Information Security in IoT Devices Using Lightweight Cryptography

Project report submitted in partial fulfilment of the requirement for the degree of Bachelor of Technology

in

Computer Science and Engineering/Information Technology

By

Tejansh Dalal (151377)
Paras Verma (151407)

Under the supervision of

Dr. Ravindara Bhatt

To

Department of Computer Science and Engineering and Information Technology

**Jaypee University of Information Technology Waknaghat,
Solan - 173234, Himachal Pradesh**

Certificate

Candidate's Declaration

I hereby declare that the work presented in this report entitled **"Information Security in IoT Devices Using Lightweight Cryptography"** in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering/Information Technology** submitted in the department of Computer Science & Engineering and Information Technology, Jaypee University of Information Technology Waknaghat is an authentic record of my own work carried out over a period from August 2018 to May 2019 under the supervision of **Dr. Ravindara Bhatt** Assistant Professor (Senior Grade), Department of CSE and IT.

The matter embodied in the report has not been submitted for the award of any other degree or diploma.

(Student Signature)
Tejansh Dalal, 151377

(Student Signature)
Paras Verma, 151407

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

(Supervisor Signature)
Dr. Ravindara Bhatt
Assistant Professor (Senior Grade)
Computer Science & Engineering and Information Technology
Dated:

ACKNOWLEDGMENT

We It is our privilege to express our sincerest regards to our project supervisor Dr. Ravindara Bhatt for their valuable inputs, able guidance, encouragement, wholehearted cooperation and direction throughout the duration of our project.

We deeply express our sincere thanks to our Head of Department Prof. Dr. Satya Prakash Ghrera for encouraging and allowing us to present the project on the topic “Information Security in IoT Devices Using Light Weight Cryptography” at our department premises for the partial fulfilment of the requirements leading to the award of Bachelors of Technology degree.

.

We are also thankful to all other faculty members for their constant motivation and helping us bring in improvements in the project.

Finally, we like to thank our family and friends for their constant support. Without their contribution it would have been impossible to complete our work.

Tejansh Dalal, Paras Verma
JUIT Waknaghat, May 2019

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

IoT	Internet of Things
AES	Advanced Encryption Standard
TEA	Tiny Encryption Algorithm
HIGHT	High security and lightweight
QoS	Quality of service
RFID	Radio Frequency Identification
UDP	User Datagram Protocol
ECC	Elliptic Curve Cryptography
DES	Data Encryption Standard
FIPS	Federal Information Processing Standard
SEA	Scalable Encryption Algorithm
CoAP	Constrained Application Protocol
MITM	Man in the middle
SPN	Substitution permutation network

LIST OF FIGURES

LIST OF GRAPHS

PERFORMANCE ANALYSIS

LIST OF TABLES

ABSTRACT

Internet of Things is known as present-day technology, but it is there from a long and distinct period of history from when we have the internet which connects numerous devices which convey information with each other and does not require any human interaction. IoT systems works on the collection and interpretation of data to provide useful services, the data that is being used have worth in the modern era, the data gathered from systems is vulnerable to cyber-attacks.

So, the security plays a significant part in network to preclude the unapproved access, that can make a wrong use application or data. Security is considered in all layers of IoT Framework, major from the perspective of making standards from top to bottom level. IoT nowadays is widely used and is very essential in modern world full of technologies.

IoT applications are serviceable to everyone but it will be not much desired by the users if any system is unable to secure the data from the world because the data is critical, and it should not be available to everyone. Lightweight encryption is a part of traditional cryptographic algorithms which are relevant in feasibility of low resource devices in IoT.

How the lightweight cryptography techniques are used to achieve secure data transfer in IoT and comparison between them is briefed in this report.

CHAPTER - 1

INTRODUCTION

Internet of Things or Internet of Everything or Web of Things is a fresh computing setting, that had made a lot of devices to be connected to web. These devices interact with each other by the use of the network and provide the services as required or assigned to them. So, to use this fresh setting efficiently and securely, node security was very important. The network will be compromised hugely and may get damaged, if there is concession in one in every of the nodes. But, because of the extent of resources of forced devices, it is very tough to implement easy scientific cryptographic bash.

Use of small computational electrical equipment such as industrial controller, radio frequency identification (R.F.I.D) tag, sensible card and detector nodes is very common these days. Changes from computer to small appliances reflects the very good contrast of current security views. In this case it becomes very difficult to implement standard crypto logical algorithms for small appliances, because the resources are very difficult or impossible to handle, because in many standard crypto logical standards, the barrier between performance, resource requirements and security standards are developed for personal computer and high resources environments. Once applied, the display cannot be up to the mark

.

Lightweight cryptography is a sub part in cryptography, which directs to ensure customized results for processing low resources devices. There is a large amount of labour stolen with light cryptography by the tutorial community; This includes the thrifty implementation of easy cryptography standards, and therefore the current lightweight algorithms and protocol style and analysis

.

For sure communication, cryptography and secret writing are used for hundreds of years. Throughout history, the best advantage on cover writing is done by military communication and hence progress from there. The need to ensure industrial and peculiar communication is punctual. Beginning in the 1980s through the Internet, the age of 1960 had become absurd. It did not expand until the use of the World Wide Internet was done in 1989. World

Wide Web is a concert electronic protocol which allows people in matching information, information and commerce to an electronic medium. An unimaginable ache for information security has been caused by this new policy of data. An agreement in cryptography and its covert writing makes the people to use different ways to protect the data to make it more secure as the technology is increasing day by day and these devices are becoming more vulnerable to the attacks.

Internet of Things may be unfamiliar worldwide but it’s promptly creating advancements within the ground of up to date fragile media communication. IoT may be an international motion that data, processes, unites people and objects to produce network connections that area unit additional pertinent and useful than ever before. While not demanding human relations from human to human or human from computer, the flexibility of transferring knowledge over a network is given by network of counterfeit computing objects like sensors, R.F.I.D tags, actuators, cell phones and various digital machines.

IoT can produce approx. $3000 billion in earning until 2020, According to a report. Moreover, the quantity of smartphones and tablets can bypass 7.03 billion units by 2020. Wherever a large bulk of info is transferred through a mesh, these devices can create a big and tangled network. IoT have risks and disputes, like a way to grip large quantity of info, address security peril, and the way to encrypt and decrypt large information and as it is cultivating promptly, we must take care of the things.

When there are many sensible devices connected in the IoT environment, then to solve these challenges, the increasing demand for the use of cryptographic answers applied in embedded applications. However, these sensible devices are usually forced to be resource or known as low resource devices in terms of providing less computational power, small size, small battery storage and less memory.

In addition, tight hinders contain the large development of sensible devices, which meet the need to develop a replacement crypt analytic algorithm rule, with strong security mechanisms, with varying functionalities for low security applications and comprehensive computing, performs encryption and decryption, with low power consumption. This is current topic of research known as lightweight cryptography.

The two main reasons to switch to new technology for IoT are mentioned below:

Efficiency of end-to-end communication - It can be explained as to use lightweight symmetric key formula with the less power consumption as compared to other algorithms to get more secure end to end system security in small scale devices having limited resources.

Adaptability in low resources smart devices - The impression of light cryptography is less if compared with the classical algorithms. It is likely to have additional network references for less resource sensible devices.

Cryptography is progressing, recent technologies are there to attack, having widely studied design and implementation. One of these cutting-edge technologies is Lightweight Cryptography. It is an algorithm that is used for implementation of cryptography in restricted environment systems, including sensors, home security, health care equipment's, smart cards, R.F.I.D tags, manufacturing and so on.

Cryptography is being used to provide secure communication from a long time. In the history and at present, military is widely using it for the communication and from then the cryptography had been in progress from there. Since then secure communication is required in all the fields from home to the business. Beginning in the age of 1980. Although the net had been unreal at the end of the 1960s, but it did not go public until the net was unreal in World Wide 1989.

Lightweight cryptography delivers the required security. Lightweight properties like chip size, memory usage, energy consumption etc. evaluate in terms of hardware implementation. In software implementation, small codes and RAM sizes are better for lightweight applications.

Lightweight cryptography provides the desired protection. Lightweight cryptography does not take advantage of safety efficiency business dislikes every time. There are many new technologies of lightweight cryptography so we can use the most efficient and secure among them or as there is requirement of the system.

PROBLEM STATEMENT

For past few time, Lightweight Cryptographic techniques are a dreadful necessity that are operated by lack of unrealistic ideas that are qualified of running on the gadgets with very less calculating power. We can think of example of tags of R.F.I.D, gadgets in wireless detector networks and many small Internet enabled devices that are going to take a toll over the markets due to IoT advancement.
By the use of square ciphers, lightweight stream ciphers, single-pass authenticated mystery writing, hash operators to advance the security in IoT gadgets large number of cryptographers had addressed these issues.

Since in present scenario IoT is welcomed in work areas, homes, social areas, commercial MNC that will open up the gate for privacy and security provocation. The prime reasons of IoT being operated in today's world is found because of the privacy and security provocation. If harmed, then this context could be circumvented that an attacker has been found in IoT. Large condemn on IoT are because of activities like fishing, spoofing, deprivation of favour, DDoS, injection of false signals. Such strike could destroy Internet of Things authentication, privacy, integrity security services. It is also going to have an impact on the secrecy of the users. Internet of Things comes up with an incentive security answer based on every layer, a larger portion of these zones are still vulnerable to the strike.

Special resources like real time machine, power, Internet of Things status don’t fall in parallel with the customary decryption and encryption techniques. HEIGHT, AES, PRESENT, RC5, RSA and others in literature review are numerous types of lightweight cryptographic centrally symmetric algos. This present answer doesn’t warrant the reliability of large level of security in actual-time communication, the length of cryptography and large level of protection for memory requirements. Performance time includes the main management and distribution, encoding and image which determines the effectiveness of the protocol. The huge key size is gradually calculated pessimistically on Ecuadorian block scale, centre will provide full privacy and integrity for symmetric algorithm, which will come up with the real time info and will have a large smack on the processes and to utilize their resources.

OBJECTIVE

To build lightweight algorithm which will use lesser resources.

A secure algorithm which is less vulnerable than other algorithms to attacks.

To design a new algorithm keeping in mind to have lesser hardware requirements to decrease implementation costs.

To increase trust of users we should have the security services that are mentioned below in IoT:

Confidentiality: It means to keep the data safe or the keep the information safe so unauthorized person could not access it. Only authorized person should be able to get access to the data.

Integrity: It ensures that the information or data has not been changed and the data is authentic. There is no change in the data in between the communication and the information or the information source is real.

Authentication: In this there are some rules which defines the identity of the user by asking user the credentials to access secure system. The credentials are then checked for the identification of the user if the credentials are true then the user is verified else not.

Authorization: It is the process in which we check if the user has the access to the files or the resources which it is requesting to grant access or not. Every user in the system have different roles and thus have authorized to have different file access rules. We can take example of the university resource admin, teachers, director and students all have access to it but with some rules such as students can only read files but teacher can read, write and delete files from the resource because they were authorized to do so in their login credentials.

METHODOLOGY

Lightweight Symmetric Cryptography in IoT

Advanced Encryption Standard: It is used in the application layer as an inbuilt solution for CoAP. National Institute of Standards and Technology created this symmetric block cipher. This algorithm uses SPNs and uses 4 x 4 matrix with 128 bits of block length. Each byte is changed by substitution of bytes from S-box, shifting of rows, mixing of columns and then adding round keys in each round. The key size used in AES can be 128 or 192 or 256 bits. AES is still vulnerable to MITM attack.

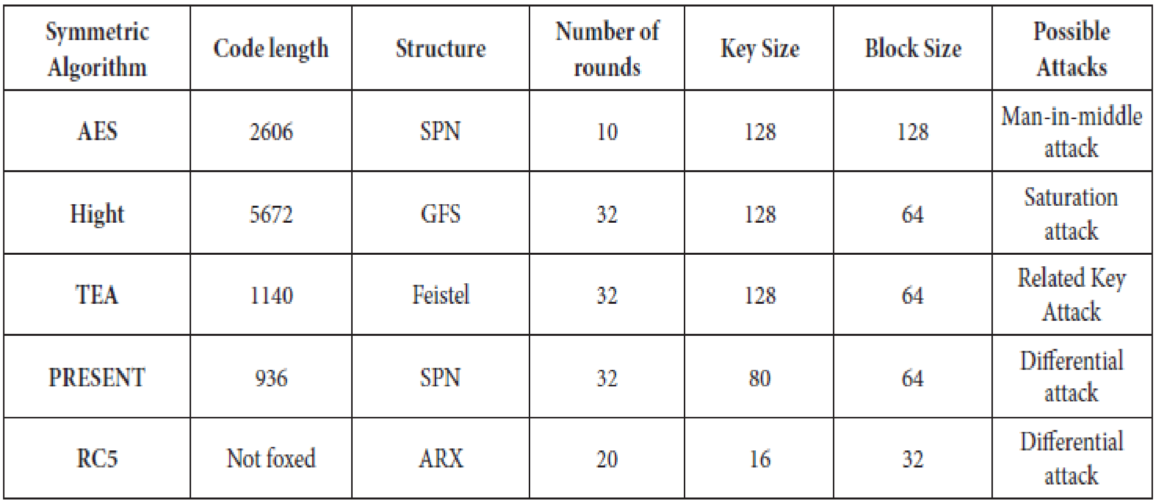
Tiny Encryption Algorithm: It is used in small systems that have limited resources means that have small memory like sensor networks or smart things. It is a very small code to reduce the memory usage. It uses simple operation, addition and transfer of XOR and does not make the program complex. It has block size of 64 bits and have key size of 128 bit. TEA does not use any S-boxes or any other computations. There are many versions of it such as XTEA, Block TEA and XXTEA. The new versions are proposed to provide extra security in TEA. Due to the simplicity of TEA it is vulnerable to many attacks, so its application was in less secure systems having very few resources.

High security and lightweight: To work for the Feistel Network, it uses simple operations like addition and subtraction modulo 2^8, bitwise rotations and XOR. Having a block size of 64 bits, which works in 32 rounds on 128-bit keys. During encryption and decryption, the key is generated in HIGHT. A similar implementation of the HIGHT was suggested which have few lines of code to save memory, uses less power and increase the performance of R.F.I.D systems.

RC5: This was first crafted for rotation, which is free of data. Structure of RC5 algorithm is Feistel like network. RC5 encryption and decryption code can be written in very few lines of code. It is a lightweight algorithm mostly used in wireless sensor networks. RC5 is labelled as RC5-w/r/b, where w is for words shape, r is for the no. of rounds, and b is key size. It can work from 0 to 255 rounds using 0 to 255 key bytes. The standard key size is of 16 bytes with 20 rounds. Differential cryptanalysis can be used to perform differential attack on RC5.

PRESENT: It is a lightweight block cipher that is based on substitution permutation networks. It uses only 4 bits of S-box, also the key size of this algorithm is smaller as compared to other. It has a smaller number of rounds that makes this algorithm best to use in small devices it also increases the throughput. PRESENT is unsafe in 26 out of the 31 rounds are sensitive to the attack.

Comparison of common Lightweight Symmetric Cryptography algorithms for IoT:



Symmetric Algorithm	Code length	Structure	Number of rounds	Key Size	Block Size	Possible Attacks
AES	2606	SPN	10	128	128	Man-in-middle attack
Hight	5672	GFS	32	128	64	Saturation attack
TEA	1140	Feistel	32	128	64	Related Key Attack
PRESENT	936	SPN	32	80	64	Differential attack
RC5	Not foxed	ARX	20	16	32	Differential attack

Lightweight Asymmetric Algorithms for IoT:

RSA: RSA is public key encryption technology. In this user creates a public key and then publishes it. RSA key is multiplication of two large prime numbers its key is public but factoring the large number to get back two numbers is difficult and cannot be done it need time very much by the supercomputers also. this key provides better security to RSA algorithm as to deduce it key lots of computational power and time is required.

RSA encryption is directly linked to the key size, so the key size is generally 1024 or 2048 bit long. Many companies are not using this public key encryption with the key size of 2048 bit to achieve more security.

Elliptic Curve Cryptography: It is a public key encryption technology. It uses the elliptical curve theory which is used for making more faster, smaller, and efficient crypto keys. The key is the product of very large prime numbers, rather than the conventional method, through the properties of elliptic curve equations.

It is an encryption system in which reverse engineering is not possible. Experts says that it is a next generation technology that provides better security than the other public key cryptography algorithms built earlier.

CHAPTER - 2

LITERARY SURVEY

Lightweight Cryptographic Algorithms for Internet of Things

In this increasing time of new things IoT is also growing. Contemporary things such as objects that can be seen physical such as phones, laptops, ACs, chargers and many more. IoT can be simply seen as a network of acceptable and manageable sensible objects which are efficient in doing communication, calculation. Wireless connections could be used to connect objects in IoT.

To begin the transfer of data between the gadget's components are required by IoT. Items can be expanded by auto-ID technique, usually the R.F.I.D tag, so the item can be clearly identified. R.F.I.D tags allows the item to communicate wirelessly to a specific type of information, which brings us to different call, the potential to see the info R.F.I.D tags will be inactive tags etc. The ID info and the signal is occasionally captured by an on-board battery that is being contained by the Active tag. The no. of life-operators which are completely functionable would be adjusted from 1-10 metres, flexibility in apps such as quality management and direction will be allowed. Because of this multi-seeing, and large cost effectiveness, for IoT actual-time apps indoor restriction R.F.I.D is being largely used. Risks and favours provided by the R.F.I.D system are secured by cryptography using lightweight algorithms.
The strikes addressed by the distribution of safe R.F.I.D tags include:

1. Viruses: R.F.I.D can also suffer from virus attacks, like any of the numerous info system. The main goal of virus is the backend database. The R.F.I.D virus can harm or disclose the data saved in the database or cut in the service or obstruct the comm b/w the reader and the database.
We should decrease the database connected risks; we should screen the R.F.I.D database.

2. Physical attacks: When the tags are physically obtained by the attacker and then he changes its info it is known as physical attack. It could be done in many ways, like checking

an attacker to change the data or read on the tag. The comm b/w reader and the tag could be destroyed using an Electro Mag. interference.
To make our own items known by R.F.I.D reader one can simply destroy the tag from the items by any device or by a knife.

3. Replay attacks: To make a response to the reader plea, attacker impart the comm and b/w the tag and the reader and document the tags response. To ingress the safe facility, a criminal record the comm. b/w the proximity card and access card, this is an e.g. of replay attacks.

4. Insert attacks: An attacker attempts to put system order into R.F.I.D system alternative of sending the normal info, in these attacks. Tag conveying the system order in its memory is an e.g. of R.F.I.D Insert Attack.

5. Repudiation: When we have no method to verify that a specific action has been taken by the user if he denies it, it's called repulsion. In the case of RFID, reconsideration could happen in 2 ways: one is a receiver or sender who could deny taking steps like sending an R.F.I.D request and we have no evidence of this. The 2nd is the holder of an E.P.C number or the holder of the database denies that he has any data about an object or tag related to an individual.

6. Spoofing: The attacker is adjudged as the authorized user of system in spoofing attack. By making the use of the naming service of user an attacker can represent himself as a valid one. By making use of the spoofed info, an attacker can validly enter into the system, then by using the R.F.I.D info he can do anything he wants like changing R.F.I.D id, answering the invalid mails etc.

7. Denial of Service: The I.D saved in the database server gets compared with the I.D received by the reader whenever it requests for the info. Both backend server and R.F.I.D reader are endangered to denial of service attack. The service gets intersperse during the DOS attack when the tag gets failed to discover the reader. Therefore, we need to safeguard that both database servers and reader have ways to repudiate the service attack.

8. Tracking: An attacker could trace the speed of an item and location by reading the info obtained from the R.F.I.D tag. The R.F.I.D can recognize the position of the object once the object gets connected to an object and it enters the zone of R.F.I.D reader. An attacker could trace your object even if the R.F.I.D reader is making use of encrypted mgs to communicate, whenever we a link a R.F.I.D tag to an object.

9. RFID Sniffing: In deploying RFID solutions is a major concern. RFID readers always request to send back their identification information to the tag. The information that is being stored on the back-End server is being verified by the data sent using the tag by the reader. To differentiate B/W a data sent by a real R.F.I.D and by a fake R.F.I.D reader is very difficult for most of the R.F.I.D tags. To pursue the tag and utilize it for its own motive the attacker could make use of its R.F.I.D reader.

10. RFID Counterfeiting: Based on usage of power, RFID could be distributed into 3 categories:

1. Original tag
2. Tag using symmetric key
3. Tag using public/general key

The duplicity of original tags can be easily done because they don't use encryption. Since we know that travel industry and supply management the strikers could write info about any original black tag and modify the info in taggable original tags to gain access to or verify authenticity of a product.

Things that can be done on basic tags by the attackers are:

1. They can change current info in the original tag or make valid tags in the invalid tags and vice versa.
2. Can decrease the price of an expensive object to purchase it at a lower cost.
3. Attacker could change an object's tag with another tag implanted in another object.
4. Can make their personal tag by making use of personal info attached with another tag.

Therefore, while dealing with personal items like passports etc some type of cryptographic technique should be used. If you want to make the use of the original tag, do make sure that you are using proper security measures, surveillance or audit programs to recognize inconsistencies in the RFID framework.

Lightweight Cryptography

Some algorithms are required to provide security in the restricted environment systems where there is less memory and power like health care, security sensors and R.F.I.D tags. Power usage and memory of the device is needed to be taken care while designing the algorithm. Small size code due to small memory and less RAM is required in lightweight systems. In lightweight cryptography it is important to take care of system configurations while designing the algorithm. Lightweight cryptography provides additional protection. Lightweight cryptography does not always able to provide security due to less available resources. Nowadays, many lightweight block ciphers are introduced such as RECTANGLE, PRINT cipher, EPCBC, ITUbee, Piccolo, PRINCE, LED, MIBS, KLEIN, TWINE and L-Block. All these lightweight algorithms are based upon two structures FEISTEL and SPNs.

The substitution permutation network is created through some round function which is used upon full information block. There are some safety issues in the slow spread of normal Feistel type structures. Therefore, to highlight these issues, in order to distinguish the ciphers in ancient Feistel type structures, enough ciphers are required to support the circulatory network, therefore, this replacement consumption will increase the consumption of energy compared to the network.

There are additional features in standard Feistel type structures:

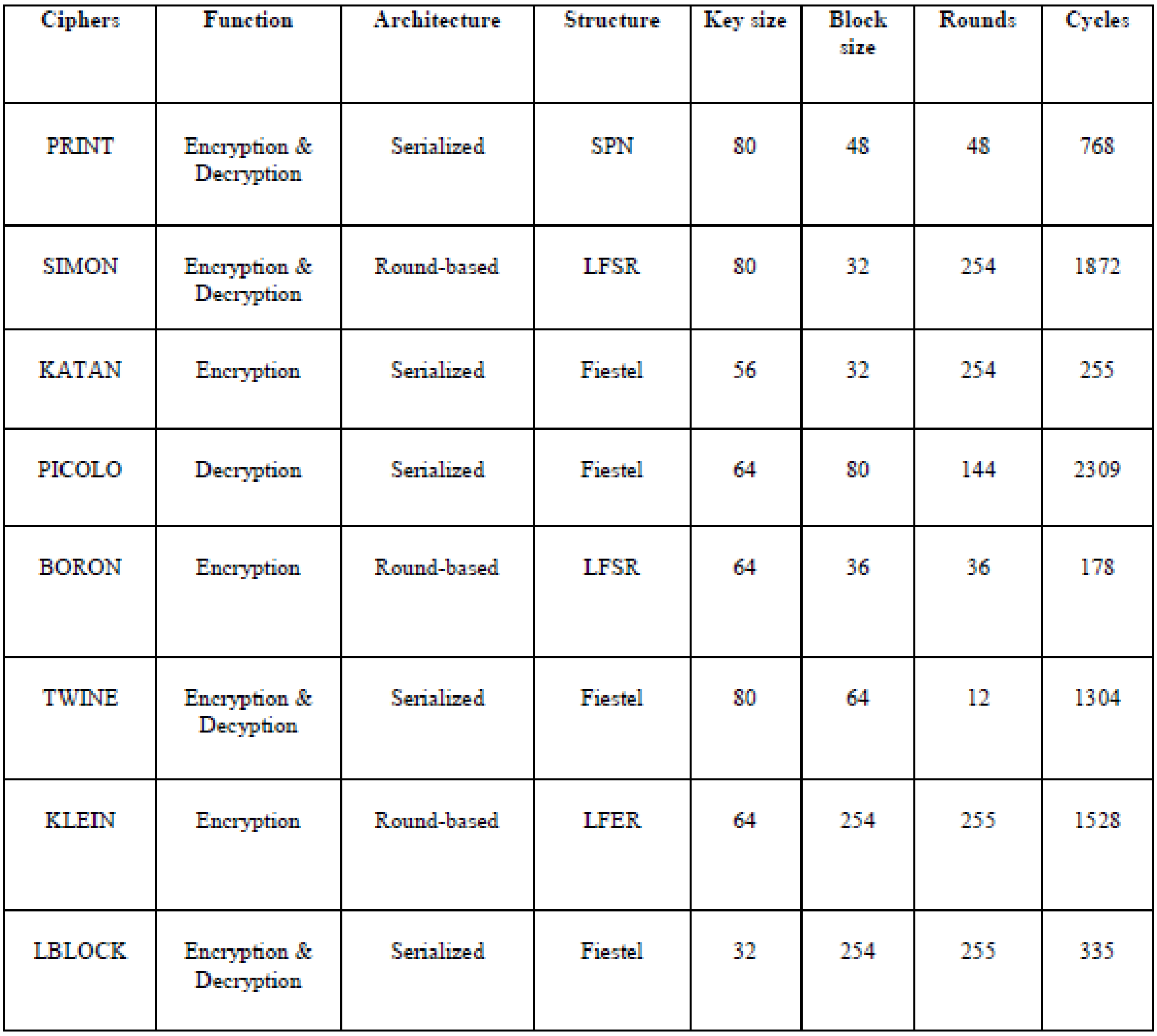
1. Very easy and small round function.
2. Similar code for both decryption and encryption processes by which the cost of computation in decryption process reduces.

Internet of Things: Need of Lightweight Cryptography

1. Consistent in end to end communication: To obtain security in the transmitted data for low power devices, it is very important to have a reliable end to end communication with cryptographic operations with a limited amount of energy consumption.

2. Good in lower configuration devices: Lightweight cryptography will be useful in low end devices as it will use very few resources as compared to classical cryptography algorithms. Lightweight cryptography will provide more resource to the system as it will not be consumed by the encryption/decryption process. So low cost equipment devices can be implemented in a single integrated circuit due to restricted pricing and power consumption whenever low hardware properties are important in the system.

The table beneath shows the comparison of lightweight cryptographic algorithms:



Ciphers	Function	Architecture	Structure	Key size	Block size	Rounds	Cycles
PRINT	Encryption & Decryption	Serialized	SPN	80	48	48	768
SIMON	Encryption & Decryption	Round-based	LFSR	80	32	254	1872
KATAN	Encryption	Serialized	Fiestel	56	32	254	255
PICOLO	Decryption	Serialized	Fiestel	64	80	144	2309
BORON	Encryption	Round-based	LFSR	64	36	36	178
TWINE	Encryption & Decyption	Serialized	Fiestel	80	64	12	1304
KLEIN	Encryption	Round-based	LFER	64	254	255	1528
LBLOCK	Encryption & Decryption	Serialized	Fiestel	32	254	255	335

Lightweight Cryptography: Applications in IoT devices

Security based warnings and their antidote for IoT

The problem in the IoT system is that these systems can become the target of cyber-attacks as these devices deal with real world information. Let's take an example for implementation of IoT in a factory. The IoT devices will gather information from different sensors and then analyse the information to provide real time management. This will improve the productivity and stability. If the information sensed by the sensors are incorrect then there will be incorrect results that will lead to great loss. And the information sensed can be production related secret so that should be secret and should be prevented from the outside world.

Cryptography is meant to handle information, apply security to information to apply privacy and integrity. Lightweight cryptography is good for secure limited resource systems.

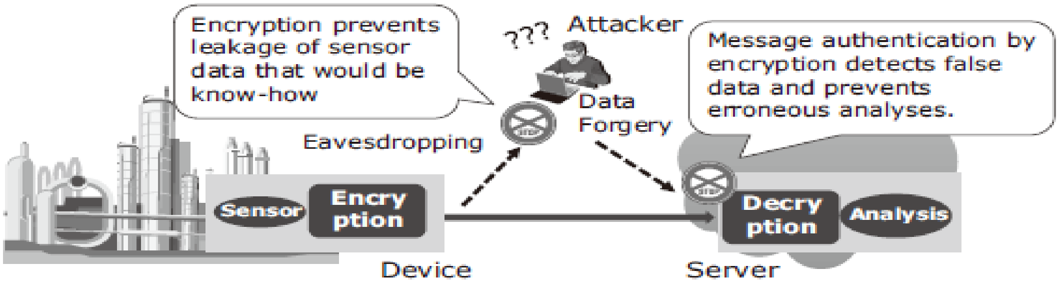

Encryption prevents leakage of sensor data that would be know-how
???
Attacker
Message authentication by encryption detects false data and prevents erroneous analyses.
Data Forgery
Eavesdropping
Sensor
Encry ption
Decry ption
Analysis
Device
Server

Fig. 1 Encryption-based countermeasure against attack on data collection.

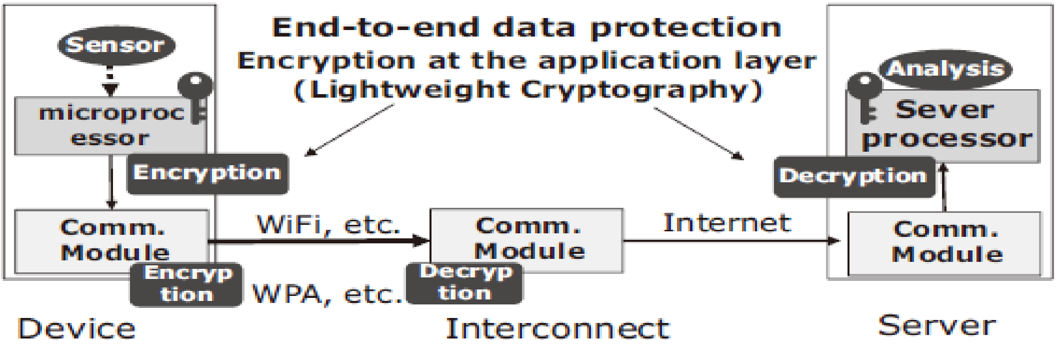


Fig. 2 Example of lightweight cryptography applications.

Lightweight Cryptography

Requirements: Lightweight Cryptography

The following factors are required in lightweight cryptography:

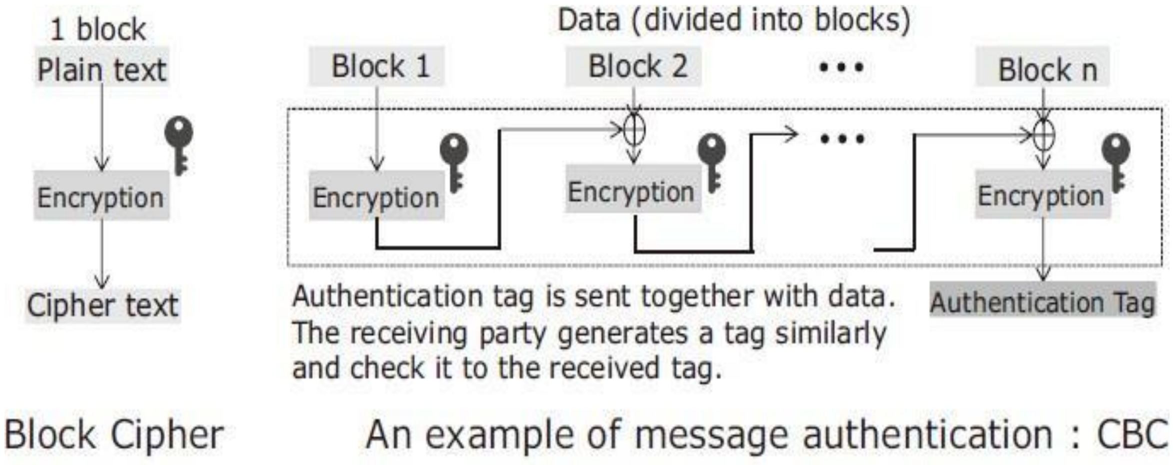
1. Size
2. Power
3. Power consumption
4. Process speed

Firstly, we must find the system to apply IoT in that system. Power consumption should be less, and it is very important as these devices have very low power and some of the devices are battery-based devices. The algorithm should not affect the performance of the system. Performance should be high as some devices transfer large information in real time so the delay should be low.

With the advancement in technology cryptography has become the basic thing to adopt. In low resource systems lightweight cryptography provide a quite level of security. These algorithms provide the integrity in the data with different key lengths and does not compromise the security of the system.

Symmetric Key and Public Key Cryptography

Cryptography can further be divided into two parts symmetric key and public key cryptography. In symmetric key cryptography we use same secret key for both encryption and decryption. On the other hand, in public key cryptography it uses the secret key in encryption process, and it separates the common key and the secret key. Symmetric key cryptography is old technique while public key cryptography is new technique. Public key cryptography is slower that symmetric key cryptography. Public key cryptography is introduced to remove the problem of sharing the secret key in symmetric cryptography. Public key cryptography eliminated the need of sharing of key by using pair of both public private keys.



Authentication tag is sent together with data. The receiving party generates a tag similarly and check it to the received tag.

Block Cipher

An example of message authentication : CBC

Fig. 3 An Example of block cipher mode of operation.

Lightweight Cryptographic Measures for IoT

The IoT network utilizes the system to associate and impart between the things associated with the IoT network. In the wake of making a continuous discussion, IoT is considerably more associated with the additional work. Numerous designs were proposed for the improvement of IoT. The creators have portrayed three stratified developments models that IoTs have. The 3 layers of system are idea layer, network layer and application layer. A five-layer development was recommended that included transport, decisions, applications, business and processing layers.

A wide scope of information is shared among you and the client's solicitation prerequisites. Accordingly, security and protection of the IoT are more mind boggling than different networks in light of the fact that the client's data is shared like place and different information. It is critical to keep up security benefits in the IoT with the goal that the client can pick up certainty.

Confidentiality: It means to keep the data safe or the keep the information safe so unauthorized person could not access it. Only authorized person should be able to get access to the data.

Integrity: It ensures that the information or data has not been changed and the data is authentic. There is no change in the data in between the communication and the information or the information source is real.

Authentication: In this there are some rules which defines the identity of the user by asking user the credentials to access secure system. The credentials are then checked for the identification of the user if the credentials are true then the user is verified else not.

Authorization: It is the process in which we check if the user has the access to the files or the resources which it is requesting to grant access or not. Every user in the system have different roles and thus have authorized to have different file access rules. We can take example of the university resource admin, teachers, director and students all have access to it but with some rules such as students can only read files but teacher can read, write and delete files from the resource because they were authorized to do so in their login credentials.

The security design was investigated to spare conversion information between colleagues and certificate the previously mentioned administrations. An assessment circular segment of standard and security was likewise displayed, however there is yet the test of sorting out the open information in the IoT. As it comprises of various connections, the standard engineering depends on everything with 4 layers. In each layer, the convention will give an insurance convention, which will help shield security administrations.

Advanced Lightweight Data Encryption Technique

The expanding utilization of unavoidable gadgets inside the field of hardware had raised the matters with respect to security. In installed applications, executing undeniable cryptographic surroundings wouldn't be reasonable gratitude to the limitations like power dispersal, security, esteem because of these requirements, the fundamental target is on utilizing lightweight cryptography. For exchanging data, Cryptography is an approach that has been formed.

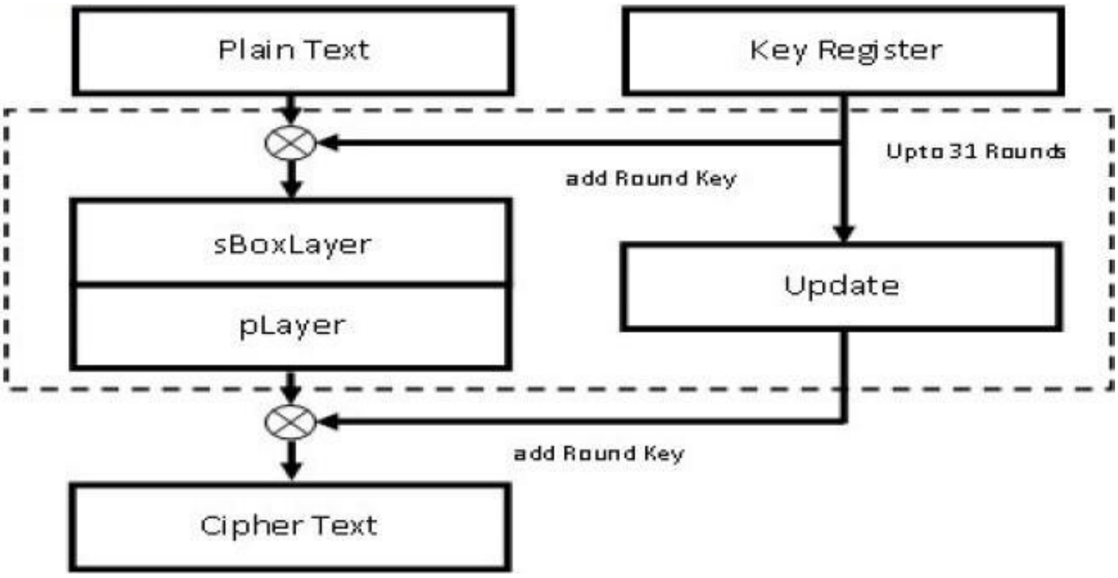
Cryptography right now plays a continuously important job in popular society, and it is fundamental to unwind issues such as verification, integrity, secrecy and untrustworthy elements. In advanced correspondences, the data is circulated through the wires or air as it's not from listening stealthily. In this manner, classification of the exchanging information is of greatest significance. encoding could be a strategy that that is meant to be sent to scrambled information utilizing a key. The encoding technique isn't secret anyway the key's exclusively familiar to the sender and beneficiary of data. The beneficiary changes the received data utilizing the decoding technique to get the underlying data.

Cryptography is of two elemental sorts:

1. Symmetric cipher utilize divided public key and private key is utilized by asymmetric cipher.
2. For firm communications for large period of time, Symmetric key cryptography has a same shared secret key for decoding and encoding

Symmetric key cryptography incorporates two totally various methodologies for encoding and interpreting. In first strategy which is stream cipher, the pieces of data are encoded/unscrambled each one in turn. Transmission blunder in one ciphertext square have impact on elective square and intense to implement appropriately. Nonetheless, inside the 2nd procedure that is called block cipher, squares of the info record that incorporate assortment of bits are scrambled / unscrambled. Transmission blunders in one ciphertext blocks has no impact on elective block and simpler to actualize.

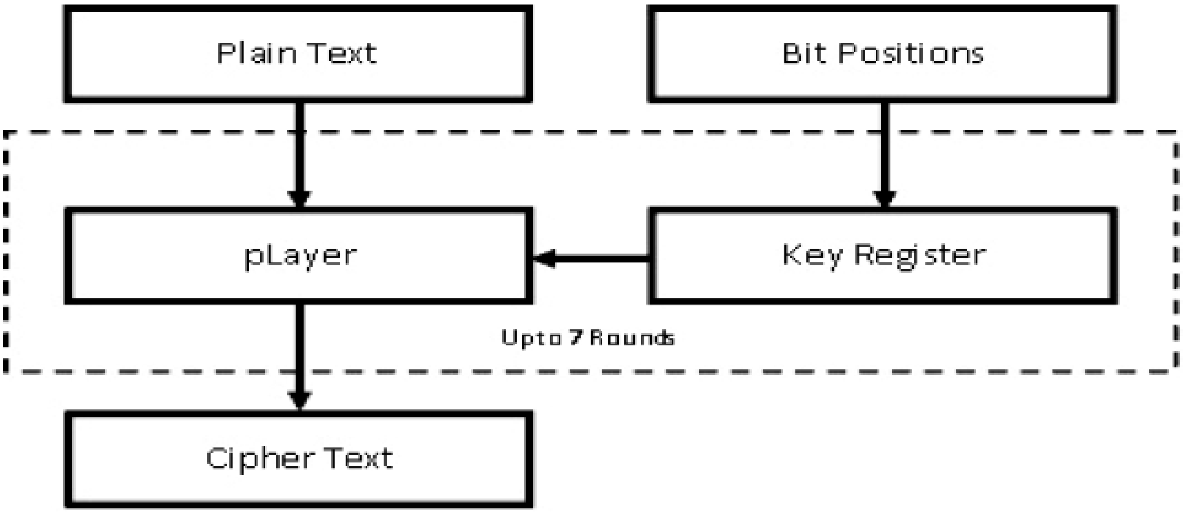
PRESENT



PRESENT is a SPN with 64-bit unsegregated block cipher. The 128 bits is for the key. The 128-bit output and 128 bits input along with the 30 S-boxes comprised the Substitution layer. Through the cautious choice of s-box, it's conceivable to accomplish big security level. The permutation layer is an extremely customary and bunch guidance activity is executed. The yield from permutation layer is XORed with key and is given as input to the S-box.

SYSTEM ANALYSIS

SUGGESTED SYSTEM



As we talked about over, this study depends on cryptography, we give reasonable changes to those plans, to make the suggested framework. Here, S-box of PRESENT calculation is expelled and provided GRP permutation apparatus. Algorithm cantered is to execute lightweight structure to keep away from large power dissemination and substantial memory necessity. To give a great security and minimal effort, there is want of a lightweight crypto algorithm whose inclusion zone would be minimal. The basic algorithm like DES, AES have colossal memory prerequisite and wouldn't be plausible to actualized for inserted framework plan. Numerous lightweight algorithms have been planned before and different assaults have been demonstrated on them. PRESENT algorithm is IEC/ISO institutionalized.

The point of this effort is to give satisfactory security to the computerized frameworks. The lightweight cryptography is a bio metric calculation mix of PRESENT calculation with gathering guidance permutation. The created calculation is exceedingly verified and need just less zone when contrasted with AES.

The feature of the assumed encryption framework is given. Figure above delineates the common block figure of the assumed framework which is included of PLayer where group stage is executed.

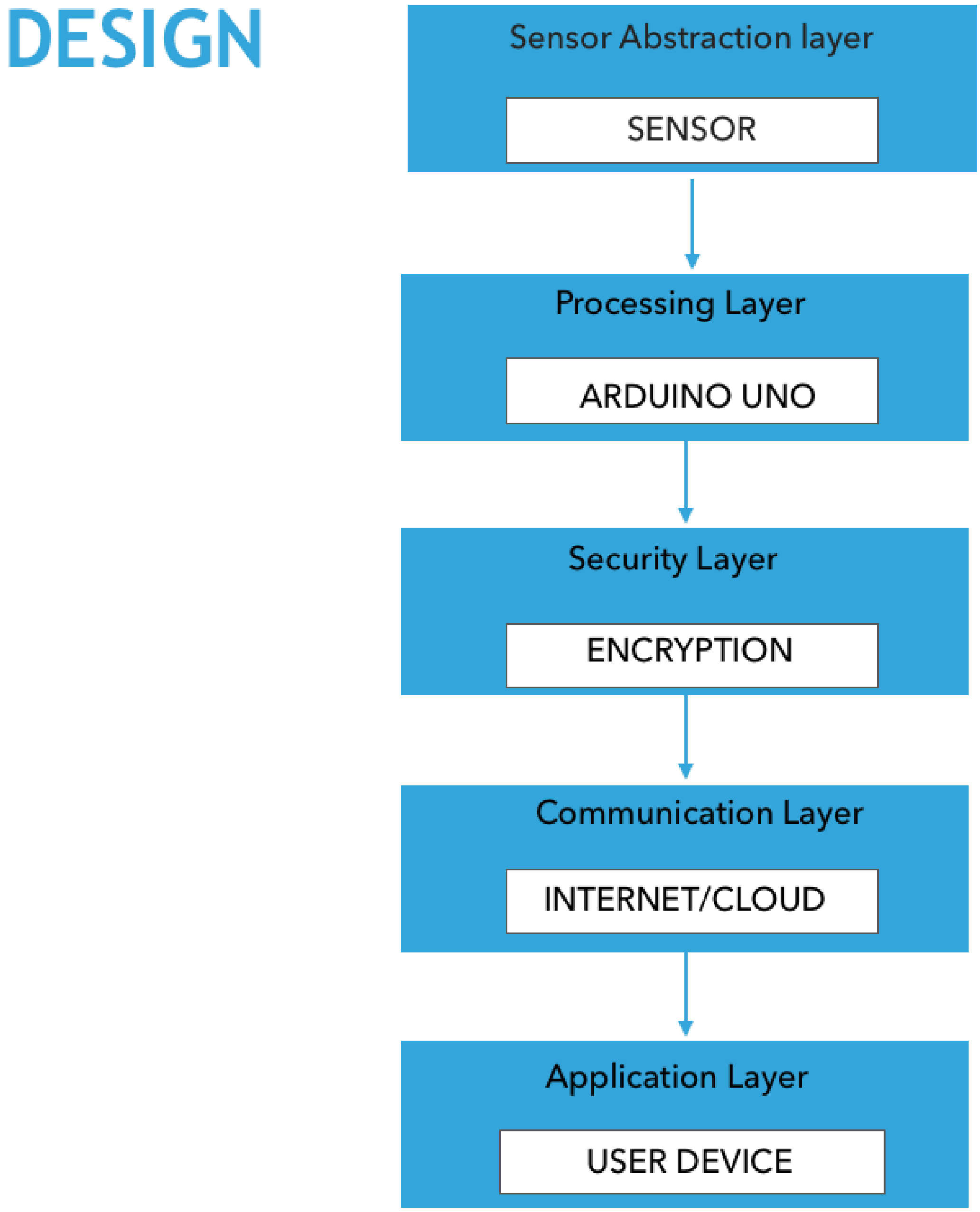
The common block figure of the assumed framework comprises of two chief modules:

Player: Fundamentally here group permutation is executed.

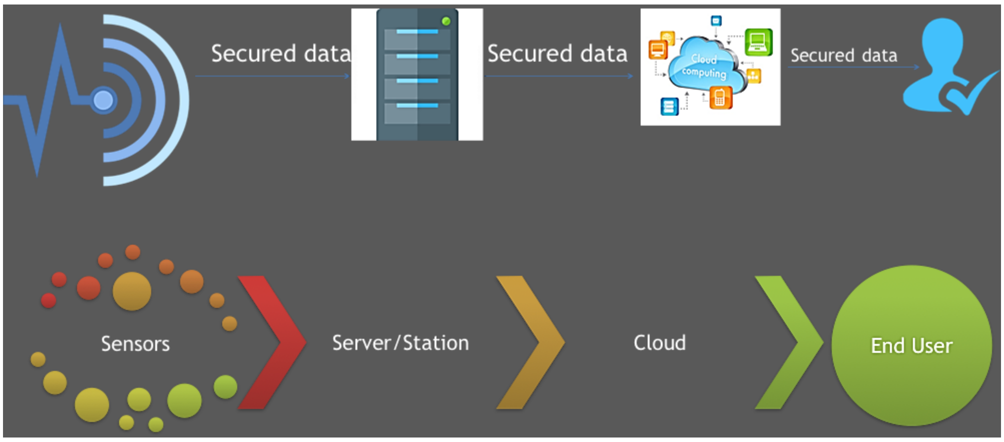
Key register: Here the key is produced for every round is stored group instruction on 8-bit framework.

CHAPTER - 3

SYSTEM DEVELOPMENT



FUNDAMENTAL DESIGN:

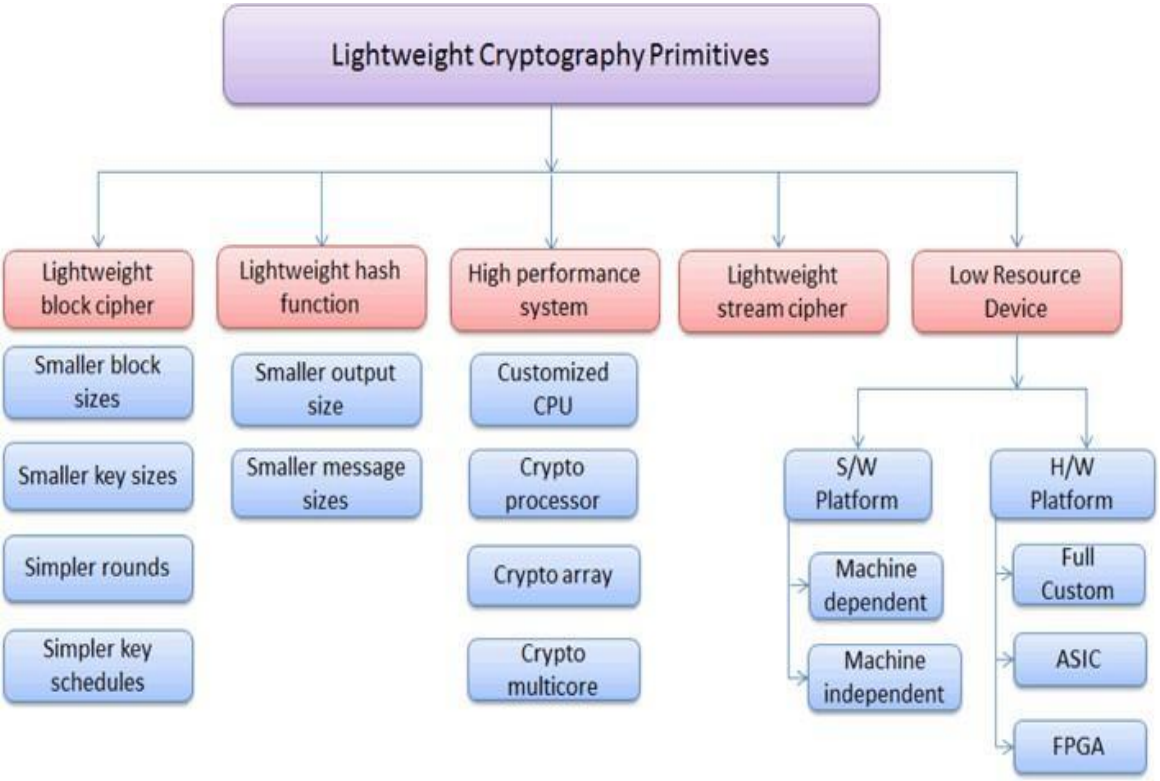


In this data will be sensed from the sensors and then the data is encrypted and is passed through the server station to cloud and the end user will be able to find the data on the cloud which is in the encrypted form. End user can decrypt the data using the cipher key and use the data, in this way data remain secure throughout the process of transmission.

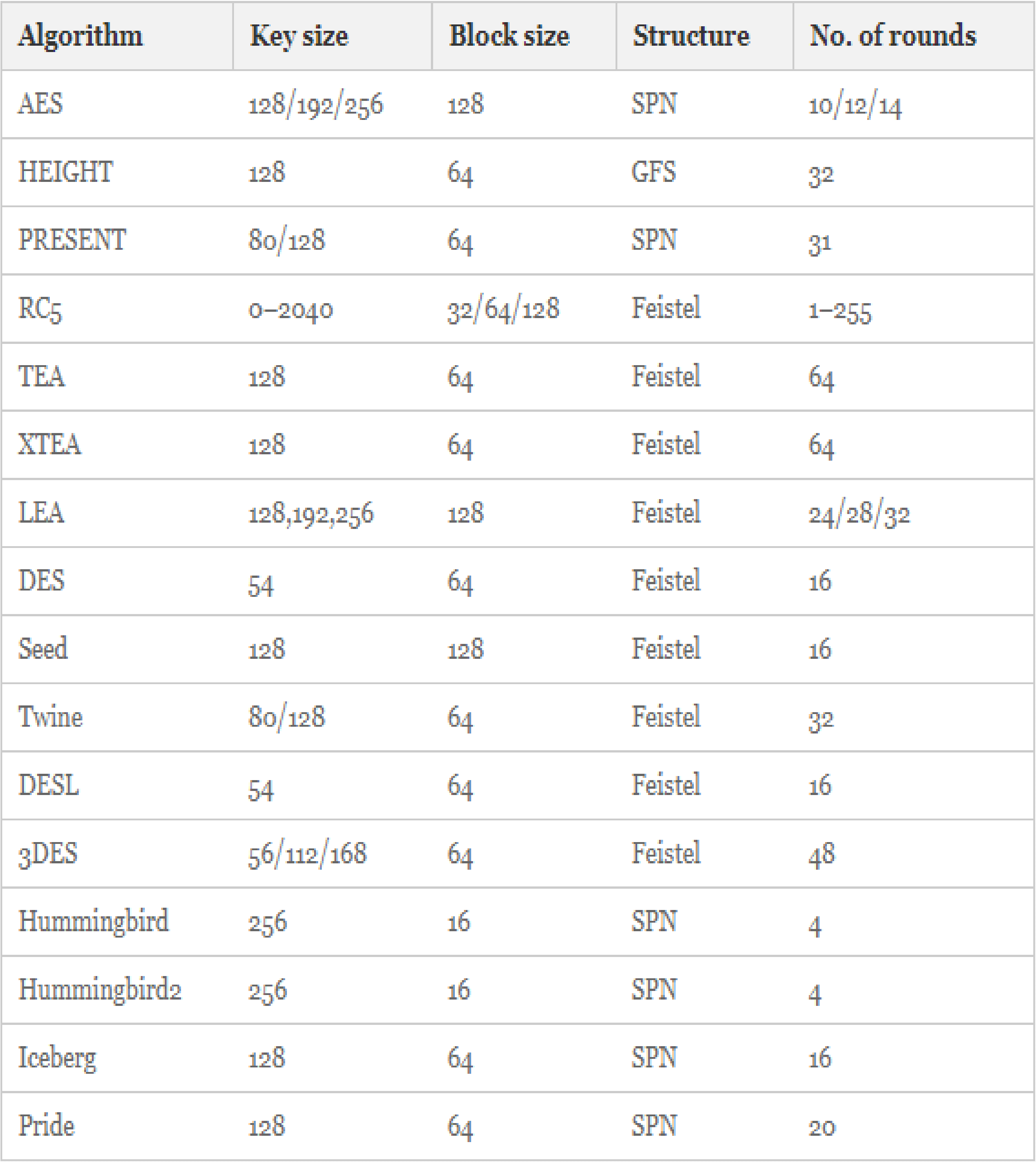
Elementary Lightweight Cryptography:

In this section we will talk about the various natives of light-weight cryptographic algorithm as appeared in Diagram no and furthermore, we show some light-weight calculations in the Table-dependent on their square length, number of rounds, key magnitude, structure.

Elementary Lightweight Cryptography:



Few cryptography algorithms



Algorithm	Key size	Block size	Structure	No. of rounds
AES	128/192/256	128	SPN	10/12/14
HEIGHT	128	64	GFS	32
PRESENT	80/128	64	SPN	31
RC5	0–2040	32/64/128	Feistel	1–255
TEA	128	64	Feistel	64
XTEA	128	64	Feistel	64
LEA	128,192,256	128	Feistel	24/28/32
DES	54	64	Feistel	16
Seed	128	128	Feistel	16
Twine	80/128	64	Feistel	32
DESL	54	64	Feistel	16
3DES	56/112/168	64	Feistel	48
Hummingbird	256	16	SPN	4
Hummingbird2	256	16	SPN	4
Iceberg	128	64	SPN	16
Pride	128	64	SPN	20

Advanced Encryption Standard

We demonstrate the different natives of lightweight cryptography algorithm and furthermore, we have outlined a few lightweight calculations inside the table on their square length, scope of rounds, structure and key size.

The upper hand of Advanced Encryption Standard is:

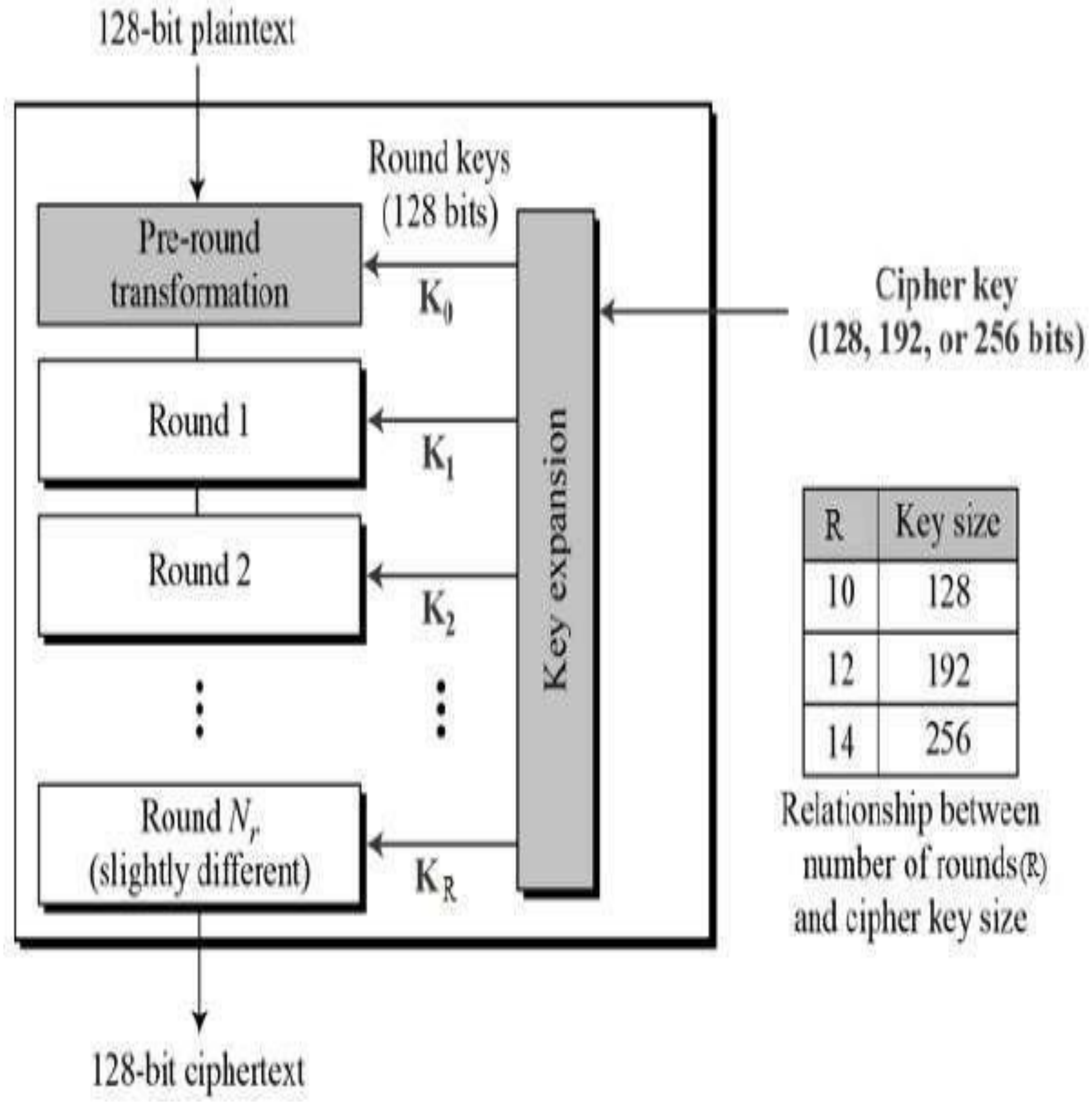
Symmetric key symmetric square code
128-bit data can be transferred
128 or 192 or 256-bit key size
Powerful and quicker than Triple D.E.S
Generate full specification and outline details
Software feasible in C and Java language

Performance of Advanced Encryption Standard:

Work are frequently reached out for thick systems to encourage right and higher analysis contrasted with condition of fine art. Separate investigation might be depleted creating against impact conventions for stationary, moderate or quick paced R.F.I.D Sensor coordinated gadgets whenever conceivable outcomes of group or networks change with elapsed time. Security is high all through bunch of encryptions.

Boxes with solitary cryptography are more grounded Substitution box. The idea of our DESL algo is actually equivalent to the DES calculation, aside from the (I.P) and wiring and the S-box.

The simplified Advanced Encryption Standard design:

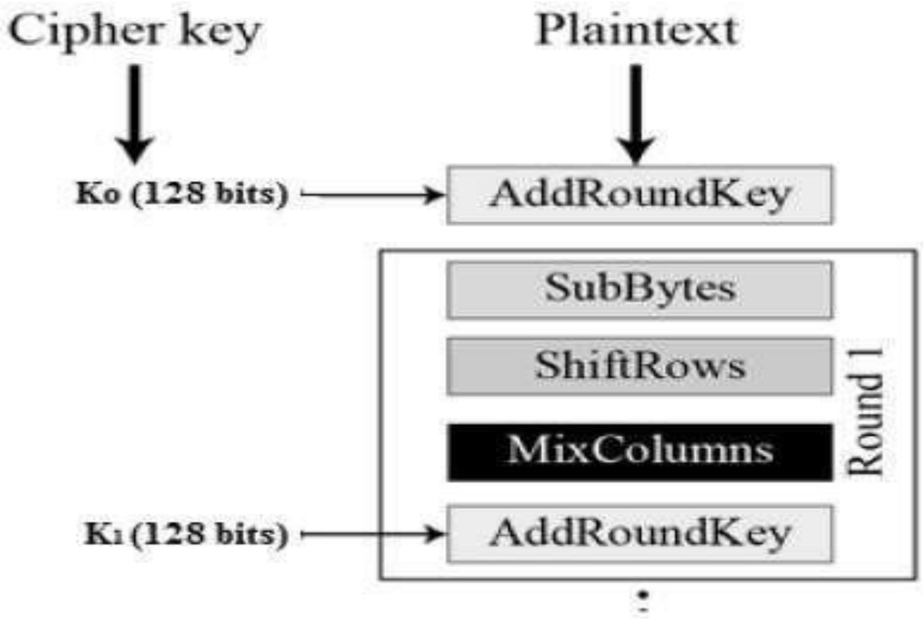


R	Key size
10	128
12	192
14	256

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

Encryption Process

Procedure of encryption in Advanced Encryption Standard:



Byte Substitution

The input bytes (16 bytes) are replaced by looking up values in S-box and the values results in a matrix of 4x4.

Shift rows

Shift rows method consists following steps in order:

1. First row is not shifted.
2. Second row is shifted one-byte position to the left.
3. Third row is shifted two positions to the left.
4. Fourth row is shifted three positions to the left.
5. The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other in 4x4 matrix.

Decryption Process

Add round key

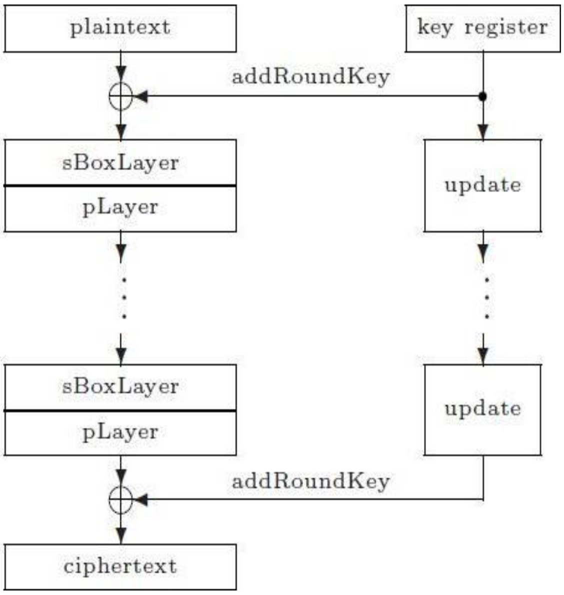
Mix columns

Shift rows

Byte substitution

PRESENT

```
generateRoundKeys()
for i = 1 to 31 do
addRoundKey(STATE,$K_i$)
sBoxLayer(STATE)
pLayer(STATE)
end for
addRoundKey(STATE,$K_{32}$)
```

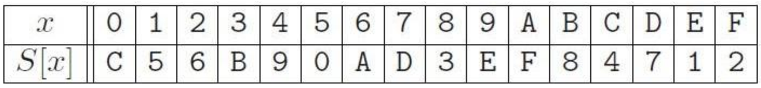


These diagrams and others are back of an envelope wherever we tend to accept necessities: 32-bit arithmetic ADD, 32-bit XOR, SHIFT, 192 bits. All diagrams do not have any administration rationale which could significantly build the predetermined space. Everything about thirty-one circular comprises of associate XOR task to present a round key for $1 \leq j \leq 32$, wherever K_{32} is utilized for post brightening, a straight bitwise permutation and an indirect substitution layer. The indirect surface utilizes one 4-bit Substitution box that is connected multiple times in parallel in each circular. The figure is spoken to in pseudo code in Diagram, and each stage is as of now per flip. The look clarification zone unit given in Context four and all through we tend to assortment bits from 0 with bit zero on the best possible of a block or word.

addRoundKey. Given round key Ki = $k^i_{63}\dots k^i_0$ for $1 \le i \le 32$ and current STATE $b_{63}\dots b_0$, addRoundKey consists of the operation for $0 \le j \le 63$,

$$b_j \rightarrow b_j \oplus k^i_j.$$

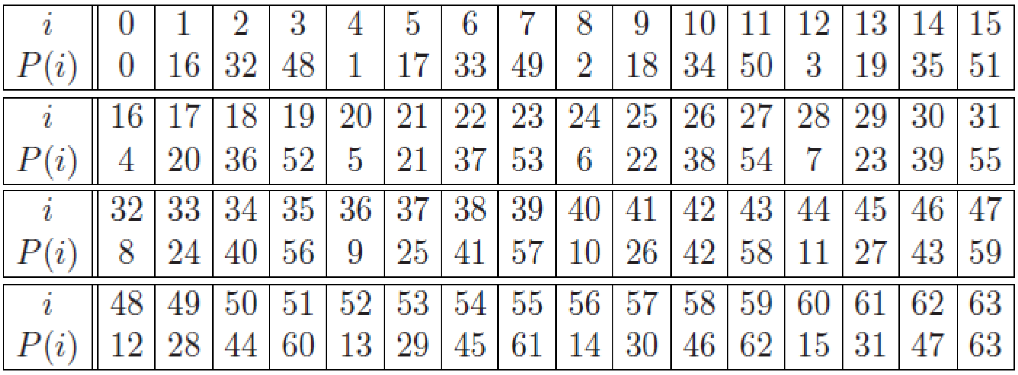
sBoxLayer. The S-box used in PRESENT in a 4-bit to 4-bit S-box $S : F^4_2 \rightarrow F^4_2$. The action of this box in hexadecimal notations given by the following table.



x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

For sBoxLayers the current STATE $b_{63}\dots b_0$ is considered as 16 4-bit words $w_{15}\dots w_0$ where $w_i = b_{4*i+3} \,||\, b_{4*i+2} \,||\, b_{4*i+1} \,||\, b_{4*i}$ for $0 \le i \le 15$ and the output nibble $S[w_i]$ provides the updated state value in the obvious way.

pLayer. The bit permutation used in PRESENT is given by the following table. Bit i of STATE is moved to bit position P(i).

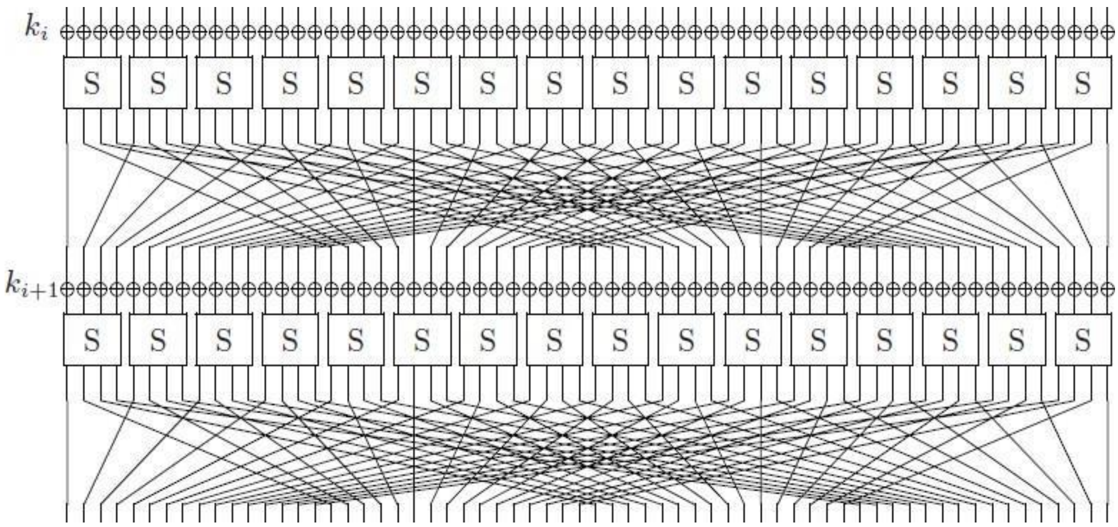


i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P(i)$	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P(i)$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

The key schedule. PRESENT can take keys of either 80 or 128 bits. However, we focus on the version with 80-bit keys. The user supplied key is stored in a key register K and represented as $k_{79}k_{78}\dots k_0$. At round i the 64-bit round key $K_i = k_{63}k_{62}..k_0$ consist of 64 leftmost bits of the current contents of register K. Thus, at the round i we have that:

$$K_i = k_{63}k_{62}\dots k_0 = k_{79}k_{78}\dots k_{16}.$$

After extracting the round key K_i, the key register $K=k_{79}k_{78}\dots k_0$ is updated as follows.

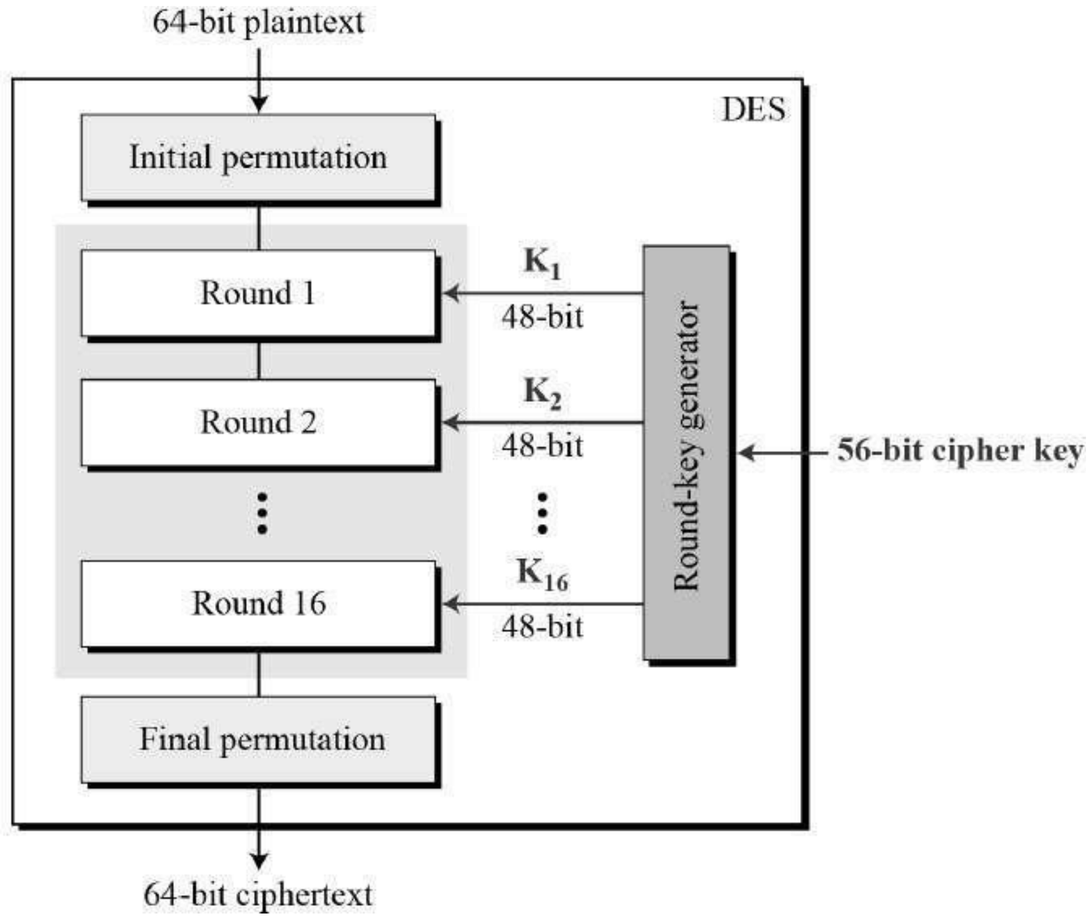


1. $[\mathrm{k}_{79}\mathrm{k}_{78}\dots\mathrm{k}_1\mathrm{k}_0] = [\mathrm{k}_{18}\mathrm{k}_{17}\dots\mathrm{k}_{20}\mathrm{k}_{19}]$
2. $[\mathrm{k}_{79}\mathrm{k}_{78}\mathrm{k}_{77}\mathrm{k}_{76}] = S[\mathrm{k}_{79}\mathrm{k}_{78}\mathrm{k}_{77}\mathrm{k}_{76}]$
3. $[\mathrm{k}_{19}\mathrm{k}_{18}\mathrm{k}_{17}\mathrm{k}_{16}\mathrm{k}_{15}] = [\mathrm{k}_{19}\mathrm{k}_{18}\mathrm{k}_{17}\mathrm{k}_{16}\mathrm{k}_{15}] \oplus \texttt{round\_counter}$

Thus, key register is rotated by 61-bit positions to the left, the leftmost four bits are passed through the PRESENT s-box and the round_counter value i is exclusive-ored with bits $k_{19}k_{18}k_{17}k_{16}k_{15}$ of K with the least significant bit of round_counter on the right. The key scheduled for 128-bit keys is presented in an appendix.

Data Encryption Standard:

Universal structure of Data Encryption Standard:



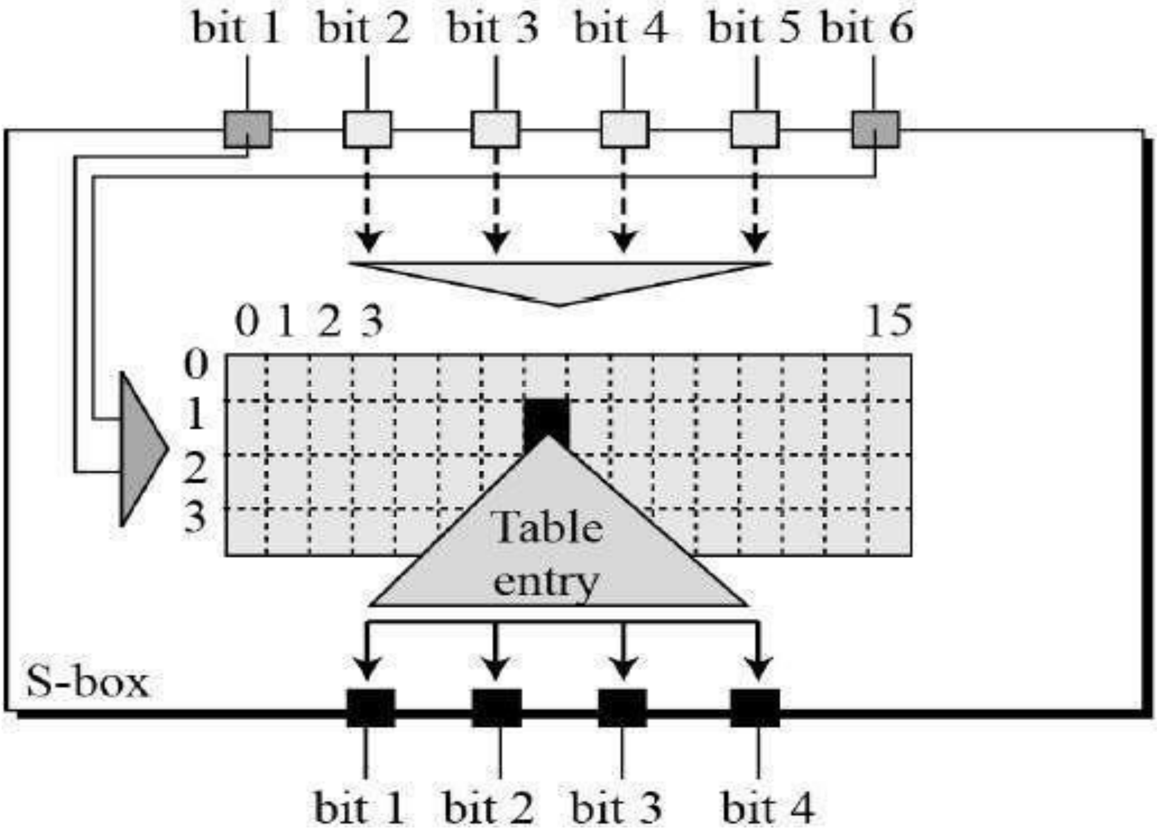
DES require following things:

Round function

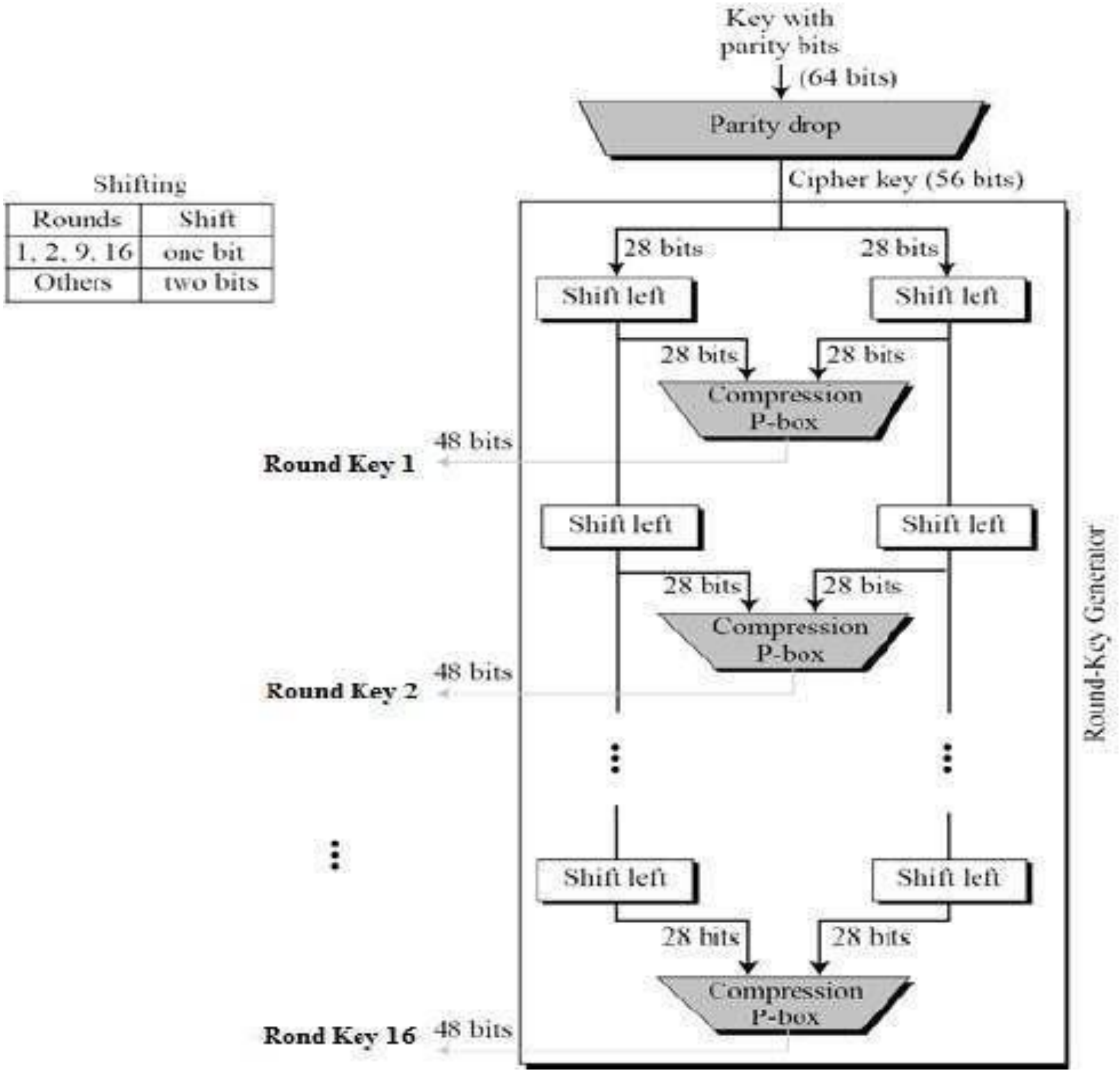
Key scheme

Any further handle − Initial and final permutation

The Substitution-box (S-box) rule is displayed beneath:



Key Generation



DES Analysis:

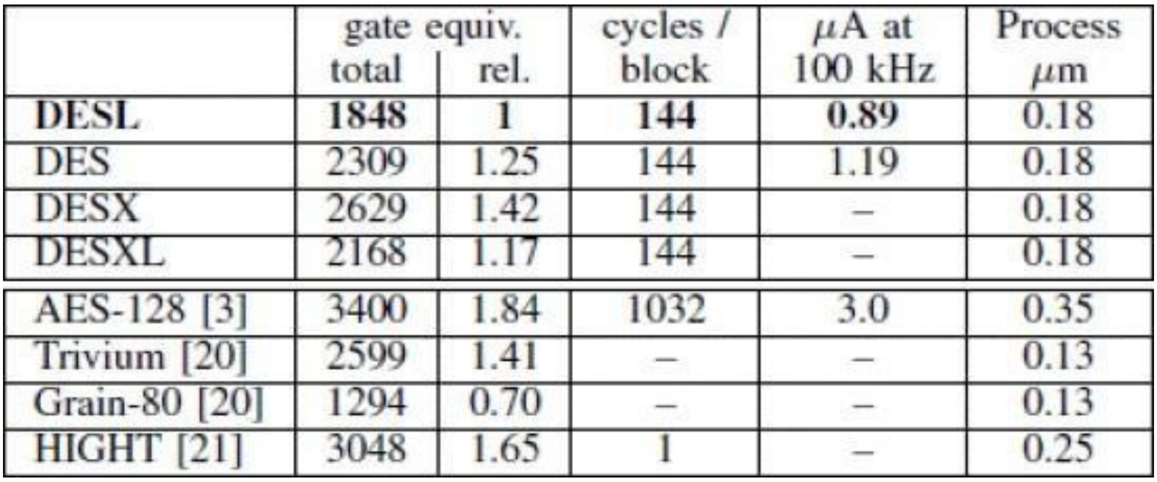
Things that make DES cipher powerful:

Avalanche effect: Little change in the plaintext will results in the large change in the ciphertext.

Completeness: Every piece of the ciphertext relies upon numerous bits of plaintext.

DESL

First difference among DESL and DES is in the f-function. We are supplanting eight unique DES Substitution Boxes with a solitary cryptographically more grounded S-box. The plan of our DESL algo is actually equivalent to the DES algo, aside from the (I.P) and wiring and S-box. The converted s-box module actualizes just a one S-box. As should be obvious in Diagram 2, this module neither require the check control signal nor a yield multiplexer, which spares another 192 transistors.



	gate equiv.		cycles /	μA at	Process
	total	rel.	block	100 kHz	μm
DESL	**1848**	**1**	**144**	**0.89**	0.18
DES	2309	1.25	144	1.19	0.18
DESX	2629	1.42	144	–	0.18
DESXL	2168	1.17	144	–	0.18
AES-128 [3]	3400	1.84	1032	3.0	0.35
Trivium [20]	2599	1.41	–	–	0.13
Grain-80 [20]	1294	0.70	–	–	0.13
HIGHT [21]	3048	1.65	1	–	0.25

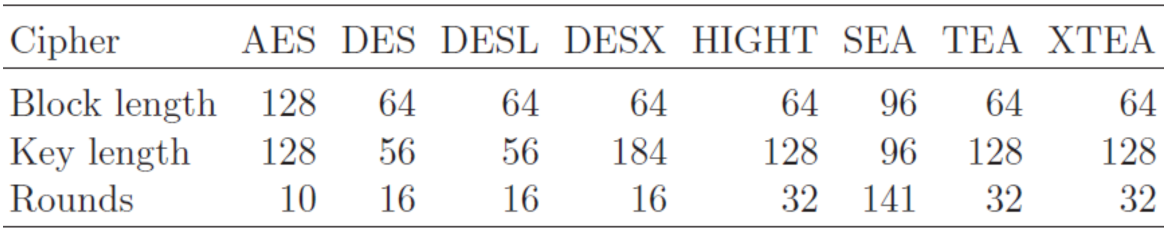
At long last, we can close, that DESL is progressively secure against direct cryptanalysis and the Davies-Murphy assault, increasingly measure upgraded, and more power effective than DES, which makes it particularly appropriate for RFID applications. Besides, DESL is valued to be contemplate as an option for stream figures.

CHAPTER – 4

PERFORMANCE ANALYSIS

Overview

A small explanation of every cipher is provided in this context. An outline of the ciphers' boundaries is being provided in Table. Limits of S.E.A could be selected and the values that fit our execution are being provided in this table:



Cipher	AES	DES	DESL	DESX	HIGHT	SEA	TEA	XTEA
Block length	128	64	64	64	64	96	64	64
Key length	128	56	56	184	128	96	128	128
Rounds	10	16	16	16	32	141	32	32

Different figures like HIGHT utilize 128-bit key to give high security however utilize a littler square size than AES to address the issues of a limited domain. Figures like SEA are kept adaptable in key size so every client may design it for the security objective and execution required.

AES

The heir of Data Encryption Standard is the A.E.S also called Rijndael. National Institute of Standards and Tech as a US F.I.P.S announced it in the yr. 2001. The winner of 5-yr standardization process was the cipher developed by J. Daemen and V. Rijmen. In numerous crypto apps it has been widely applied, being the defacto standard symmetric block cipher. The 128-bit block with a 128, 192 or 256-bits key as input is used by the A.E.S block cipher. 4×4 array of bytes is being operated in it. SubBytes, MixColumns, AddRoundKey and ShiftRows are the 4 stages that are consisted in each round of A.E.S. Because of the possession of the byte-oriented design, A.E.S is well known for its efficiency, principally on the 8-bit arch. The innovation of our assembler inaction of the AES comes from the A.E.S inaction by B. Gladman.

DES

The Data Encryption Standard (DES) is a cipher selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976. The size of block that the block cipher D.E.S is 64 bits. The 64 bits of key are consisted in the algo whereas only the keys used by the algo are 56, furthermore are the parity check bits.

For the reason of Moore’s Law, D.E.S is not considered to be safe.

In rational time D.E.S can be busted by exhaustive key search. EFF D.E.S cracker and COPACABANA are the numerous established D.E.S crackers. Attacks such as linear cryptanalysis, Davies’ attack and differential cryptanalysis are also been issued.

D.E.S and some other alternative of D.E.S are still being used in some apps where there is no issue of security. DESX the block cipher DESX (or DES-X) is an addition to D.E.S. It is defined by DESXK, K1, K2 (M) = K2 $\oplus$DESK(M $\oplus$K1).

D.E.S.L like the above mentioned DESX DESL (DES Lightweight Extension) is an addition to D.E.S to obey with the demands of small computational gadgets like Smart Cards R.F.I.D gadget.

S-box that is being repeated 8 times is used to deduce the size requirement of the chip. Therefore, it uses 38% less transistors than the smallest DES implementation issued.

HIGHT

HIGHT is a block of a 64-bit block length and a 128-bit key length. It was proposed to be used for computing devices such as a sensor in U.S.N or a R.F.I.D tag at CHES ’06 due to its low- resource hardware implementation. Like many of the discussed ciphers, HIGHT makes use of simple operations such as exclusive-or, addition mod 28, and bitwise rotation. The cipher is a variant of generalized Feistel network. It consists of an initial transformation, 32 rounds using 4 sub keys at a time, a final transformation and a key schedule producing 128 sub keys. HIGHTs key schedule algorithm is designed to keep the original value of the master key after generating all whitening keys and all sub keys. Therefore, the sub keys are generated on the fly in encryption and decryption.

SEA

The Scalable Encryption Algorithm SEA (n, b) is designed to be parametric in plaintext or key and processor size.
SEA (n, b) parameters in our case are plaintext or key size of 96-byte, processor word size 8 byte and number of words per Feistel branch 6 byte.
Therefore, we have a suggested number of cipher rounds are 92 rounds.
As we used the standard implementation provided by the author, we have 94 rounds.

SEA is used for the systems and processors having limited instruction set. It uses only bit operations such as addition mod 2b, word rotation, exclusive-or, bit rotation and S-box.

TEA

Focal point of the T.E.A design is on implementation and simple illustration. TEA is a block-cipher operating on 64-bit blocks with a 128-bit key. The Feistel structure is dominated by suggested 64 same rounds consisting of bit operations like shift, add / sub, mod 28 and exclusive-or operations.

XTEA

The effective key size of Tiny encryption algorithm is 126 bits instead of 128 bits. Therefore, two adjustments were made in 1996, the first adjustment was to change the main code/program and second adjustment is to present the main material more slowly. After the adjustments the algorithm will become more secure and the vulnerabilities are repaired without making the algorithm complex.

RESULTS

We present the consequences of our usage. The outcomes are contrasted with a usage of the A.E.S that was upgraded for the 8-bit A.V.R microcontroller condition also. The correlation centres around code estimate, since memory is a significant for size and cost of an implanted or universal gadget, and on execution time, for example throughput, as execution time compares to the power utilization of a gadget

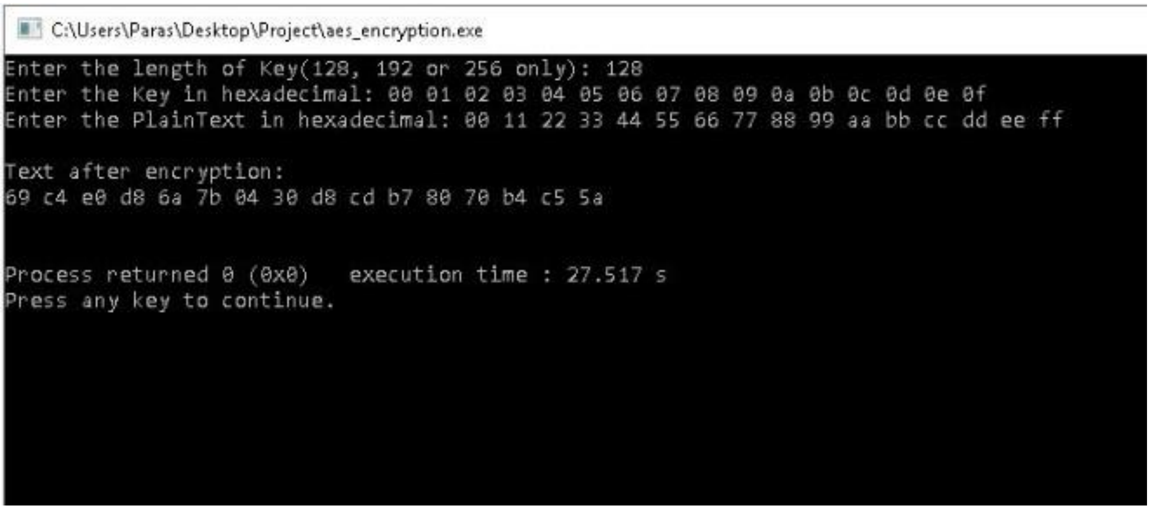
TESTING

Testing the algorithm for the correctness using a plaintext and cipher key.

Key: **00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f**

Plaintext: **00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff**

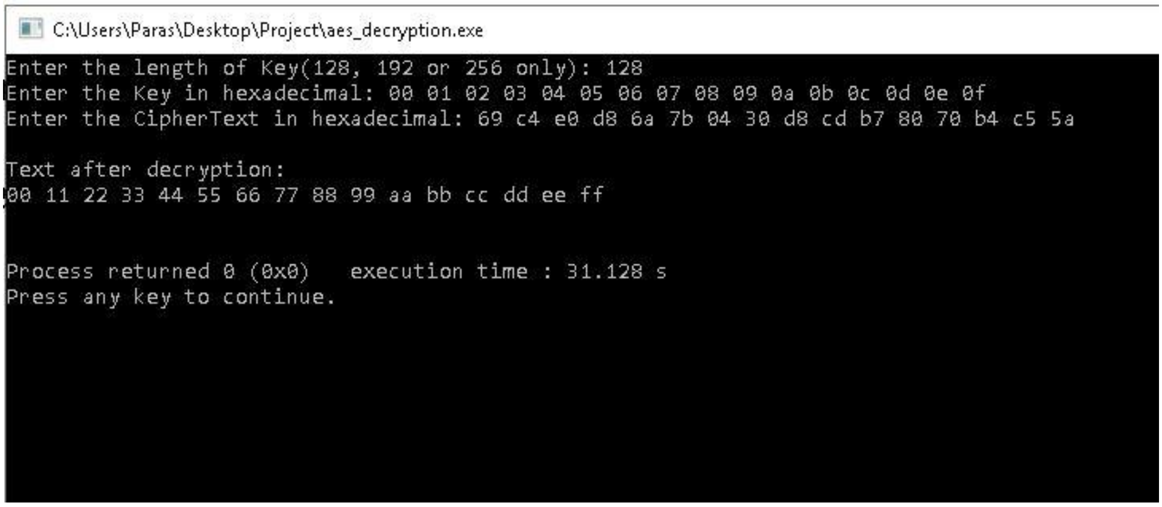
Encryption



C:\Users\Paras\Desktop\Project\aes_encryption.exe

```
Enter the length of Key(128, 192 or 256 only): 128
Enter the Key in hexadecimal: 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
Enter the PlainText in hexadecimal: 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff

Text after encryption:
69 c4 e0 d8 6a 7b 04 30 d8 cd b7 80 70 b4 c5 5a


Process returned 0 (0x0)   execution time : 27.517 s
Press any key to continue.
```

Decryption



C:\Users\Paras\Desktop\Project\aes_decryption.exe

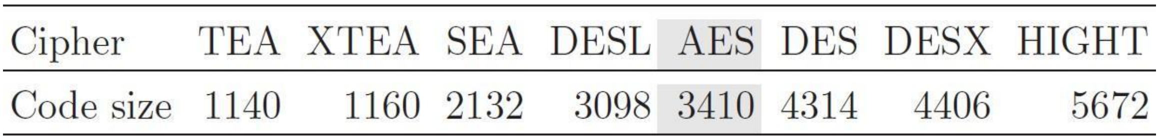
```
Enter the length of Key(128, 192 or 256 only): 128
Enter the Key in hexadecimal: 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
Enter the CipherText in hexadecimal: 69 c4 e0 d8 6a 7b 04 30 d8 cd b7 80 70 b4 c5 5a

Text after decryption:
00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff


Process returned 0 (0x0)   execution time : 31.128 s
Press any key to continue.
```

MEMORY USAGE

As installed framework improvement is unequivocally cost driven, there are high limitations in the span of accessible Flash memory and SRAM. This manifest much more to applications like pervasive registering or even R.F.I.Ds, where power utilization is a significant issue, as well. The Flash memory of the gadget is utilized to store code and investigate tables, if required. Little SRAM is utilized for dynamic access while execution of program.

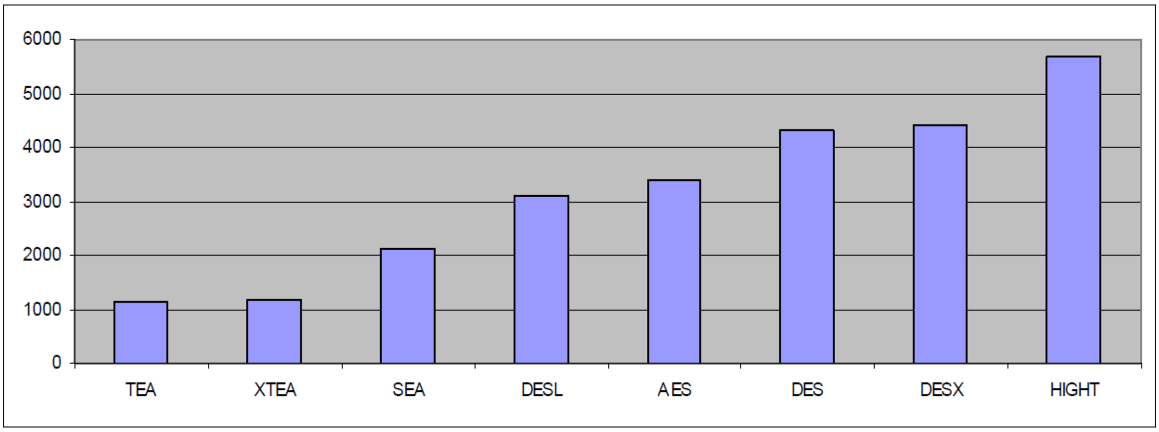
Table below demonstrates the memory distribution in flash memory of each cipher. Figure 1 demonstrates the outcomes requested by size.

Memory allotment of Ciphers in Flash memory (in Bytes)



Cipher	TEA	XTEA	SEA	DESL	AES	DES	DESX	HIGHT
Code size	1140	1160	2132	3098	3410	4314	4406	5672

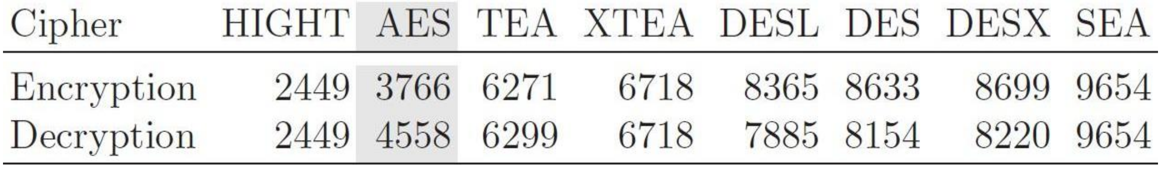
Size of various ciphers in bytes



PERFORMANCE

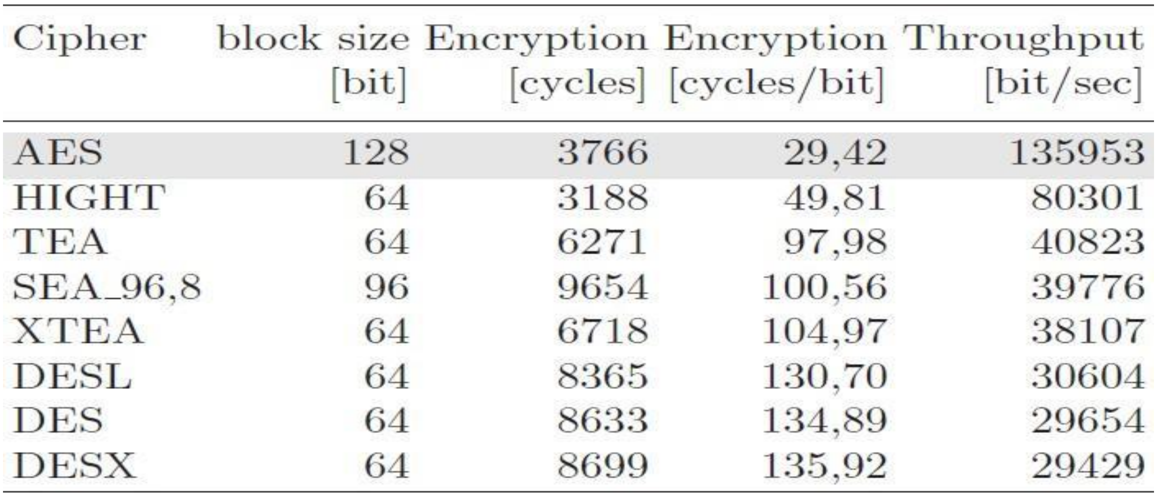
Processes are frequently stretched out for advanced systems to ask right and higher investigation contrasted with state of fine art. Separate investigation might be depleted creating hostile to impact conventions for stationary, moderate or quick paced R.F.I.D sensor incorporated gadgets whenever conceivable outcomes of bunch or network adjustment with elapsed time is high all through group authentication.

CPU cycles used by algorithms in encryption and decryption process:



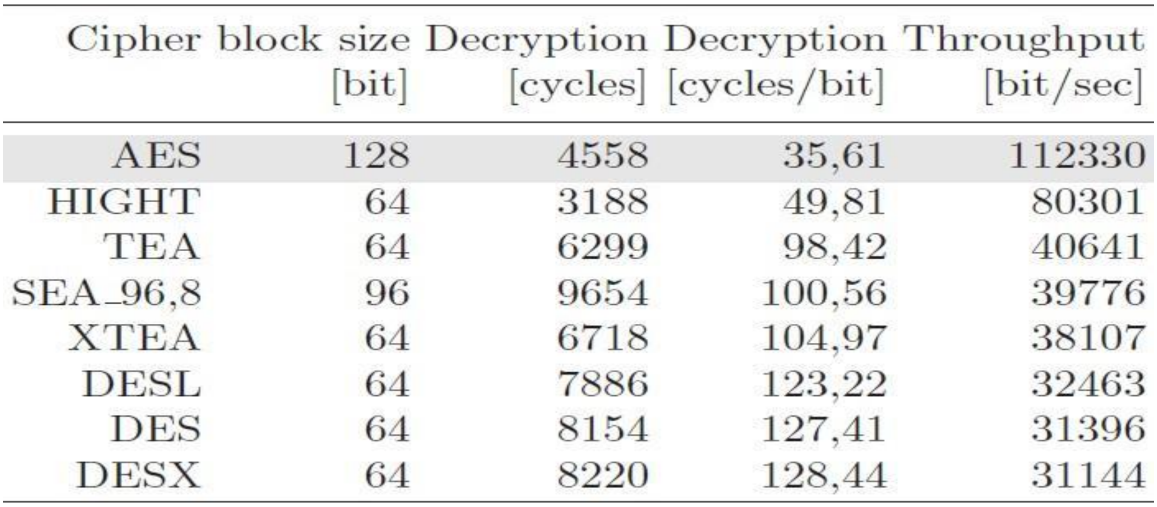
Cipher	HIGHT	AES	TEA	XTEA	DESL	DES	DESX	SEA
Encryption	2449	3766	6271	6718	8365	8633	8699	9654
Decryption	2449	4558	6299	6718	7885	8154	8220	9654

Throughput while Encryption Process



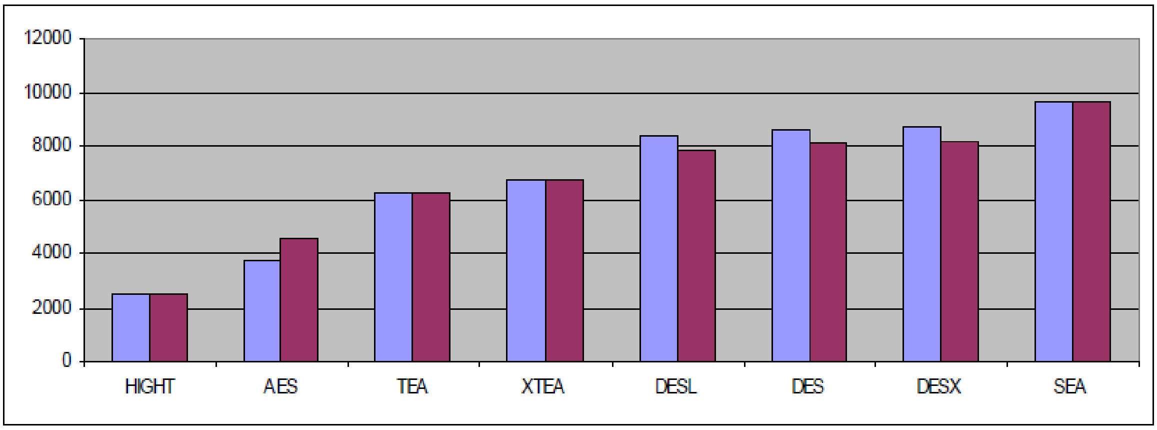
Cipher	block size	Encryption	Encryption	Throughput
	[bit]	[cycles]	[cycles/bit]	[bit/sec]
AES	128	3766	29,42	135953
HIGHT	64	3188	49,81	80301
TEA	64	6271	97,98	40823
SEA_96,8	96	9654	100,56	39776
XTEA	64	6718	104,97	38107
DESL	64	8365	130,70	30604
DES	64	8633	134,89	29654
DESX	64	8699	135,92	29429

Throughput while Decryption Process

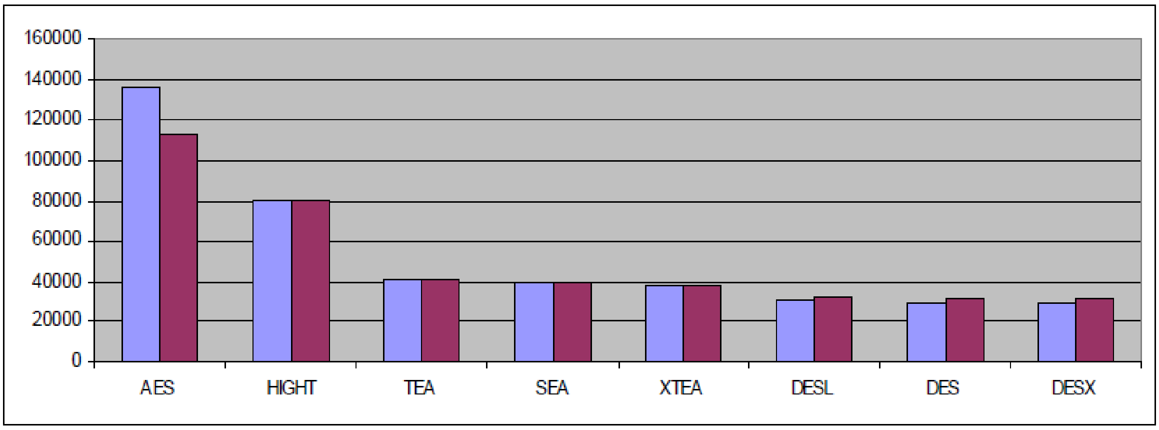


Cipher	block size	Decryption	Decryption	Throughput
	[bit]	[cycles]	[cycles/bit]	[bit/sec]
AES	128	4558	35,61	112330
HIGHT	64	3188	49,81	80301
TEA	64	6299	98,42	40641
SEA_96,8	96	9654	100,56	39776
XTEA	64	6718	104,97	38107
DESL	64	7886	123,22	32463
DES	64	8154	127,41	31396
DESX	64	8220	128,44	31144

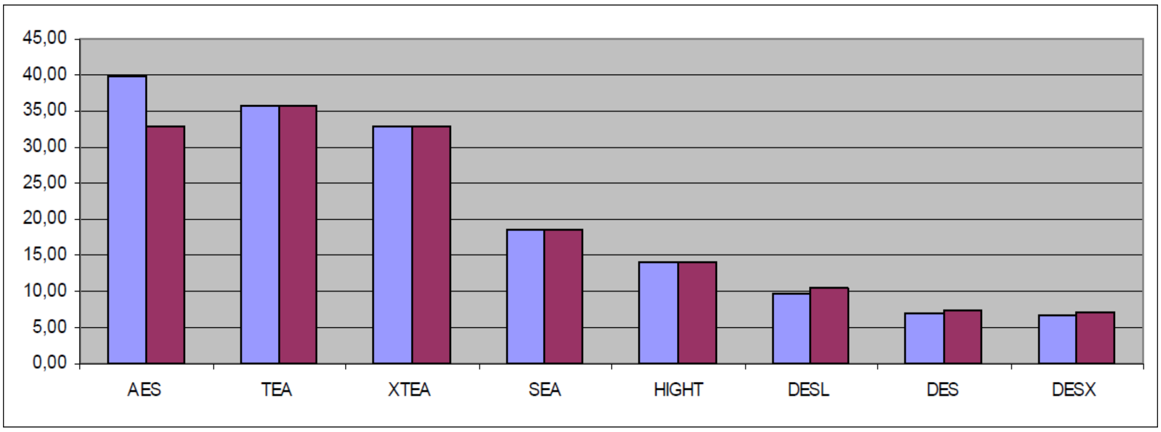
Cycle compute of ciphers



Throughput of decryption and encryption



Throughput cryptograph size balance of coding and decoding.



CHAPTER-5

CONCLUSION

Lightweight cryptography algorithms have been gove over by us personally. Numerous gadgets with low-power can process in IoT condition. These segments are constrained/confined with size, battery life-cycle, power consumed, and activities performed. While security and protection challenges are perceived, the issue of IoT gadgets remains a worry in light of the significance of keeping up trust among IoT clients. Likewise, we have a synopsis of the lightweight assortments of lightweight cryptographic algo that are simple to implement for hardware and bundle process. A portion of the assaults of cryptanalytic calculations are demonstrated by styles, which we have the inclination related with the portrayed archive. It is fundamental to advance a protected and lightweight cryptography algo that utilizes a little space, a quick procedure and a low power utilization. Amid this article, we have the chance to design a subject that will be executed in a savvy home condition. Work are frequently stretched out for thick systems to encourage right and higher investigation contrasted with condition of craftsmanship. We tend to make reference to issues, for example, the structure of the diagram, the span of the block, the extent of the key, the new digital assaults. Later on, we will research, however this arrangement is costly and, if fitting, for the influenced condition. Likewise, an equation must be built up that relies upon the edge of every parameter of the gadget, which has just been sorted out for our arranging point.

REFRENCES

1. Seung-Tae Khang, Jong Won Yu, Wang-Sang Lee, "Compact folded dipole rectenna with RF-based energy harvesting for IoT smart sensors", Electronics Letters, vol. 51, no. 12, pp. 926-928, 2015.

2. Godfrey Anuga Akpakwu, Bruno J. Silva, Gerhard P. Hancke, Adnan M. Abu-Mahfouz, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges", Access IEEE, vol. 6, pp. 3619-3647, 2018.

3. Dechuan Chen, Weiwei Yang, Jianwei Hu, Yueming Cai, Xuanxuan Tang, "Energy-Efficient Secure Transmission Design for the Internet of Things with an Untrusted Relay", Access IEEE, vol. 6, pp. 11862-11870, 2018.

4. Zhi-Kai Zhang , Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, “IoT Security: Ongoing Challenges and Research Opportunities”, IEEE, 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, pp 2163-2871, 2014

5. Kruthika Rathinavel, Manisa Pipattanasomporn, Murat Kuzlu, Saifur Rahman, "Security concerns and countermeasures in IoT-integrated smart buildings", Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) 2017 IEEE, pp. 1-5, 2017.

6. Litun Patra, Udai Pratap Rao, "Internet of Things — Architecture applications security and other major challenges", Computing for Sustainable Global Development (INDIACom) 2016 3rd International Conference on, pp. 1201-1206, 2016.

7. Lijing Zhou, Licheng Wang, Yiru Sun, Pin Lv, "BeeKeeper: A Blockchain-Based IoT System With Secure Storage and Homomorphic Computation", Access IEEE, vol. 6, pp. 43472-43488, 2018.

8. Aruna U. Gawade, Narendra M. Shekokar, "Lightweight Secure RPL: A Need in IoT", Information Technology (ICIT) 2017 International Conference on, pp. 214-219, 2017.