ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 6, Issue 2, pp: (107-110), Month: April - June 2018, Available at: www.researchpublish.com

Energy Analysis of Cryptographic Algorithms for Sensing Vital Parameters on Android Applications

[1]Anusha J, [2]Chaitra S J, [3]Deeksha K G, [4]Haripriya Reddy R, [5]Santosh Kumar G,

[1, 2,3,4]Student, [5]Asst. Prof., CSE, DBIT

Abstract: **Due to great development in the recent technologies there is a major challenge for battery usage and secure data transfer on mobile platform. The solution to conserving battery power lies in using communication means that guarantee the confidentiality, authentication and integrity of communications. Reliable and secure communication can be achieved using cryptography and authentication protocols. In the current study, comparative analysis of battery usage is shown by using Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) algorithms to achieve end-to-end encryption. Pulse rate and body temperature are the basic parameters for monitoring and diagnosing human health. In order to secure these vital parameters cryptographic algorithms are implemented.**

Keywords: **Security, Cryptography, RSA, ECC, Cloud security, Arduino, Sensors.**

1. INTRODUCTION

As the technological enhancements in the smart phone segment has given rise to a rapid growth in mobile networks and services in recent days, the aim have emerged as an important tools in our daily lives. Due to ever emerging smart phone market and user base, key business players in e-commerce, educational services and other markets are including mobile devices and smart phones for application and service development.One of the key challenge in the mobile and smartphone segment has been the limitations of resources like battery power, CPU and memory. Significant portion of battery capacity is consumed by complex applications used in mobile and handheld devices.

In this project, we provide an analysis on battery power usage of smartphones using RSA (Rivest

Shamir Adleman) and ECC (Elliptical Curve Digital Signature) cryptography algorithms for data encryption using an android based healthcare application.

The advancement of cloud computing and smart devices has an important and productive impact on the lives of users, especially in regard to elements of healthcare. There are multiple types of sensors available in the market that enable individuals to use medical devices, to remotely monitor their health activities. Also the data collected by these medical devices can be made available in cloud enabled applications, thereby enabling physicians to respond quickly in the event of emergencies. However there is a need to address important concerns such as patient security, privacy, confidentiality, and identity theft. The solution is to use appropriate cryptography algorithms to encrypt data while being uploaded to cloud enabled applications.

In this paper, the design and implementation of an android based health care application that collects vital signs like pulse rate and body temperature, and send the encrypted data to an application available on cloud. By incorporating 2 key cryptography algorithms viz RSA and ECC for data encryption and also analyze the battery power dissipation while uploading the data to the server.

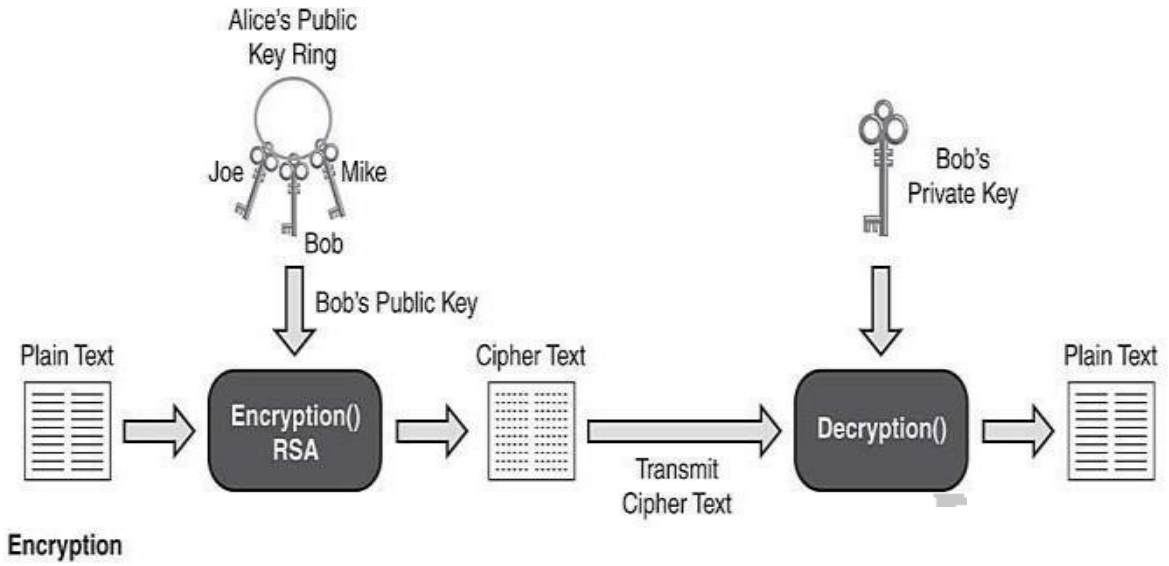
ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 6, Issue 2, pp: (107-110), Month: April - June 2018, Available at: www.researchpublish.com

2. SYSTEM MODEL

The system will consist of two parts: a smartphone application and a web portal on the cloud. The mobile application will be used to periodically sense body temperature, pulse rate and location parameters and upload the encrypted data to cloud using REST APIs. The application on the cloud stores the body parameters in a database, which can be viewed using web application screens. The mobile application provides options (RSA/ECC) to encrypt the data before upload. The time taken for the encryption will be displayed on the mobile application screens.

3. ALGORITHMS

RSA Algorithm



RSA steps:

1. Key generation

- Select p and q(both prime)
- Calculate n (n= p*q)
- Select integer d (gcd($_{\phi}$(n,d)=1)); 1<d<$_{\phi}$(n)
- Calculate e (e=d^{-1} mod $_{\phi}$(n))
- Public key (KU ={e,n})
- Private key (KR = {d,n})

2. Encryption

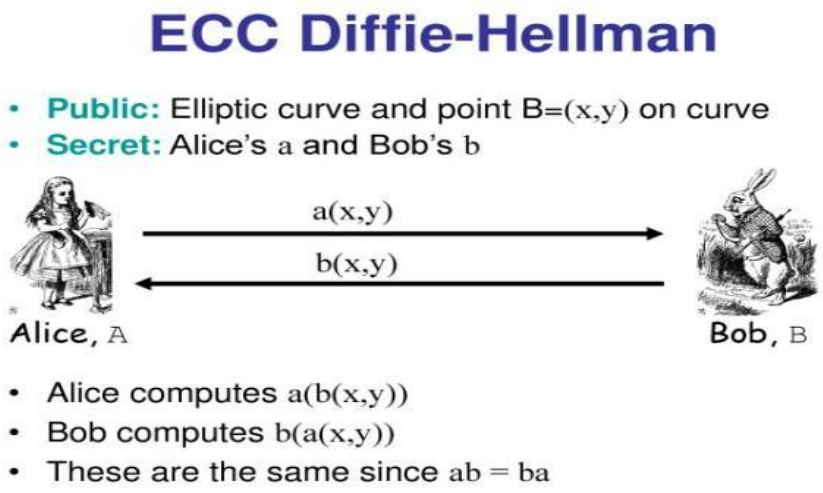
- Plain text M<n
- Cipher text $C=M^e \pmod n$

3. Decryption

- Cipher text C
- Plain text $M = C^d \pmod n$

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 6, Issue 2, pp: (107-110), Month: April - June 2018, Available at: www.researchpublish.com

ECC Algorithm



4. IMPLEMENTATION

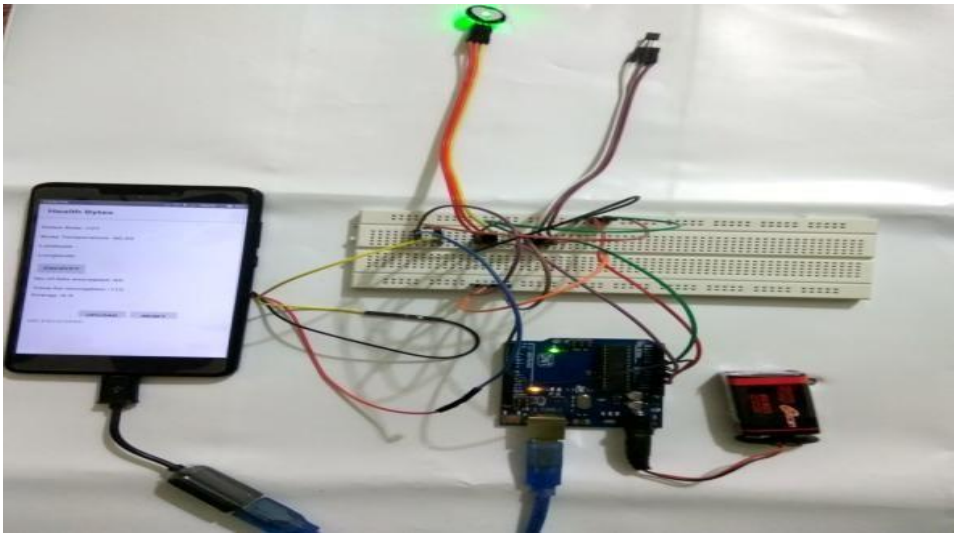
The implementation and testing of the Health Bytes application, performed using the hardware and software. This paper highlights the implementation phase with code segments and pseudo code for such important functions, as well as the testing of the application in terms of system functionality and performance.

The implementation of our proposed system can be organized into 4 phases namely

1) Sensor data capture using electronic sensors and arduino uno microcontrollers
2) Interface module to integrate the sensor nodes via micro controller with the android application.
3) Android application with required user interface to facilitate the user to capture sensor data, encrypt and upload the details to server.
4) An n-tier JAX-RS web application to persist user data.
5) Energy and power is calculated using,

$$P_{Inst} = (V_R / R) \times V_{PDA}$$

$$E = \sum P_{Inst} \times T$$



ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 6, Issue 2, pp: (107-110), Month: April - June 2018, Available at: www.researchpublish.com

5. RESULT ANALYSIS

Since ECC uses smaller key size when compared to RSA , time taken for encryption by ECC is less. For same level of security ECC uses less energy than RSA.

6. CONCLUSION

Using this experiment it can be concluded that ECC algorithm can be used to encrypt and secure data as it consumes less energy than RSA. This is important as mobile platforms have limited battery resource .The main aim of this project is to analyze power consumption of a mobile hand -held device, since power consumption is time dependent.

Future scope:

An extensive study can be made on different mobile platforms running different OS (ios/windows).

REFERENCES

[1] K Satish Kumar, R Sukumar, P Asrin Banu "An Experimental study on Energy Consumption of Cryptographic Algorithms for Mobile Hand-Held Devices"-2012

[2] Salomi S. Thomas, Mr. Amar Saraswat, Anurag Shashwat, Dr.Vishal Bharti-" Sensing Heart beat and Body Temperature Digitally using Arduino"- 2016

[3] Mohammed Aledhari, Ali Marhoon, Ali Hamad, and Fahad Saeed "A New Cryptography Algorithm to Protect Cloud-based Healthcare Services" -2017

[4] Longhao Zou,, Ali Javed, and Gabriel-Miro Muntean-"Smart Mobile Device Power Consumption Measurement for Video Streaming in Wireless Environments: WiFi vs. LTE".

[5] Arvinderpal S. Wander, Nils Gura, Hans Eberle, Vipul Gupta, Sheueling Chang Shantz, Energy Analysis of Public-Key Cryptography on Small Wireless Devices, The IEEE PerCom 2005.

[6] Ann Hibner Koblitz , Neal Koblitz , Alfred Menezes, Elliptic Curve Cryptography : The Serpentine Course of a ParadigmShift

[7] Chu -Hsing Lin , Jung -Chun Liu , Chun -Wei Liao, Energy analysis of multimedia video decoding on mobile handheld devices, Computer Standards & Interfaces Volume 32 Issue 1-2,2009.

[8] Nachiketh R.Potlapally,Srivaths Ravi,Anand Raghunathan and Niraj K . Jha , A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols ,2006.

[9] Wendy Chou, Dr. Lawrence Washington , Elliptic Curve Cryptography and Its Applications to Mobile Devices,2004.