CRYPT ALARM

Tailored Algorithms for Security Applications

a spin-off of

UNIVERSITA' degli STUDI di ROMA
TOR VERGATA

Shield My SMS

Shield My SMS is an Android App that allows to exchange encrypted Short Messages.
Messages are encrypted with a secret symmetric key shared between sender and receiver.
The customer can choose the encryption algorithm among the following ones:
- QP-Dyn 64 bits (or higher)
- AES 128 bits
- 3DES 128 bits

Essential features:

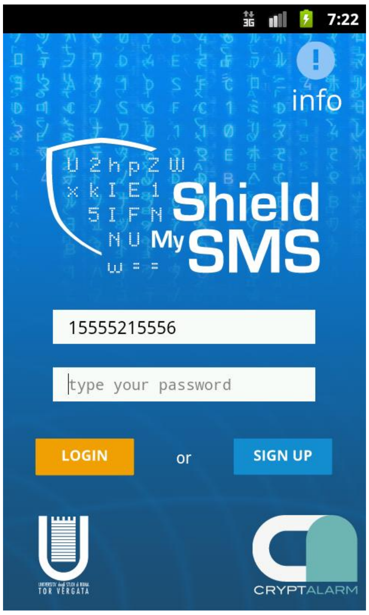
- Great performance in terms of speed and CPU load
- Encrypted messages are stored in the App database. They are decrypted and shown as plain text only when the user wants to see them.
- Messages can be encrypted with a session key. In this case the public key will be sent together with the message to allow decryption.
- Configurations and messages can be exported or imported to/from the SDCARD.
- The App includes a complete user guide.
- Nice look.

The App can be used with different SIMs; one passphrase per SIM is allowed.
Each time the passphrase is typed, the App produces the secret and the public key of the user.
These, together with the receiver public key, allow the creation of a shared secret key (SSK) which is then used to encrypt messages with the chosen algorithm.
The App includes a repository of public keys which can be updated by:

- Downloading new keys from different kinds of certification authorities (web sites, PKI, …).
- Through direct communication with the owner.
- Loading from the SDcard directory.
- Pasting from clipboard.

The 4 command icons

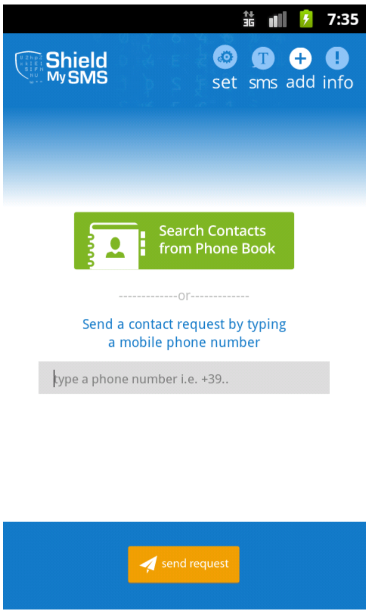
- set to modify the App settings
- sms to see the list of contacts whose public key is stored and of active chats. Selecting one of them, messages are decrypted and shown.
- add to send contact requests to others
- info to access the user guide



15555215556

type your password

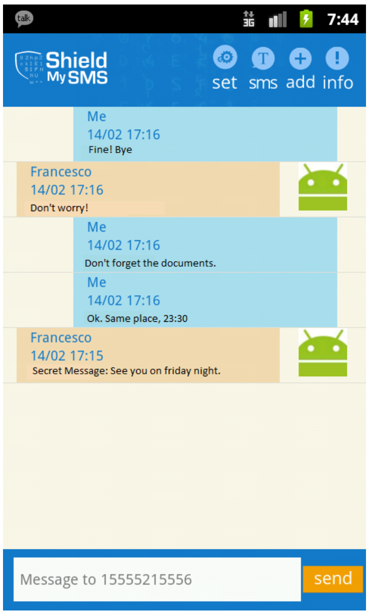
Select phone number, type passphrase and tap:
- Login to enter into an existing account
- Sign up: to create a new account



Send a contact request by typing a mobile phone number

type a phone number i.e. +39..

No external server required in this mode: users can directly request public keys to other users.



Me
14/02 17:16
Fine! Bye

Francesco
14/02 17:16
Don't worry!

Me
14/02 17:16
Don't forget the documents.

Me
14/02 17:16
Ok. Same place, 23:30

Francesco
14/02 17:15
Secret Message: See you on friday night.

Message to 15555215556

The App shows the list of contacts corresponding to encrypted messages. Selecting a name, the corresponding messages are decrypted and shown in a chat fashion.

www.cryptalarm.it

CryptAlarm s.r.l.
Operating Headquarters
Centro Interdipartimentale V.Volterra
Facoltà di Economia - Edificio Ricerca
Università di Roma “Tor Vergata”
Via Columbia 2, 00133 Roma, Italy
Tel. (+39) 06 2022498

info@cryptalarm.it