# A Comprehensive Survey on Symmetric key Encryption

Vaibhav P. Sawalkar, Niraj N. Kasliwal, Megha Singh
Dept. of CSEAssistant Professor & H.O.D., Dept. of CSE Assistant Professor & H.O.D., Dept. of CSE
MGICOET, Shegaon MGICOET, ShegaonCIIT, Indore
*vpsawalkar10@gmail.com, kasliwaln@gmail.com, megha_0801@yahoo.co.in*

***Abstract*** **–**Now a day's Cryptography is one in every of the broad areas for researchers; attributable to the conventional block cipher has lost its efficiency because of the sophistication of contemporary systems that may break it by brute force. Because of its importance, many cryptography techniques and algorithms area unit adopted by several authors to secure the info, however still there's a scope to boost the previous approaches. For this necessity, we offer the great survey which can facilitate the researchers to provide higher techniques. Using this survey we are mainly focusing on the symmetric key encryption and its different types for implementations.

***Keywords:*** *Cryptography, Symmetric Key Encryption Data Security, DES, AES, IDEA.*

*****

## I. INTRODUCTION

In the environment of distributed security, at this point once the web providesessential communication between tens of millions of individuals and is being progressively used as a tool for commerce, security becomes a tremendously necessary issue to traumatize. There are many aspects to security several and lots of and plenty of applications, ranging from secure commerce and payments to personal communications and protective passwords one essential side for secure communications is that of Cryptography. The conception of securing messages through cryptography contains a long history. Indeed, statesman is attributable with making one of the earliest crypto logical systems to send military messages to his generals. Cryptography is that the science of exploitation arithmetic to code and rewrite data. Cryptography permits you to store sensitive information or transmit it across insecure networks (like the Internet) in order that it can't be scan by anyone except the meant recipient. Whereas cryptography is that the science of securing knowledge, cryptanalytics is that the science of analysing and breaking secure communication. Classical cryptanalytics involves a remarkable combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are known as attackers. Cryptanalytics embraces each cryptography and cryptanalysis. The safety of encrypted knowledge is entirely obsessed on 2 things: the strength of the crypto logical formula and also the secrecy of the key. A crypto logical formula, plus all possible keys and every one the protocols that create it work comprise a cryptosystem. [1].

## II. WHY CRYPTOGRAPHY IS IMPORTANT

### *A. Benefits of Cryptography*

Cryptography is an essential information security tool. It provides the four most basic services of information security which are as follows:

- Confidentiality
- Authentication
- Data Integrity
- Non-repudiation

All these fundamental services offered by cryptography have enabled the conduct of business over the networks using the computer systems in extremely efficient and effective manner.

### *B. Drawbacks of Cryptography*

Apart from the four fundamental elements of information security, there are other issues that affect the effective use of information −

- A strongly encrypted, authentic, and digitally signed information can be difficult to access even for a legitimate user at a crucial time of decision-making. The network or the computer system can be attacked and rendered non-functional by an intruder.

- **High availability,** one of the fundamental aspects of information security, cannot be ensured through the use of cryptography. Other methods are needed to guard against the threats such as denial of service or complete breakdown of information system.

- Another fundamental need of information security of **selective access control** also cannot be realized through the use of cryptography. Administrative controls and procedures are required to be exercised for the same.

- Cryptography does not guard against the vulnerabilities and threats that emerge from the poor design of systems, protocols, and procedures. These need to be fixed through proper design and setting up of a defensive infrastructure.

- Cryptography comes at cost. The cost is in terms of time and money −

- Addition of cryptographic techniques in the information processing leads to delay.
- The use of public key cryptography requires setting up and maintenance of public key infrastructure requiring the handsome financial budget.

- The security of cryptographic technique is based on the computational difficulty of mathematical problems. Any breakthrough in solving such mathematical problems or increasing the computing power can render a cryptographic technique vulnerable.[2]

### C. *Types of Cryptographic Algorithms*

There are many ways in which of classifying crypto logical algorithms. For functions of this paper, we are going to be classified supported the quantity of keys that are utilized for secret writing and secret writing, and additional outlined by their application and use. The 3 kinds of algorithms which will be mentioned below are:

- Secret Key Cryptography (SKC): Uses one key for each secret writing and secret writing
- Public Key Cryptography (PKC): Uses one key for secret writing and another for secret writing
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information or data. [10].

## III. SYMMETRIC KEY ENCRYPTION:

With secret key cryptography, one secret's used for each encoding and cryptography. In this sender uses the key (or some set of rules) to encipher the plain text and sends the cipher text to the receiver. The receiver applies a similar key (or rule set) to rewrite the message and recover the plain text. As a result of one secret's used for each functions, secret key cryptography is additionally referred to as symmetric key cryptography.

Secret key cryptography schemes area unit typically categorized as being either stream ciphers or block ciphers. Stream ciphers operate one bit (byte or laptop word) at a time and implement some sort of feedback mechanism so the key's perpetually ever-changing. A block cipher is questionable as a result of the theme encrypts one block of knowledge at time victimization an equivalent key on every block. In general, an equivalent plain text block can invariably code to an equivalent cipher text once victimization an equivalent key during a block cipher whereas an equivalent plain text can code to completely different cipher text during a stream cipher.

Stream ciphers are available many flavours however 2 area unit price mentioning here. Self-synchronizing stream ciphers calculate every bit within the key stream as an operate of the previous n bits within the key stream. it's termed "self-synchronizing" as a result of the cryptography method will keep synchronized with the secret writing method simply by knowing however way into the n-bit key stream it's. One drawback is error propagation; an unconnected bit in transmission can lead to n unconnected bits at the receiving aspect. Synchronous stream ciphers generate the key stream during a fashion freelance of the message stream however by victimization an equivalent key stream generation operate at sender and receiver. Whereas stream ciphers don't propagate transmission errors, they are, by their nature, periodic so the key stream can eventually repeat.

Block ciphers will operate in one amongst many modes; the subsequent four area unit the foremost important:

1) Electronic Codebook (ECB).
2) Cipher Block Chaining (CBC).
3) Cipher Feedback (CFB).
4) Output Feedback (OFB).

Symmetric key cryptography includes the following algorithms.[9]

## IV. THE DES ALGORITHM

### A. *About DES*

The Data cryptography normal (DES) is Associate in Nursing superannuated symmetric-key technique of information cryptography. DES works by victimisation a similar key to write in code and decipher a message, thus each the sender and also the receiver should understand and use a similar personal key. Once the go-to, symmetric-key formula for the cryptography of electronic knowledge, DES has been outdated by the safer advanced cryptography normal (AES) formula. DES works by victimisation a similar key to write in code and decipher a message, thus each the sender and also the receiver should understand and use a similar personal key. Once the go-to, symmetric-key formula for the cryptography of electronic knowledge, DES has been outdated by the safer advanced cryptography normal (AES) formula. Originally designed by researchers at IBM within the early Seventies, DES was adopted by the U.S. government as a politician Federal information science normal (FIPS) in 1977 for the cryptography of economic and sensitive nevertheless unclassified government laptop knowledge. It absolutely was the primary cryptography formula approved by the U.S. government for public speech act. This ensured that DES was quickly adopted by industries like money services, wherever the requirement for robust cryptography is high. The simplicity of DES additionally saw it employed in a good style of embedded systems, good cards, SIM cards and network devices requiring cryptography like modems, set-top boxes and routers.

### B. *Des Key Length and Brute-Force Attacks*

The Data cryptography normal could be a block cipher that means a science key and formula are applied to a block of information at the same time instead of one bit at a time. To

write in code a plaintext message, DES teams it into 64-bit blocks. Every block is enciphered victimisation the key into a 64-bit ciphertext by suggests that of permutation and substitution. The method involves sixteen rounds and might run in four totally different modes, encrypting blocks singly or creating every cipher block obsessed on all the previous blocks. Secret writing is just the inverse of cryptography, following similar steps however reversing the order within which the keys are applied. For any cipher, the foremost basic technique of attack is brute force that involves attempting every key till you discover the proper one. The length of the key determines the amount of doable keys -- and thus the feasibleness -- of this sort of attack. DES uses a 64-bit key, however eight of these bits are used for parity checks, effectively limiting the key to 56-bits. Hence, it might take a most of 2^56, or 72,057,594,037,927,936, try to seek out the right key. Even though few messages encrypted victimisation DES cryptography are seemingly to be subjected to the present quite code-breaking effort, several security consultants felt the 56-bit key length was inadequate even before DES was adopted as a typical. (There have continually been suspicions that interference from the National Security Agency weakened IBM's original algorithm). Even so, DES remained a trustworthy and wide used cryptography formula through the mid-1990s. However, in 1998, a laptop engineered by the Electronic Frontier Foundation (EFF) decrypted a DES-encoded message in fifty six hours. By harnessing the facility of thousands of networked computers, the subsequent year copulate cut the secret writing time to twenty two hours. Apart from providing backwards compatibility in some instances, reliance these days upon DES for knowledge confidentiality could be a serious security style error in any system and may be avoided. There are far more secure algorithms offered, like AES. Very like an inexpensive traveling bag lock, DES can keep the contents safe from honest individuals; however it will not stop a determined felon.

### *C. Successors to DES*

Encryption strength is directly tied to key size, and 56-bit key lengths became too tiny relative to the process power of contemporary computers.. So in 1997, the National Institute of Standards Associate in Nursing Technology (NIST) proclaimed an initiative to decide on a successor to DES; in 2001, it hand-picked the advanced cryptography normal as a replacement the information cryptography normal (FIPS 46-3) was formally withdrawn in might 2005, tho' Triple DES (3DES) is approved through 2030 for sensitive government info. 3DES performs 3 iterations of the DES algorithm; if keying choice darling is chosen, a special secret's used anytime to extend the key length to 168 bits. However, as a result of the chance of a meet-in-the-middle attack, the effective security it provides is just 112 bits. 3DES cryptography is clearly slower than plain DES

### *D. 4.4 Legacy of DES*

Despite having reached the top of its helpful life, the arrival of the information cryptography normal served to market the study of cryptography and also the development of latest cryptography algorithms. Until DES, cryptography was a dark art confined to the realms of military and government intelligence organizations. The open nature of DES meant lecturers, mathematicians and anyone fascinated by security might study however the formula worked and check out to crack it. Like any common and difficult puzzle, a craze or during this case, an entire trade was born. [4]

## V. THE IDEA ALGORITHM

### *A. About IDEA*

IDEA is Associate in nursing encryption formula developed at ETH in city, Svizzera. It uses a block cipher with a 128-bit key, and is usually thought-about to be terribly secure. it's thought-about among the simplest in public notable algorithms. Within the many years that it's been in use, no sensible attacks on that are revealed despite of variety of tries to seek out some.

The Data coding commonplace (DES) formula has been a preferred secret key coding formula and is employed in several industrial and money applications. Although introduced in 1976, it's proven proof against all types of cryptography. However, its key size is just too tiny by current standards and its entire fifty six bit key house is searched in just about twenty two hours .International encryption formula (IDEA) may be a block cipher designed by Xuejia Lai and James L. Massey of ETH-Zürich and was 1st delineate in 1991. It's a minor revision of Associate in nursing earlier cipher, PES (Proposed coding Standard); plan was originally known as IPES (Improved PES). Plan was used because the interchangeable cipher in early versions of the gorgeous smart Privacy cryptosystem.

IDEA was to develop a powerful coding formula, which might replace the DES procedure developed within the U.S.A. within the seventies. It's conjointly attention-grabbing in this it entirely avoids the employment of any operation tables or S-boxes. Once the illustrious PGP email and file coding product was designed by Phil Zimmermann, the developers were craving for most security. Plan was their 1st alternative for encryption supported its tested style and its nice name.

### *B. The IDEA Coding Formula*

1. It provides high level security not supported keeping the formula a secret, however rather upon cognitive content of the key
2. It is totally such and simply understood
3. It is accessible to everyone
4. It is appropriate to be used in a very wide selection of applications
5. It can be economically enforced in electronic parts (VLSI Chip)
6. It can be used with efficiency
7. It may be exported world wide
8. It is patent protected to forestall fraud and piracy.

### *C. Description of plan*

The block cipher plan operates with 64-bit plaintext and cipher text blocks and is controlled by a 128-bit key. The basic innovation within the style of this formula is that the use

of operations from 3 completely different pure mathematics teams. The substitution boxes and therefore the associated table lookups employed in the block ciphers accessible to-date are utterly avoided. The formula structure has been chosen such, with the exception that completely different key sub-blocks area unit used, the coding method is similar to the secret writing method.

### 1. *Key Generation*

The 64-bit plaintext block is partitioned off into four 16-bit sub-blocks, since all the pure mathematics operations employed in the coding method operate 16-bit numbers. Another method produces for every of the coding rounds, six 16-bit key sub-blocks from the 128-bit key. Since an additional four 16-bit key-sub-blocks area unit needed for the next output transformation, a complete of fifty two (= eight x half dozen + 4) completely different 16-bit sub-blocks have to be compelled to be generated from the 128-bit key. The key sub-blocks used for the coding and therefore the secret writing within the individual rounds area unit shown in Table one. The fifty two 16-bit key sub-blocks that area unit generated from the 128-bit key area unit made as follows: First, the 128-bit secret's partitioned off into eight 16-bit sub-blocks that area unit then directly used because the 1st eight key sub-blocks. The 128-bit secret's then cyclically shifted to the left by twenty five positions, once that the ensuing 128-bit block is once more partitioned off into eight 16-bit sub-blocks to be directly used because the next eight key sub-blocks. The cyclic shift procedure delineate higher than is continual till all of the specified fifty two 16-bit key sub-blocks are generated.

### 2. *Encryption*

The practical illustration of the coding method is shown in Figure one. The method consists of eight identical coding steps (known as coding rounds) followed by Associate in Nursing output transformation. The structure of the primary spherical is shown very well. In the primary coding spherical, the primary four 16-bit key sub-blocks area unit combined with 2 of the 16-bit plaintext blocks exploitation addition modulo 216, and with the opposite 2 plaintext blocks exploitation multiplication modulo 216 + one. The results area unit then processed additional as shown in Figure one, whereby 2 a lot of 16-bit key sub-blocks enter the calculation and therefore the third pure mathematics cluster operator, the in small stages exclusive OR, is used. At the tip of the primary coding spherical four 16-bit values area unit made that area unit used as input to the second coding spherical in a very part modified order. The method delineate higher than for spherical one is continual in every of the next seven coding rounds exploitation completely different 16-bit key sub-blocks for every combination. throughout the next output transformation, the four one6-bit values made at the tip of the eighth coding spherical area unit combined with the last four of the fifty two key sub-blocks exploitation addition modulo 216 and multiplication modulo 216 + 1 to make the ensuing four 16-bit cipher text blocks.

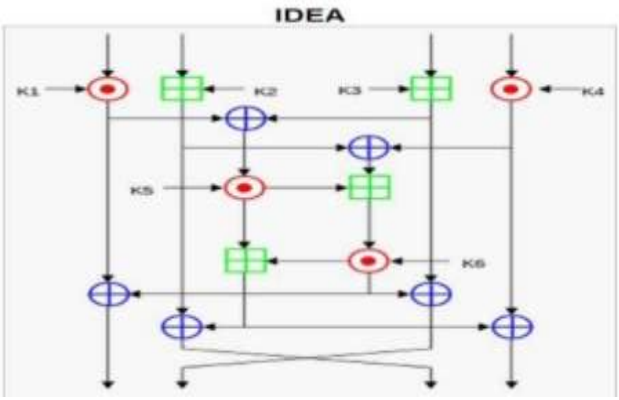


Figure 1. An Encryption Round of IDEA. [8]

### 3. *Decryption*

The process method used for secret writing of the cipher text is actually an equivalent as that used for coding of the plaintext. The sole distinction compared with coding is that in secret writing, completely different 16-bit key sub-blocks area unit generated. More exactly, every of the fifty two 16-bit key sub-blocks used for secret writing is that the inverse of the key sub-block used throughout coding in respect of the applied pure mathematics cluster operation. To boot, the key sub-blocks should be employed in the reverse order throughout secret writing so as to reverse the coding method as shown in Table two.

**Modes of operation:** IDEA supports all modes of operation as delineate by office in its publication FIPS eighty one. A block cipher encrypts and decrypts plaintext in fixed-size-bit blocks (mostly sixty four and 128 bit). For plaintext exceptional this fastened size, the only approach is to partition the plaintext into blocks of equal length and encode every individually. This technique is known as Electronic Code Book (ECB) mode. However, Electronic Code Book isn't an honest system to use with tiny block sizes (for example, smaller than forty bits) and identical coding modes. As ECB has disadvantages in most applications, different ways named modes are created. They're Cipher Block Chaining (CBC), Cipher Feedback (CFB) and Output Feedback (OFB) modes.

**Weak keys for plan:** According to Daemon's report massive categories of weak keys are found for the block cipher formula plan. Plan incorporates a 128-bit key and encrypts blocks of sixty four bits. For a category of 223 keys plan exhibits a linear issue. For a particular category of 235 keys the cipher incorporates a international characteristic with likelihood one. For an additional category of 251 keys solely 2 encryptions and determination a collection of sixteen nonlinear mathematician equations with twelve variables is enough to check if the used key belongs to the current category. If it does, its specific worth is calculated with efficiency. it's shown that the matter of weak keys is eliminated by slightly modifying the key schedule of plan.

## D. THE STRENGTH OF IDEA

IDEA uses 128-bit key, which is double than key size of DES. Thus, to break into IDEA, $2^{128}$ encryption operations are required. [5]

## VI. THE AES ALGORITHM

### A. About AES

The selection process to find this new encryption algorithm was fully open to public scrutiny and comment; this ensured a thorough, transparent analysis of the designs. Fifteen competing designs were subject to preliminary analysis by the world cryptographic community, including the National Security Agency (NSA). In August 1999, NIST selected five algorithms for more extensive analysis. These were:

- MARS, submitted by a large team from IBM Research
- RC6, submitted by RSA Security
- Rijndael, submitted by two Belgian cryptographers, Joan Daemen and Vincent Rijmen
- Serpent, submitted by Ross Andersen, Eli Biham and Lars Knudsen
- Twofish, submitted by a large team of researchers including Counterpane's respected cryptographer, Bruce Schneier

Implementations of all of the above were tested extensively in ANSI, C and Java languages for speed and reliability in encryption and decryption, key and algorithm setup time, and resistance to various attacks, both in hardware- and software-centric systems. Members of the global cryptographic community conducted detailed analyses (including some teams that tried to break their own submissions).
After much enthusiastic feedback, debate and analysis, the Rijndael cipher -- a mash of the Belgian creators' last names Daemen and Rijmen -- was selected as the proposed algorithm for AES in October 2000 and was published by NIST as U.S. FIPS PUB 197. The Advanced Encryption Standard became effective as a federal government standard in 2002. It is also included in the ISO/IEC 18033-3 standard which specifies block ciphers for the purpose of data confidentiality.
In June 2003, the U.S. government declared that AES might be accustomed defend classified info, and it shortly became the default encoding algorithmic program for safeguarding classified info likewise because the 1st publically accessible and open cipher approved by the United States intelligence agency for classified info. AES is one among the Suite B cryptographically algorithms employed by NSA's info Assurance board of directors in technology approved for safeguarding national security systems. Its victorious use by the U.S. government junction rectifier to widespread use within the non-public sector, leading AES to become the foremost well-liked algorithmic program utilized in bilateral key cryptography. The clear choice method helped produce a high level of confidence in AES among security and cryptography consultants. AES is safer than its predecessors -- DES and 3DE because the algorithmic program is stronger and uses longer key lengths. It conjointly permits quicker encoding than DES and 3DES, creating it ideal for software system Applications, computer code and hardware that need either low-latency or high output, such as firewalls and routers. It utilized in several protocols like SSL/TLS and might be found in newest applications and devices that require encoding practicality.

### B. How AES encoding works

AES contains 3 block ciphers, AES-128, AES-192 and AES-256. Every cipher encrypts and decrypts information in blocks of 128 bits exploitation cryptographically keys of 128-, 192- and 256-bits, severally. Bilateral or secret-key ciphers use an equivalent key for encrypting and decrypting, therefore each the sender and also the receiver should apprehend and use an equivalent secret key. All key lengths square measure deemed sufficient to shield classified info up to the "Secret" level with "Top Secret" info requiring either 192- or 256-bit key lengths. There square measure ten rounds for 128-bit keys, twelve rounds for 192-bit keys, and fourteen sphericals for 256-bit keys -- a round consists of many process steps that embrace substitution, transposition and mixture of the input plain text and rework it into the ultimate output of cipher text.
As a cipher, AES has verified reliable. The sole victorious attacks against it are side-channel attacks on weaknesses found within the implementation or key management of sure AES-based encoding merchandise. (Side-channel attacks do not use brute force or theoretical weaknesses to interrupt a cipher; however rather exploit flaws within the approach it's been enforced.) The BEAST browser exploit against the TLS v1.0 protocol may be a smart example; TLS will use AES to write in code information, however attributable to the data that TLS exposes, attackers managed to predict the formatting vector block used at the beginning of the encoding method [7].

### C. Features of AES Encryption Algorithm

Advanced Encryption Standard (AES) algorithm works on the principle of Substitution Permutation network. AES doesn't use a Feistel network and is fast in both software and hardware. AES operates on a 4×4 matrix of bytes termed as a state The Advanced Encryption Standard cipher is specified as a number of repetitions of transformation sounds that convert the input plaintext into the final output of cipher text. Each round consists of several processing steps, including one that depends on the Encryption key. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

### D. Advantages of AES Encryption Algorithm

Advanced Encryption Standard not only assures security but also improves the performance in a variety of settings such as smartcards, hardware implementations etc. AES is federal information processing standard and there are currently no known non-brute-force direct attacks against AES. AES is strong enough to be certified for use by the US government for top secret information Alternative to Advanced Encryption Standard – The ciphers which are used alternatively to Advanced Encryption Standard are SSl and TLS. RC4 encryption is next to AES. RC4 is of 128- bits RC4 is a fast cipher and is always subjected to many types of attacks. That is the reason WEP wireless encryption is poor. Thus AES is given priority than other standards.

### E. Limitations of AES Encryption Algorithm

The primary drawback to using advanced encryption standard (AES) algorithm with a 256 bit key to share sensitive data is that a symmetric key algorithm, meaning each recipient must receive the key through a different channel than the message.

And hence we are moving toward the IDEA algorithm which provides better functionality over the previous encryption algorithm under the scenario of security issues of shared data on cloud computing. [6].

## VII. CONCLUSION

AES and IDEA algorithm may be a proprietary and universally applicable block coding formula, which allows the effective protection of transmitted and hold on information against unauthorized access by third parties. With a key of 128 bits long, plan is way safer than the wide notable DES supported a 56-bit key. The basic criteria for the event of plan were strength for all security needs and simple hardware and code implementation. The formula is employed worldwide in numerous banking and trade applications. They predestine the formula to be used in a very nice range of business applications.

## REFERENCES

[1] S.William,"Cryptography and Network Security: Principles and Practice", 2nd edition, Prentice-Hall, Inc., 1999.
[2] http://www.tutorialspoint.com/
[3] https://www.google.co.in/?gfe_rd=cr&ei=xBJVV57BKobE9AW7_bPQAQ&gws_rd=ssl#q=symmetric+key+encryption
[4] http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard
[5] https://www.skillset.com/questions/what-is-the-primary-drawback-to-using-advanced-encryption-standard-aes-algorithm-with-a-256-bit-key-to-share-sensiti-4254
[6] http://electronicsbus.com/advanced-encryption-standard-aes-encryption-algorithm/
[7] http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard
[8] https://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm
[9] http://www.garykessler.net/library/crypto.html
[10] http://www.garykessler.net/library/crypto.html