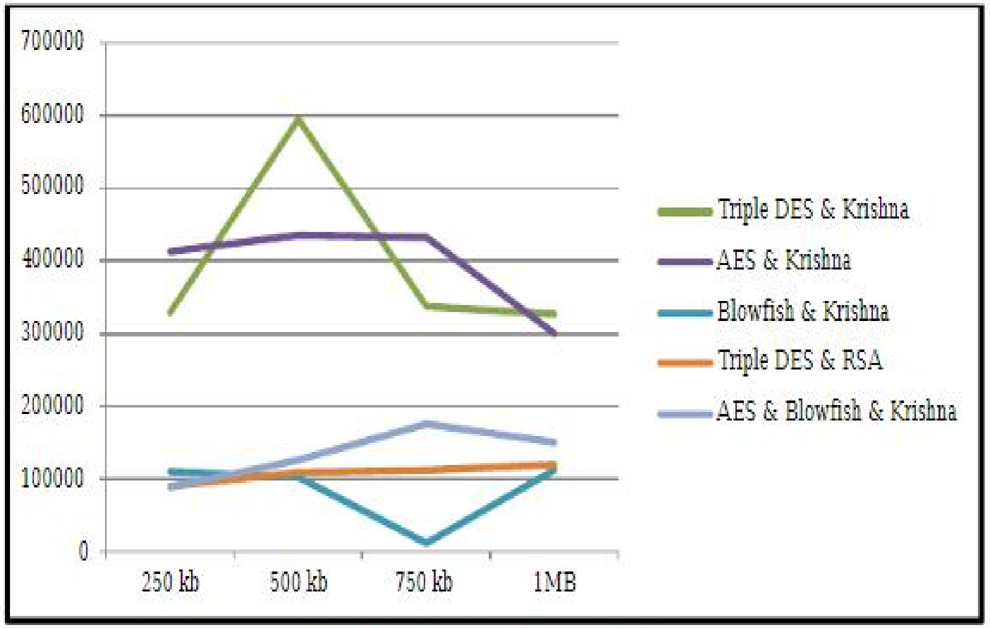
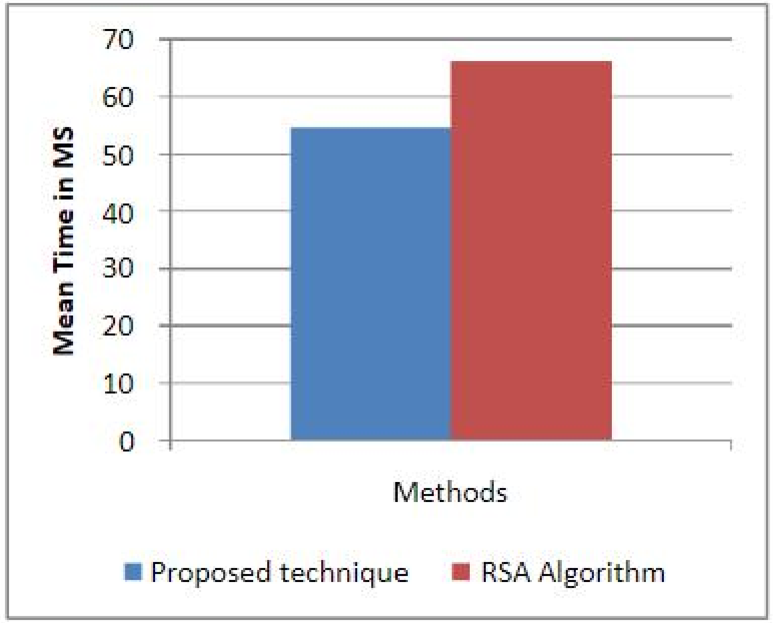


Fig. 8. The throughput for each algorithm.

INNOVATION IN DESIGN



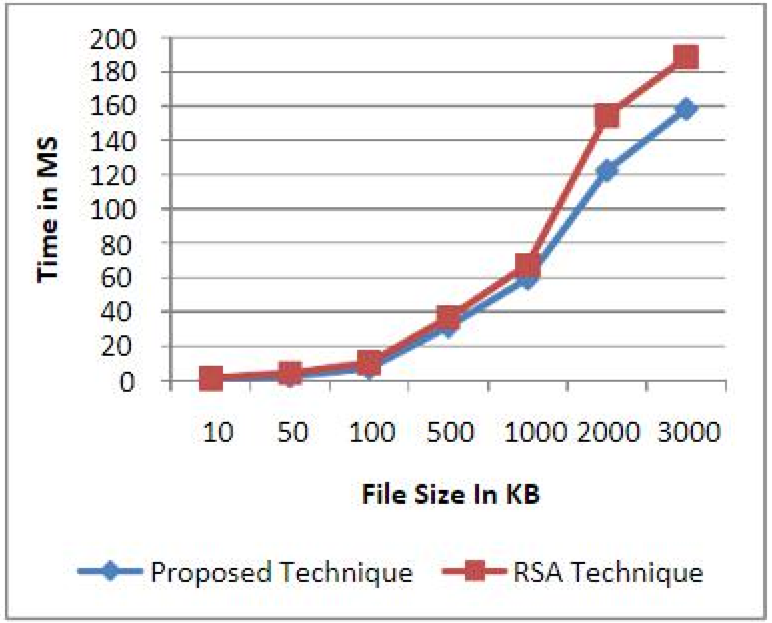


Figure 3: Encryption time

RESULT AND DISCUSSION

summarizes the number of papers that usescryptographic algorithms solely as well as algorithms that have been used along with some other algorithms like in case of hybrid cryptography. It can be noticed that hybrid cryptography is a demanding approach for today. Hybrid cryptography is gaining its strength as the naïve researchers laid more emphasis on combination of different cryptographic

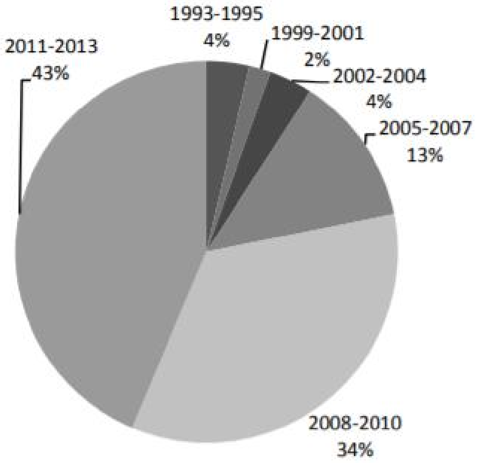
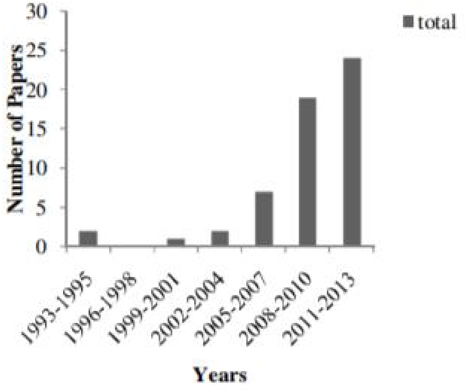


Fig 1: Percentage of papers used in the study



Conclusion

With the results of increased efficiency, speed and throughput of various algorithms by the combination of various algorithms and techniques, hybrid cryptography has a great scope in the near future. Hybrid cryptography has been creating various opportunities for the naïve researchers and allows them to work upon various challenging limitations of algorithms in their original forms. Hybrid cryptography is easy to work upon and a great number of chances for improvement are there. A number of different useful techniques and algorithms have been prescribed in this paper that can be used for providing security in the insecure media. This paper has been providing the study of past 20 years in the search for hybrid cryptographic algorithms that may help researchers to orientate their study areas and to choose various cryptographic algorithms for their studies. The study indicates the maximum use of RSA in the hybridization of various algorithms because of its Integer Factorization Problem. Diffie-Hellman being very secure is the prior choice for eliminating various limitations of cryptographic algorithms. AES and DES have limited scope of use because of the problem of key management. No doubt, the number of cryptographic algorithms presented here is neither complete nor exhaustive but a sample of papers that demonstrates the advantages and limitations of used cryptographic algorithms.

REFERENCES

- [1] S. Mohanty, B. Majhi, and V. Iyer, “A Strong Designated Verifiable Group Signature”, Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Multi-Conference on 22-23 March 2013, page(s): 518-523.
- [2] H. WANG, Z. SONG, X. NIU, and Q. DING, “Key Generation Research of RSA Public Cryptosystem and MATLAB Implement”, Sensor Network Security Technology and Privacy Communication System (SNS & PCS), 2013 International Conference on 18-19 May 2013, page(s): 125-129.
- [3] Y. L. Huang, F. Y. Leu, Y. K. Sun, C. C. Chu, and C. T. Yang, “A Secure Wireless Communication System by Integrating RSA and Diffie-Hellman PKDS in 4G Environments and an Intelligent Protection-key Chain with a Data Connection Core”, Industrial Electronics (ISIE), 2013 IEEE International Symposium on 28-31 May 2013, page(s): 1-6.

REFERENCE

- Basin, D., Cremers, C., Miyazaki, K., Radomirovic, S., & Watanabe, D. (2015, May/June). Improving the Security of Cryptographic Protocol Standards. IEEE Security & Privacy, 13(3), 24:31.
- Bauer, F.L. (2002). Decrypted Secrets: Methods and Maxims of Cryptology, 2nd ed. New York: Springer Verlag.
- Belfield, R. (2007). The Six Unsolved Ciphers: Inside the Mysterious Codes That Have Confounded the World's Greatest Cryptographers. Berkeley, CA: Ulysses Press.
- Denning, D.E. (1982). Cryptography and Data Security. Reading, MA: Addison-Wesley.
- Diffie, W., & Landau, S. (1998). Privacy on the Line. Boston: MIT Press.