

Cloud Cryptography Algorithms

Megha Gupta^{1,*}, Ayush Jain²

Abstract

Nowadays the information is being produced increasingly more by means of the enterprises and is being elevated swiftly that want will be saved and used e.g., e-mails, facts, photograph album, tax document, financial transaction, and so on. Now statistics owners are required to store their nearby facts organization on the cloud for its elasticity with financial savings. This not simplest gives flexibility to users but additionally makes our content material on hand to us whenever and anywhere we want them. In cloud computing, the information of customers could be saved in storage furnished with the aid of cloud carrier companies (CSP's). Cloud carrier companies must be having an ideal process to defend user's information, specifically the data from revelation to customers who are not authorized. If we backup our documents to the cloud, then we may be sure that our information will in no way be misplaced. This paper proposes an algorithm which might encrypt the files uploaded on cloud garage services and would decrypt the documents when they have been downloaded the use of the keys that were generated on the time of encryption. This might help in preventing undesirable intrusion into private information documents and might at ease user's information.

Keywords: Cloud, Symmetric & Asymmetric Key, Cryptography, Encryption, Decryption.

INTRODUCTION

Cloud computing is the most essential part in the cloud world. Its advantages are nowadays typically carried out in the IT fields. Cloud computing is a secured technology for difficult structures with large scale offerings allocating amongst a couple of customers. Hence, authorization of each customer and offerings is a splendid difficulty for the consider and secured of the cloud computing precise platform has delivered latest security problems to examine. Cloud computing is firstly the arrangement of programs, information and facts as a provider. These services are furnished over the internet or community, frequently on a pay-in step with-use primarily based version. Cloud computing provides a useful process of gaining access to cloud services, with no dependency on of the hardware you're using or your physical location. It comforts the want to keep records for your computer, mobile gadgets or gadgets and the idea that the facts will be as soon as possible and easily accessible through internet. Cloud computing gives users with a digital setup which permits them to shop information as well as run software. Cloud computing provides new protection demanding situations as patron

*Author for Correspondence

Megha Gupta

Associate Professor Department of Computer Science,
Poornima Institute of Engineering and Technology, Jaipur,
Rajasthan, India

Student, Department of Computer Science, Poornima Institute
of Engineering and Technology, Jaipur, Rajasthan, India

Received Date: April 01, 2022

Accepted Date: April 22, 2022

Published Date: May 21, 2022

Citation: Megha Gupta, Ayush Jain. Cloud Cryptography Algorithms. Research & Reviews: Journal of Computational Biology. 2022; 11(1): 13–21p.

cannot consider carriers. Cloud computing cryptography relies upon a safe and secured computing structure. Cloud computing is a computing model that is achieved by means of economies of scale and is distributed on big scale. Cloud architectures are developed in step with contemporary and urgent needs of the consumer [1].

CLOUD SERVICES

Software as a Service (SaaS)

Software as a Service (SaaS), represent the largest cloud market which could be very helpful and is still growing right away. SaaS uses the

internet to offer applications which can be controlled by using a 3rd-celebration companies or providers and whose inter face is accessed at the consumer's or consumer's facet. With SaaS, it's clean for organizations and corporation sonically arrange the maintenance and guide.

Due to the fact the entirety can be controlled with the aid of providers or service vendors like applications, information, middleware, virtualization, servers, garage, and networking [1]. SaaS offering types include e-mail and collaboration like GitHub, client dating control, and healthcare-associated packages. Some huge businesses that are not traditionally idea of as software providers or providers have began building SaaS as an extra source of sales which will benefit an aggressive advantage of extra customers and customers. SaaS saves time of person because in SaaS, person does no longer need to download and installation any packages.

Platform as a Service (PaaS)

In the PaaS models, cloud providers supply a "computing platform", which incorporates running machine, programming language execution surroundings for examples like java, python, C++, and so on., internet server and database. Platform as a Service (PaaS) gives a few applications like Microsoft Azure, the underlying laptop and storage assets scale robotically to healthy application demand so that the person does not have to take care of source manually and the whole lot is achieved automatically. The latter has also been proposed with the aid of a structure aiming to facilitate real-time operations in cloud environments. The purchaser does no longer involve in coping with or controlling the underlying cloud infrastructure inclusive of network, servers, operating structures, or storage [2].

Infrastructure as a Service (IaaS)

Cloud carrier, referred to as IaaS, is carrier models for getting access to, supervise, and dealing with far flung information center infrastructures, inclusive of, storage, networking, and networking offerings. Instead of purchasing hardware from elsewhere for permanent use, customers should purchase IaaS based on consumption, similar to strength or different software billing and pay in line with use. Compared to Software as a Service and Platform as a Service, IaaS users are responsible for coping with packages, information, runtime, middleware, and OSes. Cloud Service Provider (CSP) nevertheless manages virtualization, servers, difficult drives, garage, and networking [3].

SECURITY IN CLOUDCOMPUTING

For protection cause there are potentially additional challenges to make cloud computing environments as cozy as in-house IT systems. At the equal time, current, properly understood technology may be attached, such as information encryption, VLANs, and firewalls. Security and privateness we can say impact the whole cloud computing stack, when you consider that there's a sizeable use of 0.33-birthday celebration offerings and infrastructures which can be used to host crucial facts or to perform evaluative operations. In this situation, the accept as true with in the direction of carriers is fundamental to make certain the desired degree of privacy and safety for applications hosted within the cloud. Legal and regulatory troubles also want a few attentions. When records and information of user are moved into the Cloud, companies may additionally choose to situate the many where on the earth. The bodily location of data facilities determines these to flaws that can be carried out strictly to the control off acts. One trouble is that precise cryptography techniques couldn't be used because they may be no longer allowed in a few countries. Similarly, U.S. Laws can impose those sensitive statistics, consisting of affected person health information, are to be stored inside national borders so that there could be not any trouble [4].

CRYPTO CLOUD COMPUTING

Cryptography inside the cloud uses encryption strategies to comfy data to be able to be stored and used inside the cloud. It lets in customers to effectively and securely get admission to shared offerings, as any data this is hosted by means of cloud providers is protected with the process of encryption. Cryptography within the cloud secures touchy and useful data without postponing statistics alternate. Most cloud computing infrastructures do no longer provide safety in opposition to

doubtful cloud operators, which poses an undertaking for groups and groups that want to save touchy, private and personal data which include medical facts, economic information, or high-effect commercial enterprise information this is very critical. Companies and agencies want to take a records-centric approach to protect their sensitive statistics with the intention to defend towards superior threats within the complex and evolving environments of virtualization, cloud offerings, and mobility [5].

IMPORTANCE OF CRYPTO CLOUDCOMPUTING

The following are some blessings of encryption inside the cloud surroundings. The encryption allows to

- A. Ensure the privateness of the corporation records, wherein in encrypted information is in the transmission, in use and at storage vicinity as properly.
- B. Achieve Secure Multi-Tenancy within the Cloud. Encrypting records in the cloud and preserving encryption key by means of which data proprietor can keep away from the cloud service issuer to get admission to the information.
- C. Provide a Safe Harbor from Breach Notification, if an information breach happens and, in my opinion, identifiable records is misplaced, the breached birthday party must notify all individuals who are impacted.
- D. Provide Confidence of records back ups are secure in cloud environment from the breached celebration.
- E. Expand sales potential to clients with touchy or regulated records via preserving the important thing through cloud records owner and offers cloud provider vendors a competitive part [6].

CRYPTOGRAPHY & ITS TECHNIQUES/ALGORITHMS

Cryptography is the method of converting regular undeniable textual content of the message into unintelligible textual content which cannot be understood by any attacker and also reverse process. It is a process of storing and sending and receiving the facts in a particular shape so that simplest the ones for whom it's far supposed can read and procedure it for use. Cryptography now not most effective protects information from theft or modification however also can be used for consumer authentication in order that handiest authorized character can get entry to the facts Figure 1.

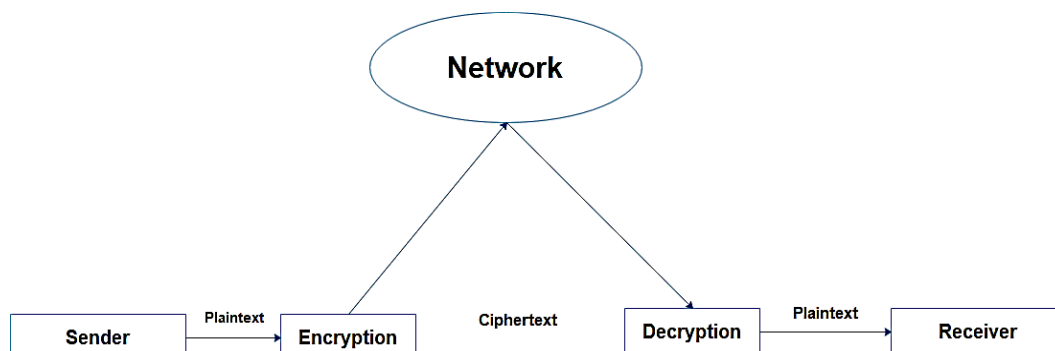


Figure 1. Network Communication Model.

Modern Cryptography Issues with:

- **Confidentiality**-Information cannot be understood through everybody
- **Integrity**-Information can't be altered.
- **Non-repudiation**-is the warranty that the person who is sending cannot deny the validity of something.
- **Authentication**-Sender and receiver can verify every different and may make sure that legal sender and receiver are collaborating inside the transmission.
- **Cryptography** is used in lots of applications like laptop passwords, banking transactions cards like debit/credit playing cards, and e-trade transactions on online buying sites.

- **Encryption** is the method of changing a everyday message additionally called plaintext right into a meaningless message referred to as Ciphertext.
- **Decryption** is the process of converting a ciphertext message into its previous form or original text.

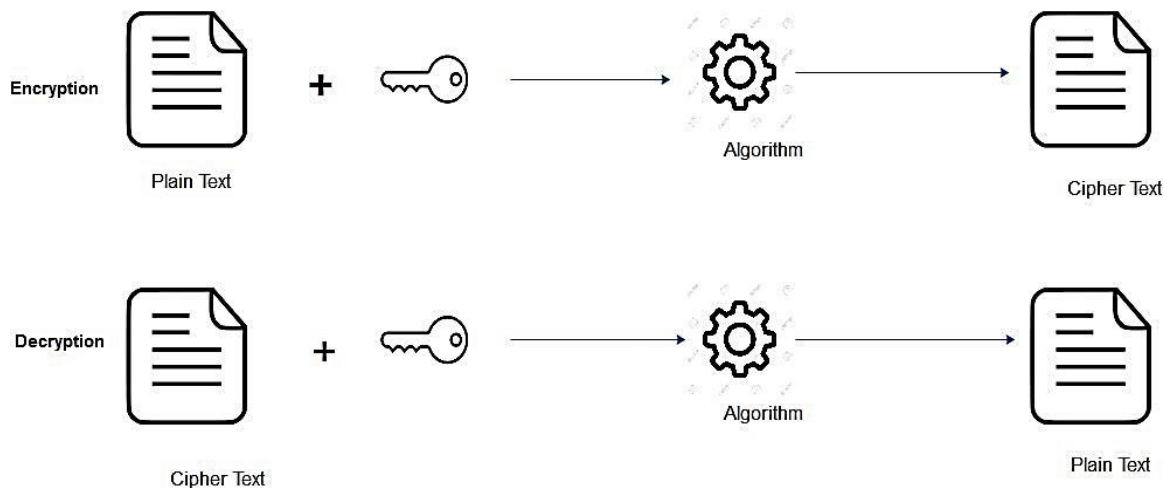


Figure 2. Encryption to Decryption.

The encryption algorithms play critical role and act as important device for defensive statistics and secured community communicate. The encryption algorithms convert the information into jumbled shape by using the “key” and the decryption may be performed via the person simplest the usage of the same key Figure 2.

The following are the various algorithms available in cryptography: [Table 1]

1. Data Encryption Standard (DES)
2. 3DES–TripleDES
3. SDES–simplified DES
4. Rivest Cipher5
5. Rivest cipher6
6. Blowfish
7. Advanced Encryption Standard (AES)

Table 1. Comparison of Different Algorithms

Algorithm	RC4	Blowfish	AES	DES	Triple DES
Key size(s)	40–1024	128–448	128, 192, 256	56	112/168, but equivalent security of 80/112
Speed	Very fast	Fast	Fast	Slow	Very slow
Speed depends on key size	No	No	Yes	Yes	No
Security/comments	Of questionable secure for moderate number of encrypted sessions of moderate length. RC4 has the redeeming feature of being fast. However, it has	Believed secure, but with less attempted cryptanalysis than other algorithms. Attempts to cryptanalyse Blowfish soon after publication are promising (Schneier, 19952 & 19963). But unlike AES, it doesn't appear to have received much attention recently in	Secure, though with some reservations from the crypto community. It has the advantage of allowing a 256-bit key size, which should protect against certain future attacks (collision attacks and	Insecure: A \$10,000 Copacobana machine can find a DES key in an average of a week, as (probably) could a botnet with thousands	Insecure: A \$10,000 Copacobana machine can find a DES key in an average of a week, as (probably) could a botnet

Algorithm	RC4	Blowfish	AES	DES	Triple DES
	various weaknesses in the random number sequence that it uses: see Klein (2008)1.	the cryptographic literature. Blowfish has been superseded by Twofish, but the latter is not supported as standard in Java (at least, not in Sun's JDK).	potential quantum computing algorithms that would have 264 complexity with a 128-bit key and could become viable in the lifetime of your data	of machines. The simple answer is: "Don't use it-it's not safe". (RFC 4772).	with thousands of machines. The simple answer is: "Don't use it-it's not safe". (RFC 4772)

Data Encryption Standard

DES is an old symmetric-key approach of data encrypting. DES makes use of the same key to encryption process and decrypt process a message; hence, the sender and the receive reach ought to have as well as provide the equal private key. DES has been changed by using more secure (AES) algorithm Figure 3.

3DES–Triple DES

Which is being carried out to every block 3 times. The actual cipher's key size become fifty-six-bits whilst the DES set of rules was designed at the beginning. In widespread, this become good enough as well, however the computational power availability made the brute-pressure attacks possible by being elevated. This problem changed into overcome through Triple DES, which furnished a moderate-n-smooth approach in which the important thing length is being increased to protect such attacks. In addition, this overrides the necessity of designing a very new block cipher algorithm.

SDES-Simplified DES

The result would be an 8(eight)-bit block of ciphertext which has been encrypted. The decryption algorithm uses an enter of eight-bit block of ciphertext produced through the encryption set of rules in the encryption technique and the equal10-bit key used in cipher text production, in which the output might be the original eight-bit block of plaintext (original text).

RC5 (Rivest Cipher 5)

Is asymmetric-key block cipher distinguished by way of its simplicity. Ronald Rivest designed this for the duration of 1994. In RC5 both the encryption and decryption extend the random key into 2 (r+1) phrases with a view to be utilized in sequence. These could be used simplest as soon as every all through the encryption and decryption tactics. RC5 can be the usage of a not static block length of thirty-two/sixty-four/one twenty-eight bits, a key size of 0-2040 bits and the wide variety of rounds might be zero-255, in which the parameters proposed in authentic had been 64 bits of the block length [7].

Rivest Cipher 6

Ron Rivest designed this, which is a symmetric key block cipher. This turned into designed to attain the necessity of AES opposition & derived from RC5. It has 128-bits of block length and helps 128, 192 and 256 bits of key sizes as much as 2040-bits. But it may be parameterized like RC5 to help a wide form of phrase-lengths, key sizes, and the wide variety of rounds. This and RC5 are similar in shape.

Blowfish

It makes use of a sixty-four-bit block period and anon static length of key, between thirty-two bits to four fourth eight bits. The encryption includes16 round Feistel cipher, the use of big key-dependent S-containers. It is recommended that you shouldn't use Blowfish to encrypt documents large than four GB because of its small 64-bit block length as compared to different algorithms.

AES

AES is a substitute of DES and depended on as the same old by using the numerous organizations. Low RAM desires and excessive speed were the main motive it became decided on to cover pinnacle-

secret records. The algorithm can work properly on an extensive variety of hardware, from 8-bit clever playing cards to excessive-overall performance processors.

Though AES is extraordinarily green in 128-bit shape, it also uses keys of 192 and 256 bits for heavy safety. It uses ten rounds for 128-bit keys, twelve rounds for 192-bit keys, and fourteen rounds for 256-bit keys that is one of the reasons why AES is higher than DES. The identical secrets used for each encryption and decryption of facts, so each the sender and the receiver have to have the same keys.

To date, no sensible assaults towards AES have been located. It is used in many one-of-a-kind protocols and transmission technologies, consisting of WPA2 safety of Wi-Fi community, Voice-over-IP technology, and signaling statistics [8].

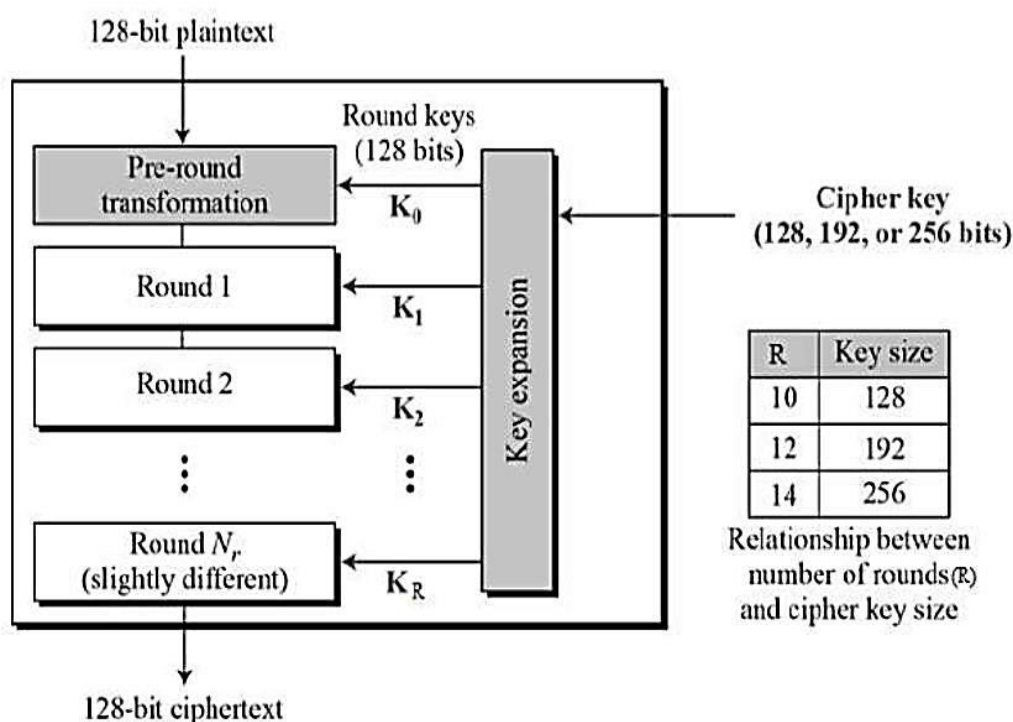


Figure 3. Plain text to cipher text.

Steps in AES Encryption Process

Byte Substitution

The sixteen enter bytes are replaced via using a set table S-box (substitution-container) available in layout. The end result is in the shape of a multi-dimensional array of four rows and four columns [Figure 4].

Shift Rows

All the 4-row soft the multi-dimensional array a removed to the left. Any input that ‘fails’ are again inserted at the proper side of the rows [Figure 5]. Shift process is as follows-

Mix Columns

All columns of 4bytes are converted using a unique mathematics characteristic internally. This internally running feature takes the input the 4 bytes of a column and provides outputs 4 absolutely new bytes, which update the previous preceding column. The result is another new matrix (rows and columns) including sixteen new bytes. It ought to be stated that the step isn't always executed in final round [9] [Figure 6].

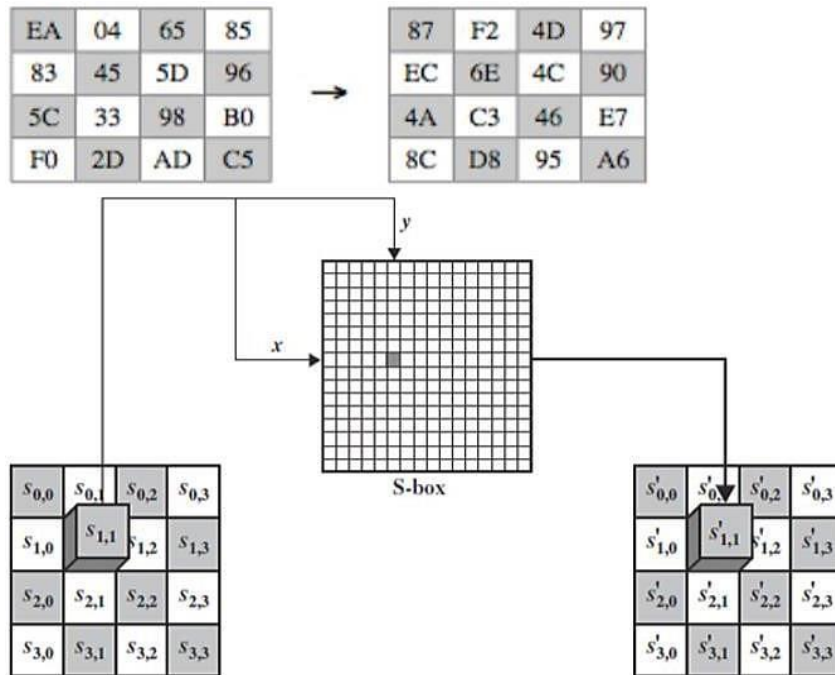


Figure 4. Byte substitution.

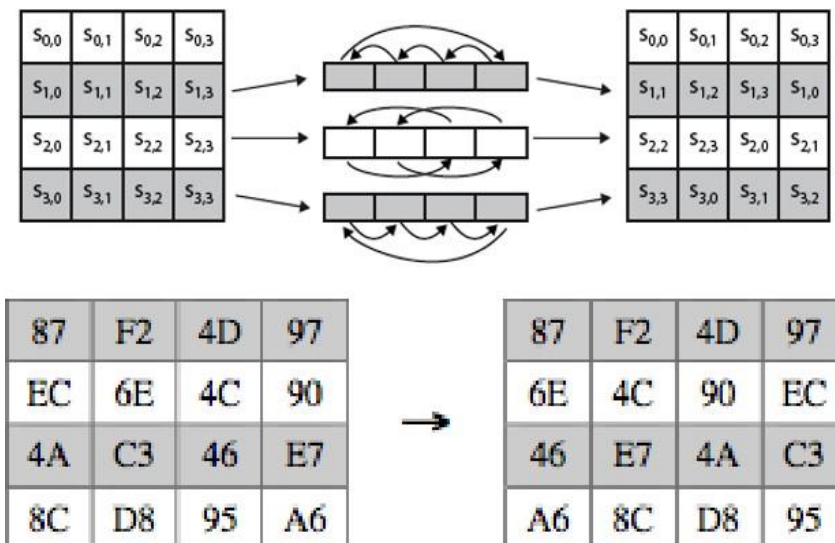


Figure 5. Shift Rows.

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

16 byte State

b1	b5	b9	b13
b2	b6	b10	b14
b3	b7	b11	b15
b4	b8	b12	b16

Figure 6. Mix Columns.

Add Round Key

The sixteen bytes of the multi-dimensional array are actually regarded as 128 bits and are performed XORed to the 128 bits of the spherical key. If that is the final round, then the result might be the ciphertext. Else, the output 128 bits are translated as sixteen bytes and we begin some other same round as preceding rounds.

Steps in AES Decryption Process

The procedure of decryption of an AES is the reverse process of the AES encryption process [10] [Figure 7].

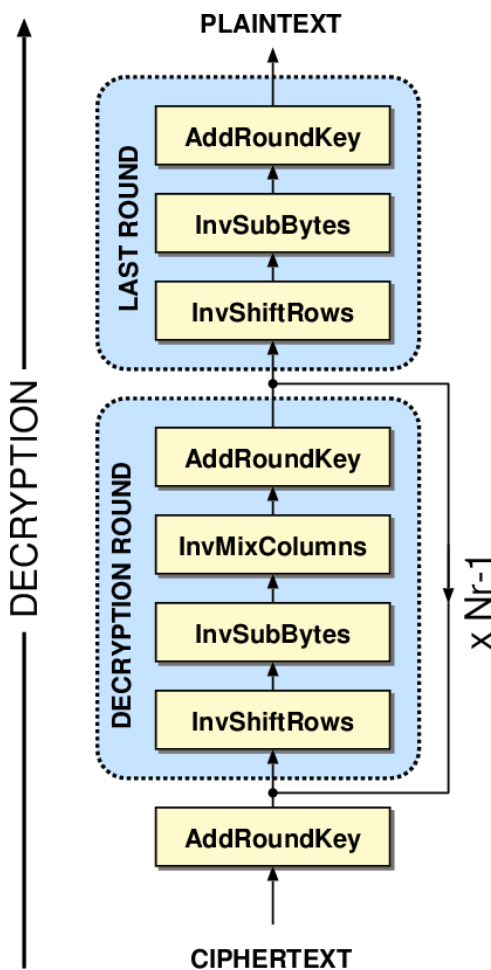


Figure 7. AES Decryption Process.

Drawbacks of AES

Following are some drawbacks of AES:

1. It uses too uncomplicated algebraic architecture.
2. Similar way is used to encrypt every block in the encryption process.
3. Difficult process while implementing with software [10].

Future Scope

The ability of the AES encryption set of rules can be superior by increment the key length from 128 bits to 512 bits and in order that the wide variety of rounds can be elevated as a way to offer a more secured encryption feature for secure verbal exchange. Moreover, look at of optimization tactics for the implementation for helping numerous key lengths and modes of operations have giant future scope for the paintings.

CONCLUSION

With internet as well as community are incrementing right away. Daily quite a few virtual records are being exchanged among many clients. Some records are touchy that is to shield from attackers. Encryption algorithms play crucial roles to cozy unique records from unauthorized get entry to. Many kinds of algorithms are existed to encrypt data. More secured fashionable (AES) algorithm is the green algorithms and it's far broadly used and accompanied on all components of systems. This algorithm permits mutoscope with specific key sizes together with 128,192, and 256 bits with 128 bits block cipher. In this paper, explains some of essential capabilities of the AES set of rules and offers a few past research on cryptographic algorithms which have completed on it to evaluate the overall performance of AES to encrypt statistics under specific parameters and conditions. According to the effects received from research that have been done indicates that AES has the capability to provide anew full greater security compared to other algorithms.

Acknowledgement

I would like to thank and express my gratitude and appreciation to all those who helped me to complete this research paper. A special thanks to my guide, Dr. Megha Gupta whose help, stimulating suggestions and encouragement, helped me in writing this research paper. At last, I am thankful to my family & friends whose encouragement and continuous inspiration helped me to complete this paperwork.

REFERENCES

1. National Institute of Standards and Technology, Computer Security Resource Center 2016, available <http://csrc.nist.gov/groups/SNS/cloud-computing>
2. Srinivas, J., K. Venkata Subba Reddy, and A. Moiz Qyser. "Cloud computing basics." International journal of advanced research in computer and communication engineering 1.5 (2012): 343–347.
3. A Vouk, Mladen. "Cloud computing—issues, research and implementations." Journal of computing and information technology 16.4 (2008): 235–246.
4. Alharthi, Abdulrahman, et al. "An overview of cloud services adoption challenges in higher education institutions." Proceedings of the 2nd International Workshop on Emerging Software as a Service and Analytics. Vol. 1. SCITEPRESS-Science and Technology Publications, 2015.
5. Rivest, R.L., Adleman, L. and Dertouzos, M.L., 1978. On data banks and privacy homomorphisms. Foundations of secure computation, 4 (11), pp. 169–180.
6. Rivest, Ronald L., Len Adleman, and Michael L. Dertouzos. "On data banks and privacy homomorphisms." Foundations of secure computation 4.11 (1978): 169–180.
7. Kelly, James Mark. "Cloud Computing and Cryptography."
8. Kamara, Seny, and Kristin Lauter. "Cryptographic cloud storage." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2010.
9. Aw Ideler, Hugo. "Cryptography as a service in a cloud computing environment." EINDHOVEN UNIVERSITY OF TECHNOLOGY, Department of Mathematics and Computing Science (2012).
10. Zhang, Shuai, et al. "Cloud computing research and development trend." 2010 Second international conference on future networks. IEEE, 2010.