Contemporary Light Weight Cryptography in IoT: Comparative Study and Scope of Improvements

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

in

Computer Science and Engineering

By

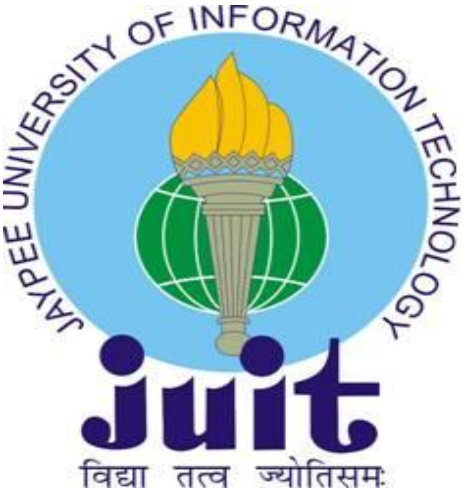
Chaitanya Negi (141341)

Ayush Sharma (141380)

Under the supervision of

Dr. Hemraj Saini

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 **"Contemporary Light Weight Cryptography in IoT: Comparative Study and Scope of Improvements"** in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering** 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 2017 to December 2017 under the supervision of **Dr. Hemraj Saini** Associate Professor ,Department of CSE and IT.

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

Chaitanya Negi (141341) Ayush Sharma (141380)

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

Dr. Hemraj Saini

Associate Professor

Department of CSE and IT

Dated:

ACKNOWLEDGEMENT

It is our privilege to express our sincerest regards to our project supervisor **Dr. Hemraj Saini** for their valuable inputs, able guidance, encouragement, whole-hearted 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 "Contemporary Light Weight Cryptography in IoT: Comparative Study and Scope of Improvements" at our department premises for the partial fulfilment of the requirements leading to the award of B-Tech degree.

At the end I would like to express my sincere thanks to all my friends and others who helped me directly or indirectly during this project work.

Date: May, 2018

Chaitanya Negi(141341)

Ayush Sharma(141380)

TABLE OF CONTENTS

CERTIFICATE……......**i**

ACKNOWLEDGEMENT…….....**ii**

LIST OFABBREVIATIONS……...……**iv**

LIST OF FIGURES…….…… **v**

LIST OF GRAPHS…….…….……**vi**

LIST OF TABLES ……..…… **vii**

ABSTRACT……..... **viii**

CHAPTER-1 INTRODUCTION

1.1 INTRODUCTION 1
1.2 PROBLEM STATEMENT 4
1.3 OBJECTIVES 5
1.4 METHODOLOGY 6

CHAPTER-2 LITERATURE SURVEY 9

CHAPTER-3 SYSTEM DEVELOPMENT 20

3.1 ADVANCED ENCRYPTION STANDARD (AES) 25
3.2 PRESENT 28
3.3 DATA ENCRYPTION STANDARD (DES) 31
3.4 DESL 34

CHAPTER-4 PERFORMANCE ANALYSIS 35

CHAPTER-5 CONCLUSION

5.1 CONCLUSION 42

FUTURE SCOPE 43

REFRENCES 45

LIST OF ABBREVIATIONS

IoT	Internet Of Things
RFID	Radio-Frequency Identification
AES	Advanced Encryption Standard
HIGHT	High security and lightweight
ECC	Elliptic Curve Cryptography
TEA	Tiny Encryption Algorithm
UDP	User Datagram Protocol
CoAP	Constrained Application Protocol
DES	Data Encryption Standard
FIPS	Federal Information Processing Standard
SEA	Scalable Encryption Algorithm
QoS	Quality of service
&	And

LIST OF FIGURES

1.) LITERATURE SURVEY ……...9

1.1) Encryption-based Countermeasure against attack on data collection……...13

1.2) Example of lightweight cryptography applications……...13

1.3) An example of block cipher mode of operation……....15

1.4) Demonstration of Present Algorithm……22

2.) SYSTEM DEVELOPMENT…….

2.1) Light-weight cryptographic primitives…….23

2.2) Schematic of A.E.S structure……....26

2.3) Encryption Process of A.E.S……27

2.4) Present Algorithm……28

2.5) D.E.S …….....31

LIST OF GRAPHS

1.) PERFORMANCE ANALYSIS……... 43

1.1) Code size of ciphers in bytes……38

1.2) Cycle count of ciphers……..40

1.3) Throughput of encryption and decryption……....41

1.4) Throughput code size ratio of encryption & decryption……..41

LIST OF TABLES

1.) INTRODUCTION…….....1

1.1) Comparison of symmetric Lightweight Cryptography algorithms in …….7

2.) LITERATURE SURVEY ……..…...9

2.1) The Comparison of Light weight Cryptographic Algorithms……12

3.) SYSTEM DEVELOPMENT…….....20

2.1) Some light-weight cryptographic algorithms……..……....24

4.) PERFORMANCE ANALYSIS…….…….....35

2.1)Memory allocation of program code in Flash in bytes…….…….38

2.2) Performance of encryption and decryption in measured CPU cycles…..…...39

2.3) Throughput of encryption…….……39

2.4) Throughput of decryption…….…...….40

ABSTRACT

The Internet of Things (IoT) is a new-fashioned technology that is the future of the next era of the internet which connect various physical objects that communicate with each other without the aid of human interactions.

With the IoT system that make use of data values in the real world, that data collected from devices can also be a target of cyber-attacks.

Security plays important role in network to prevent the unauthorized access, misuses of data, monitoring and data, modification etc. All layer in IoT architecture security considered as extremely important from viewpoint of designing criteria from bottom label to top label. IoT application is becoming important in day to day lifestyle such as healthcare, smart grid, smart home, smart parking.

IoT application is useful to people but if the IoT system can't protect the user data from hacker, attacks, and vulnerabilities. Lightweight encryption is a sector of a classical cryptographic algorithms that is pertinent for resource constrained devices in IoT.

Related work for lightweight techniques used for secure data transmission is described in this report.

CHAPTER- 1

INTRODUCTION

On a brand new computing setting known as “Internet of Things (IoT)” or “Smart Object” networks, lots of forced devices are connected to the web. The devices act with one another by the network and supply new expertise to us. so as to relish this new setting, security of forced finish nodes is vital. If one in every of the nodes were compromised, the network may be suffered seriously. However, it's tough to implement comfortable scientific cryptographic functions on forced devices because of the limitation of their resources.

The preparation of tiny computing devices like Radio Frequency Identification (R.F.I.D) tags, industrial controllers, detector nodes and sensible cards is turning into rather more common. The shift from desktop computers to tiny devices brings a good vary of recent security and privacy considerations. It's difficult to use standard cryptological standards to tiny devices. In several standard cryptological standards, the trade-off between security, performance and resource needs was optimized for desktop and server environments, and this makes them tough or not possible to implement in resource-constrained devices. once they is enforced, their performance might not be acceptable.

Lightweight cryptography could be a sub-field of cryptography that aims to produce solutions tailored for resource-constrained devices. There has been a large quantity of labour done by the tutorial community associated with light-weight cryptography; this includes economical implementations of standard cryptography standards, and therefore the style and analysis of recent light-weight algorithms and protocols.

Cryptography and secret writing are used for secure communication for thousands of years. Throughout history, military communication has had the best influence on secret writing and therefore the advancements therefrom. The requirement for secure industrial and personal communication has been junction. Age, that began within the 1980's. though the net had been unreal within the late 1960's, it didn't gain a public face till the globe Wide net was unreal in 1989. the globe Wide net is associate electronic protocol that permits folks to speak mail,

information, and commerce through a digital medium. This new methodology of data exchange has caused an incredible want for information security. A proper understanding of cryptography and it's secret writing can facilitate folks develop higher ways that to shield valuable data as technology becomes quicker and more powerful.

Internet of Things (IOT) may be a novel worldview that's quickly creating progress within the field of up-to-date remote media communication. IoT may be a international movement that data, processes, unites folks and things to make network connections that area unit additional pertinent and helpful than ever before. It's a system of reticular computing things, like sensors, R.F.I.D tags, actuators, and cell phones; digital machines; and other people that gives the flexibility to transfer knowledge over a network while not requiring human-to-computer or human-to-human interactions.

According to the report in IoT, that exclude Personal Computers, tablets, and smartphones, can generate about $300 billion in revenue till 2020. Moreover, the amount of smartphones and tablets can reach up to 7.03 billion units by 2020. These devices can produce a large and complicated network wherever a vast quantity of information is communicated throughout the network. As IoT is growing speedily, it faces risks and challenges, like a way to handle vast amounts of information, process power upset energy consumption, address security threats, and the way to encrypt/decrypt of big information.

To address these challenges when several sensible devices are connected in an IoT surroundings, the increasing demand for the utilization of applicable cryptographic answer into the embedded applications. However, these sensible devices typically have forced resources or they will be known as low-resource devices with reference to their low computation power, restricted battery life, small size, little memory, and restricted power provide.

Moreover, the tight constrains inherent the mass developments of sensible devices that clogging the necessities of developing a replacement cryptanalytic algorithmic rule, that performs sturdy security mechanism, encryption/decryption, with low power applications and different functionalities for the pervasive computing. This new research space is referred as light-weight cryptography.

The two main reasons for switching to new technology for IoT are listed below.

“Efficiency of end-to-end communications” to use the light-weight symmetry key formula so as to realize end-to-end security and with lower power consumption within the low resources devices.

“Adoptability in low resources smart devices” - Lightweight cryptography’s footprints are a lot of smaller than classical ones. It's the probabilities of additional network reference to lower resource sensible devices.

Cryptographic technologies are advancing: new techniques on attack, design and implementation are extensively studied. One of the state-of-the-art techniques is “Lightweight Cryptography (LWC)”. Lightweight cryptography is a cryptographic algorithm or protocol tailored for implementation in constrained environments including RFID tags, sensors, contactless smart cards, health-care devices and so on.
Cryptography and secret writing are used for secure communication for thousands of years. Throughout history, military communication has had the best influence on secret writing and therefore the advancements therefrom. The requirement for secure industrial and personal communication has been junction. Age, that began within the 1980's. though the net had been unreal within the late 1960's, it didn't gain a public face till the globe Wide net was unreal in 1989.

The hardware implementations of lightweight cryptography, energy consumption and/or chip size are the important measures to evaluate the lightweight properties. In software implementations, the smaller code and/or RAM size are preferable for the lightweight applications.

Light-weight cryptography also delivers adequate security. Light-weight cryptography does not always exploit the security-efficiency trade-offs. We have tendency to report recent technologies of light-weight cryptographic primitives.

1.1 PROBLEM STATEMENT

Lightweight cryptography has been a awfully necessary for the previous couple of years, driven by the shortage of primitives capable to run on devices with terribly low computing power. we are able to suppose for example of RFID tags, devices in wireless sensor network or, a lot of typically, tiny internet-enabled appliances expected to flood the markets because the web of Things (IoT) arises.

Many cryptographers have self-addressed these problems by suggesting light-weight stream ciphers, block ciphers, hash operate and recently one-pass authenticated secret writing.

Now one day IoT is accepting homes, work spaces, social spaces or business companies that can open the doors of security and privacy challenges. Therefore, due to security and privacy issues, the main reasons for IoT operational reasons are being found. If damaged, the concept can be avoided that the IoT has an attacker. Many attacks on IoT are like anger, spoofing, service denied, executing attacks, fake signals are injection. These attacks can crush IoT privacy, integrity, and authentication protection services; In addition, it will affect the privacy of users. The IoT provides an early security solution based on each layer, the area of this area is still sensitive to attacks.

Traditional corruption and verification schemes do not match well on its unique resources such as power, real-time implementation in the IOT situation. Therefore, IOL is well-known in lightweight cryptography solutions. There are various types of lightweight centro-symmetric and unwanted cryptography algorithms such as AES, HIGHT, RC5, Present, RSA, ECC and many in literature. This current solution does not guarantee affiliate at maximum level of security in real-time communication for a lot of time processing, code length, and memory needs. The execution time includes key management and time for distribution, encoding and image that decides the protocol's effectiveness. Measures gradually measuring their large key size negatively on the Ecuadorian square scale, while the Center for the symmetric algorithm will provide confidentiality and integrity completely, however no confirmation will be rejected. This will bring real-time information and impact on the process and use its resources.

1.3 OBJECTIVE

A safe solution that will require less power.

A safe and secure solution that is less dangerous than current attacks

Design new ciphers with the goal of having low hardware implementation costs.
Efficiency of end-to-end communication. Application of the lightweight symmetric key algorithm allows lower energy consumption for end devices.

The security services required to be maintained in IoT so as to enhance the trust of users are

Confidentiality: "Data at rest or in transit is only accessible to the sender or receiver."

Integrity: "While data is in transmission no intruder is able to modify the original contents of the data."

Authentication: "The identity of the sender should be verified to the receiver to judge the validity of data."

Authorization: "Only legitimate users are able to access the resources of the IoT and maintain connect among others."

1.4 METHODOLOGY

Symmetric Lightweight Algorithms For IoT

Advanced Encryption Standard (AES): AES is used as an inbuilt solution in COAP at application layer. It is a symmetric block cipher given by NIST. It uses substitution permutation network and works on 4*4 matrix having block length of 128 bits. Every byte gets affected by subbytes, shiftrows, MixedColumns, AddRoundKey. Key size than can be used is 128, 192, 256 bits. AES is still vulnerable to man-in-middle attack.

High security and lightweight (HIGHT): Hight uses very basic operations like addition mod 2^8 or XOR to work for Feistel network. It has a block size of 64 bits, work in 32 rounds on128 bit keys. Its keys are generated while encryption and decryption phase. A parallel implementation of higth was proposed that requires less power, mentioned in few lines of code, and improves speed for RFID systems. Higth is vulnerable to saturation attack.

Tiny Encryption Algorithm (TEA): TEA is used for constrained environments like sensor networks or smart things. It is written in very few lines of code. It does not use a complex program but requires simple operations of XOR, adding and shifting. It uses a block size of 64 bits and 128 bit keys and does not make use of existing tables or any predefined computations. Number of variants exists for TEA like extended TEA, Block TEA and so on. These extensions try to resolve the problems in original TEA like equivalent keys. But still due to its simple operations TEA and its variant are susceptible to number of attacks.

PRESENT: It is based on SPN and is used as ultra lightweight algorithm for security. It works on substitution layer uses 4-bit input and output S-boxes for hardware optimization. It has key size of 80 or 128 bits and operates on 64-bit blocks. PRESENT has been presented as a lightweight cryptography solution in “Lightweight Cryptography”. PRESENT is vulnerable to differential attack on 26 out of the 31 rounds.

RC5: It was first coined by Rivest for rotations that are data independent. It posses Feistel structure and can work well as lightweight algorithm as it is used in wireless sensor scenarios. RC5 is considered as w/r/b, where w refers to word size, r stands for number of working rounds, and b will tell about the number of bytes in encryption key. RC5 generally works on 32 bit size but its variants can be 16, 32, 64. It can work for 0, 1, .., 255 rounds using 0,1,..255 key bytes. Standard key size is 16 byte on 20 rounds of operation. RC5 is vulnerable to differential attack.

Comparison of symmetric Lightweight Cryptography algorithms in 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

Asymmetric Light-weight Algorithms for IoT

RSA: -

RSS works on a public and private key pair by choosing two major key numbers. Find out their modules and select their encryption keys and thus calculate the key of the dishonest. Public key is published openly while private key is stored.

Elliptic Curve Cryptography (ECC): It requires less key size as compared to RSA. Hence it has fast processing and less storage requirements. is built on a geographic system where it takes two points on the LCD curve. The key used to use Disclaimer Cost is used to key the key. Secure hardware processing on ECC is offered for small areas that will get faster in real time. ECC is optimized 6LoWPAN working on its complex zip operation. Instead of using micro-processor operations for multiplying, a small transition is used to optimize for the use of less powerful devices.

CHAPTER -2

LITERATURE SURVEY

2.1 Lightweight Cryptographic Algorithms for IoT

IoT is rising by time, in this increasing era of modern things. modern things may be any physical objects like phone, laptop, AC, charger and lots of additional. IoT may be outlined as a network of unambiguously acknowledgeable, accessible, and manageable sensible things that are capable of communication, computation and supreme higher cognitive process. Things in IoT may be connected via wireless connections.

The IoT needs components to start communication between devices. Objects got to be increased with an Auto-ID technology, generally an RFID tag, so the item is unambiguously identifiable. RFID tag permits the item to wirelessly communicate sure kinds of info, that leads us to a different demand – the power to watch data. RFID tags will be passive, active, or battery assisted passive tags .An active tag has an on board battery and sporadically transmits its ID signal and hold on info. a full of life reader's operating vary will be adjusted from 1m to tens of meters, permitting flexibility in applications like quality direction and management. as a result of its multi beholding, non-line of sight, and high cost-effectiveness, RFID has been wide used for indoor localization to IoT real-time locating applications. The risks involved and services given by RFID systems are protected by cryptographically securing data using light weight algorithms. The risks addressed by the deployment of secure RFID tags include .

1.Counterfeit goods. Cryptography is employed to form RFID tags troublesome to clone or modify. the complete counterfeit craft engines, the risks and liability problems concerned are troublesome to even measure.

2. Secure logging. Tamper resistant recording of environmental data such the temperature is significant in offer chain management of merchandise like recent goods and medical supplies.

3. Privacy protection. The Electronic Product Code (EPC) used in Gen2 differs from product bar codes in that it is indeed unique. It may be used to track an individual tag. This cause raise in serious privacy issues if such tags are attached to personal items. Therefore the RFID tag should also identify the reader as trusted before traceable information.

4. Returns. When a tag is returned to a store or manufacturer an authenticated reset/write mechanism allows it to be reused. The tags maintain some quantity of persistent memory; browse, write and lock operations to the current memory should be authenticated to forestall tamper and unauthorized modification. authenticated reads permit information to be visible just for the tags owner.

2.1.1 Lightweight Cryptography Algorithms designed for implementation in constrained environments where low power and memory is there including sensors, healthcare devices, RFID tags, etc. In hardware implementations, device memory and power consumption are the important things to measure the lightweight properties. In software implementations, the light code or low RAM size are preferred for the lightweight applications. The implementation properties, the light-weight primitives' area unit superior to standard cryptographic ones. light-weight cryptography additionally delivers adequate security. light-weight cryptography doesn't continuously exploit the security-efficiency trade-offs. The report of recent technologies of light-weight cryptographical primitives. Nowadays, within the space of light-weight block cipher a number of the light-weight block ciphers are projected, like present, LBlock, TWINE , KLEIN, MIBS, LED, PRINCE, Piccolo, ITUbee , EPCBC, PRINT cipher and RECT- ANGLE. Structures of those light-weight ciphers as like traditional block ciphers are typically developed into 2 main classical structures: SPNs and Feistel-type structures.

The SPN structure is formed via round function on the full information block. The slow diffusion of the normal Feistel- sort structures has some security issues. Therefore, to unravel these issues the ciphers in ancient Feistel-type structures plenty of rounds in distinction to the ciphers supported SPNs is needed; so, this will increase energy consumption. still, compared to SPNs, the standard feistel-type structures have additional features.

• it has a little and easy round function.

• it's a similar program for encryption and decipherment processes to cut back decipherment implementation price.

Need for light Weight Cryptography Algorithms in IoT

1. Reliability of end-to-end communication: To get security of the data transmitted. For the low powered devices, the cryptographic operation with a restricted quantity of energy consumption is very important.

2. **Applicability to lower resource devices:** The light-weight cryptographic primitives would open prospects of a lot of network connections with lower resource devices. The light-weight cryptographic primitives are smaller than the standard cryptographic ones. However, lowest price devices will embed solely application-specific ICs because of restricted price and power consumption, wherever hardware properties are crucially necessary.

The below Table illustrates the Comparison of Light weight 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

2.2 **Lightweight Cryptography Applicable to Various IoT Devices**

2.2.1 Security Threats and Countermeasures for IoT, (Based on Encryption)

The real security risk of the IOT system from the standard IT system is that the real-world information diagnostics tools will also become the target of cyber tax. For example, by applying information from different types of sensors through the purpose of implementing IOTs on a plant, put in production equipment's and analyzing it and running automatic management management in real time. Improve productivity and stability. If the information of the sensing element should be incorrect in this method, the result of false analysis will be encouraged and the result of an incorrect management will result in a large loss in consequence. In addition, after measuring information and management commands, it is learned that trade and production related secrets are essential to prevent writing.

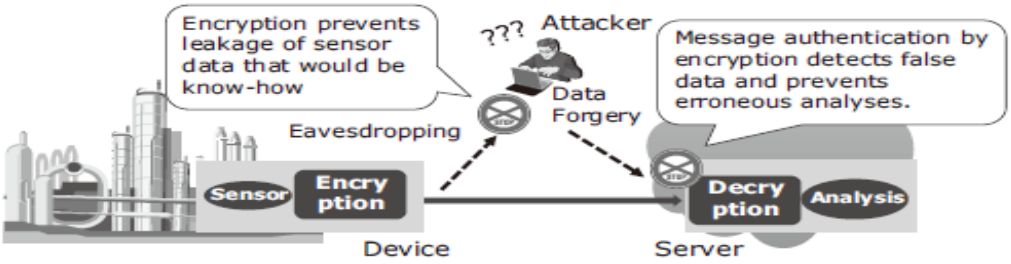


Fig. 1 Encryption-based countermeasure against attack on data collection.

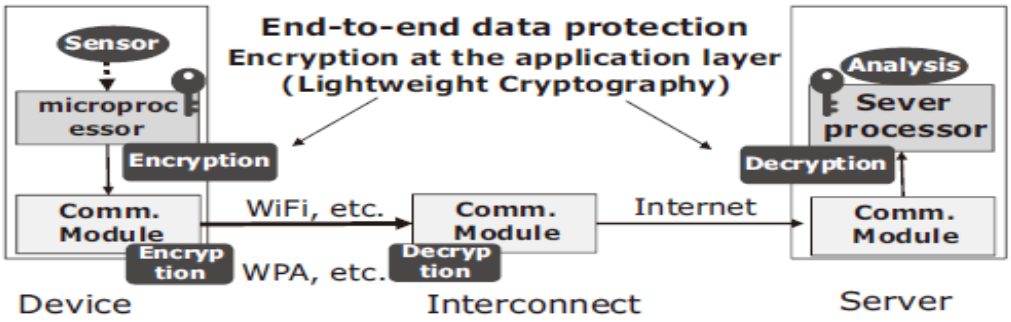


Fig. 2 Example of lightweight cryptography applications.

Crack typing means to handle the elements of the element, to enforce the protection of information for privacy and integrity, which may have a good measure of risk. Lightweight cryptography is the acceptance of the Safe-Graphic application, even limited resource tools. The cryptography is already applied standard ally on the link layer layer on a mobile phone such as a mobile phone. Even in that case, under the application layer, it is effective to safeguard the information from the device to the end to the end of the device, and safeguard security safely from the communication system.

2.2.2 **Lightweight Cryptography**

2.2.2.1 Requirements for Lightweight Cryptography

The following factors require the lightweight script in the execution.

• Size

• Power

• Power consumption

• process speed

The first problem is determining the opportunity to apply to a device. Power is especially important with RFID and devices with power components, while power consumption is very important with battery-based devices. It is necessary for high performance. With a large transfer of information, devices such as cameras or a vibration detection element are very important for the real-time management process of low-delay vehicle control systems.

With compatible security, the writing is that the technical purpose for the original purpose of the general system is to adopt lightweight cryptographics technology that has been estimated to have a considerable level of security from estimated contemporary cryptography. It is even when length or length of secret length is applied to request a minimum quality corruption.

2.2.2.2 Symmetric Key and Public Key Cryptographies

The cryptography can be divided into symmetric and public key cryptography. For symmetric it uses the same secret key for encoding and decoding. In contrast, the public key uses a secret key in cryptography coding and separates the common key from the secret encryption key, and it is difficult. The general public key-optimization computer standards are generally more than 1,000 times the correct key of the key, but this technology is also used in the secret key cryptography and the secret key used in your digital signature. On the contrary, with a system that has communication of dynamic communication with some parts, such as communication systems between vehicles, public key recording services are effective. Synthetic key cryptography consists mainly of basic functions such as block or flow, and the methods used to use the basic function in a packet are called operation blocking mode for coding and / or verification.

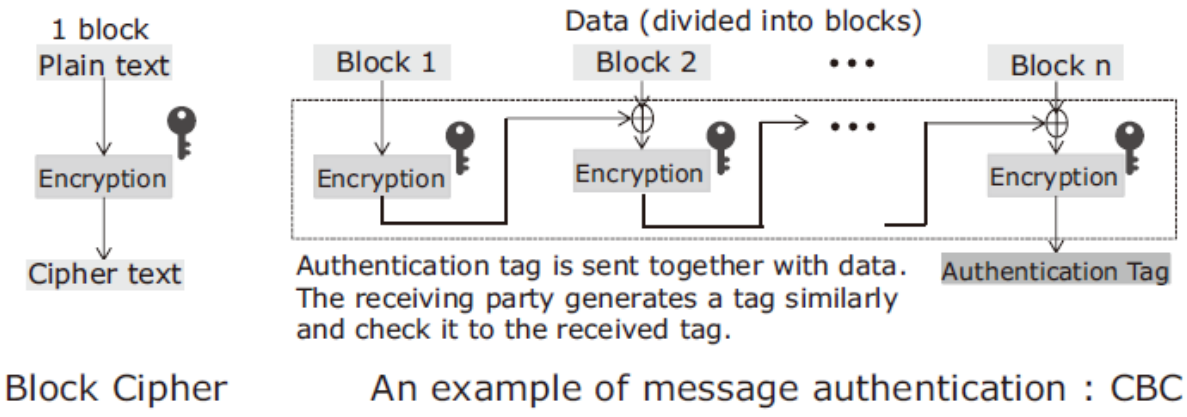


Fig. 3 An Example of block cipher mode of operation.

2.3 Lightweight Cryptographic Measures for IoT

The IoT network uses the network to connect and communicate between the things connected to the IoT network. After making a real-time conversation, IoT is much more involved in the extra work. Many architectures were proposed for the improvement IoT. The authors have described three stratified constructions architectures that IOT have. The three layers of the network are network layer, application layer and idea layer. A five-layer construction was proposed that included processing, business, applications, decisions and transport layers.
A wide range of data is shared between you and the user's request requirements. Therefore, the security and privacy of the IoT are more complex than other networks because the user's personal info is shared like location and other informations. It is important to maintain security services in the IoT so that the user can gain confidence.

Confidentiality: Only the sender or receiver has access to the data which is in transit.
Integrity: While the data is transmitting, no one can edit the original information of the data.
Authentication: The identifier of the sender for the identification of the database must be verified to the recipient.
Authorization: Only valid users can access the IOT resources and maintain the relationship between them.

The security architecture was analyzed to save conversion data between business partners and guarantee the aforementioned services. An inspection arc of security and quality was also presented, but there is still the challenge of organizing the open data in the IOT. As it consists of multiple attachments, the standard architecture is based on all things with four layers. In each layer, the protocol will provide a protection protocol, which will help protect security services from one layer to the data.

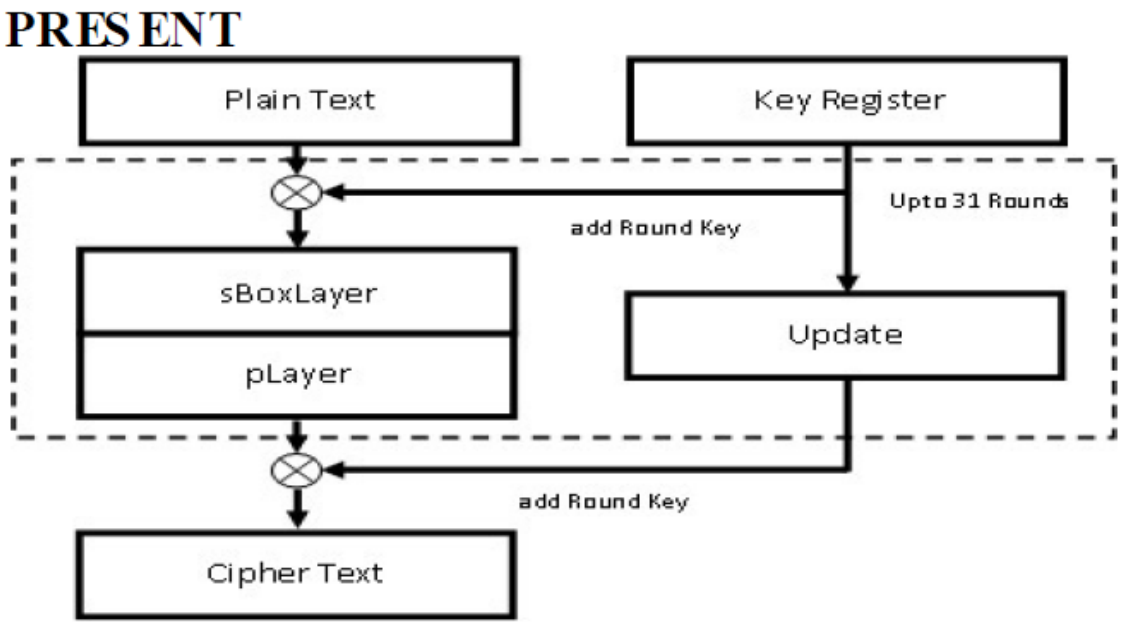
2.4 Advanced Lightweight Data Encryption Technique

The increasing use of pervasive devices within the field of electronics has raised the issues regarding security. In embedded applications, implementing a full-fledged cryptographic surroundings wouldn't be sensible thanks to the constraints like power dissipation, security, value and space, as a result of these constraints, the main target is on using light-weight cryptography. Cryptography could be a methodology that has been developed for transferring information securely.

Cryptography currently plays an progressively necessary role in trendy society, and it's essential to unravel issues that involve authentication, integrity, secrecy, and dishonest entities. In digital communications, the information is distributed through the wires or air and so it's not from eavesdropping. Therefore, confidentiality of the transferring data is of maximum importance. encoding could be a method that that's aimed to be sent to encrypted data using a key. The encoding method isn't confidential however the key's solely familiar to the sender and receiver of information. The receiver transforms the received information using the decoding method to get the initial information. There are two basic sorts of cryptography :

- Asymmetric encoding uses public key and symmetric encoding uses shared non-public key. asymmetric ciphers have 2 keys,a mathematical connected non-public key and a public key.
- Symmetric key cryptography, that uses a shared key in each ends for encoding and decoding, has been used for secure communications for long period of time.

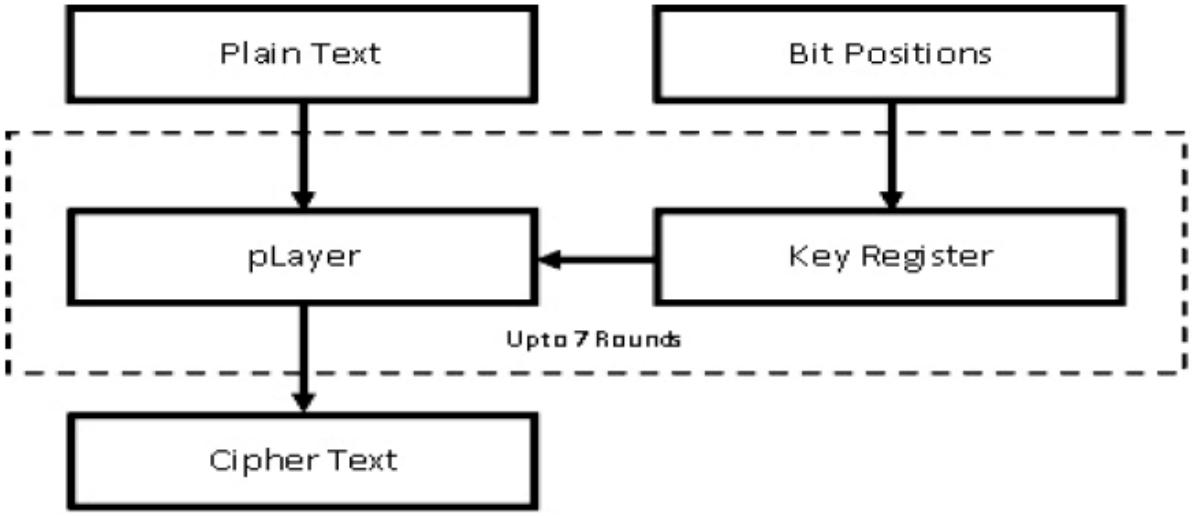
Symmetric key cryptography includes 2 completely different strategies for encoding and decoding. in the 1st technique which is stream cipher, the bits of information are encrypted/decrypted one at a time. Transmission error in one cipher text block have effect on alternative block and tough to implement properly. However, within the second technique that is named block cipher, blocks of the input file that include variety of bits are encrypted/decrypted. Transmission errors in one cipher text block have no effect on alternative block and easier to implement.



PRESENT is a substitution and permutation network with 64-bit iterated block cipher. The key is 128 bit. The substitution layer comprises 30 S-boxes with 128 bit input and 128 bit output. Through the careful selection of s-box, its possible to achieve high security level. The permutation layer (P-layer) is a very regular and group instruction operation is performed. The output from P-layer is xored with key and given to s -box as the input.

SYSTEM ANALYSIS

PROPOSED SYSTEM



As we discussed above, this study is based on cryptography, we provide suitable modifications to those designs, to make the proposed system. Here, S-box of PRESENT algorithm is removed and provide GRP permutation mechanism. Algorithm focused is to implement lightweight design to avoid high power dissipation and large memory requirement. To provide a high security and low cost, there is need to have a lightweight crypto algorithm whose coverage area would be less. The standard algorithm like AES,DES have huge memory requirement and would not be feasible to be implemented for embedded system design. Many lightweight algorithms have been designed in the past and various attacks have been proven on them. PRESENT algorithm is ISO/IEC standardized.

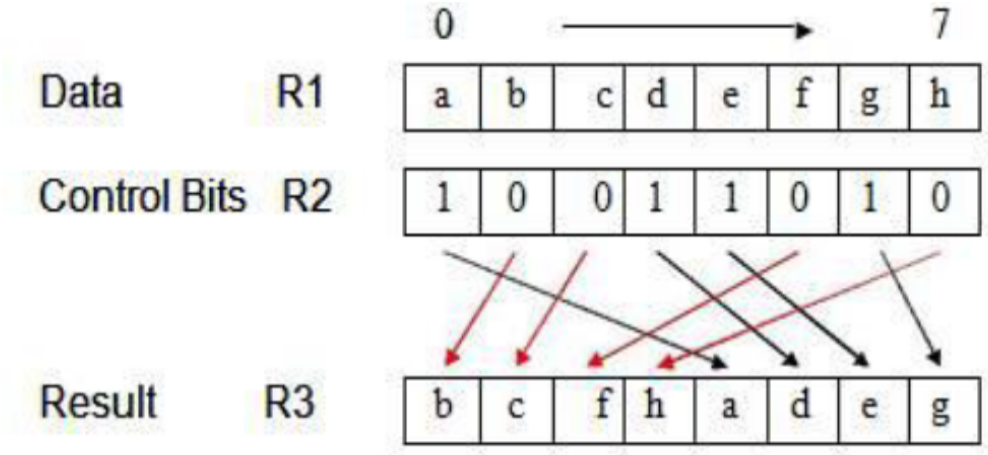
The aim of this work is to provide adequate security for the digital systems. The lightweight cryptography is a biometric algorithm combination of PRESENT algorithm with group instruction permutation. The developed algorithm is highly secured and need only less area when compared with Advanced Encryption Standard.

the detail of the proposed encryption system is provided. Figure above illustrates the general block diagram of the proposed system which is comprised of PLayer where GRP permutation is performed. The general block diagram of the proposed system comprises of two main modules:

1 Player – Basically where GRP permutation is performed

2 Key register-where key is generated for each round is stored

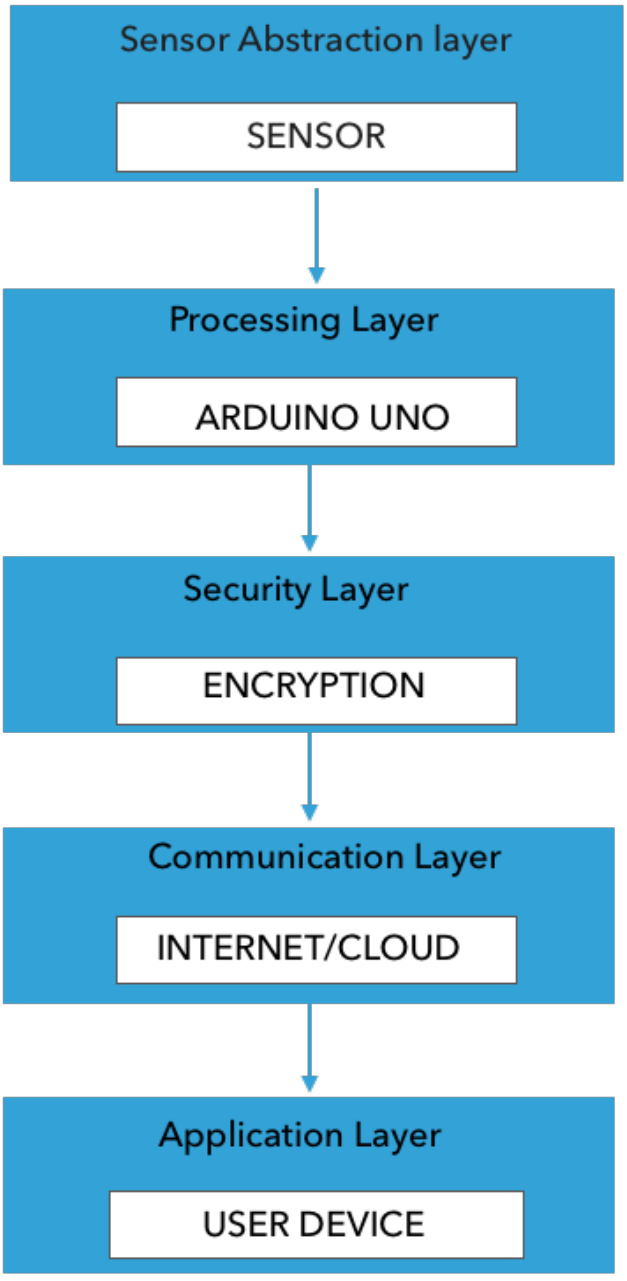
GRP instructionon 8-bit Systems



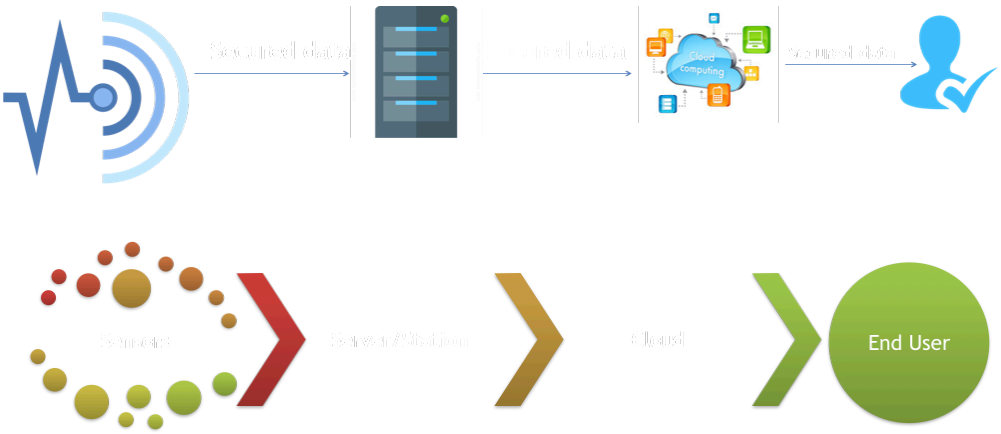
CHAPTER - 3

SYSTEM DEVELOPMENT

DESIGN

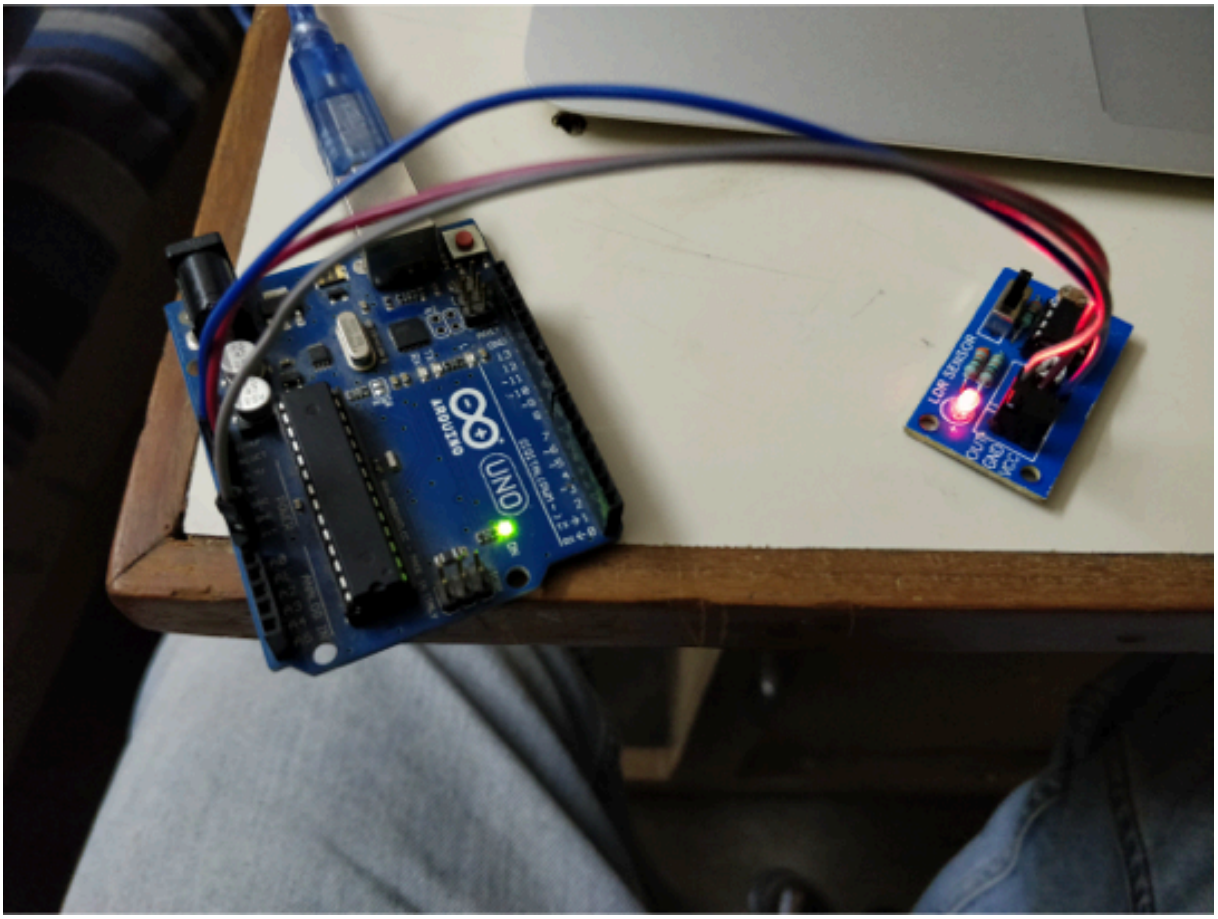


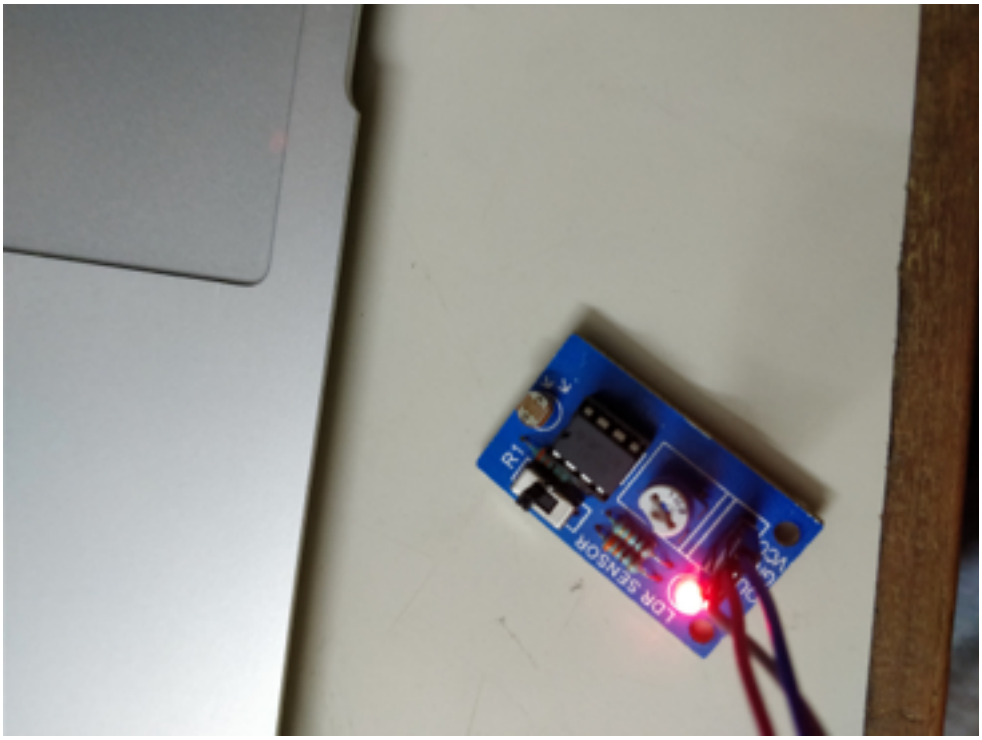
BASIC DESIGN:-



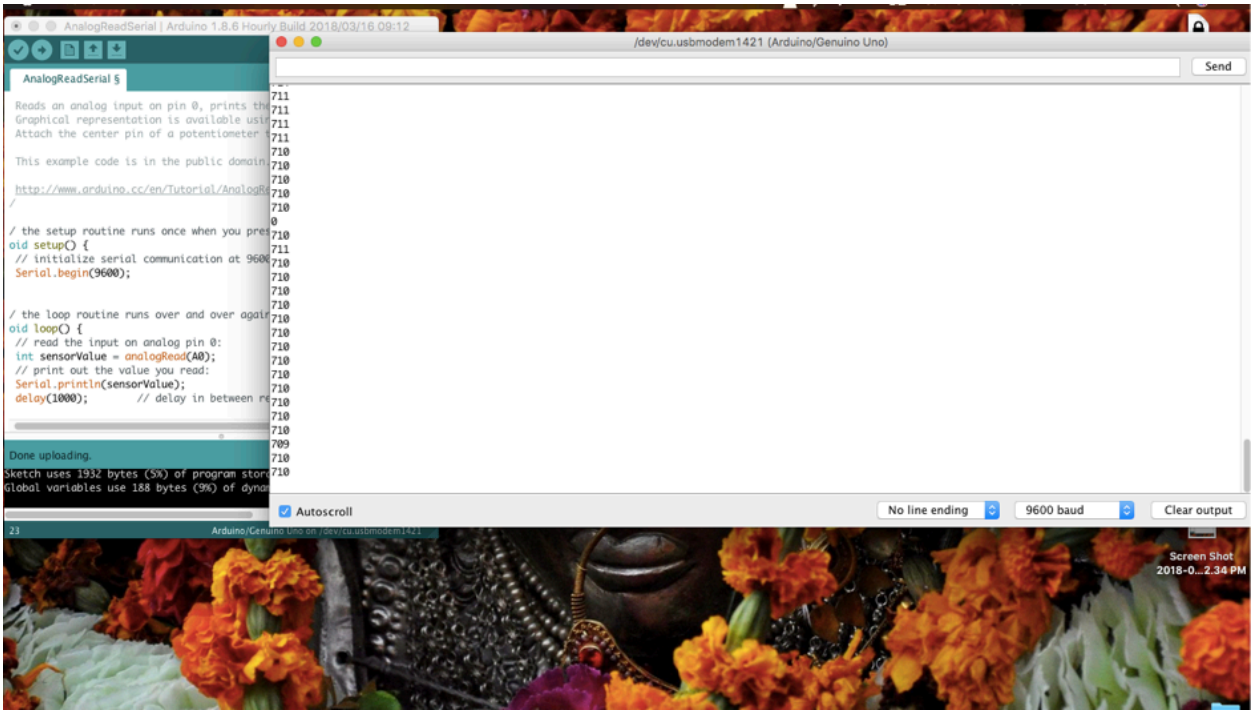
Arduino Uno:-

The open-source Arduino Software (IDE) makes it easy to write code and upload it to the board. It runs on Windows, Mac OS X, and Linux. The environment is written in Java and based on Processing and other open-source software.





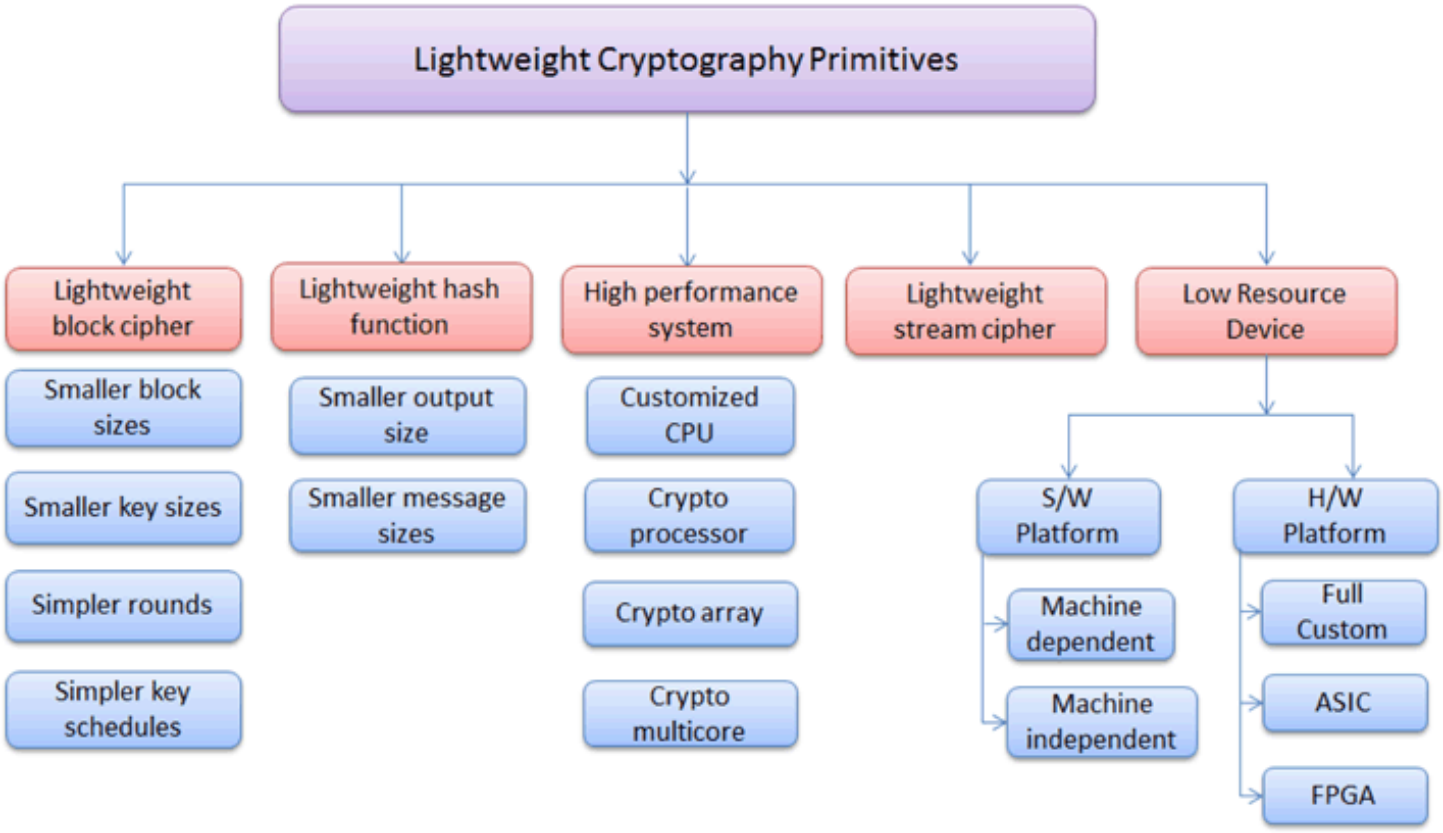
WORKING ON ARDUINO: -



Lightweight cryptographic primitives:-

In this chapter we will discuss the different primitives of light-weight cryptographic algorithms as shown in Figure no and also, we show many light-weight algorithms in the Table-based on their block length, key size, no. of rounds, structure and key size.

Light-weight cryptographic primitives:-



Some light-weight cryptographic 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

3.1 Advanced Encryption Standard ("AES")

We show the various primitives of light-weight cryptographic algorithms and also, we have summarized several light-weight algorithms within the Table on their block length, key size, range of rounds and structure.

The options of AES are : −

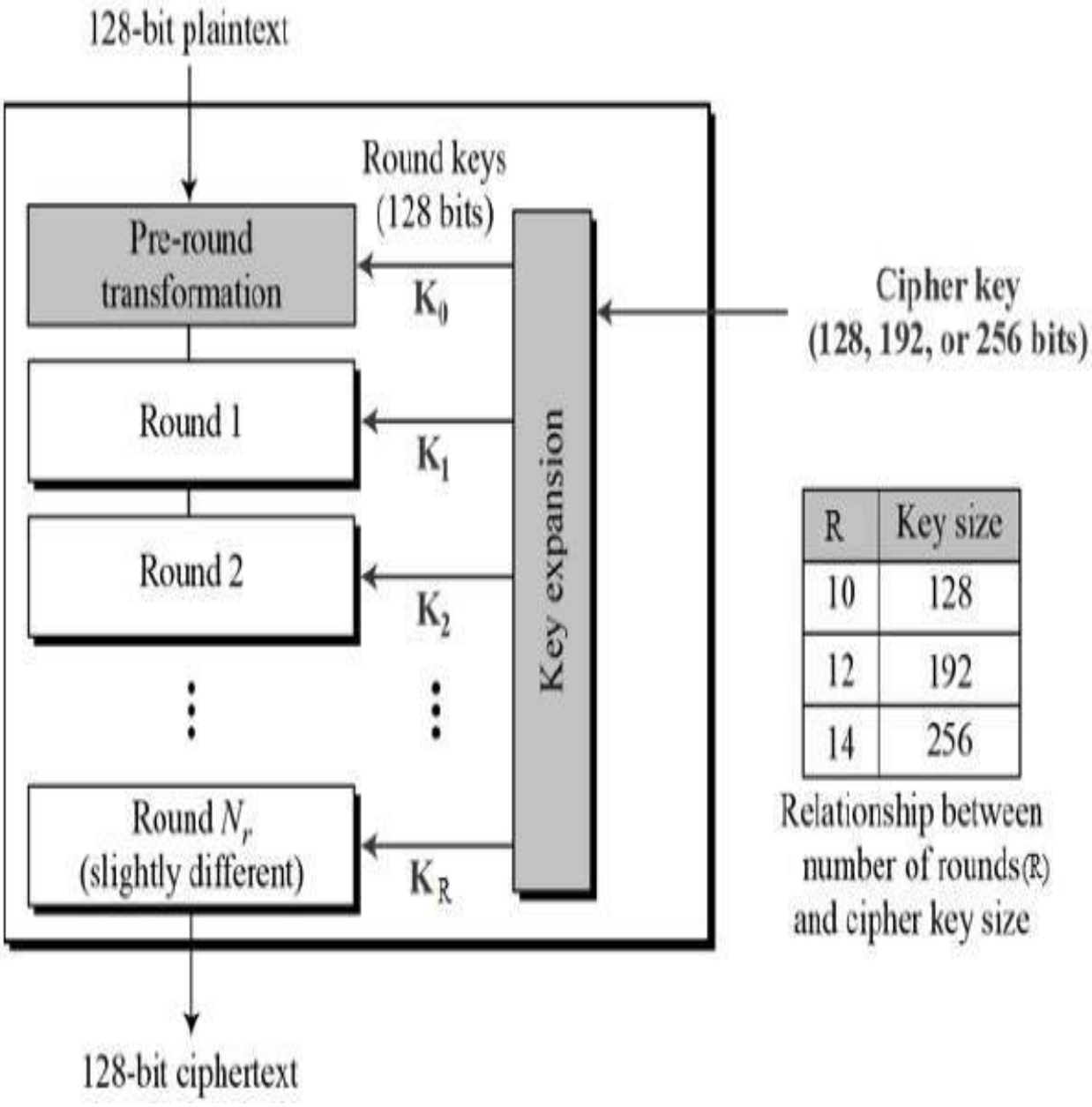
- "Symmetric key symmetric block cipher"
- "128-bit data, 128/192/256-bit keys"
- "Stronger and faster than Triple-DES"
- "Provide full specification and design details"
- "Software implementable in C and Java"

Operation of AES

Work are often extended for dense networks to urge correct and higher analysis compared to state-of- art work. Separate analysis may be drained developing anti-collision protocols for stationary, slow or fast-paced RFID-Sensor integrated devices wherever possibilities of cluster or network modification with time is high throughout cluster authentication

Boxes with a single cryptographically stronger S-box .The design of our DESL algorithm is exactly the same as for the DES algorithm, except for the (I.P) and (I.P−1)wiring and the s-box module. The changed s-box module implements only one S-box

The schematic of A.E.S structure:-.–

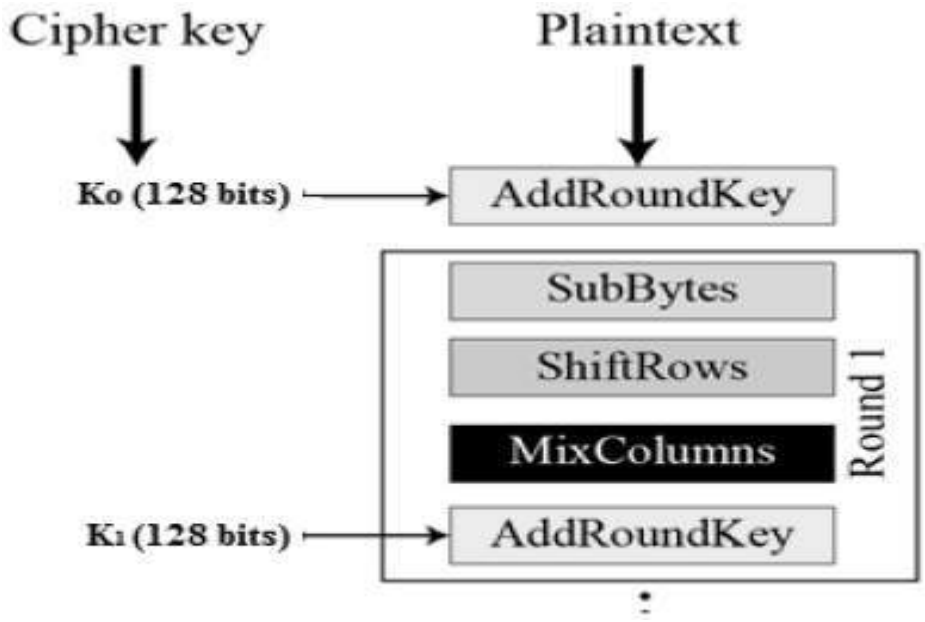


R	Key size
10	128
12	192
14	256

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

Encryption Process

Process is shown below:-



Byte Substitution (Sub-Bytes)

16 input bytes are replaced by (S-box table. Result is shown in a matrix of 4X4.

Shift-rows

Shif-rows follows the following steps :-

- "First row is not shifted."
- "Second row is shifted one (byte) position to the left."
- "Third row is shifted two positions to the left."
- "Fourth row is shifted three positions to the left."
- "The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other."

Mix-Columns:-

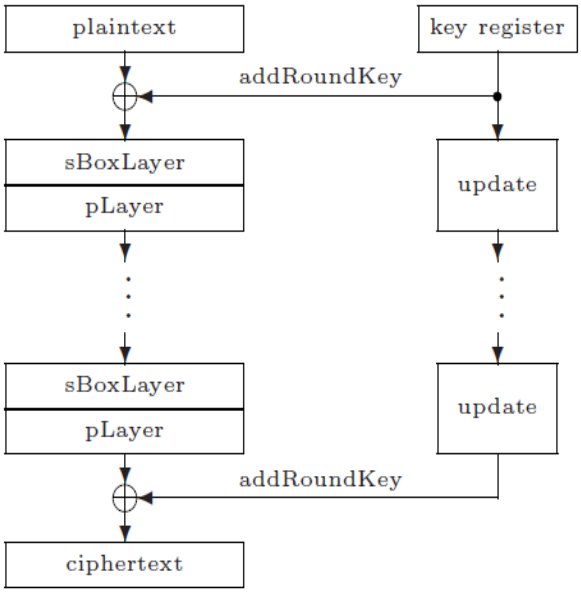
Add-roundkey:-

Decryption Process

- "Add round key"
- "Mix columns"
- "Shift rows"
- "Byte substitution"

3.2 PRESENT

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



These figures and others are "back-of-an-envelope" wherever we have a tendency to assume requirements: 32-bit XOR , 32-bit arithmetic ADD, 192-bit FF , SHIFT. All figures lack any management logic which could considerably increase the specified space. every of the thirty one spherical consists of associate xor operation to introduce a round key Ki for one ≤ j ≤ thirty two, wherever K32 is employed for post-whitening, a linear bitwise permutation and a non-linear substitution layer. The non-linear layer uses one 4-bit S-box S that is applied sixteen times in parallel in every spherical. The cipher is represented in pseudo-code in Figure one, and every stage is currently per flip. the look explanation area unit given in Section four and throughout we have a tendency to variety bits from zero with bit zero on the proper of a block or word.

addRoundKey. Given round key $K_i = \kappa_{63}^i \dots \kappa_0^i$ for $1 \leq i \leq 32$ and current STATE $b_{63} \dots b_0$, addRoundKey consists of the operation for $0 \leq j \leq 63$,

$$b_j \rightarrow b_j \oplus \kappa_j^i.$$

sBoxlayer. The S-box used in PRESENT is a 4-bit to 4-bit S-box $S : \mathbb{F}_2^4 \rightarrow \mathbb{F}_2^4$. The action of this box in hexadecimal notation is 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 sBoxLayer the current STATE $b_{63} \dots b_0$ is considered as sixteen 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 $0 \leq i \leq 15$ and the output nibble $S[w_i]$ provides the updated state values in the obvious way.

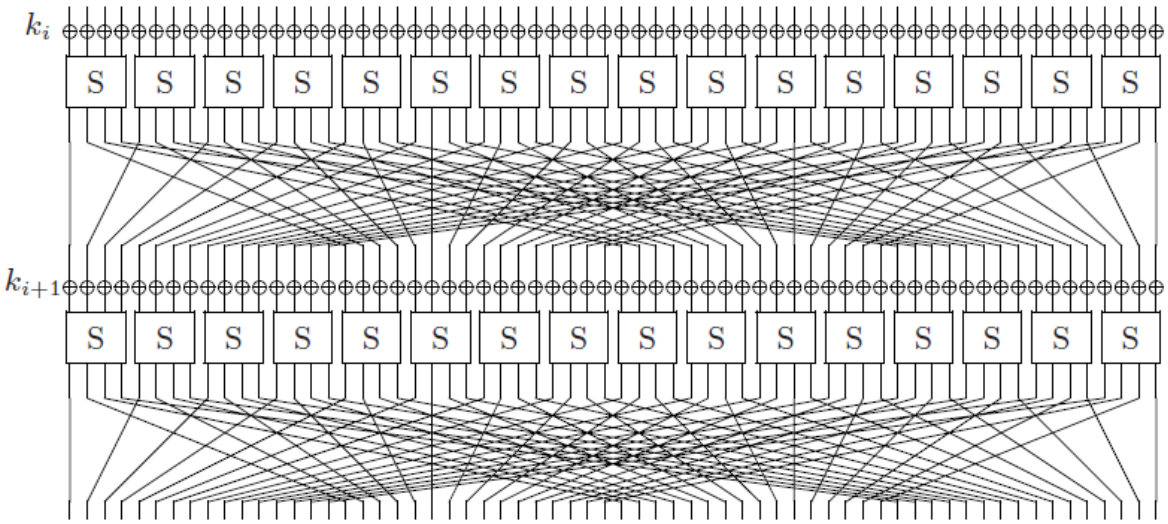
pLayer. The bit permutation used in PRESENT is given by the following table. Bit i of STATE is moved to bit position $P(i)$.

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 $K_i = \kappa_{63}\kappa_{62} \dots \kappa_0$ consists of the 64 leftmost bits of the current contents of register K. Thus at round i we have that:

$$K_i = \kappa_{63}\kappa_{62} \dots \kappa_0 = k_{79}k_{78} \dots k_{16}.$$

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

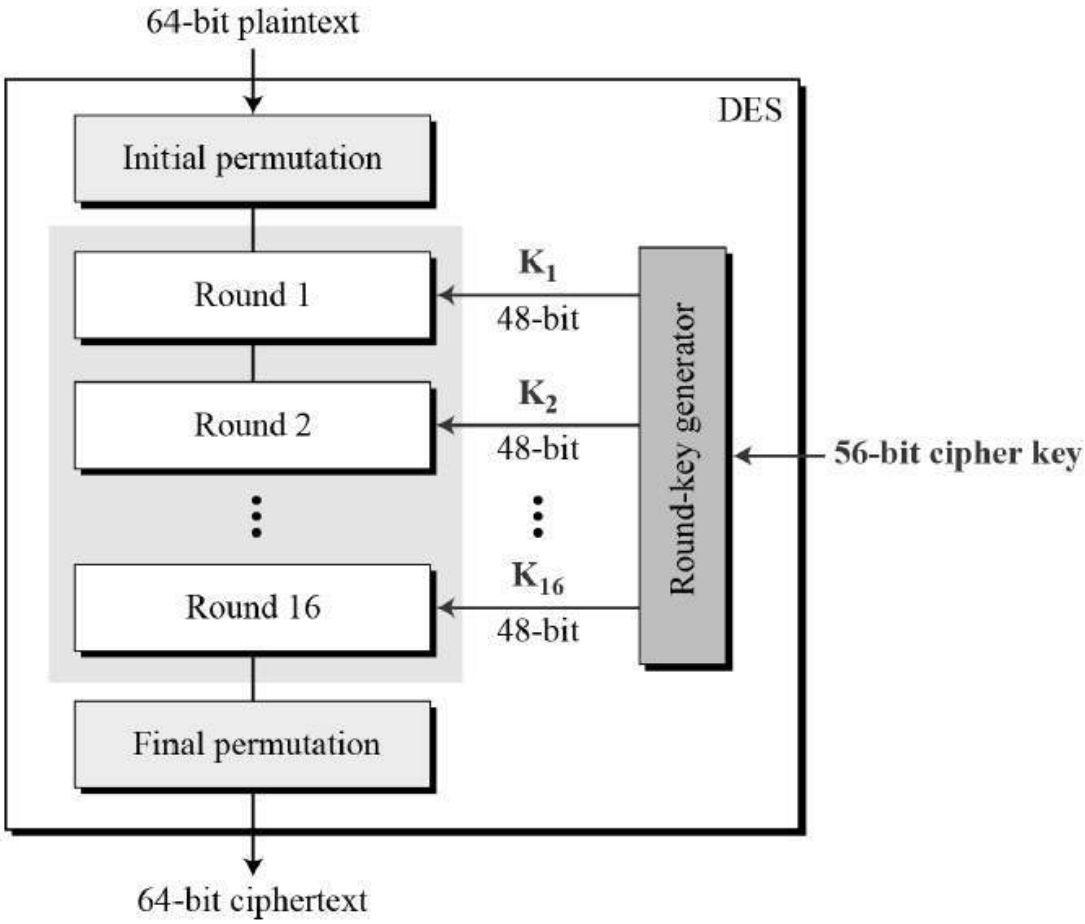


1. $[k_{79}k_{78}\ldots k_1k_0] = [k_{18}k_{17}\ldots k_{20}k_{19}]$
2. $[k_{79}k_{78}k_{77}k_{76}] = S[k_{79}k_{78}k_{77}k_{76}]$
3. $[k_{19}k_{18}k_{17}k_{16}k_{15}] = [k_{19}k_{18}k_{17}k_{16}k_{15}] \oplus \texttt{round\_counter}$

Thus, the key register is rotated by 61 bit positions to the left, the left-most 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 schedule for 128-bit keys is presented in an appendix.

3.3Data Encryption Standard (DES)

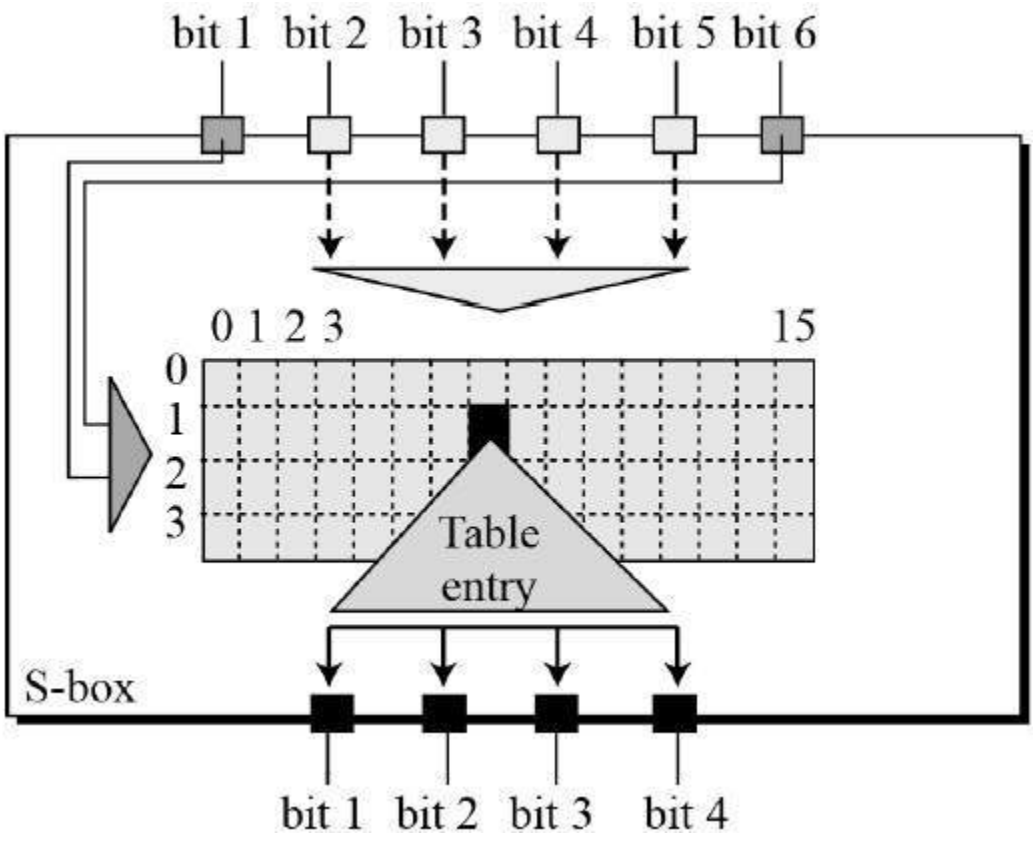
General Structure of DES is shown below:-



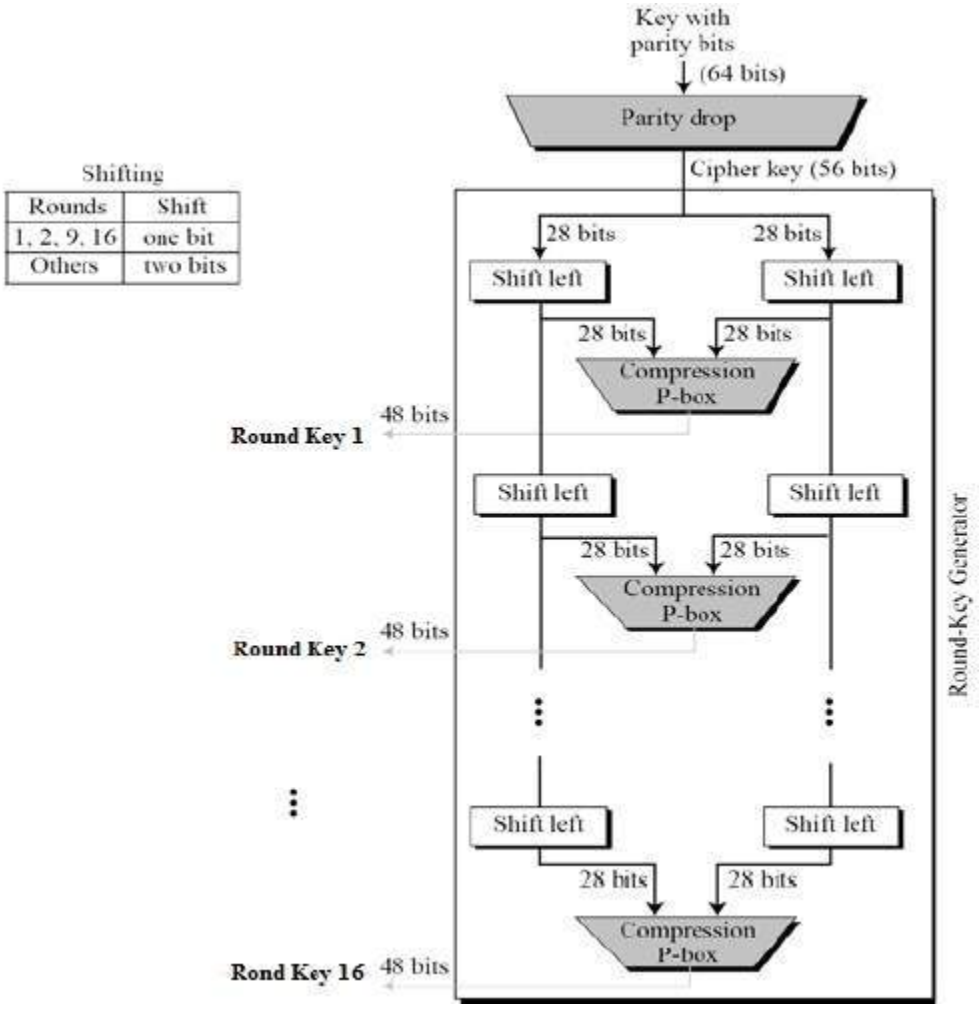
Properties required to satisfy DES are−

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

The S-box rule is illustrated below –



Key Generation



DES Analysis:

Properties that make cipher very strong are :-

- **Avalanche effect** – "A small change in plaintext results in the very grate change in the ciphertext."
- **Completeness** – "Each bit of ciphertext depends on many bits of plaintext."

3.4 DESL

First diff. between DESL and DES is in the f-function. We are replacing eight original DES S-Boxes with a single cryptographically stronger S-box .The design of our DESL algorithm is exactly the same as for the DES algorithm, except for the (I.P) and (I.P−1)wiring and the s-box module. The changed s-box module implements only one S-box. As one can see in Figure 2, this module neither needs the *count* control signal nor an output multiplexor, which saves another 192 transistors (48 GE).

	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

Finally, we can conclude, that DESL is more secure against linear and differential cryptanalysis and the Davies-Murphy attack, more size-optimized, and more power efficient than DES, which makes it especially suited for RFID applications. Furthermore, DESL is worth to be considered as an alternative for stream ciphers.

CHAPTER – 4

PERFORMANCE ANALYSIS

4.1 Overview

This Section provides a short description of each cipher. An overview of the ciphers' parameters is given in Table . Parameters of SEA can be chosen, the values that fit our implementation are given 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

Other ciphers like HIGHT use 128 bit key to provide high security but use a smaller block size than AES to meet the needs of a restricted environment. Ciphers like SEA are kept flexible in key size so each user may configure it for the security goal and performance needed.

4.1.1 AES

The Advanced Encryption Standard (AES) , also known as Rijndael, is the successor of the Data Encryption Standard (DES). It was announced by National Institute of Standards and Technology (NIST) as a U.S. FIPS in 2001. The cipher developed by J. Daemen and V. Rijmen was the winner of a 5-year standardization process. It has been deployed widely in many crypto applications, being the de-facto standard symmetric block cipher. AES is a block cipher using an 128 bit block with an 128, 192 or 256 bit key as input. It operates on a 4×4 array of bytes. Each round of AES consists of four stages, namely AddRoundKey, SubBytes, ShiftRows, and MixColumns. The AES is known to be quite efficient, especially on 8-bit architectures, owing to its byte-oriented design. Our assembler implementation of th AES is inspired by the AES implementation of B. Gladman.

4.1.2 DES

The Data Encryption Standard (DES) is a cipher selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976. As a block cipher DES operates on blocks with a size of 64 bits. The key also consists of 64 bits; only 56 of these are actually used by the algorithm, the other ones are parity check bits.

DES is not considered as secure anymore because of Moore's Law.

D.E.S can be broken by exhaustive key search in reasonable time. There are several confirmed DES crackers such as the EFF DES Cracker or the COPACOBANA . Furthermore attacks like differential cryptanalysis, linear cryptanalysis, and Davies' attack have been published.

Yet for some applications where security is not as critical, DES and variants of it are still in use.

DESX The block cipher DESX (or DES-X) is an extension to DES. It is defined by DESXK,K1,K2 (M) = K2 $\oplus$DESK(M $\oplus$K1).

DESL Like the above mentioned DESX DESL (DES Lightweight Extension) is an extension to D.E.S to comply with the requirements of small computational devices like RFID devices or Smart Cards. To decrease chip size requirements it uses only one S-Box repeated eight times. It therefore requires 38% less transistors than the smallest DES implementation published.

4.1.3 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 tagat 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.

4.1.4 SEA

The Scalable Encryption Algorithm (SEAn,b) is designed to be parametricin plaintext/key and processor size.

SEA (n,b) parameters in our case are plaintext/key size n = 96, processor wordsize b = 8, and number of words per Feistel branch nb = n2b = 6. Therefore we

have a suggested number of cipher rounds of nr = 3n4 + 2 ・(nb + ⌊b/2⌋) = 92.

As we used the standard implementation provided by the author we have 94rounds.

The cipher is targeted for processors with a limited instruction set and thereforeuses only bit operations such as exclusive-or, word rotation, bit rotation,addition mod 2b, and a substitution box.

4.1.5 TEA

The "Tiny Encryption Algorithm" (TEA) focus on the design of simple description and implementation. 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.

4.1.6 XTEA

Effective key length of TEA is 126 bits not 128. So in 1996 two adjustments were made, the first was to adjust the key schedule and the second was to introduce the key material more slowly. With these adjustments the weaknesses should be repaired and the simplicity is almost retained.

4.2 Results

We present the results of our implementations. The results are compared to an implementation of the A.E.S that was optimized for the 8-bit A.V.R microcontroller environment as well. The comparison focuses on code size, because memory is an important for size and price of an embedded or ubiquitous device, and on execution time, i.e. throughput, as execution time corresponds to the power consumption of a device.

4.2.1 Memory Usage

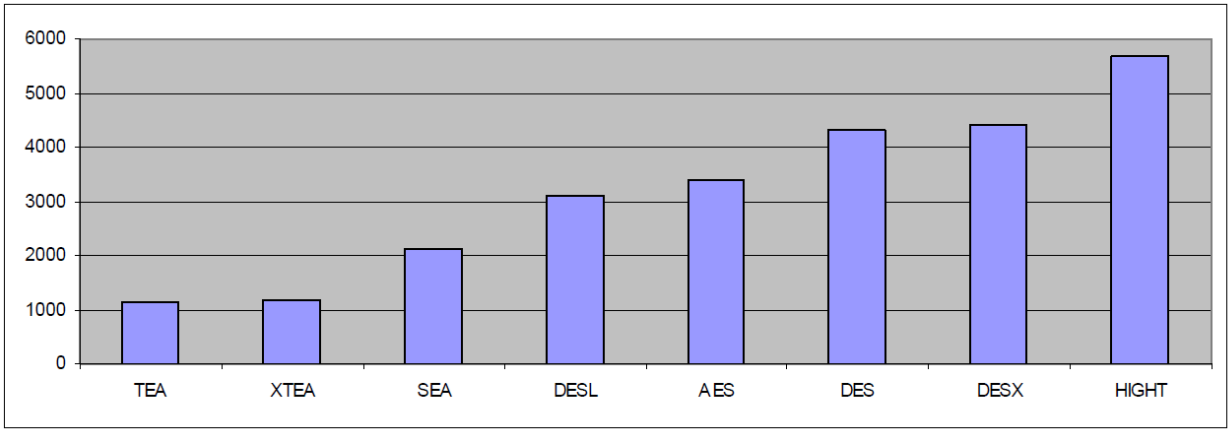
As embedded systems development is strongly price-driven, there are high restrictions in the size of available Flash memory and SRAM. This shows even more to applications like ubiquitous computing or even RFIDs, where power consumption is an important issue, too. The Flash (program) memory of the device is used to store code and look-up tables, if applicable. The smaller SRAM is used for dynamic access during program execution.

Table shows the memory allocation in flash memory of every cipher. Figure 1 shows the results ordered by size.

Memory allocation of code in Flash {Bytes}

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

Code size of different ciphers in bytes



4.2.2) **Performance**

Work are often extended for dense networks to urge correct and higher analysis compared to state-of- art work. Separate analysis may be drained developing anti-collision protocols for stationary, slow or fast-paced RFID-Sensor integrated devices wherever possibilities of cluster or network modification with time is high throughout cluster authentication.

Performance of coding and decoding in measured [CPU cycles]

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

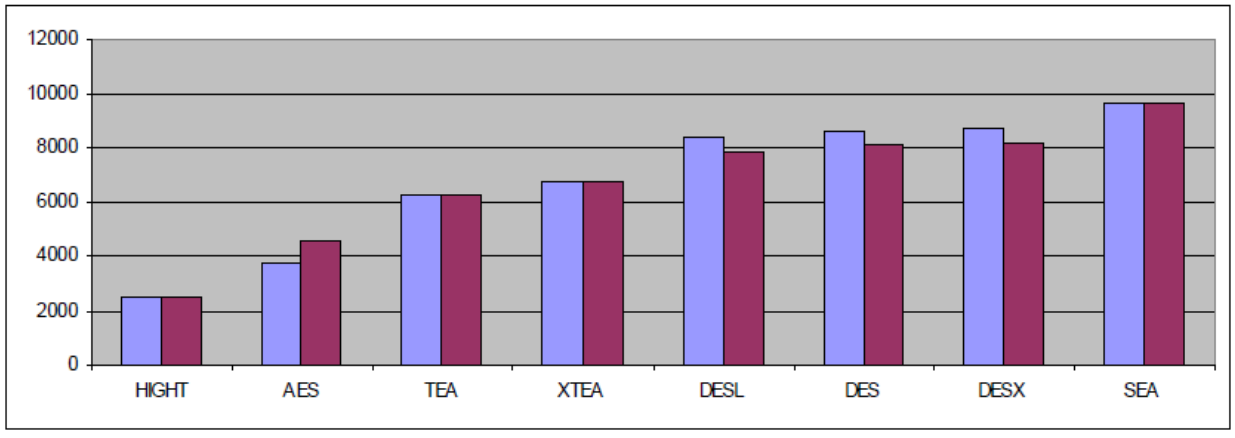
Throughput of encryption

Cipher	block size [bit]	Encryption [cycles]	Encryption [cycles/bit]	Throughput [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

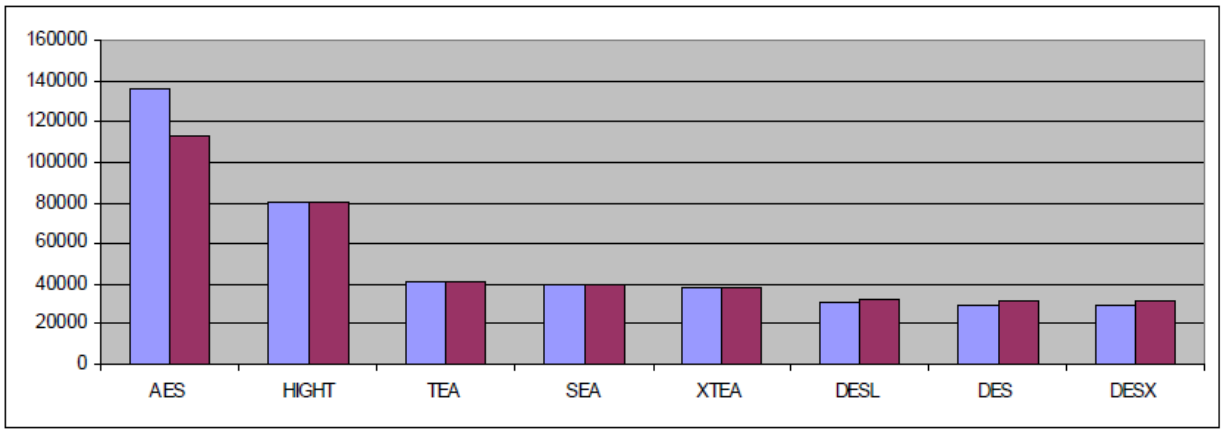
Throughput of decryption

Cipher	block size [bit]	Decryption [cycles]	Decryption [cycles/bit]	Throughput [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

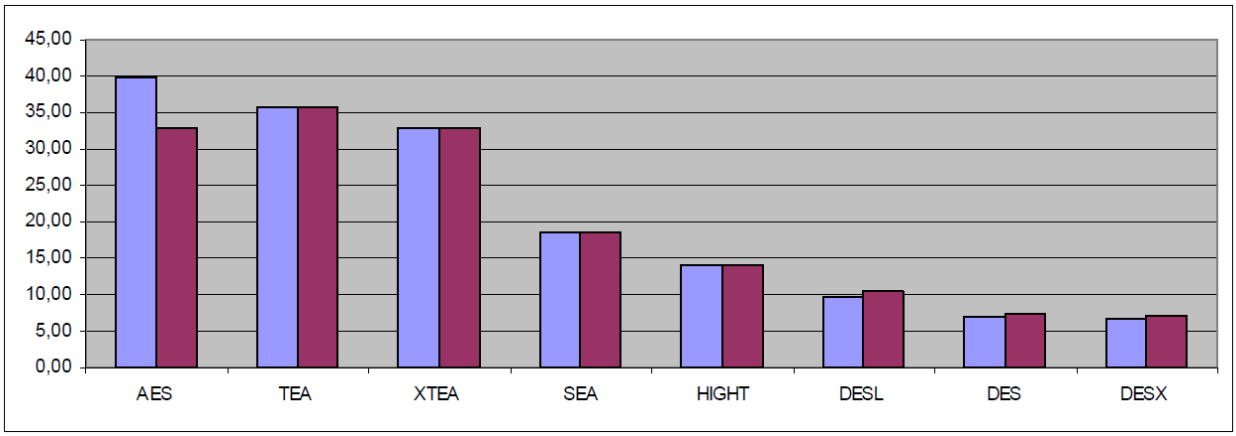
Cycle count of ciphers



Throughput of encryption and decryption



Throughput code size ratio of coding & decoding.



CHAPTER-5
CONCLUSIONS

5.1 Conclusions

We have gone over light-weight cryptanalytic algorithms intimately. Many devices with low-power can compute in IoT environment. These components are limited/restricted with size, battery life-cycle, power used, and operations performed.
While security and privacy challenges are recognized, the issue of IOT devices remains a concern because of the importance of maintaining trust among IOT users.
In addition, we have a summary of the lightweight varieties of lightweight cryptographic algorithms that are simple to use for hardware and package process.
Some of the attacks of cryptanalytic algorithms are indicated by styles, which we have the tendency associated with the delineated document. It is essential to promote a secure and lightweight cryptography algorithm that requires a small space, a fast process and a low power consumption. During this article, we have the opportunity to plan a topic that will be implemented in an intelligent home environment. Work are often extended for dense networks to urge correct and higher analysis compared to state-of- art work. We have a tendency to mention problems, such as the structure of the cipher, the size of the block, the size of the key, the new cyber-attacks. In the future, we will investigate, but this solution is expensive and, if appropriate, for the affected environment. In addition, a formula must be developed that depends on the edge of each parameter of the device, which has already been organized for our planning topic.

5.2 FUTURE SCOPE

Future RFID-Sensor integrated networks can have the higher antenna styles, cloud capabilities, massive memory capacity, multiplied reading and interrogation vary, quick process etc. compared to RFID networks or wireless sensing element networks. Integration of ultra-lightweight cryptography with restricted operations will minimize the price with improved security. The probabilistic approach bestowed during this thesis for the sweetening of the extent of security in authentication and distance bounding protocols will function a basis for future studies within the analysis of identification, cluster authentication, cluster authentication encoding, and secure possession transfer protocols that is that the necessity of the speedily growing field of interest in light-weight cryptography.

Now-a-days style of applications area unit exploitation R.F.I.D-Sensor integrated networks. little or no work has been allotted over the topology style of R.F.I.D and sensing element network devices for rising the data exchange and data storage prices. thence it may be one among the size wherever future work will continue. In R.F.I.D-Sensor integrated networks, R.F.I.D devices area unit principally used for correct identification. Now, if multiple RFID devices respond at a similar time and there's restricted variety of channels then collisions occur. numerous R.F.I.D tag-to-tag or reader-to- reader anti-collision algorithms area unit developed however partitioning collisions with improved potency continues to be unattainable for dense networks thanks to information measure or resource limitations.

Work are often extended for dense networks to urge correct and higher analysis compared to state-of- art work. Separate analysis may be drained developing anti-collision protocols for stationary, slow or fast-paced RFID-Sensor integrated devices wherever possibilities of cluster or network modification with time is high throughout cluster authentication. Further, in RFID-Sensor integrated multi-hop networks, error correcting codes, random variety generation processes, storage capability, quick process algorithms, routing etc. play an important role within the overall performance of the system.

Hence these parameters are needed to be analyzed. It may be analyzed the means during which 188 reusability of resources to implement cryptography primitives and protocols gift within the system are often any optimized.

With multi-hop property of RFID-Sensor integrated Edouard Manet devices, QoS is one very important problems of secured network, particularly for transmission services. In future, additional attention are often drawn on QoS parameters and routing protocols. one among the restrictions during this work has been that it failed to consider the interest of objects or users to become a part of a gaggle. Future work are often extended by considering the thing class, handiness, demand etc. into thought. One will build attempt to live the hardware price of cluster authentication and constitution projected during this thesis by mensuration the world of its parts implementation.

REFERENCES

[1] Ahamad MM, Abdullah MI (2016) Comparison of encryption algorithms for multimedia. RajshahiUniv J Sci Eng 44:131–139

[2] Al Salami S, Baek J, Salah K, Damiani E (2016) Lightweight encryption for smart home. In: Proceeding of 2016 11th International

[3] Conference on Availability, Reliability and Security (ARES), IEEE, pp 382–388

[4] Aumasson JP, Henzen L, Meier W, Naya-Plasencia M (2013) Quark: a lightweight hash. J Crypto 26(2):313–339

[5] Babbage S, Dodd M (2008) The MICKEY stream ciphers. In: Proceeding of New Stream Cipher Designs, Springer, Berlin, pp 191–209

[6] Badel S, Dağtekin N, Nakahara JJ, Ouafi K, Reffé N, Sepehrdad P, Vaudenay S (2010) ARMADILLO: a multi-purpose cryptographic primitive dedicated to hardware. In: Proceeding of International Workshop on Cryptographic Hardware and Embedded Systems, Springer, Berlin. pp 398–412

[7] ECRYPT (2017) eSTREAM: the ECRYPT stream cipher project .http://www.ecrypt.eu.org/stream/.

[8] Eisenbarth T, Kumar S (2007) A survey of lightweight-cryptography implementations. IEEE Desi Test Comput 24(6):1–12Ernest W (2017). http://semiengineering.com/lightweight-cryptography-for-the-ioe/.

[9] MeeraSaif, NidiyaHabeeb ,"Advanced Lightweight Data Encryption Technique "Volume 6 Issue No. 9 2016 IJESCMusaliar College of Engineering and Technology, Kerala, India

[10] Saurabh Singh, Pradip Kumar Sharma, Seo Yeon Moon, Jong Hyuk Park "Advanced lightweight encryption algorithms for IoT devices:survey, challenges and solutions" 18 April2017

[11]Isha and Ashish Kr. Luhach "Analysis of Lightweight Cryptographic Solutions for Internet of Things" Lovely Professional University, Jalandhar - 144411, Punjab, IndiaJuly 2016