# Comparative study of some cryptographic algorithms

**Prof. Devendra Vashi**
Institute of Technology
Nirma University
devendra.vashi@gmail.com

**Dr. Kuntal Patel**
School of Computer Studies
Ahmedabad University
kuntal.patel@ahduni.edu.in

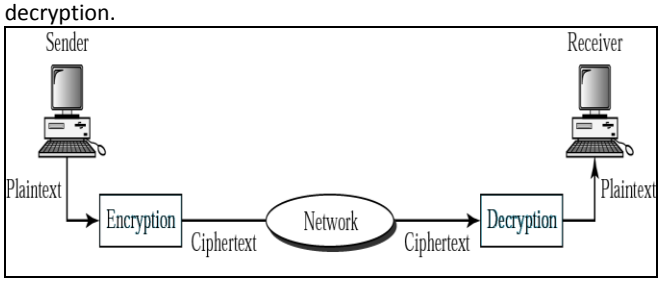
***Abstract*— *in privacy preserving data mining technique cryptographic process is good to implement properly for making data private while sending data to third party. This paper is just a study of some of the encryption and decryption technique like DES, RSA and hash function which can be implemented for cryptography. This paper is also emphasized on comparative study on different encryption technique and how is useful in cryptographic technique.***

***Keywords****: Cryptography, symmetric key, asymmetric key, encryption, decryption, ciphertext, DES, RSA*. AES

## I. INTRODUCTION

The requirement of information security within an organization is important today as many of the organizations are using computer based information system. Such computerized systems are networked based. The need of information security is even more sensitive for system that can be accessed over public telephone network, data network, or the Internet.

Generally in cryptographic technique the actual data is converting to in unknown format which is called encryption and converted data is called cypher text. Same way in reverse manner that encrypted data is convert it in actual format of data which is called decryption.




[Fig.1: Cryptography components][5]

## II. NEED OF CRYPTOGRAPHIC TECHNIQUE

Why do we need to implement cryptographic technique in our system? The answer is mentioned below:

**1.** Confidentiality: while sending data to anyone on the network the information has to be confidential which should not revealed to unknown party
**2.** Integrity: while sending the data on the network the data should not be altered
**3.** Non-repudiation: after sending the data sender should not change his or her objectives of sending data
**4.** Authentication: at the time of sending and receiving the data sender and receiver should confirm their identity

## III. DIFFERENT TYPES OF CRYPTOGRAPHIC TECHNIQUE

The major categories of cryptographic techniques are: classical techniques, modern techniques, and public-key encryption. In Classical techniques there are substitution techniques and transposition techniques. Caesar cipher, Monoalphabetic cipher and Polyalphabetic ciphers are the examples of classical techniques. In Modern techniques there are block cipher, stream cipher and DES algorithm. RSA algorithm is the widely used Public Key technology. Summarize into three broad categories as under:

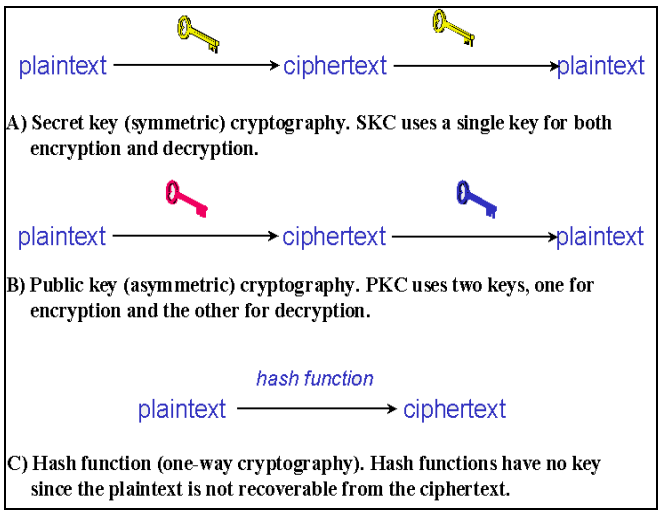
**A.** Symmetric Key Cryptography: This type of cryptographic technique uses a single key for encryption and decryption of the information [23]. They are also known as single key cryptography or secret key cryptography.

**B.** Public Key Cryptography: This type of cryptographic technique uses one key for encryption and another for decryption for the information [23]. They are also known as double key cryptography or asymmetric key cryptography.

**C.** Hash Functions: This type of cryptographic technique uses a mathematical transformation to encrypt the information

### A. SYMMETRIC KEY CRYPTOGRAPHY:

In such kind of cryptographic technique sender uses a single key to encrypt the information and same key is used by the receiver to decrypt the data which is shown in the figure-2. So In this cryptographic technique a single key is used for both encryption and decryption [8, 24, 26]. So in such kind of technique key must be known to both the parties and it should be private to them only. This technique is categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) [7, 6] at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. So in this case, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher which shows in figure-2. [23, 24, 26]



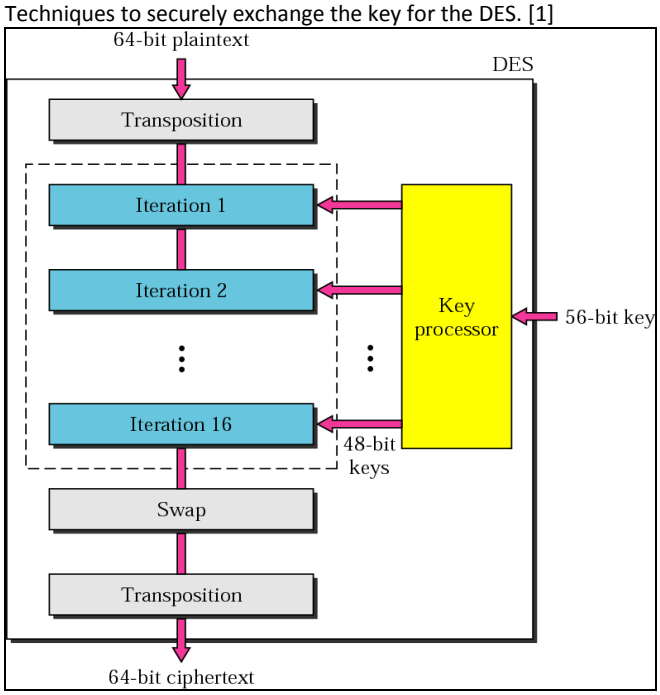

[Fig.2: secret-key, public key, and hash function cryptography][26]

In this cryptographic techniques mainly **DES** algorithm is first choice of the user.

Data Encryption Standard **(DES**) [20]: Data Encryption Standard is a block-cipher employing a 56-bit key that operates on 64-bit blocks. Data Encryption Standard has a complex set of rules and transformations that were designed specifically to yield fast hardware implementations and slow software implementations, although this latter point is becoming less significant today since the speed of computer processors is several orders of magnitude faster today than twenty years ago. IBM had also proposed a 112-bit key for Data Encryption Standard, which was rejected at the time by the government [24, 26]; however, conversion was never seriously considered.

The problem with the Data Encryption Standard is that has not been completely solved is the problem of distributing the secret key to the various end points in the communication. One probable solution is to simply deliver the key manually, which can be expensive and time-consuming too. Another probable solution is which is currently being investigated is to use public-key techniques to securely exchange the key for Data Encryption Standard. [1]

Techniques to securely exchange the key for the DES. [1]




**[Fig. 3:** Data Encryption Standard**]**

**B. PUBLIC KEY CRYPTOGRAPHY:**

PUBLIC KEY CRYPTOGRAPHY depends upon the existence of so-called one-way functions, or mathematical functions that are easy to compute whereas their inverse function is relatively difficult to compute. Let me give you two simple examples:

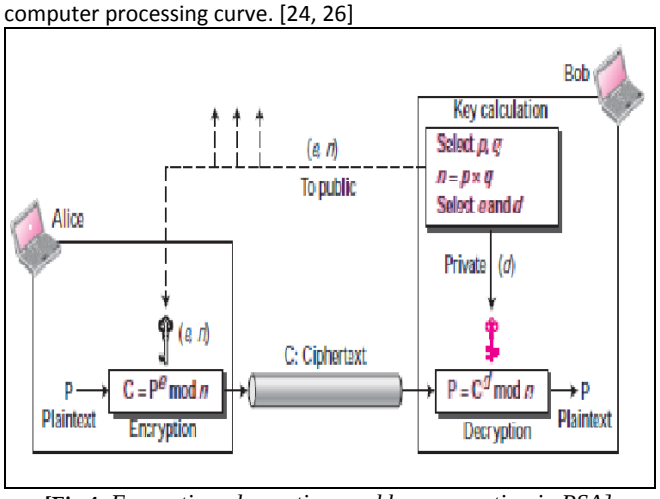
**I.** Multiplication vs. factorization: say for example two prime numbers are there, 3 and 7, and that I want to calculate the product; it should take almost no time to calculate that value, which is 21. Now suppose, instead, that I tell you that I have a number, 21, and I need you tell me which pair of prime numbers I multiplied together to obtain that number. So you will finally come up with the solution but whereas calculating the product took milliseconds, factoring will take longer. The problem becomes much harder if I start with primes that have 400 digits or so, because the product will have ~800 digits.[23,24,26]

**II.** Exponentiation vs. logarithms: say for example I want to take the number 3 to the 6th power; again, it is relatively easy to calculate 36 = 729. But if I tell you that I have the number 729 and want you to tell me the two integers that I used, x and y so that logx 729 = y, it will take you longer to find the two values.[23,26]

Generic PUBLIC KEY CRYPTOGRAPHY [23, 24] employs two keys that are mathematically related although knowledge of one key does not allow someone to easily determine the other key. One key is used to encrypt the plaintext and the other key is used to decrypt the ciphertext. The important point here is that it does not matter which key is applied first, but that both keys are required for the process to work (Figure 1B). Because a pair of keys are required, this approach is also called asymmetric cryptography. [23, 26]

PUBLIC KEY CRYPTOGRAPHY algorithms that are in use today for key exchange or digital signatures include: [24]

**RSA:** RSA can be used for key exchange, digital signatures, or encryption of small blocks of data. In RSA variable size encryption block and a variable size key is used. The key-pair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules [24]; these prime number may be 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors. The public key information includes n and a derivative of one of the factors of n; generally an attacker cannot be able to determine the prime factors of n (private key). That is why the RSA algorithm is secure. The ability for computers to factor large numbers, and therefore attack schemes such as RSA, is fast improving and systems today can find the prime factors of numbers with more than 200 digits. However, if the created large number is two prime factors that are roughly the same size, then there is hardly any factorization algorithm that will solve the problem in a reasonable amount of time; Regardless, one presumed protection of RSA is that users can easily increase the key size to always stay ahead of the computer processing curve. [24, 26]




**[Fig.4:** *Encryption, decryption, and key generation in RSA]*

RSA can be used for key exchange as well as digital signatures and the encryption of small blocks of data. Today, RSA is principally used to encrypt the session key used for secret key encryption (message integrity) or the message's hash value (digital signature). RSA's mathematical toughness comes from the ease in calculating large numbers and the difficulty in finding the prime factors of those large numbers. Although employed with numbers using hundreds of digits, the math behind RSA is relatively straight-forward.

Following are the basic steps to create an RSA public/private key pair:

I. Choose two prime numbers, p and q. From these numbers you can calculate the modulus, n = p q.[23]

II. Select a third number, e, that is relatively prime to (i.e., it does not divide evenly into) the product (p-1) (q-1). The number e is the public exponent.

III. Calculate an integer d from the quotient (ed-1) / [(p-1) (q-1)]. The number d is the private exponent.[23]

The public key is the number pair (n, e). Although these values are publicly known, it is computationally infeasible to determine d from n and e if p and q are large enough.

To encrypt a message, M, with the public key, create the ciphertext, C, using the equation:

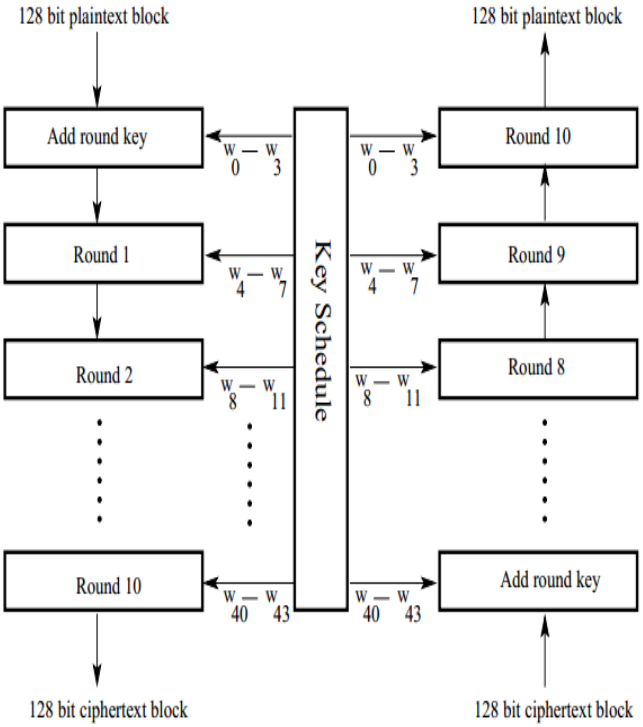
$C = M^e \bmod n$

The receiver then decrypts the ciphertext with the private key using the equation:

$M = C^d \bmod n$

**C. AES:** The Advanced Encryption Standard or AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. [27]

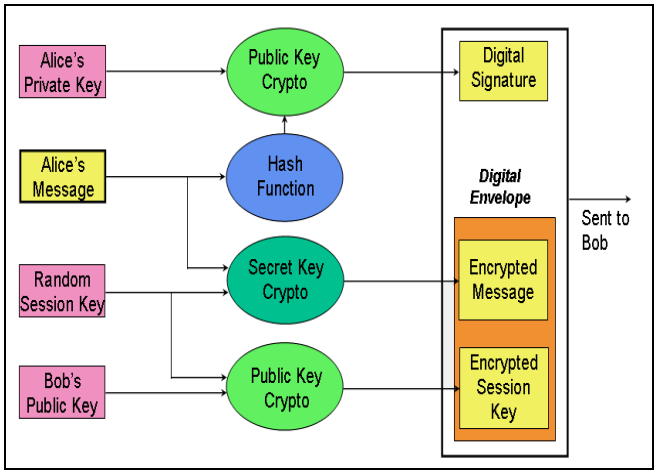
AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. (Rijndael was designed to handle additional block sizes and key lengths, but the functionality was not adopted in AES.) Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of ciphertext. [27]




[Fig.5: AES]

## IV. WHY DO WE NEED DIFFERENT TECHNIQUES?

So based on above study, can't we have only one cryptographic technique?




[Fig.6: Sample application of the three cryptographic techniques for secure communication][26]

SYMMETRIC KEY CRYPTOGRAPHY is preferably suited to encrypting messages so that we can provide privacy and confidentiality to the user. The sender can generate a session key on a per-message basis to encrypt the message; the receiver, of course, needs the same session key to decrypt the message. [23, 26]

Key exchange, of course, is a key application of PUBLIC KEY CRYPTOGRAPHY. Asymmetric schemes can also be used for non-repudiation and user authentication; if the receiver can obtain the session key encrypted with the sender's private key, then only this sender could have sent the message. PUBLIC KEY CRYPTOGRAPHY could, theoretically, also be used to encrypt messages although this is rarely done because secret-key cryptography operates about 1000 times faster than PUBLIC KEY CRYPTOGRAPHY. So each cryptographic technique is having different purpose.

## V. RESEARCH CHALLENGES

Now a days all most each and every application is using data mining techniques and most of the techniques are concerned with privacy. Meaning is that we need to provide privacy so private data will be secured. There are some of the research challenges which are mentioned bellow:

*A.* **Cybercrime, System Threats, and External Threats like hackers**

Cybercrime is the serious issue now days. Most of the banking systems are facing lots of problem regarding this. Banking are losing millions or rupees due to these. Such kinds of crime happens just because of less awareness of internet and security issues.

Sometimes someone may came to know the privacy policy about organization and it may possible that it will reveal some of the secret data to third party which will be the problematic for system itself.

There insider threats as well as outsider threats like hackers. Hackers may hack your password by using your personalize data they may hack your banking or any personal system. Sometimes hackers are simply sending you some fake email of lottery and they are trying to collect some personal information which will be helpful to them for hacking your account.

*B.* **Credit Card Fraud**

One more area where some kinds of security should be apply which is credit card. Generally while using of credit card at any store or shopping Centre they do not ask for any verification as well as any pin no. so if you lose your credit card it is quite easy to use it by any one and anywhere.

*C.* **Medical Health care related issues**

Majority of insurance company and government agencies are asking medical healthcare related data for the particular disease for taking the survey so that they can generate some pattern and make some policies regarding some new insurance after mining .But by the same time they are also getting some personal data which should not happen because such data will be used for hacking the system or it is the matter of privacy of any person.

## VI. PRIVACY PRESERVING DATA MINING BY USING CRYPTOGRAPHIC TECHNIQUE

In most of the cases multiple parties are sharing their private aggregated data without reveling any sensitive data to the third parties so data will not be misuse. Say for example just to know the market trends there some supermarket stores wish to share their data amongst all parties without reveal the data of individual store. One better example is medical healthcare data are asking by different government organization as well as the insurance company for the survey purpose so in this case also personal data should not be revealed.

So Cryptography is a good technique through which we can protect the sensitive data which can be encrypted. This is very good method for preserve the data. There are different methods of cryptography available like horizontal partitioning and vertical partitioning. But this method fails give productive results in the case of more no of parties. So this method is somewhat difficult to apply for a big databases. This is the only major disadvantage.

## VII. COMPARISON BETWEEN CRYPTOGRAHIC TECHNIQUES

| Factors | AES | DES | RSA |
|---|---|---|---|
| Developed in | 2000 | 1977 | 1978 |
| Key Size | 128, 192, 256 bits | 56 bits | >1024 bits |
| Block Size | 128 bits | 64 bits | Minimum 512 bits |
| Scalability | Not Scalable | It is scalable algorithm due to varying the key size and Block size. | Not Scalable |
| Algorithm | Symmetric Algorithm | Symmetric Algorithm | Asymmetric Algorithm |
| Encryption | Faster | Reasonable | Slower |
| Decryption | Faster | Reasonable | Slower |
| Power Consumption | Low | Low | High |
| Security | Excellent Secured | Not Secure Enough | Least Secure |
| Deposit of keys | Needed | Needed | Needed |
| Inherent Vulnerabilities | Brute Forced Attack | Brute Forced, Linear and differential cryptanalysis Attack[20] | Brute Forced and Oracle attack[20] |
| Key Used | Same key used for Encrypt and Decrypt | Same key used for Encrypt and Decrypt | Different key used for Encrypt and Decrypt |
| Rounds | 10/12/14 | 16 | 1 |
| Stimulation Speed | Faster | Faster | Faster |
| Trojan Horse | Not proved | No | No |
| Hardware & Software Implementation | Faster | Better in hardware than in software | Not Efficient |
| Ciphering & Deciphering Algorithm | Different | Different | Same |

[TABLE-1: COMPETITION BETWEEN AES, DES AND RSA TECHNIQUE][20]

## VIII. SOME IMPORTANT OBSERVATION

Based on the literature study we have found following important observations related to AES, DES and RSA algorithm which are given below:

1. DES technique is useful for the long messages to encrypt and decrypt.
2. RSA technique is useful for short messages to encrypt and decrypt.
3. AES and DES are based on symmetric key cryptography where same key is shared by the sender and receiver during implementation.
4. RSA is asymmetric key cryptography where sender and receiver are using separate keys for encryption and decryption.
5. In AES encryption and decryption processes are faster than DES and RSA.
6. RSA is only one round encryption/decryption process whereas in DES and AES multiple rounds are carried out for encryption and decryption process.

## IX. CONCLUSION AND FUTURE WORK

Cryptography has evolved as an important area of research to enhance the information security over communications lines. According to the criticalness of the information, cryptographic algorithms can be used for enhancing our network based applications. In today's world Cryptographic technique is as good as the practice for securing the data as we can encrypt and decrypt both. Hash function will be useful as it is a one way encryption so private data will be secure of the owner. Here we have studied AES, DES and RSA technique and we are going to propose privacy preserving data mining technique by using these

cryptographic techniques individually or may be hybrid approach. We will be recommending use of two cryptographic techniques for privacy preserving in data mining technique.

## X. REFERENCES


[1] Michael Willett, “Cryptography Old and New”, Computers & Security ,1982 – Elsevier

[2] Michael Willett, “A Tutorial on PUBLIC KEY CRYPTOGRAPHY”, Computers & Security, 1982 – Elsevier

[3] Faisal Nabi, "Secure business application logic for e-commerce systems", Computers & Security, 2005-Elsevier

[4] http://en.wikipedia.org/wiki/Cryptography

[5] Behrouz A. Forouzozan, TCP/IP Protocol Suite, Third Edition TMH

[6] Sadaqat Ur Rehman, Muhammad Bilal, Basharat Ahmad, Khawaja Muhammad Yahya, Anees Ullah, Obaid Ur Rehman, "Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN)", IJCSI, January 2012

[7] Michael J. Beller, Li-Fung Chang, Yacov Yacobi,"Privacy and Authentication on a Portable Communications System", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 11, NO. 6, AUGUST 1993 821

[8] WHITFIELD DIFFIE, MARTIN E. HELLMAN,"New Directions in Cryptography", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

[9] HORST FEISTEL, WILLIAM A. NOTZ, J. LYNN SMITH, Some Cryptographic Techniques for Machine-to-Machine Data Communications", PROCEEDINGS OF THE IEEE, VOL. 63, NO. 11, NOVEMBER 1975

[10] Jyotirmayee Rautaray, Raghvendra Kumar, "PRIVACY PRESERVING IN DISTRIBUTED DATABASE USING DATA ENCRYPTION STANDARD (DES)",IJIRSET

[11] N V Muthu lakshmi,Dr. K Sandhya Rani, "Privacy Preserving Association Rule Mining in Horizontally Partitioned Databases Using Cryptography Techniques", IJCSIT, Vol. 3 (1) , 2012, 3176 – 3182

[12] Ashraf El-Sisi, "Fast Cryptographic Privacy Preserving Association Rules Mining on Distributed Homogenous Database", The International Arab Journal of Information Technology, Vol. 7, No. 2, April 2010

[13] Jiawei Han, Micheline Kamber, Jian Pei, Data Mining: Concept and Techniques, Elsevier.

[14] Nishant Doshi, "A novel approach for cryptography technique on Perturbed data for Distributed Environment", IJCIS,Vol.2, No.3, September 2012

[15] N V Muthu lakshmi,Dr. K Sandhya Rani,"Privacy Preserving Association Rule Mining in Horizontally Partitioned Databases Using Cryptography Techniques", IJCSIT, Vol. 3 (1) , 2012, 3176 - 3182

[16] Sivasankar Vakkalagadda, Satyanarayana Mummana, "A Cryptographic Privacy Preserving Approach over Classification", IJETT-Volume4 Issue7- July 2013

[17] R Mani Kumar, S.Rambabu, "A High Performance Privacy Preserving Clustering Approach in Distributed Networks", IJETT– Volume 17 Number 2 – Nov 2014

[18] Ms.S.Nithya, Mrs. P.Senthil Vadivu, "EFFICIENT DECISION TREE BASED PRIVACY PRESERVING APPROACH FOR UNREALIZED DATA SETS", IJACST, Volume 2, No.6, June 2013

[19] Vina M. Lomte, Hemlata B. Deorukhakar, "A Survey of Random Decision Tree Framework Privacy Preserving Data Mining", Volume 3 Issue 11, November 2014

[20] Dr. Prerna Mahajan & Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology, Volume 13 Issue 15 Version 1.0 Year 2013, Online ISSN: 0975-4172 & Print ISSN: 0975-4350

[21] http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard

[22] http://www.saylor.org/site/wp-content/uploads/2012/06/Advanced-Encryption-Standard.pdf

[23] http://www.nmis.isti.cnr.it/casarosa/SIA/readings/SEC_OverviewCryptography.pdf

[24] http://www.garykessler.net/library/crypto.html

[25] http://securitynet.org/network-security-cryptography/

[26] http://people.eecs.ku.edu/~saiedian/teaching/Fa10/710/Readings/An-Overview-Cryptography.pdf

[27] http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard