MobileAppEncryption

Vishal Koosuri
Mitin Sharma

April 2017

1 Abstract

In today's world, mobile phones have evolved in a greater extent than ever before. With this sort of an evolution in mobile phones, there is a constant need to mobilize the daily needs. As mobilisation plays an important part, it is also very important to consider how secure it is. So, to secure our devices from the constant threat of vulnerabilities that lie around us security plays a vital role. To communicate with the people around us, and to ensure some private virtual communication space while communicating with our loved ones or discussing an important business plan Cryptography or Cryptology plays a major role.

As the name says, Cryptos meaning hidden or secret and logos means study, to put it simple it is the study of techniques for secure communication, preventing intrusion and providing data confidentiality, integrity, authentication, and non-repudiation. In Cryptography, Encryption plays a crucial role in adding additional layer of Security to the devices or software(in here, apps) that we use in our day to day lives.

2 Introduction

Cryptology or Cryptography has always been one of the fascinating areas of study. It has gained huge popularity such that around 77 percent of Google Internet Traffic is now encrypted. Due to this increase in the trend for Cryptography in the past few years, we were excited to take-up Security Algorithms and Protocols as an area of study.

To ensure proper understanding of the concepts of Cryptography, we are going to implement this on a Mobile Chat app. This application establishes an ad-hoc network to quickly connect with its peers. So, to ensure that this connection is private and secure we are going to implement 128-bit AES encryption algorithm.

3 Related Work

In the past, there have been few applications which kind of implement the ad-hoc networks like FireChat. This has gained huge popularity especially during the Hong-kong protests, Ecuadorian protests, etc. This application provides an end-to-end encryption.

4 Methodology

To construct our application we are making use of resources like Android Studio, as we plan on building a native Android application.

5 Experiments

We have tried to implement the Hill Cryptosystem that we wrote in the class to check how Encryption works by writing a small text application to encrypt the text we enter.

6 Analysis

With some minor tweaks to the code, everything worked pretty well, and this has further given us confidence towards implementing AES-128.

7 Conclusion

Experimenting with the Hill Cryptosystem was exciting part that we had done so far. And, we are looking forward to implement it with AES-128 and make our chat app robust; so that communication would remain private. This certainly seems an uphill task given the time constraint but we are pretty sure we could make this happen.

8 References

- https://en.wikipedia.org/wiki/
- http://www.brighthub.com/computing/enterprise-security
- http://www.pcmag.com/news
- http://www.cisco.com
- https://www.opengarden.com/
- http://www.webopedia.com/