ABSTRACT

Data are today an asset more critical than ever for all organizations we may think of. Recent advances and trends, such as sensor systems, IoT, cloud computing, and data analytics, are making possible to pervasively, efficiently, and effectively collect data. However for data to be used to their full power, data security and privacy are critical. Even though data security and privacy have been widely investigated over the past thirty years, today we face new difficult data security and privacy challenges. Some of those challenges arise from increasing privacy concerns with respect to the use of data and from the need of reconciling privacy with the use of data for security in applications such as homeland protection, counterterrorism, and health, food and water security. Other challenges arise because the deployments of new data collection and processing devices, such as those used in IoT systems, increase the data attack surface. In this paper, we discuss relevant concepts and approaches for data security and privacy, and identify research challenges that must be addressed by comprehensive solutions to data security and privacy.

TABLE OF CONTENTS

1. Introduction

Cryptography is an effective way for protecting sensitive information .it is a method for storing and transmitting data in form that only those it is intended for read and process. The evolution of encryption is moving towards a future of endless possibilities. Stenography is the art of passing information through original files. It is arrived from Greek word meaning “covered writing”. Stenography refers to information or file that has been concealed inside a picture, video or audio file.

Concepts used in Cryptography

a. Plain Text: The original message that the person want to communicate is defined as plain text. For an example, Alice is a person wishes to send “Hey, How are you” message to person Bob, “Hi friend how are u “is referred as plain text.

b. Cipher Text: The message which cannot be understood by anyone is defined as cipher text for an example “ib%ipvbufzpv@ “is a cipher text produced for plain text “Hi, How are you“.

c. Encryption: Converting plain text to cipher text is referred as encryption. It requires two processes. Encryption algorithm and a key. It is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm–a cipher–generating cipher text that can be read-only if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

d. Decryption: Converting cipher text to plain text is referred as decryption. This may also need two requirements Decryption algorithm and key. Figure 1 shows the simple flow of commonly used encryption algorithms.

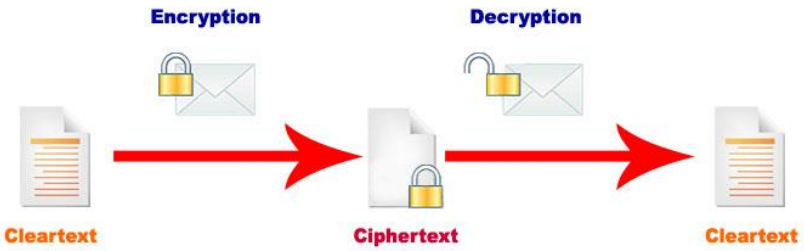
e. Key: Combination of numeric or alpha numeric text or special symbol is referred as key .it may use at time of encryption or decryption .key plays a vital role in cryptography because encryption algorithm directly depends on it. Keys are stored in encrypted form. OpenPGP stores the keys in two files on your hard disk; one for public keys and one for private keys. These files are called *keyrings.* As you use OpenPGP, you will typically add the public keys of your recipients to your public keyring. Your private keys are stored on your private keyring.

Symmetric key

In symmetric key schemes. the encryption and decryption keys are the same. Communicating parties must have the same key in order to achieve secure communication. An example of a symmetric key is the German military's Engima Machine There were key settings for each day.

Public key

In public encryption process schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key that enables messages to be read Public-key encryption was first described in a secret document in 1973 before then all encryption schemes were symmetric-key (also called private-key)



2. Feasibility Study

Cryptography allows people to keep confidence in the electronic world. ... The rapid increase of information transmitted electronically resulted to an increased reliance on **cryptography** and authentication. The simplest example of **cryptography** is transformation of information to prevent other from observing its meaning.

In the present era, not only business but almost all the aspects of human life are driven by information. Hence, it has become imperative to protect useful information from malicious activities such as attacks. Let us consider the types of attacks to which information is typically subjected to. Data security normally covers two things: first, protecting your data from being completely or partially lost. This can happen due to a natural disaster (for example, your hard disk crashes, or a company office is burnt or destroyed in an earthquake). It can also happen due to a person's actions, through malice or accident - somebody deletes a file you are working on, or a file gets corrupted, or some employee who has been fired deletes all customer records on their way out the door.

The second thing data security covers is the prevention of data being copied or stolen without authority. For example, someone gets hold of your credit card or social security details … or one country steals the specifications for a stealth fighter from another country.

As you can see, data security applies at the personal level … and to small companies … and to large ones … and to entire nations.

There are various ways in which data security can be put in place; too many or too technical to describe here, but briefly speaking: back up data, encrypt (i.e. code) the data, prevent physical access to the computers it is held in, use firewalls or other software, hardware based security, data masking, data erasure, etc.

Targeted data breaches are growing by 27%. Securing customers', employees', clients', stakeholders' data from cyber threats, risks, breaches, and vulnerabilities should be the top priority for every well-informed leadership. Ignoring data security leads to operational disruptions, compromise of confidential information, loss of reputation, and damaging lawsuits.

Less than 40% of organizations claim to be appropriately prepared for dealing with coordinated cyber-threats. There are still a large number of companies looking for security professionals who can effectively manage their multi-dimensional security challenges.

Job opportunities in data/information security are likely to grow by 37% from 2012 to 2022. The median annual salary for an information security analyst is $98,350. You get to choose from a variety of job roles ranging from Information Security Analyst, Computer Forensics Analyst, Penetration Tester, and IT Security Consultant to Security Systems Administrator and Chief Information Security Officer.

Organizations, across industries, should also regularly train their IT/security professionals and get them certified.

3. Innovations in Project

In today's digitized and connected world, businesses and private citizens as well as politics and society see themselves confronted every day with challenges resulting from security vulnerabilities and threats via IT attacks. The industry is in an arms race with attackers trying to break cryptographic keys, protocols, and implementations. As a result, systems that are using cryptography have to be continuously improved and updated to withstand new attacks. Widespread cryptographic processes are continuously facing erosion: The increase in computing power of potential attackers is forcing us to adjust and strengthen security parameters permanently (e.g., the length of cryptographic keys), and to retire and replace outdated algorithms and protocols. In extreme cases individual cryptographic algorithms may be broken overnight. This ongoing race will be significantly impacted by the development of quantum computers. In comparison to classical computers, quantum computers shorten the time required for attacks on cryptographic algorithms substantially. So far, quantum computers have been primarily the subject of academic research, and the first commercial prototypes do not yet present an imminent threat to today's cryptography.

However, China and other countries are massively investing in the development of quantum computers so that it is only a matter of time until a sufficiently powerful quantum computer will dramatically change today's cryptography. With the help of quantum

computers, attackers will be able to render not only individual services and products insecure – they will be able to completely break cryptographic algorithms like RSA, DSA, DH, and ECC. Therefore, encrypted data and digital signatures protected by these algorithms will become vulnerable immediately. The consequences of this will affect individuals and companies as well as economy and society in general. Today, we encrypt data as it travels over the internet and when it is at rest on a storage device. But we have to decrypt data to use or analyse it, creating a potential security vulnerability. Homomorphic encryption is a new idea that solves that problem, allowing users to process data without decrypting it. With homomorphic encryption, we process encrypted data and produce encrypted results. The biggest problem we face with data security is not whether or not data is encrypted, it's that we use the same code as the attackers. The next big idea in security is moving target defence. The idea is simple: constantly change the attack surface so the attackers can't spend time reverse attacking.

4. DESIGN AND ALGORITHMS OF DATA SECURITY

4.1 DESIGN OF AES ALGORITHMS

It is important to know that the secret key can be of any size and in our proposed AES algorithm; key size of 320 bits is used instead of three different key sizes such as 128, 192 and 256 bits. From the research it has been found that the AES parameters depend on its key size. In proposed algorithm the number of rounds has been increased to 16 as it uses the 10 rounds for 128 bit key size. The security of the system is increased by increasing the number of rounds and results in providing privacy to the unauthorized users. The proposed table has been drawn with the increase in number of rounds which helps in providing the more security to the system and better performance. With the increase in number of rounds it will be difficult for the hackers to hack the system. It is believed that no simplification in

transformation will allow breaking the AES algorithm. Therefore, key size of 320 bits has been chosen in order to provide the better results. 4.1. Modified AES encryption process It has been shown in Fig. 4.1. It can be defined as the conversion of Plaintextto the Ciphertext. InAES encryption process instead of 10 rounds we have increase the number of rounds to 16. The initial key has been generated from the Polybius square. The encryption process undergoes the Sub bytes, ShiftRows, MixColumns and AddRound Key operations in AES which have been shown below.

4.2 Modified AES decryption process

Decryption is the process of converting cipher text into Plain text. Corresponding to the transformations in the encryption, Decryption process undergoes InvSubBytes, InvShiftRows, InvMixColumns, and AddRoundKey are the transformations used in the decryption as shown in Fig. 4.2.

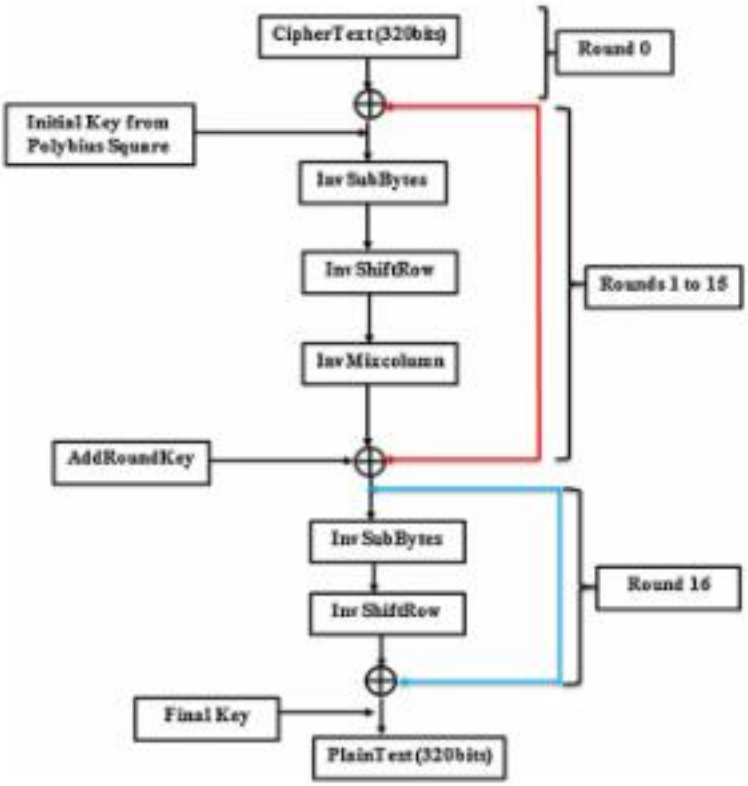


Fig. 4.2. AES decryption process

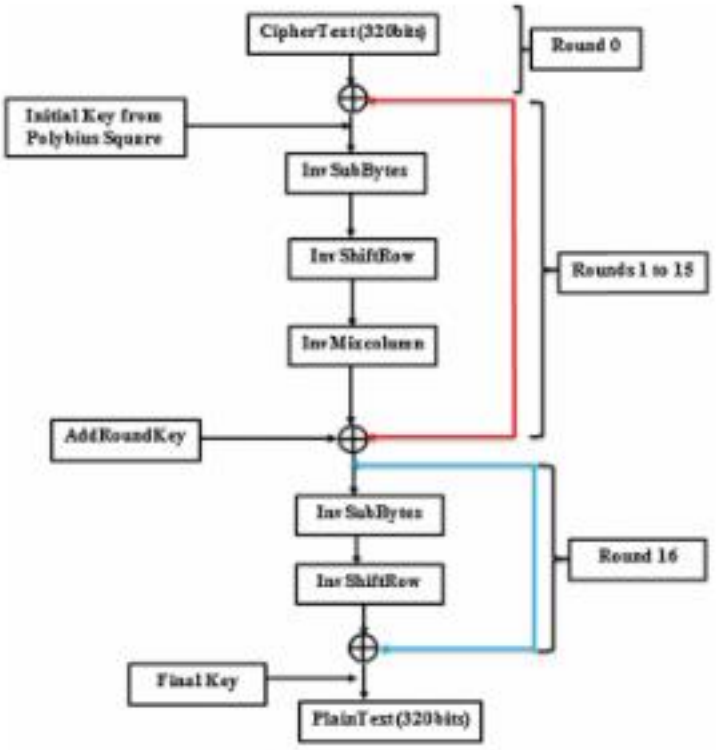
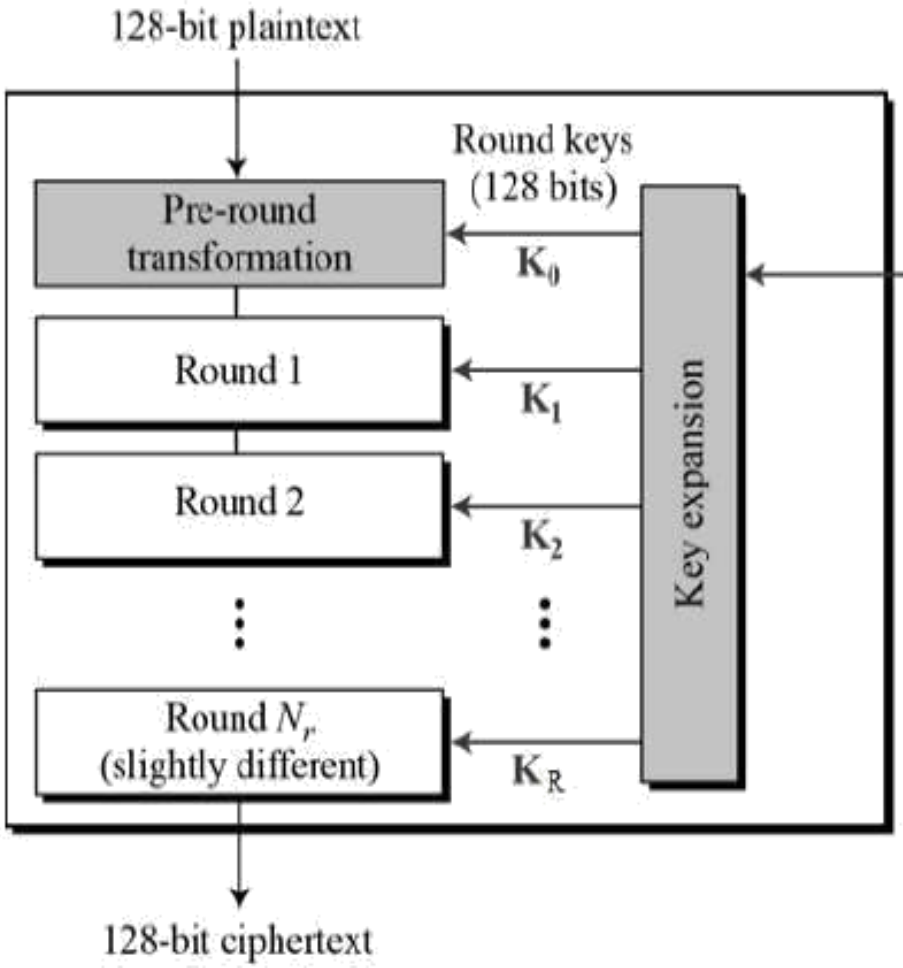


Fig. 4.2. AES decryption process



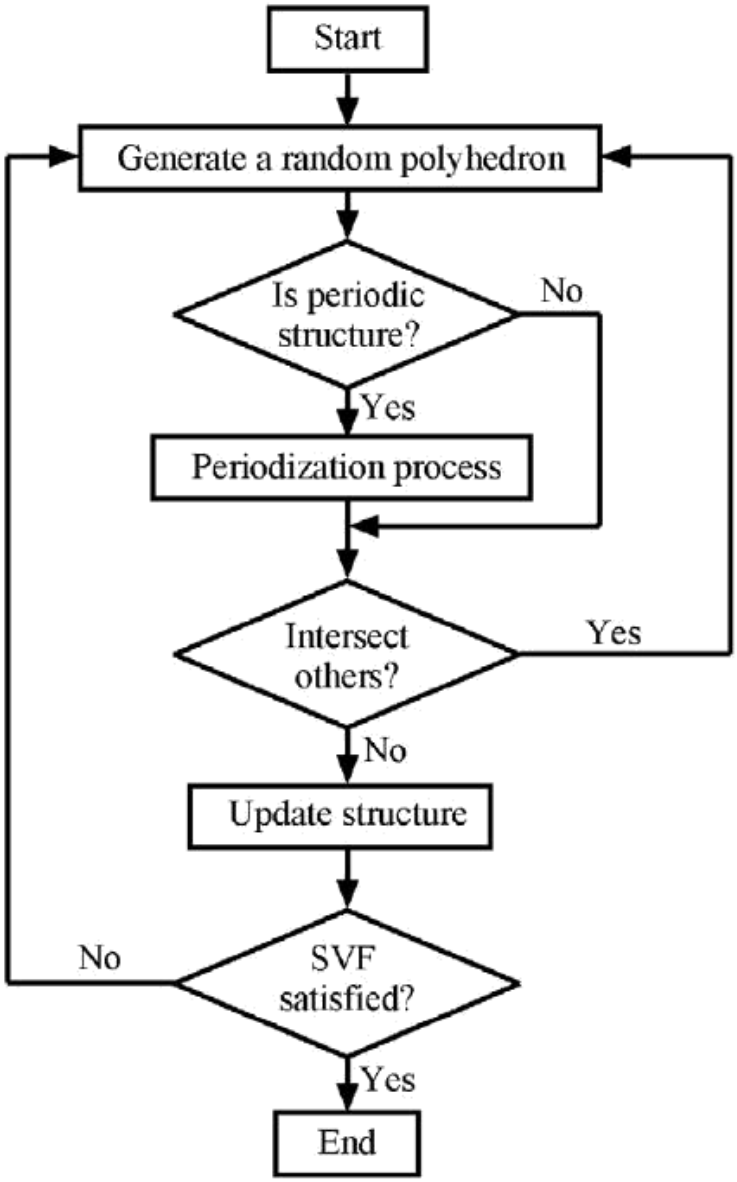
Cipher key
(128, 192, or 256 bits)

R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

4.3 DESIGN FOR RSA ALGORITHMS

Several algorithms in common employ public-key cryptography, probably the best known being the algorithm named after its inventors, Ronald Rivest, Adi Shamir and Leonard Adleman. Its principle is, if user A need to send information to user B, he can take the user B's encryption key (public key) firstly. Then encrypt plaintext into cipher text through the encryption function and transfer it to user B. If user B receives this cipher text from user A, he will decrypt cipher text with decrypting function through their decryption key (private key). Figure 1 shows the scenario to be followed in RSA Algorithms

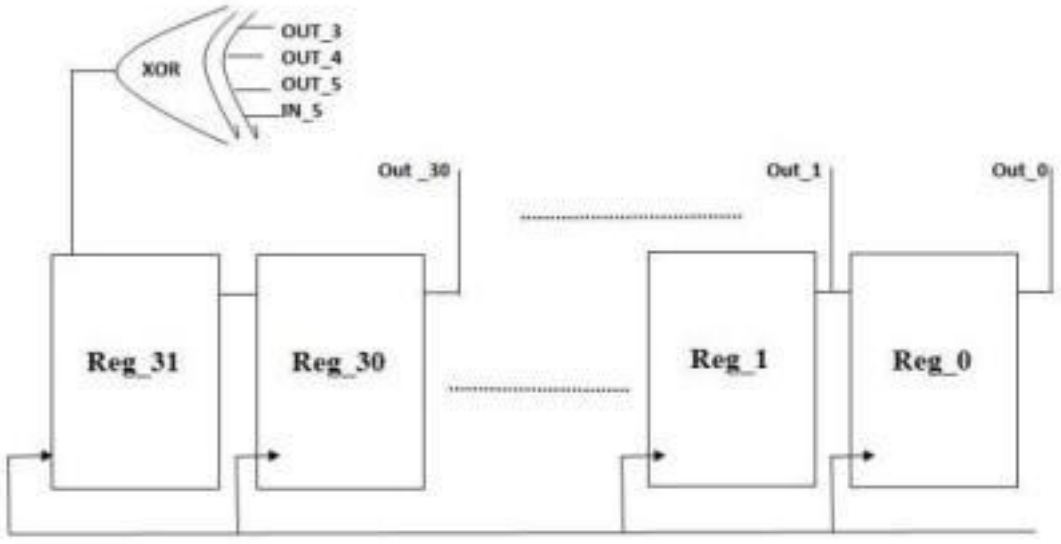

Start
Generate a random polyhedron
Is periodic structure?
No
Yes
Periodization process
Intersect others?
Yes
No
Update structure
SVF satisfied?
No
Yes
End

5. IMPLEMENTATIONS FOR RSA ALGORITHMS

The implementation process of RSA Algorithm contains following stages

A. PSEUDO RANDOM GENERATOR

To implement the RSA cryptosystem it is need to generate two random numbers. For generating the random numbers Linear Feedback Shift Register (LFSR) is used. Linear Feedback Shift Register is one of the most promising techniques used to generate pseudo random numbers. It generates a periodic sequence so that the numbers generated by the LFSR will be repeated only after certain interval. Linear feedback shift register can generate a (2n-1)-bit long random sequence without repeating. It can produce a sequence of over 4 billion random bits. In this paper the RSA algorithm contains 32 -bit LFSR. This LFSR consists of 32 registers and one XOR gate. It performs a XOR operation between the certain inputs and feedback the output to 32nd register. The random numbers that are generated from LFSR are stored in FIFO and it stops working when it's full. The numbers from the FIFO are given as input to the primality tester and check for the number to prime. If the number is found to be prime number then it is saved or else the number is discarded. This process is repeated until two prime numbers are obtained.



Pseudo random number generator

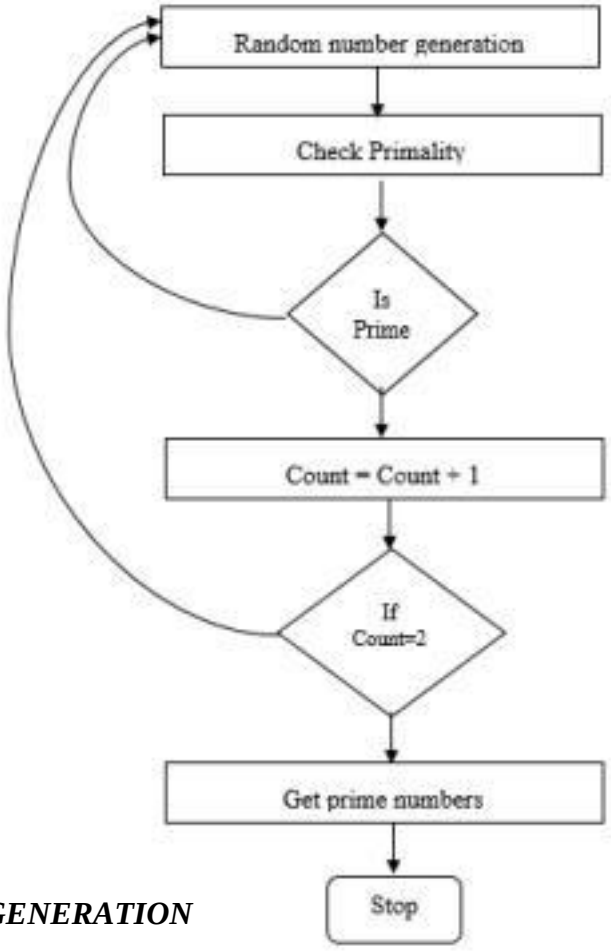
B. PRIMALITY TEST

The pseudo random numbers which are generated by the LFSR may contain both composite and prime

numbers. But algorithm need only prime numbers to implement the RSA cryptosystem. The basic purpose of the primality test is to find whether the random number generated by the

LFSR is prime number or not. The Miller-Rabin probabilistic primality test is one of the fast methods to determine the prime number. This process is stopped as soon as two prime numbers are obtained. The flow chart for the primality test is shown in figure 2 below

Figure 2:



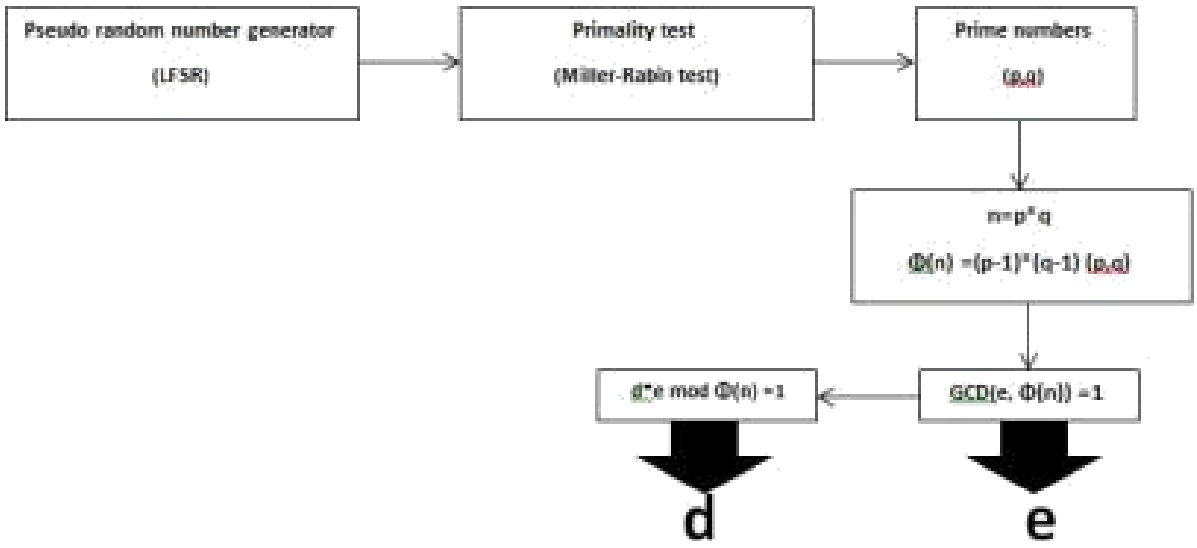
C. KEY GENERATION

In RSA algorithm two separate keys are generated namely encryption key ’e’ and decryption key’d’. At first,

two prime numbers (p, q) are taken from the primality tester. By applying some mathematical operations on these two prime numbers the values of n and Φ(n) are calculated , where n=p*q and Φ(n) = (p-1)*(q-1). Now select the value for ‘e’ such that it is relatively prime to Φ(n) i.e. GCD of (e, Φ(n)) =1,and the value of ‘e’ should be less than Φ(n), thus it is required to calculate the value decryption key ‘d’ which satisfies the following equation 1

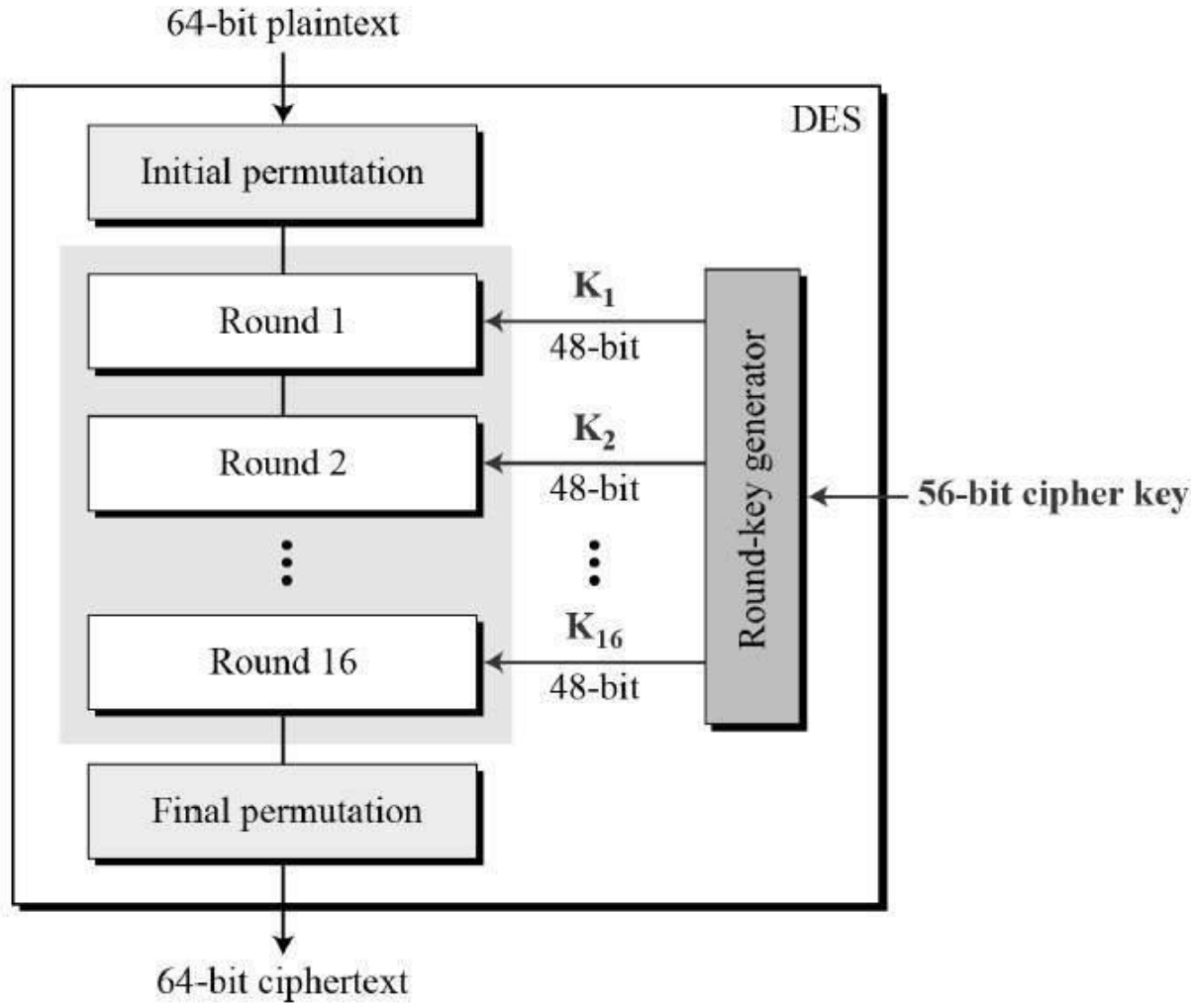
$$d*e \bmod \Phi(n) = 1 \quad (1)$$

The following block diagram gives the scenario of the key generation of the RSA Cryptosystem.



6. DES ALGORITHMS

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).



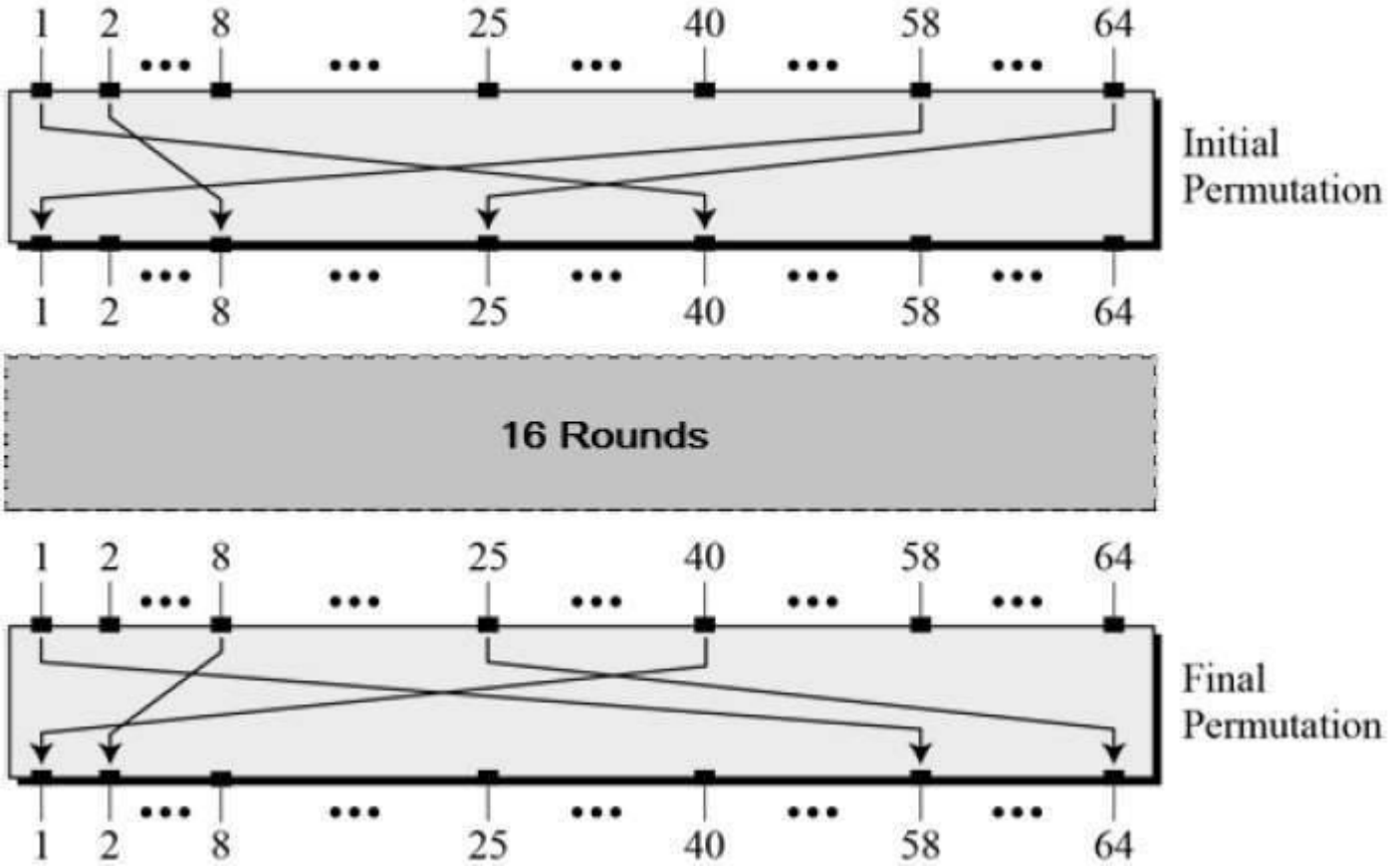
epicted in the following illustration −

Since DES is based on the Feistel Cipher, all that is required to specify DES is −

- Round function
- Key schedule
- Any additional processing − Initial and final permutation

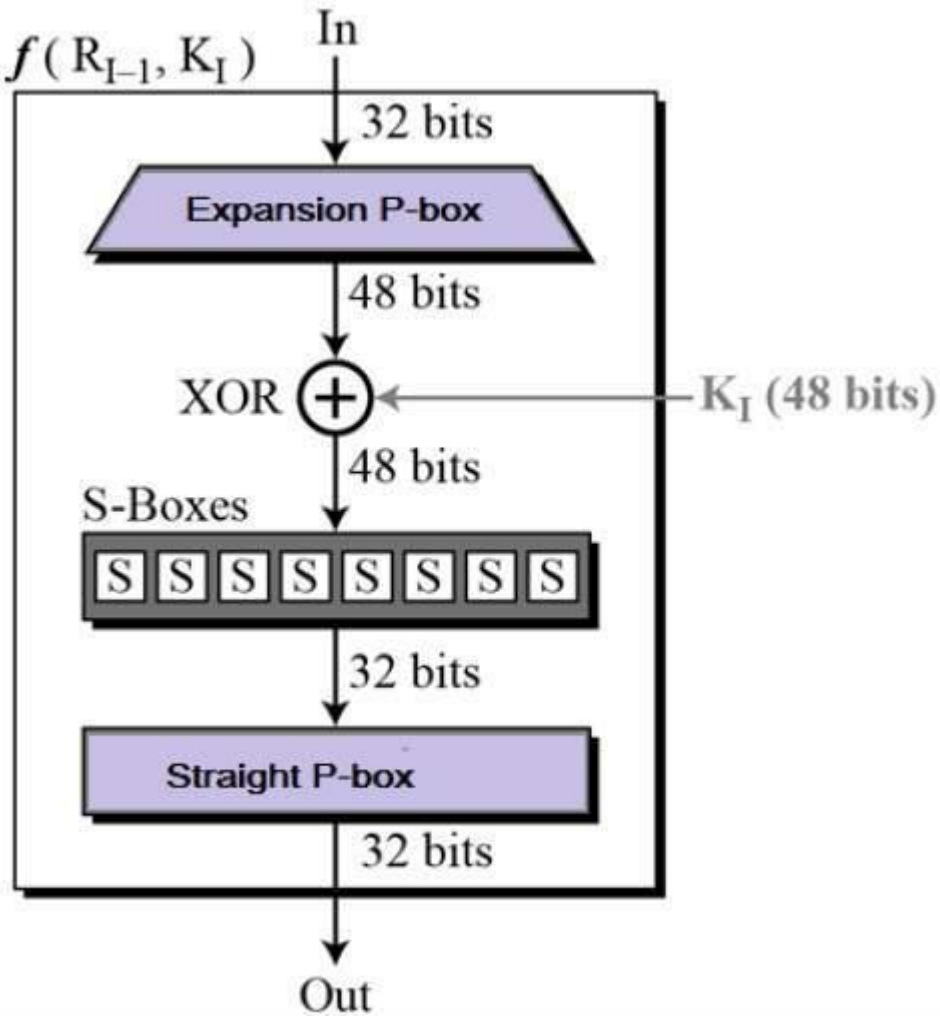
Initial and Final Permutation

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES. The initial and final permutations are shown as follows −



Round Function

The heart of this cipher is the DES function, *f*. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



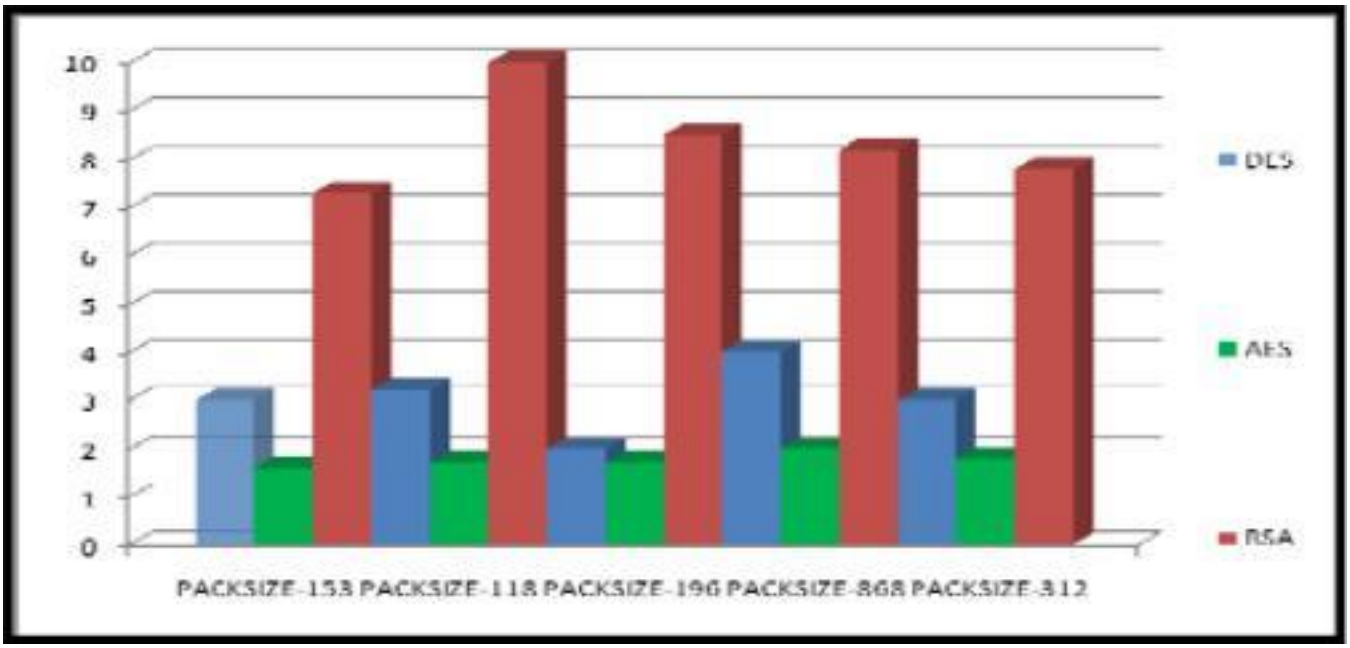
- **Expansion Permutation Box** − Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically depicted in the following illustration −

7. Output Validation and Comparison

Comparative Analysis of AES, DES and RSA

S.NO	Factors Analysed	DES	AES	RSA
1.	Developed	1977	2000	1978
2.	Key Length Value	138, 192, 256 bits	56 bit	>1024 bits
3.	Type of Algorithm	Symmetric	Symmetric	Asymmetric
4.	Encryption Ratio	Low	High	High
5.	Security attacks	Inadequate	Highly secured	Timing attack
6.	Stimulation Speed	Fast	Fast	Fast
7.	Scalability	Scalable algorithm	No Scalability occurs	No Scalability occurs
8.	Key Used	Same key used for Encrypt and Decrypt Process	Different Key used for Encrypt and Decrypt Process	Different Key used for Encrypt and Decrypt Process
9.	Power Consumption	Low	Low	High
10.	Hardware and Software implementation	Better in hardware than in software.	Faster and efficient	Not very efficient

Comparative status of Decryption Time among DES, AES and RSA



8.Applications of Encryption Algorithms

1. Authentication/Digital Signatures
2. Time Stamping
3. Electronic Money
4. Encryption/Decryption in Email
5. Sim Card Authentication
6. Encryption in Social apps like WhatsApp, Instagram and Facebook

9.Future scopes of Encryption Algorithms

The future of Encryption algorithms lies in having more secure than these all algorithm mentioned above. In 2010, a new encryption known as Homomorphic Encryption was discovered and was known for its better performance than all mentioned above.

9.1 Homomorphic Encryption

Homomorphic encryption makes it possible to analyse or manipulate encrypted data without revealing the data to anyone. Something as simple as looking for a coffee

shop when you're out of town reveals huge volumes of data with third parties as they help you satiate your caffeine craving—the fact that you're seeking a coffee shop, where you are when you're searching, what time it is and more. If homomorphic encryption were applied in this fictional coffee search, none of this information would be visible to any of third parties or service providers such as Google. In addition, they wouldn't be able to see what answer you were given regarding where the coffee shop is and how to get there.

11. Conclusion

In Data communication, encryption algorithm plays an important role. These encryption techniques are studied and analysed well to promote the performance of the encryption methods also to ensure the security. It was concluded that AES algorithm consumes least encryption and decryption time and buffer usage compared to DES algorithm. But RSA consume more encryption time and buffer usage is also very high. We also observed that decryption of AES algorithm is better than other algorithms. From the simulation result, we evaluated that AES algorithm is much better than DES and RSA algorithm.

12. Bibliography

1. Cryptography and Network Security" Seventh Edition by William Stallings.
2. Cryptography Theory & Practice by Douglas Stinson
3. Bruce Schneier's Applied Cryptography
4. Peter Fleischer, Jane Horvath, Shuman Ghosemajumder *(2008).*
5. www.scholar.google.in
6. E.Thamiraja ,G.Ramesh,R.Uma rani "A Survey on Various Most Common Encryption Techniques" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 ISSN: 2277 128X
7. Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani "New Comparative Study Between DES, 3DES and AES within Nine Factors" Journal Of Computing, Volume 2, Issue 3, March2010,Issn2151-9617
8. Aman Kumar , Dr. Sudesh Jakhar , Mr. Sunil Makkar "comparative analysis between DES and RSA algorithm" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 ISSN: 2277 128X
9. Diaasalama, Abdul kader, MohiyHadhoud, "Studying the Effect of Most Common Encryption Algorithms", International Arab Journal of e-technology, vol 2, no.1, January 2011.
10. Diaa Salama Abd Elminaam1, Hatem Mohamed Abdual Kader2, and Mohiy Mohamed Hadhoud2," Evaluating the Performance of Symmetric Encryption Algorithm ", International Journal of Network Security, Vol.10, No.3, PP.213 {219, May 2010.
11. Humane Agawam & Manish Sharma" Implementation and analysis of various Cryptography" Dec-2010
12. Gurjeevan Singh, Aswan Kumar Single, K. S. Sandha, "Through Put Analysis of Various Encryption Algorithms", IJCST Vol.2, Issue3, September 2011
13. Paar, Cristof et al. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. Springer.p. 30ISBN 9783642041006 http://books.google.com/books?id=f24wFELSzkoC&pg =PA30
14. RSA Cryptography Specifications http://www.rsa.com http://www.ietf.org
15. Performance Evaluation Of Symmetric Algorithms Published In Volume 3, No. 8, August 2012 Journal Of Global Research In Computer Science
16. Performance Evaluation of Symmetric Encryption Algorithms D. S. Abdul. Elminaam, M. Abdul Kader, M. M. Hadhoud published in Communications of the IBIMA Volume 8, 2009 ISSN: 1943-7765
17. www.di-mgt.com.au/rsa_ *alg.html* developed by Davidireland
18. Alexandre Berzati ,Jean-Guillaume Dumas , Louis Goubin discussed "Fault attacks in RSA public key "Published in: · Proceeding CT-RSA '09 Proceedings of the Cryptographers' Track at the RSA Conference 2009 on Topics in Cryptologyages 414 - 428

19. “Secure Data Hiding Algorithm Using Encrypted Secret message “ by Harshitha K M, Dr. P. A. Vijaya published in International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012 1 ISSN 2250-3153
20.