

# **Data Security using Hybrid Encryption And Decryption Algorithms**

**A PROJECT REPORT**

*for*

**Information Security Analysis and Audit**

*in*

**B.Tech (IT)**

*by*

**Omkar Kulkarni (19BIT0196)**

**Kausik Nandhan (19BIT0215)**

**Harsh Mangal (19BIT0162)**

**Fall Semester, 2021**

*Under the Guidance of*

**Sumaiya Thaseen**

**SITE**



**VIT<sup>®</sup>**  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

**School of Information Technology and Engineering**

**NOV, 2021**

# **Data Security using Hybrid Encryption and Decryption Algorithms**

Omkar Kulkarni, Kausik Nandhan, Harsh Mangal

## **Abstract**

We see data being sent from one person to another frequently through various social media platforms. Not every platform is ensuring safety of your data when it's being transferred. Data security is a need for the present generation. With concepts like Big Data, Data Visualization, Data Analytics etc need data on a massive scale, ensuring its safety is a must. An end-to-end encryption of the data using some cryptographic algorithms would definitely make the task easier. Our project describes two Hybrid encryption and decryption – ECC secret key derivation, ECC+AES and RSA+AES and is used to encrypt and decrypt any user defined message.

## **Keywords**

Encryption, Decryption, Hybrid, Secret Key, Public key, Private Key, RSA, AES, ECC, ECDH

## **Introduction**

There are two types of cryptography that has been used in this project.

Symmetric and Asymmetric cryptography.

Symmetric cryptography, is the use of a single shared secret to share encrypted data between parties. The ciphers in this category are called symmetric because you use the same key to encrypt and extract data. In simple words, the sender encrypts data using passwords, and the recipient must know that password in order to access the data.

Symmetric encryption is a two-way process. With a blank text block and a specific key, symmetric ciphers will always produce the same ciphertext text. Similarly, using that same key in that ciphertext block will always produce real clear text. Symmetric encryption helps protect data between organizations with shared verification keys and is often used to keep data confidential.

Some famous symmetric encryption techniques are:

AES (Advanced Encryption Standard), DES (Data Encryption Standard), Blowfish etc.

Asymmetric Encryption uses two different, yet related, keys. One key, Public Key, is used for encryption and another, Secret Key, for decryption. As mentioned in the name, The Secret Key is intended to be private so that only the authorized recipient can remove the encryption message.

This algorithm uses a production protocol (a type of mathematical function) to produce a key pair. Both keys are mathematically connected. This relationship between keys varies from one algorithm to another.

The algorithm is basically a combination of two functions - an encryption function and a scripting function. In other words, encryption is encrypted and encryption removes the encryption.

Some famous asymmetric encryption techniques are:

Rivest Shamir Adleman (RSA), Digital Signature Standard (DSS), Elliptical Curve Cryptography (ECC), Elliptical Diffie-Hellman exchange (ECDH) method etc.

## **Related Work**

### **Efficient Data Access Control with Fine-Grained Data Protection in Cloud-Assisted IIoT**

#### **Introduction:**

IIoT (Industrial Use of Internet of Things) is used to build digitalized industrial systems. IIoT uses the radio-frequency identification (RFID) technique, which allows the users to identify items and anchor time-series IoT data for them. To store IoT data in cloud, requires a data access control mechanism to protect sensitive data. CP-ABE (Cypher policy-attribute-based encryption) hybrid cloud infrastructure guarantees strong privacy to the user. Our scheme adopts CP-ABE tasks to cloud service which guarantees item-level data protection to prevent key leakage problem.

#### **Conventional Approach:**

Cryptographic methods are used for encryption of data access control mechanism. This method is only used for the authorized participants only.

#### **Problems:**

--> Using primitive encryption process and distributive decryption keys for only authorized persons to encrypt IoT is very ineffective.

--> CP-ABE is another method which is a fine fit for enforcing fine-grained access control but it is very expensive and it is too slow to meet the high requirement of the time series IoT data in an industrial context. CP-ABE is vulnerable to privacy vulnerability and CP-ABE relies on a key authority to derive all the ABE keys from a master.

#### **Techniques Used:**

--> We devise a set of encryption technique to ensure item level data protection while enabling the private cloud CP-ABE tasks over IoT data. With these techniques our scheme

enables industrial participants to only execute lightweight symmetric encryption tasks to meet the high throughput requirement of time-series IoT data.

--> To further improve the performance of our scheme, we devise a set of optimization techniques with new tradeoffs for the private cloud to execute CP-ABE tasks in a scalable way. With these techniques, our scheme enables the private cloud to execute CP-ABE encryption/decryption tasks in batch level and CP-ABE re- encryption tasks regardless of the size of IoT data

--> We implement a prototype of the private cloud as a distributed computing infrastructure, which is customized for CP-ABE tasks. We evaluate several critical performance metrics for our implementation. Comparing with a raw CP-ABE processing engine, our scheme achieves two times of speedup ratio.

#### **Advantages:**

--> Fine-grained access control is achieved with this scheme.

--> Our scheme consists of a master node and a set of slave nodes to support scalable task processing.

--> Our implementation adopts a two-layer task schedule framework to achieve a balance between load balancing and schedule flexibility.

#### **Limitations:**

--> CP-ABE decryption tasks need pruning algorithms which are quite expensive.

-->Our scheme requires professional configured, resource-abundant CSP deployment is necessary to process large numbers of CP-ABE tasks for time-series IoT records in the industrial system.

#### **Conclusion:**

Our design ensures a secure industrial data access control scheme for cloud-aided IIoT enforce fine-grained access policies and item-level data protection.

Our scheme ensures item-level data protection for item securing them from key leakage problem.

---

## **Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of Internet of Things**

**-Yuan Li, Mingjun Hou, Heng Liu & Yi Liu**

### **Abstract-**

The paper provides a theoretical framework which classifies IoT strategies into four archetypes from two dimensions of managers' strategic intent and industrial driving force, and propose that market-based exploratory capabilities play a more important role for firms adopting get-ahead strategy, and market-based exploitative capabilities play a more important role for firms adopting catch-up strategy in market.

### **Problem:**

The main problem is to make sure IoT exploitative capability is to achieve greater efficiency and reliability of existing activities in IoT business.

### **Technique used to support capabilities:**

- the first type of supporting capabilities as market-based exploratory capabilities that support firms to explore and integrate new resources that are derived from the newly developed IoT market
- the second type of supporting capabilities as technology-based exploratory capabilities that support firms to obtain advanced IoT technologies by breaking the existing dominant design and departing from the existing technology
- the third type of supporting capabilities as market-based exploitative capabilities that support firms to develop IoT application through effectively allocating IoT resources for the existing market
- the fourth type of supporting capabilities as technology-based exploitative capabilities that support firms to obtain IoT technology by improving established designs and broadening existing skills without changing essential technology

#### **Advantages:**

The above types of capabilities respectively support the IoT get-ahead strategies under the contexts of market pull or technology push.

#### **Limitations:**

- the theoretical framework needs further support from empirical evidence.
- future studies need to pay special attention to how different cooperation relationships affect the strategic choice of firms

## **Recent Advances and Trends in Lightweight Cryptography for IoT Security**

• Nilupulee A. Gunathilake, Ahmed Al-Dubai, William J. Buchanan

#### **Abstract-**

This work contains the development of lightweight cryptographic algorithms, its current advancements and futuristic enhancements. This covers the history, parametric limitations of the invented methods, research progresses of cryptology as well as cryptanalysis.

#### **Problem-**

To provide new perspective of cryptographic vision towards light weight inventions for IoT security.

#### **Techniques/ algorithm-**

- SYMMETRIC LIGHT-WEIGHT CRYPTO- These are usually adopted from a conventional algorithm and their improved light-weight architecture is introduced as either versions or in a new name, i.e., AES based light-weight techniques.
- Block ciphers- KLEIN, Lilliput, PRESENT, Rectangle and Skinny are known as ultra-lightweight because their key sizes, block sizes and computational rounds are in the least range. This is very promising due to their satisfying scalability, but dissatisfaction in the security later
- $h$  as  $h$  functions
- Dedicated AE

### **Advantages-**

These approaches show resistance to known-key, replay and eavesdropping attacks theoretically.

### **Limitations-**

- IoT security still struggles to provide compatible cryptographic primitives in terms of lightweight to cope with possible and futuristic IoT hazards and threats.

---

## **A review on lightweight cryptography for Internet-of-Things based applications** **- Vidya Rao · K. V. Prema<sup>1</sup>**

### **Abstract-**

To analyze the various lightweight solution and their security threats under the authentication and data integrity of the IoT applications.

### **Problem-**

the major security concern of these protocols is to perform with less computation and resist to attacks like man-in-the middle, replay attacks, denial of service attacks, forgery and chosen-ciphertext attacks.

### **Techniques/ algorithm-**

- MQTT: Message Queue Telemetry Transport (MQTT) is a messaging protocol used in IoT based applications that were introduced by IBM at OASIS labs. It involves three entities, namely: the publisher, the broker and the consumer. Publishers are the sources of data; brokers maintain information about the topics sent by publishers and consumers are the one who subscribes the topic managed by the broker.
- CoAP: Constrained Application Protocol (CoAP) is an application layer protocol that defined on Representational State Transfer (REST) protocol above HTTP protocol functionalities. CoAP is divided into two sub-layers, called messaging sub-layer and request/response sublayer. The messaging sub-layer checks for duplication and asynchronous nature of the interactions. The request response sub-layer performs REST communication.
- XMPP: Extensible Messaging and Presence Protocol (XMPP) is an instant messaging (IM) standard by IETF. XMPP is used basically for multi-party chatting, voice-video calling

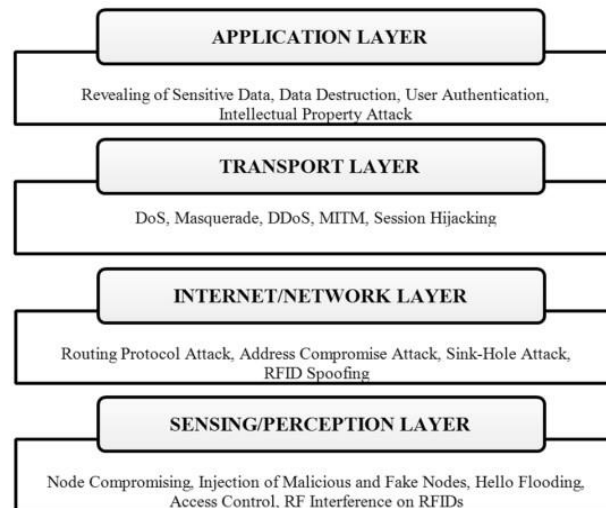


Fig. 7 IoT layers based attacks

#### Advantages-

- User authentications, access control lists, firewalls, anti-virus methods, risk management, are used to avoid attacks on the application layer
- By using Secure Routing protocols for LLNs, routing information attack can be prevented
- The devices communicate among each other over publically available communication. Thereby, these communications are susceptible to various attacks.

#### Limitations-

- A real-time security evaluation is not done. Thereby, a thorough theoretical and experimental security analysis is needed.
- elliptic curve parameters are vulnerable to node compromise attacks.

---

## A Systematic Technical Survey of Lightweight Cryptography On IOT Environment

-Abdulrazzaq H.A.Al-ahdal, Nilesh K.Deshmukh

### Abstract-

To provide a clear classification and accurate definition of LWC algorithms along with comparison and performance analysis of LWC algorithms based on important features such as latency, area, throughput, and power and energy consumption.

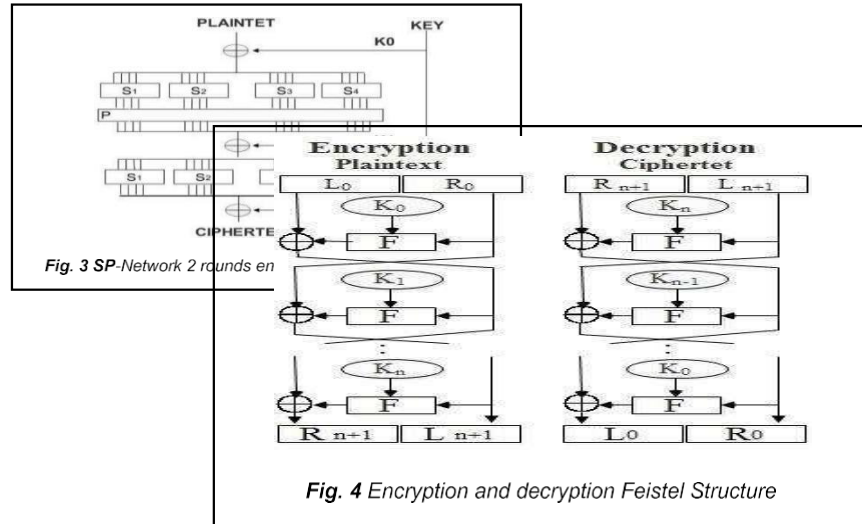
### Problem-

Security is an important factor to reduce the limitation on desktop computers as they are connected to each other which limits the IOT environment. Thus, efficient LWC algorithms are needed in IOT to make the tasks of IOT smart devices easier for convertibility, security and energy consumptions

### Techniques/ algorithm-

- Lightweight block cipher used to provide a semi-random flipping that builds protocols

- SP Network structure uses a chain of associated mathematical operations which are of several rounds or layers of substitution boxes (S-boxes) and Permutation boxes (P-boxes).



- Feisal Structure-

- Hash function

#### **Advantages-**

Due to recent developments and proposed various techniques the IOT lightweight cryptography protocols the tasks are more efficient and rapid algorithms help in building strong systems.

#### **Limitations-**

- Computing algorithms are relatively slower and still require developments in various fields
- The process of developing algorithms is ongoing but is relatively taking more time and money.

### **Time crypt: Encrypted Data Stream Processing at Scale with Cryptographic Access Control**

**Problems:** High resolution sensitive data, if server compromises privacy is risked. Data breaches all over the world. Scalability, latency and Interactivity, secure sharing.

**Technique used in the paper and why is it used:** Time crypt is a system that provides scalable and real time analytics over large volumes of encrypted time series data. In Time Crypt, data is encrypted end-to-end, and authorized parties can only decrypt and verify queries within their authorized access scope.

**Details:** Time Crypt allows users to define expressive data access and privacy policies and enforces it cryptographically via encryption.



Evaluation of TimeCrypt shows that its memory overhead and performance are competitive and close to operating on data in the clear.

**Advantages:** HEAC provides verifiable computations over cipher texts to ensure integrity. It meets the scalability, and low latency requirements associated with the time series work loads.

Confidentiality, Integrity, Hidden access patterns, access control collusion, access control extensibility.

**Comparision:** Time crypt is a system that augments time series data stories with efficient and privacy preserving processing of time series data while CP-ABE enables as encryptor to define the attribute set over a universe of attributes that a decryptor needs to possess in order to decrypt the cipher text.

**Limitations:** Can be difficult to access even for a legitimate user at a crucial time of decision-making. Various techniques lead to dela

---

### **A radio frequency identification protocol anti-tracking in 5G: An RFID protocol Anti-Tracking in 5G.**

**Problem:** RFID tags in smartphones often suffer from leaking private trace of mobile users. Majorities of existing RFID protocols are vulnerable to location-tracking threats, and to distributed denial of service (DDoS) attacks on back-end servers.

**Technique used:** A hash-band mutual authentication protocol for smartphones in 5G. RFID authentication protocol based on a hashing function can be divided into two types according to the type of information used for authentication between a reader and a tag.

**Advantages:** This protocol protects individual's location privacy against malicious hidden scanning. In public places. By the authentication of RFID readers via hash values, the proposed protocol is robust against the fore mentioned threats. Efficiency on the tag side is  $2H$ , which outperforms most of the problems related to RFID, one vector is  $k$ -bit and the other  $j$ -bit.

**Comparision:** A fundamental technology of IIoT is RFID technique, which allows industrial participants to identify items and anchor time series IoT data for them. This anti-tracking system increases the individual's privacy.

**Limitations:** Prone to Ghost tags, Vulnerable to damage, Unread tags, High cost, RFID Reader Collision, RFID tags are difficult to remove.

---

## Performance Evaluate of CP-ABE Schemes under Constrained Devices

**Problem:** The Cloud is honest but curious, sensitive information belonging to the IoT devices owners might be accessed and used beyond the intended purpose.

**Details:** Data privacy on Cloud servers should be preserved, which means they should not reveal any piece of PII.

Algorithm-1: Full-enc

Input: PK, M, A

Output: CT

Algorithm-2: Partial-Enc BBB1

Input: PK, M, A

Output: CT1

Algorithm-3: Partial-Enc BBB2 Input: PK,

CT1, A

Output: CT

**Technique Used:** Attribute Based Encryption is a new form of public key encryption. The authors proposed a new form of asymmetric encryption called Key-Policy attribute based encryption. Later CP- ABE is introduced.

**Advantages:** This scheme can perform either full or partial encryption according to the machine context, the complexity of the access policies and the data size.

---

## An Efficient Cipher Text- Policy Attribute-Based Access Control towards Revocation in Cloud Computing

**Problem** is that in data outsourcing systems, efficient enforcements of authorization policies and policy updates are the main obstacles.

In order to solve this problem, efficient and secure attributes and user revocation should be proposed in original ABE scheme, which is a challenge in existing work. **Technique used** is that we propose a new ciphertext-policy ABE construction, which largely eliminates the overhead computation at data service manager and data owner which makes it an **advantage**. It is also efficient access control mechanism based on the CP-ABE construction with one outsourcing computation provider.

**Limitations** include that the data owner needs to use every authorized user's public key to encrypt data. The application of these schemes are restricted in the real environment because it uses the access of monotonic attributes to control user's access in the system.

---

## Lightweight Cryptography: An IoT Perspective

### Problems:

Hardware implementation is a major problem. We have to use lower algorithm for lighter Gate Equivalent (GE). But due to this security might be compromised. This can be led to data breach, latency issues, data leakage etc...

### Technique used in the paper and why is it used:

Lightweight cryptography is used. It is a security system that is made of constrained devices. This system provides adequate security to these devices.

### Details:

In this process we mainly use the concept of low computing overhead, pre-image resistance and second pre-image resistance hash functions and pseudorandom numbers.

### Advantages:

-->Lightweight cryptography is important to save the energy and storage of devices. -->It is very useful for low-power embedded systems, machine to machine communication, radio frequency identification tags, nanotechnology, sensors, and smart networks.

--> Mutual authentication between devices.

-->Strong encryption methodology for transmission.

--> Secure storage environment with anytime availability.

### Comparison:

Lightweight cryptography uses hash function as algorithm for authentication.

Hash-One	16 0	16 0	1	160	80	80	0.18	2130	14/7
SPONGENT	17 6	16 0	1 6	144	80	80	0.13	1329	3960
SPONGENT	17 6	16 0	1 6	144	80	80	0.13	2190	90
D-QUARK	17 6	16 0	1 6	160	80	80	0.18	1702	704
D-QUARK	17 6	16 0	1 6	160	80	80	0.18	2819	88
PHOTON	16 0	16 0	3 6	124	80	80	0.18	1396	1332
PHOTON	16 0	16 0	3 6	124	80	80	0.18	2117	180
GLUON	16 0	16 0	1 6	160	80	80	0.18	2799	50

Table 4: Comparison of Lightweight Hash Designs on the basis of the number of cycles

### Limitations:

-->It is prone to attacks like fast algebraic attack and correlation attack

-->it may largen the processing time.

---

## **Lightweight Cryptography Algorithms for Resource Constrained IoT Devices: A Review, Comparison and Research Opportunities**

### **Problems:**

IoT in a real-world deployment is very difficult. Security is considered as the number one challenge for IoT deployments, as most of the IoT devices are physically accessible in the real world and many of them are in limited resources.

### **Technique used in the paper and why is it used:**

Lightweight block cipher for IoT is used for this. This system helps us to provide IoT deployments in real world. This system makes IoT devices to be accessible in real world with less resources and can stop exposure to foreign attackers.

### **Details:**

When billions of smart devices working in a diverse set of platforms, especially when shifting from server to sensors, gives birth to various challenges to their users such as security & privacy, interoperability, longevity & support, technologies and many more. Also, IoT devices are easily accessible and exposed to many security attacks as they interact directly with the physical world to collect confidential data or to control physical environment variables, which makes them an attractive target for attackers.

For this case, cryptography could be one of the effective measures to guarantee confidentiality, integrity and authentication & authorization of the traversing data through IoT devices.

### **Advantages:**

--> can provide security for real-world IoT systems.

-->the system makes it easier for the IoT systems to run in real-life environment

### **Comparison:**

Lightweight cryptography system various characteristics such as area logic process, power consumption etc. are calculated and this system did well to safeguard the IoT systems and devices to perform better in the real-world environment.

### **Limitations:**

-->disadvantage of asymmetric encryption is its large key which increases the complexity and slows down the process.

-->Limited memory.

-->reduced computing power, low battery power, real-time response etc..

---

## **Improved authentication and computation of medical data transmission in the secure IoT using hyperelliptic curve cryptography**

### **Problems:**

Generally, data transmission is a great challenge in any network environment but in medical data collected from IoT devices need to be transmitted at high speed to ensure that the transmitted data are secure.

### **Technique used in the paper and why is it used:**

This paper focuses on the security, speed and load of transmission. The technique used here is combined steganographic methods involving cryptographic algorithms are used. This technique provides security.

### **Details:**

Data transmission is a great challenge in any network environment. However, medical data collected from IoT devices need to be transmitted at high speed to ensure that the transmitted data are secure. This paper focuses on the security, speed and load of transmission. To prove security, combined steganographic methods involving cryptographic algorithms are used. The proposed system involves medical data that are encoded and embedded into a medical image, which is compressed and transmitted over a secure channel of cryptographic transmission.

### **Advantages:**

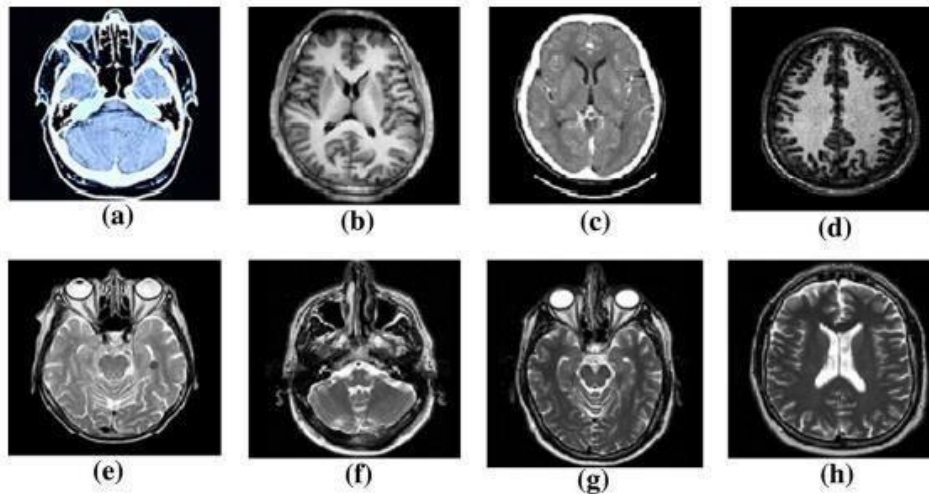
-->The image before the medical data is encoded does not change after retrieving the medical data.

-->Transmitted medical image is not distorted.

-->High quality of compressed and reconstructed images which was denoted by PSNR values.

### **Comparison:**

The data used throughout the experiment are MRI images and medical prescriptions obtained from MRI scanning. The performance of the proposed system was proven by the statistical metrics like PSNR, MAE, SSIM, SC and correlation.



(Images of the experiment using this system)

#### **Limitations:**

-->This method works better in a simulated environment only. The results prove the genuine nature of the proposed technique.

-->this system hides medical transcription data of different sizes in a sample image with average image.

### **Residential access control system using QR code and the IoT**

#### **Problems:**

Currently, residential safety is considered to be a priority by people. Most people use keys or key cards to access their residences. These things are what they have to carry with them at all times. However, if the keys or key cards are cloned, the residence can be accessed by an intruder. The common problems found in using keys to access residences are having to carry many keys, forgetting keys, losing keys, or even carrying too many items to the point that a person cannot use a key with their hand.

#### **Technique used in the paper and why is it used:**

This technique uses residential access control system (RACs) using QR codes and IoT for authentication and develop an android application to create an authentication key.

#### **Details:**

This research aims to solve the problem of using a key to access residences, buildings, or other places so that users will not need to carry additional objects or use biological information for authentication. Hence, users will be able to create keys for those who have been granted access.

### **Advantages:**

-->This system allows the users to access the lock of their house without any keys. So, the users don't have to carry it around always.

-->wireless access to the lock can be done with the help of this system.

-->security is enhanced as it is a better option than lock and keys.

### **Comparison:**

-->This method involves using keypad or biometrics together with sensors and smartphones to form a digital door lock system, creating a password from a computer or a smartphone.

-->This method provides various variables for authentication like keypad, biometrics, distance, smart feature etc. unlike other systems.

### **Limitations:**

--> possible tampering using the smart devices of ours by stealing etc...

--> limitation is the inability to access the security system remotely.

--> Using password is the easiest method, but it has the lowest security.

--> Using radio frequency identification (RFID) is convenient for access, but it needs to be carried like a key.

--> Biometrics is another method that has high security, but its limitation is the inability to access the security system remotely.

---

## **Lightweight Cryptography: A Solution to Secure IoT Problems**

In Internet of Things (IoT), the massive connectivity of devices and enormous data on the air have made information susceptible to different type of attacks. Cryptographic algorithms are used to provide confidentiality and maintain the integrity of the information. But small size, limited computational capability, limited memory, and power resources of the devices make it difficult to use the resource intensive traditional Cryptographic algorithms for information security.

### **Technique used in the paper and why is it used**

In this paper 21 lightweight block ciphers, 19 lightweight stream ciphers, 9 lightweight hash functions and 5 variants of elliptic curve cryptography (ECC) has been discussed i.e. in total 54 LWC primitives are compared in their respective classes.

## Details

Lightweight and low cost cryptographic algorithms are being developed for resource constrained IoT settings. These are evaluated on the basis of chip area occupied in hardware or memory requirements for their software implementation. IoT applications require the information security at very low latency.

## Advantages

AES is the most competitive cipher among block ciphers. In asymmetric cryptography, ECC remains the important option which provides authentication and non-repudiation in addition to the confidentiality. Ever evolving attacks underline the need for development of new lightweight ciphers which better sustain attacks and cost efficient, low cost lightweight cryptographic algorithms are crucial as more and more small scale business adopts to using IoT

## Comparison

The comparison of the ciphers has been carried out in terms of chip area, energy and power, hardware and software efficiency, throughput, latency and figure of merit (FoM). Based on the findings it can be observed that AES and ECC are the most suitable for used lightweight cryptographic primitives.

Light weight block cipher	Structure	Rounds	Key size (bits)	Block size (bits)	Weaknesses
RC5 [50], 1994	Feistel	0–255	0–2040 bits	32/64/128	Differential key attacks
TEA [51], 1994	Feistel	64	128		Bad as hash function; related key attacks
XTEA, 1997	Feistel	64	128	64	Related Key rectangle attacks on 36 round
AES [52], 1998	SPN	10, 12, 14	128, 192, 256	128	Bi-clique cryptanalysis
DESL [53], 2007	Feistel	16	56	64	–
PRESENT [50], 2007	SPN	31	80/128	64	Side channel attacks, related key attacks on 17 round
CLEFIA [43], 2007	Feistel	2488	128, 192, 256	39/128	Differential fault analysis,
KATAN and KATANTAN [55], 2009	NLFSR	254	80	32/48/64	Multidimensional meet in the middle attacks
	NLFSR	254	80	32/48/64	Theoretically broken under the single key setting
MIBS [56], 2009	Feistel with SPN round function	32	64/80	64	Many type of attacks
Humming-Bird [57], 2010	Hybrid	4	256	16	Several attacks
LED [58], 2011	SPN	8 for 64/12 for others	64/80/96/128	64	Bi-clique attacks on reduced rounds, differential fault analysis based on Super-S-box technique
TWINE [59], 2011	GFN Feistel	32	80/128	64	Meet-in-the-middle attacks
KLEIN [60], 2012	SPN	12/16/20	64/80/96	64	Truncated differential attacks
PRINCE [61], 2012	SPN	11	128	64	FX is a questionable choice for new attacks, 12 non-linear layers
ITUBEE [62], 2013	Feistel	– 20	80	80	Self-similarity cryptanalysis on 8-round
SIMON and SPECK [63], 2013	Feistel	32–72	64–256	32–128	Attacks on reduced versions and differential fault analysis
	ARX	22–34	64–256	32–128	
RECTANGLE [60], 2014	SPN	25	80/128	64	–
Midori [65], 2015	SPN	16/20	64/128		Many types of attacks
QTL, [66, 67], 2016	Feistel		64/128	64	Susceptible to linear differential attacks
ANU [68], 2016	Feistel	25	80/128	64	–
SFN [69], 2018	Feistel + SPN	32	96	64	–

## Limitations

Should focus on smaller key or block size, simpler rounds and key schedules in the development of Lightweight Block Ciphers. While in the field of Lightweight Stream Ciphers, minimization of key length, internal state and initialization vector should be researched upon. For Lightweight Hash Functions designer must try to reduce message and output size while providing high bit security. It is important for a LWC to occupy small chip area for its implementation.

-----



## Lightweight Cryptography for IoT: A State-of-the-Art Problem

With the emergence of 5G, Internet of Things (IoT) has become a center of attraction for almost all industries due to its wide range of applications from various domains. The explosive growth of industrial control processes and the industrial IoT, imposes unprecedented vulnerability to cyber threats in critical infrastructure through the interconnected systems

### Technique used

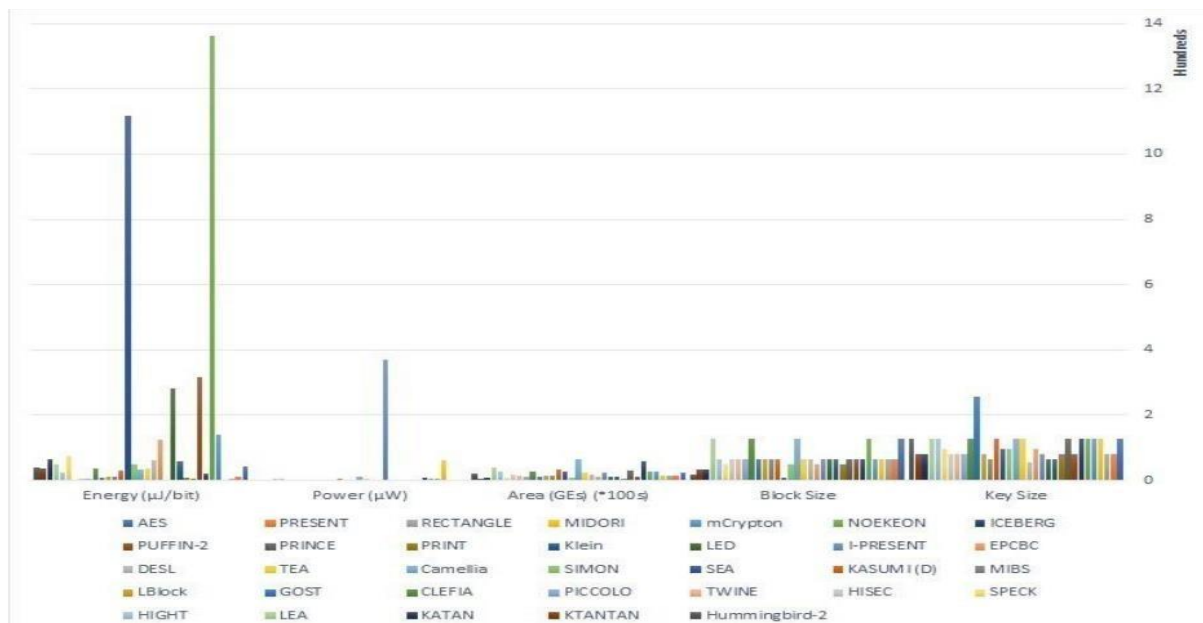
More than four dozens of lightweight cryptography algorithms have been proposed, designed for specific applications. These algorithms exhibit diverse hardware and software performances in different circumstances. This paper presents the performance comparison along with their reported crypto-analysis

### Advantages

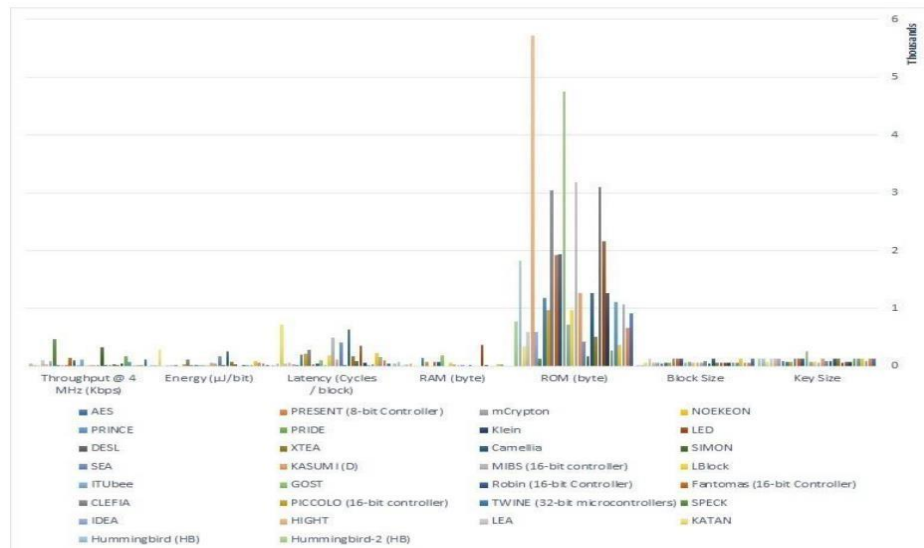
if conventional cryptography standards are applied to IoT devices, their performance may not be acceptable. The above issues with conventional cryptography are very well addressed by its subdiscipline, lightweight cryptography, by introducing lightweight features such as small memory, small processing power, low power consumption, real time response even with resource constrained devices

### Comparison

According to the graph, software efficiency competition is won by SPECK, followed by SIMON and then PRIDE. Also, IDEA, ITUbee, LEA and AES show better software efficiency compare to the other LWC algorithms



In terms of hardware efficiency, Midori, Piccolo, GOST, PRINT, PRINCE, Rectangle, PRESENT, MIBS, LBlock, TWINE, and HIGHT are the principal competitors.



### Limitations

The ideal algorithm should maintain a proper balance among cost, performance and security. Any two of the three design goals, security and low costs, security and performance, low costs and performance can be easily optimized, whereas it is very difficult to optimize all three design goals at the same time

## A Privacy-aware and Traceable Fine-grained Data Delivery System in Cloud-assisted Healthcare IIoT

### Problem

The emerging of healthcare Industrial Internet of Things (HealthIIoT) faces several fundamental security and privacy challenges, such as secure fine-grained data delivery, privacy preserving keyword-based cipher text retrieval, malicious key delegation, and efficiency of the system.

### Technique used

a Privacy-aware and Traceable Fine-grained System (PTFS) for secure data delivery in cloud assisted HealthIIoT is proposed.

### Advantages

The proposed system can achieve desirable functionalities including privacy-preserving access policy, traceability of malicious key delegation, online/offline encryption and lightweight decryption. the proposed scheme can achieve traceability and also be selectively-secure against chosen plain text and keyword attacks in the standard model.

### Comparison

Extensive simulation and experiment results demonstrate the effectiveness and efficiency of the proposed scheme for HealthIIoT.

Scheme	Access control	Single Keyword Retrieval	Traceability	Online/Offline encryption	Privacy Awareness	Lightweight Decryption	Asymmetric Pairing	Standard Model
ZXA [16]	✓	✓	✗	✗	✗	⊥	✗	✗
LSZ [17]	✓	✓	✗	✗	✗	✗	✗	✗
LS [18]	✓	✓	✗	✗	✗	✗	✓	✗
SYL+ [19]	✓	✓	✗	✗	✗	⊥	✗	✗
MML+ [20]	✓	✓	✗	✗	✗	✗	✗	✗
GSL+ [21]	✓	✓	✗	✗	✗	✗	✓	✗
LLZ+ [22]	✓	✓	✗	✗	✗	✓	✗	✗
DGC [23]	✓	✓	✗	✓	✗	✓	✗	✗
MTC+ [24]	✓	✓	✗	✓	✗	✓	✗	✗
QLS+ [26]	✓	✓	✗	✗	✓	⊥	✓	✗
SXD+ [27]	✓	✓	✗	✓	✓	✓	✗	✓
YLD+ [28]	✓	✓	✓	✗	✗	✓	✗	✗
MLC+ [29]	✓	✓	✓	✗	✓	✗	✗	✗
MML+ [39]	✓	✗	✗	✗	✗	✗	✓	✗
LLC+ [40]	✓	✗	✗	✗	✗	✗	✓	✗
CLG+ [41]	✓	✗	✗	✗	✗	✗	✗	✗
PTFS	✓	✓	✓	✓	✓	✓	✓	✓

## ECC-CoAP: Elliptic Curve Cryptography Based Constraint Application Protocol for Internet of Things

### Problem

Constraint Application Protocol (CoAP), an application layer-based protocol, is a compressed version of HTTP protocol that is used for communication. The CoAP is associated with Datagram

Transport Layer Security (DTLS) protocol for establishing a secure session

But there are several limitations regarding the key management, session establishment and multi-cast message communication within the DTLS layer are present in CoAP. Hence, development of an efficient protocol for secure session establishment of CoAP is required for IoT communication

### Technique used

The proposed protocol is an efficient and secure communication scheme to establish secure session key between IoT devices and remote server using lightweight elliptic curve cryptography

(ECC). The proposed ECC-based CoAP is referred to as ECC-CoAP that provides a CoAP implementation for authentication in IoT network.

### Advantages

It is more effective in terms of communication and computation overheads for resource constrained IoT devices. Thus ECC-CoAP becomes cost-effective solution for highly demanded client side IoT based CoAP applications

### Comparison

The proposed scheme will be used to solve the key management and related security issues of resource constraint IoT devices as well as securely operated in insecure

channel. The proposed scheme is mathematically analysed to show its strong resilience against relevant cryptographic attacks.

---

## Proposed Work

### ECC-Based Secret Key Derivation (using ECDH):

- This is non-trivial and usually involves a design of hybrid encryption scheme, involving ECC cryptography, ECDH key exchange and symmetric encryption algorithm.
- The elliptic curve cryptography (ECC) does not directly provide encryption method.
- Instead, we design a hybrid encryption scheme by using the ECDH (Elliptic Curve Diffie–Hellman) key exchange scheme to derive a shared secret key for symmetric data encryption and decryption.

The implementation involves a design of hybrid encryption scheme, involving ECC cryptography, ECDH key exchange and symmetric encryption algorithm.

- Assume we have a **cryptographic elliptic curve** over finite field, along with its generator point **G**. We can use the following two functions to calculate a **shared a secret key** for **encryption** and **decryption** (derived from the ECDH scheme):
- **calculateEncryptionKey**(pubKey) --> (sharedECKey, ciphertextPubKey)
- 1.Generate **ciphertextPrivKey** = new *random private key*.
- 2.Calculate **ciphertextPubKey** = ciphertextPrivKey \* G.
- 3.Calculate the ECDH shared secret: **sharedECKey** = pubKey \* ciphertextPrivKey.
- 4.Return both the **sharedECKey** + **ciphertextPubKey**. Use the **sharedECKey** for symmetric encryption. Use the randomly generated **ciphertextPubKey** to calculate the decryption key later.
- **calculateDecryptionKey**(privKey, ciphertextPubKey) --> sharedECKey
- 1.Calculate the ECDH shared secret:
- **sharedECKey** = ciphertextPubKey \* privKey.
- 2.Return the **sharedECKey** and use it for the decryption.
- The above calculations use the same math, like the **ECDH**.

$$(a * G) * b = (b * G) * a$$

- Now, assume that  $a = \text{privKey}$ ,  $a * G = \text{pubKey}$ ,  $b = \text{ciphertextPrivKey}$ ,  $b * G = \text{ciphertextPubKey}$ .
- The above equation takes the following form:

$\text{pubKey} * \text{ciphertextPrivKey} = \text{ciphertextPubKey} * \text{privKey} = \text{sharedECCKey}$

### ECC+AES:

Once we have the **secret key**, we can use it for **symmetric data encryption**, using a symmetric encryption scheme like AES-GCM.

It is based on the brainpoolP256r1 curve and the **AES-256-GCM** authenticated symmetric cipher.

We use the tinyec and pycryptodome Python libraries respectively for ECC calculations and for the AES cipher

### RSA+AES Hybrid Encryption:

- AES is a symmetric encryption algorithm - one key can be used to encrypt, and then decrypt the message. We securely share that key with the system you're exchanging encrypted data with, otherwise other people can decrypt your data, or pretend to create encrypted data on your behalf.
- RSA is an asymmetric encryption algorithm - a pair of keys is used, one you keep to yourself (private), and one you share with the rest of the world (public).
- If we want to exchange data with RSA, we use the other party's public key to encrypt the data, which can only then be decrypted with the private key that only they have.
- RSA is really helpful for key exchange but it's slow to use.
- AES is really fast, but suffers from the security risks of key exchange (which can be solved using RSA).

## Results—Review 2 and Review 3 results

### ECC-Based Secret Key Derivation (using ECDH):

```
C:\Users\kaus1\AppData\Local\Programs\Python\Python39\python.exe "E:/django project/GF6---Django-Login-System-main/encryption/ECC_secret key derivation .py"
compress_point runtime 0.007730807171630859
Encryption_keys runtime 0.015451431274414062
Decryption_keys runtime 0.014854669570922852
private key: 0x953a546ca998d64e6475f14067afb57625a28f5d7455612c4607868afaf25560
public key: 0x4c3cefc1c796a72716e1aa91afd850dc5c8608a5ac3ad7787b8d5414cdfc1e9c0
ciphertext pubKey: 0x2763107f17aefe5757231dd16997eb23c539bf59f7c9dd0ad938979253807db81
encryption key: 0x610bd1c5565e320ee04407eabc19a5695bc7397ebb6535746397db876a5a787a1
decryption key: 0x610bd1c5565e320ee04407eabc19a5695bc7397ebb6535746397db876a5a787a1
Total runtime of the program is 0.12518072128295898

Process finished with exit code 0
```

## ECC+AES:

```
C:\Users\kaus1\AppData\Local\Programs\Python\Python39\python.exe "E:/django project/6F6---Django-Login-System-main/encryption/ECC+AES hybrid.py"
Encryption_aes_GCM 0.004002571105957031
Decrypt_AES_GCM : 0.015607833862304688
ECC_point_to_key 0.016004562377929688
encryption runtime : 0.01613783836364746
Decryption runtime : 0.016198396682739258
original msg: b'my message is encrypted by hybrid algorithm and it is working fine with output. please send this result to anyone and work on it'
encrypted msg: {'ciphertext': b'0f1dda78c8dd677fbc4f645df3acd679b7863ea82b9f564d19807f48777960002656ba38ff72a7644d3d196bbab73e13167bd716aedec86de30df7988745c00bae1757722'}
decrypted msg: b'my message is encrypted by hybrid algorithm and it is working fine with output. please send this result to anyone and work on it'
Total runtime of the program is : 0.12707781791687012

Process finished with exit code 0
```

## RSA+AES Hybrid Encryption and Decryption:

### RSA Key generation:


```
PS C:\Users\kaus1\PycharmProjects\python-file-encrypt> python cryptor.py -g E:/key
[*] Generating RSA keys...
[*] RSA keys has been generated and saved to E:/key
RSA key generation runtime 0.497159481048584
PS C:\Users\kaus1\PycharmProjects\python-file-encrypt>
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\kaus1\PycharmProjects\python-file-encrypt> python cryptor.py -g E:/key
```

## Encryption:

```
PS C:\Users\kaus1\PycharmProjects\python-file-encrypt> python cryptor.py -e -f "E:/test/test1.pdf" -pub E:/key/public.key -d
[*] Encrypting E:/test/test1.pdf...
[*] E:/test/test1.pdf encrypted.
Encryption runtime 0.4848754405975342
PS C:\Users\kaus1\PycharmProjects\python-file-encrypt>
```

This PC > games (E:) > test			
Name	Date modified	Type	Size
 geljQfseWqBbitN.encrypted	12/9/2021 11:55 PM	ENCRYPTED File	5,185 KB

<div> <div> </div> <div> <div>This PC</div> <div>&gt; games (E:)</div> <div>&gt; key</div> </div> <div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div> </div>			
Name	Date modified	Type	Size
<div> <div></div> <div>private</div> </div>	12/9/2021 11:50 PM	KEY File	2 KB
<div> <div></div> <div>public</div> </div>	12/9/2021 11:50 PM	KEY File	1 KB

## Front-end:

Terminal: Local × Local (2) × + ▾

Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! <https://aka.ms/PSWindows>

PS E:\django project\GFG---Django-Login-System-main> python manage.py runserver

🔖

🔔 127.0.0.1:7000

## Testing Hybrid algorithm using Django

SignUp

SignIn

**Message:** Your Account has been created succesfully!! Please check your email to confirm your email address in order to activate your account. ×

### Log In to your account!

Username

Enter Your Username

Password

Enter Your Password

Log In

## Confirm your Email @ ISAA test - Django Login!!

➤ Inbox x



**review.isaa@gmail.com**

to me ▾

ISAA Project - Django Login!!

Hello kausik!!

Please confirm your email by clicking on the following link.

Confirmation Link: <http://127.0.0.1:7000/activate/OA/axexk5-0c4d30c4592b619719c856f5277bab6b>

↩ Reply

➡ Forward

## Testing Hybrid algorithm using Django

Hello !

You're successfully logged in.

sign out

continue

## Test - Django Login!!

➤ Inbox x



**review.isaa@gmail.com**

to me ▾

Hello kausik!!

This is a test!!

Thank you for visiting our website

. We have also sent you a confirmation email, please confirm your email address.

Thanking You

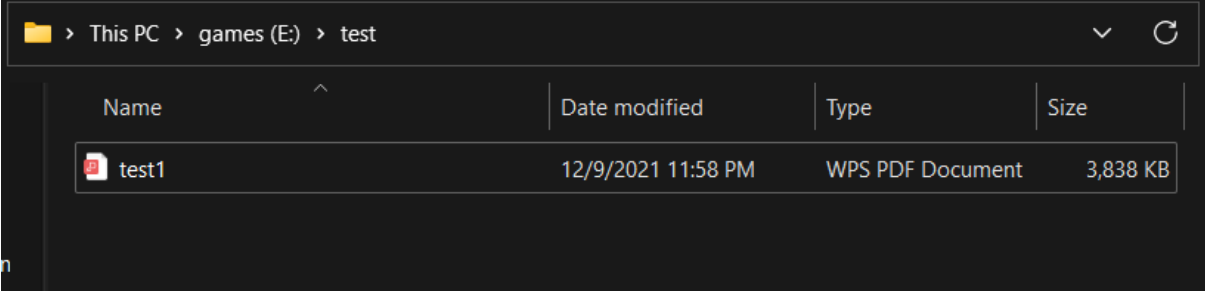
Kausik Nandhan

↩ Reply

➡ Forward



## Decryption:



```
PS C:\Users\kausl\PycharmProjects\python-file-encrypt> python cryptor.py -d -f "E:/test/geljQfseWqBbitN.encrypted" -priv E:/key/private.key
[*] Decrypting E:/test/geljQfseWqBbitN.encrypted...
[*] E:/test/geljQfseWqBbitN.encrypted decrypted.
decryption runtime 0.17093610763549805
PS C:\Users\kausl\PycharmProjects\python-file-encrypt>
```

## comparison

RSA+AES			
File Size	e_time	d_time	key_g_time
10kb	0.155s	0.149s	1.644s
15kb	0.104s	0.151s	1.654s
20kb	0.977s	0.143s	1.594s
30kb	0.101s	0.147s	1.614s
50kb	0.096s	0.1386s	1.644s

aes+ecc			
File Size	e_time	d_time	key_g_time
10kb	0.0145s	0.0165s	0.157s
15kb	0.0165s	0.0176s	0.181s
20kb	0.0134s	0.0187s	0.126s
30kb	0.0195s	0.0157s	0.173s
50kb	0.0193s	0.0167s	0.182s

As we can see RSA+AES algorithm lags behind the ECC and AES algorithm, but the Our RSA+AES algorithm has flexibility and can encrypt different type of files and large files too. Down below is the encryption and decryption times of a 15mb pdf file of our RSA algorithm

```
PS C:\Users\kausl\PycharmProjects\python-file-encrypt> python cryptor.py -d -f "E:/test/tbL0ddQmFpWSanJ.encrypted" -priv E:/key/private.key
[*] Decrypting E:/test/tbL0ddQmFpWSanJ.encrypted...
[*] E:/test/tbL0ddQmFpWSanJ.encrypted decrypted.
decryption runtime 0.27852892875671387
PS C:\Users\kausl\PycharmProjects\python-file-encrypt> python cryptor.py -e -f "E:/test/test.pdf" -pub E:/key/public.key
[*] Encrypting E:/test/test.pdf...
[*] E:/test/test.pdf encrypted.
Encryption runtime 0.6179943084716797
```

As size of the file gets bigger, RSA algorithm performs consistently and better than the other algorithm. The drawback however is RSA algorithm require much more processing power than the ECC+AES algorithm. Hence ECC+ AES algorithm is better when it comes to encrypting small files and RSA can work better with large files.

### **Conclusion**

In this project we proposed and implemented two Hybrid algorithms – ECC secret key derivation, ECC+AES and RSA+AES with varying levels of success, this project helped us get a great understanding on cryptography and the potential security flaws that we could fix. Future work includes using advanced algorithms to make our algorithms lighter so that these encryption algorithm could be used in cloud based systems with real time encryption of IoT devices. We hope to work on it in the future.

### **Code file (Google Drive Link)**

<https://drive.google.com/file/d/1CTDv0tp9G8ZaSmxc-8fK3KCts36hkP7I/view?usp=sharing>

### **References**

[https://www.researchgate.net/publication/257575022\\_Towards\\_a\\_theoretical\\_framework\\_of\\_strategic\\_decision\\_supporting\\_capability\\_and\\_information\\_sharing\\_under\\_the\\_context\\_of\\_Internet\\_of\\_Things](https://www.researchgate.net/publication/257575022_Towards_a_theoretical_framework_of_strategic_decision_supporting_capability_and_information_sharing_under_the_context_of_Internet_of_Things)

[https://www.researchgate.net/publication/345144109\\_Recent\\_Advances\\_and\\_Trends\\_in\\_Lightweight\\_Cryptography\\_for\\_IoT\\_Security](https://www.researchgate.net/publication/345144109_Recent_Advances_and_Trends_in_Lightweight_Cryptography_for_IoT_Security)

<https://link.springer.com/article/10.1007/s12652-020-02672-x>

[https://www.researchgate.net/publication/341134576\\_A\\_Systematic\\_Technical\\_Survey\\_Of\\_Lightweight\\_Cryptography\\_On\\_Iot\\_Environment](https://www.researchgate.net/publication/341134576_A_Systematic_Technical_Survey_Of_Lightweight_Cryptography_On_Iot_Environment)

<http://oaji.net/articles/2015/2028-1433398925.pdf>

[http://www.jucs.org/jucs\\_19\\_16/an\\_efficient\\_ciphertext\\_policy](http://www.jucs.org/jucs_19_16/an_efficient_ciphertext_policy)

<https://dl.acm.org/doi/abs/10.1002/dac.2960>

[https://www.researchgate.net/publication/270896791\\_CHALLENGES\\_DRAWBACKS\\_AND\\_BEST\\_PRACTICES\\_OF\\_RFID\\_TECHNOLOGY\\_IN\\_HANDLING\\_OF\\_INFORMATION\\_AND\\_LIBRARIES](https://www.researchgate.net/publication/270896791_CHALLENGES_DRAWBACKS_AND_BEST_PRACTICES_OF_RFID_TECHNOLOGY_IN_HANDLING_OF_INFORMATION_AND_LIBRARIES)

<https://www.usenix.org/system/files/nsdi20-paper-burkhalter.pdf>

<http://ieeexplore.ieee.org/document/9184078>

<https://www.usenix.org/system/files/nsdi20-paper-burkhalter.pdf>

-->Efficient Data Access Control with Fine-Grained Data Protection in Cloud-Assisted IIoT

--> Lightweight Cryptography: An IoT Perspective

--> Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities

--> Improved authentication and computation of medical data transmission in the secure IoT using hyperelliptic curve cryptography

--> Residential access control system using QR code and the IoT

Dhanda, Sumit Singh, Brahmjit Singh, and Poonam Jindal. "Lightweight cryptography: A solution to secure IoT." *Wireless Personal Communications* 112.3 (2020): 1947-1980.

Thakor, Vishal A., Mohammad Abdur Razzaque, and Muhammad RA Khandaker. "Lightweight Cryptography for IoT: A State-of-the-Art." *arXiv preprint arXiv:2006.13813* (2020).

Sun, Jianfei, et al. "A Privacy-Aware and Traceable Fine-Grained Data Delivery System in Cloud-Assisted Healthcare IIoT." *IEEE Internet of Things Journal* 8.12 (2021): 10034-10046.

Majumder, Suman, et al. "ECC-CoAP: Elliptic curve cryptography based constraint application protocol for internet of things." *Wireless Personal Communications* 116.3 (2021): 1867-1896.