

Rahasak

SCoRe Lab @ university of colombo school of computing

July 2017

1 Rahasak

1.1 About Rahasak

Rahasak is an innovative application that helps your to share your secret data such as voice calls, texts, location information and selfies without revealing to the rest of the world. It never saves your secrets on its server. Rahasak encrypts your secret information between you and your friend, so no one can see them.

1.2 Rahasak features

1. Secret calls
2. Secret texts
3. Secret location sharing
4. Secret selfies :)

1.3 Rahasak download

Rahasak app can be downloaded from google play

<https://play.google.com/store/apps/details?id=com.score.rahasakhl=en>

2 Security Architecture

Rahasak app encrypts the communication by using AES 256 keys. AES key is exchanged between the users by using 1024 bit RSA public key encryption. RSA public keys will be distributed to the users by using dual channels that is SenZ Switch and SMS.

If someone wants to break the security of the system, both mobile SMS service provider and SenZ switch need to be simultaneously compromised. It is unlikely to be happen and therefore Rahasak provides perfect data protection to their users.

3 Technologies

We mainly focused on functional programming when building the services. Following is the technology stack

1. Scala
2. Akka
3. Reactive streaming
4. Erlang
5. Android
6. Opus codec for audio compression