CRYPTOGRAPHY USED IN WHATSAPP

ABSTRACT

☒ In this era people are closely connected to each other using technology. Messaging services play a crucial role in this process.

☒ For this, WhatsApp Messenger being an exclusive cross-platform that allows to exchange text, files as well as audio and video messages.

☒ WhatsApp has 1.5 billion dynamic clients in 180 nations. However, being such a well-liked application, taking care of privacy breach is very salient. It is necessary that the application protects client's confidentiality and authenticity.

☒ Thus, to give assurance and stealth to client, for the most part cryptography is utilized as a spine of the web-based exchanges.

☒ WhatsApp utilizes End-to-End Encryption technique and uses various protocols (Signal protocol etc.) and keys (public key, private key etc.) along with algorithm like Curve25519.

KEYWORDS: public key, private key, Curve25519, End-to-End Encryption, Cryptography, Signal protocol, SHA256 hashing algorithm

INTRODUCTION

☒ The world is moving in a fast pace and it is arduous to keep in touch with the cutting edge of technology. The era has brought smart phones in use to propel with the flow.

☒ Many applications and messaging services play a vital role in this process. WhatsApp being a free messaging service application it is well accepted by people.

☒ The app is owned and administrated by Facebook Inc and helps to connect manage and companions. Furthermore, it facilitates the user for video call, share documents and images and instant messaging.

☒ As the application gets widened and the rapid increase in users, the system calls for security and privacy.

REFERENCE

1. Case study on whatsapp end to end encryption by Miss. Rachna Agrawal and Mr. Rishabh Rathore

2. WhatsApp Security Paper Analysis by Calvin Li, Daniel Sanchez and Sean Hua.

Anushka Xavier K

Computer Science Engineering

Karunya Institute of Technology and Science

IMPLEMENTATION

☒ WhatsApp uses End-to-End Encryption (E2EE) to convey messages secure, hassle-free and privately. This innovation ensures that there is no privacy breach occurs at any cost.

☒ The Encryption and Decryption of data are done at both sides – From Sender to Recipient. This ensures that the messages are secured and provides confidentiality and authenticity.

☒ WhatsApp utilizes open source Signal Protocol, created by Open Whisper Framework. It produces the private key on user's phone and stores the public keys on their server.

☒ The application uses Curve25519 encryption and SHA256 hashing algorithms to create keys and encrypt messages. When user chat with someone it saves that key exchange so that it does not have to repeat that key exchange next time the user chat.

☒ When Reinstallation of WhatsApp occurs and the chats are lost new set of keys are created due to which old messages cannot be read.

CONCLUSION

☒ Privacy and protection is a key factor in every message exchange. It is vital to encrypt and protect the client's information.

☒ End-to-End Encryption attains this goal and keeps the confidentiality of the users.

☒ Thus WhatsApp being the world's biggest platform for online communication satisfies the customer's needs and provides a safe and sound environment for people.

☒ It has risen as the renowned messaging application in today's market.