Manual of LATEBRA

Introduce

Now when a lot of organizations and persons try to infringe your privacy, the privacy protection became actual task.
This task is solved by Latebra which creates “ecosystem” to exchange by confidential E-mail/ SMS/ MMS messages and to be not afraid that somebody can read it. Latebra encrypts and protects your contact date even if your phone (or tablet) was stolen.

1 Initial Setup

1.1 App Crypto-key Generation

The work with Latebra starts with a crypto-key generation which is used for access to Application (or Latebra “ecosystem”) and contact data encryption/decryption. This crypto-key has name App Crypto-key.
You have to define usable alphabets, set security level and enter a codeword. More detail this procedure is explained below.

1.1.1 Codeword

You have to invent a codeword (or a phrase), determine languages used in correspondence and set security level when you generate a crypto-key. A codeword has to include numerals and Roman characters only without diacritical marks, but last symbol cannot be a numeral. A codeword can be a phrase not only word.

Figure 1.1 Crypto-key generation

Long codeword creates crypto-key with large length and hence your encrypted message is more difficult to crack.
Maximum codeword length is 10 symbols. Fig. 1.1 shows conditions of generating crypto-key **gOndhW8Z5rUOqxqzWH**.
How many combinations are needed to go through in order to pick up such a crypto-key?
The codeword will be a password for access to Latebra. The codeword provides not only access to Latebra but helps to restore or change App crypto-key in any time.

You have to remember codeword, it's important.

(Previous codeword(s) is useful for decryption of contact data which you forgot to decrypt before update of App crypto-key).

1.1.2 Usable Alphabets

Crypto algorithm of Latebra Light uses alphabets of English language and language of mobile device (smartphone or tablet) localization as alphabetical base on default. When you use or plan to use other languages in your messages you will have to expand list of usable languages. In other case the characters which are missed on these alphabets cannot be encrypted.

1.1.3 Security Level

You can manage security level on seek bar in Latebra from 1% till 99%. Security will be more than the level will be set larger, but the encryption in this case will be slower.

Remember!!! The more security level you will set the more time will be needed for encryption*/decryption.*

1.1.4 App Crypto-key

The App Crypto-Key generation will have been finalized by click on the button after as you have defined Usable Alphabets, set Security Level and typed a Codeword.
Next step. You have to define the mode usage of you're a codeword: would it be requested every time at startup the Application or not?

!!! We recommend to use the mode: "request codeword upon startup".

Figure 1.2 The determination of usage mode for codeword

1.2 Connection E-mail Accounts

The following step is providing Latebra connection to Email account. In this case Latebra became Email client with possibility of encryption/decryption. You have to type an address of your E-mail (Gmail or Yandex only), your password and click the button to activate.

Don't forget to turn on access to your account in Gmail for Latebra!!! It's important. Latebra cannot work with Gmail without this permission.

In present time Latebra connects directly to Gmail and Yandex only. With other E-mail services Latebra can work through copy&paste only.
Also in any case you can work in Latebra with SMS/MMS even if Latebra didn't connect with E-mail accounts.
In any time initial settings can be changed by using "Settings" . Here you always can change active E-mail account, connect some new accounts, change and restore your App crypto-key.

Figure 1.3 Turn on access to E-mail account(s)

1.3 Main window

If initial setup is finished, you can start to work with Latebra. Hereafter all management of Latebra will realize through main window to call up:

- Inbuilt “Address book” to encrypt, use, edit of contact data, generate and distribute personal crypto-key;
- The unified messaging support environment to load of received messages, view of loading messages list and activation of “Editor” for following work with selected message:
  viewing,
  decrypting,
  creating new,
  editing,
  encrypting
  and sending;
- “Editor” for fast creating, encrypting, and sending messages without preliminary loading of received messages;
- Settings of Latebra.

Figure 1.4 Main window

2 Work with Contacts

Encrypting contact data is performed by using of App crypto-key and prevents unauthorized access to them. Anybody through standard application “Contacts” can see only encrypted data. Even if your mobile device was stolen, nobody will have access to your contact data without knowledge of App crypto-key providing access to Latebra.

Figure 2.1 Alphabetical contact list partially encrypted in “Address book”

Click the button “Address book” in Latebra action bar to start your work with contact data in Latebra.

2.1 Alphabetical Contact List

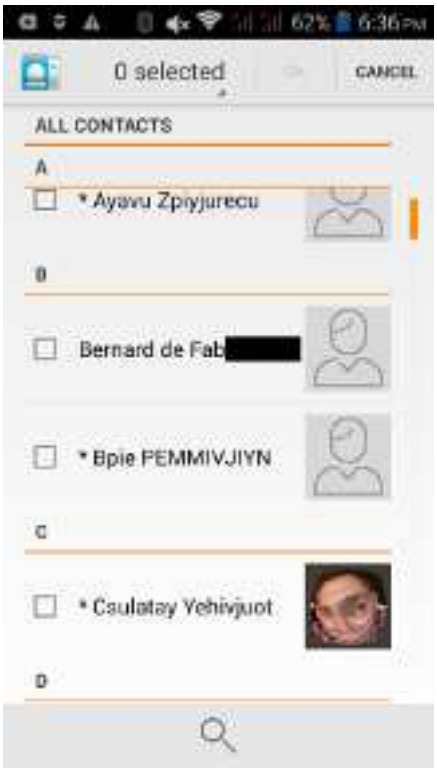
The click on the button “Address book” will open alphabetical contact list. Click on the snackbar “Filter“ to change active contact group. It will initialize shortcut menu where this changing can be done.

To left of the name locates check-box, if it is marked the contact data record will be encrypted all or partially.

“Gold key” situated to right of the name means this contact has personal crypto-key which used for encryption/decryption messaging. You can also make the following actions:

1. encrypting/decrypting contact data;
2. sorting data;
3. searching required contact;
4. opening “Contact Card“ for additional actions;
5. merge duplicate contacts (procedure “prophylaxis”).

2.1.1 Contact Data Encryption/Decryption



A contact data record in alphabetical contact list can be encrypted by click on the button , decrypted by click on the button . It can be done for all records or partially in accordance with selected option by the click on the shortcut menu (Fig.2.1).
We recommend saving the result of encryption. In this case a contact data records through standard application “Contacts“ became useless (Fig.2.2).
Only you, who know the codeword and can startup Latebra, can use their.
But you should remember if you decrypt contact data and save result, this contact data will become available for using in standard application “Contacts”.

Figure 2.2 The view of standard “Contacts”

2.1.2 Contact Data Sorting

Click on button “Sort” in the action bar to initialize shortcut menu with options of required sorting: 1) by name; 2) by surname; 3) by arrival time.

2.1.3 Search

Click on the button “Search” in the action bar to find required contact record. You just have to type required name or surname character by character and select from tapering list of offered variants. Search will be done simultaneously in contact records with similar name and surname.

2.2 Contact Card

Click on a contact record in alphabetical contact list to open a “Contact Card” with a photo and contact data: phone numbers and E-mail addresses. These contact data can be encrypted all or partially directly in the “Contact Card”.
Each fields of a “Contact Card” are control elements. Click on “Name” to show personal crypto-key (if it exists for this contact).
Click on “Phone numbers” to call the dialog:

1. to the data edit;
2. to delete their;
3. to call to selected phone number;
4. to send SMS/MMS message to the phone number.

Click on “Email” to call similar dialog to edit or delete data or to send Email to the selected Email address.

Figure 2.3 The view of Contact Card

When you select the option to send message and click suitable button, it calls up the Editor for typing, encrypting and sending a message.
A “Contact Card” is used for creation and distribution of personal crypto key, just click on the button “Gold key” in action bar.
The personal crypto-key linking with the contact is used for encryption. If a personal crypto-key for this contact is absent, a crypto key can be created and assigned directly in the Editor.

2.2.1 Personal Crypto-key

Click on the button “Gold key” in “Contact Card” action bar to generate, assign and send the Personal Crypto-key to the contact. You have to choose only the delivery method (SMS or Email).This Personal Crypto-key will be used for message encryption/decryption from/to this contact by default.
When you send this Personal Crypto-key to your addressee, he (he has to have Latebra) has to assign the crypto key to you and in this case, encryption/decryption of messages will be done in one click.
Latebra selects needed Personal Crypto-key automatically in accordance with the contact data.

2.2.2 Messaging

Click on the button “Messaging” in “Contact Card” action bar and produce the message list from this person. You just have to select in what kind of messages SMS/MMS or/and E-mails will be interesting for you.

2.2.3 Prophylaxis

Sometimes contacts are duplicated. It' creates problems to users. If you click on the button “Prophylaxis” , these duplicate contacts can be merged and the problem will be solved.

3 Work with Messages

Click on the button “Message” to load messages in Latebra.
Only users of Gmail and Yandex can work with Latebra effectively, Latebra will be Email client with encryption/decryption functionality for them. Users of other Email services can work with Latebra uses only copy&paste mode. They cannot load messages into Latebra directly.
The work with messages starts with the selection kind of messages Fig. 3.1, and then you have to click the button “next” to load messages in accordance with filter condition.
Click on any message in message list to select it for following action:

Figure 3.1 Dialog menu for message selection

Figure 3.2 Messaging

1. To load selected message into Editor for viewing, encrypting/decrypting sending and responding (click on the button);
2. To view message chain (sent messages have dark background) with addressee of selected message (click on the button);
3. To delete selected message (click on the button)

You can create and send a new message by click on action button "New" and manage E-mail accounts by click on the button "Account Management".

Figure 3.3 Message chain

3.1 Editor

There is the direct call up of the Editor for acceleration and optimization of the work with messages by clicking on the button in main window of Latebra. It provides possibility to create and send new Emails without preliminary loading others Emails, it became important when speed of Internet is low.

The Editor can be called up also by 2 other ways:

1) Click on selected message in list of messages and load it into the Editor.

2) Click on the button "New" and call up the Editor where you can create, encrypt and send a new message.

The Editor provides following functionality:

1) viewing;
2) creating and editing, including pasting of text from clipboard;
3) encrypting/decrypting;
4) saving;
5) sending of messages;
6) generation crypto-keys directly inside Editor; it can be done by just click on the button .

Figure 3.4 Creating new message in the Editor

3.1.1 Message Encryption

If you would like to provide confidentiality of your messaging you just have to click on the button "Encryption" and encrypt a message.

Remember - your correspondents have to have Latebra.

Encrypted a message will be done by crypto-key which preliminary was assigned by you or attached to this message.
If you need to respond you just have to click on the button "Reply" and use your with this correspondent crypto-key.If your correspondent didn't have personal crypto-key, it can be sent to him with this message.
When you sent crypto-key to any person, it means that you invited him in your circle of trust. If your addressee assigned this crypto-key to you, this addressee became a member of your confidential messaging. Both of you can don't think about which crypto-key has to be used for encryption/decryption. The encryption/decryption procedure of your messaging from/to this person will be done automatic in one click.
It means that you both are in Latebra "ecosystem".

Figure 3.5 Editor with encrypted message

3.1.2 Message Decryption

A message decryption is provided by just click on the button "Decryption" . The decryption will be done in one click if personal crypto-key was assigned to a sender. This service for Emails is convenient only in the case when you are a user of Gmail or Yandex.
Also this service is always convenient in the case of MMS/SMS messages.
A message can be decrypted also by crypto-key attached to the received message. In this case you will see the offer to assign this crypto-key to this correspondent as personal crypto-key.

We recommends in security purposes delete the message with crypto key after assigning of it.

It can be done just click the button .
Also this crypto-key can be used for decryption only once.

Figure 3.6 Editor with decrypted message

3.1.3 Personal Crypto-key

Click on the button “Gold Key” in Editor action bar to generate a personal crypto-key which can be assigned to the contact-which is owner of an address from the Editor input line.

3.1.4 Save Draft

Prepared message will be saved as a Draft with an address from address input line by click on the button “Save“.
The draft can have addressee or not.

Remember: New Draft will replace the previous Draft with the same address. New draft without address will replace old without address accordingly.

3.1.5 Open Draft

Click on the button “Open” to open as a Draft the last saved message with an address from address input line. When the address input line is empty, the last saved message without any address will be opened.

3.1.6 Send Message

A message is sent to an address from the address input line by click on the button “Send”. When you send encrypted message, the crypto-key will be offered for sending.

We recommend send crypto-key in first time only. It increase security of your messaging.

3.1.7 Address Input Line

In the answer mode, the address of recipient will be put in Address Input Line automatically. In case of new message you can input any address in Address Input Line manually or through the search procedure.

Using contact data suggestions helps you enter any address from your ”Address book”. If an address or/and addressee was absent in “Address book” you are forced to enter it manually. If “Gold Key“ is showed in Address Input Line it is mean that contact with this address has personal crypto-key.

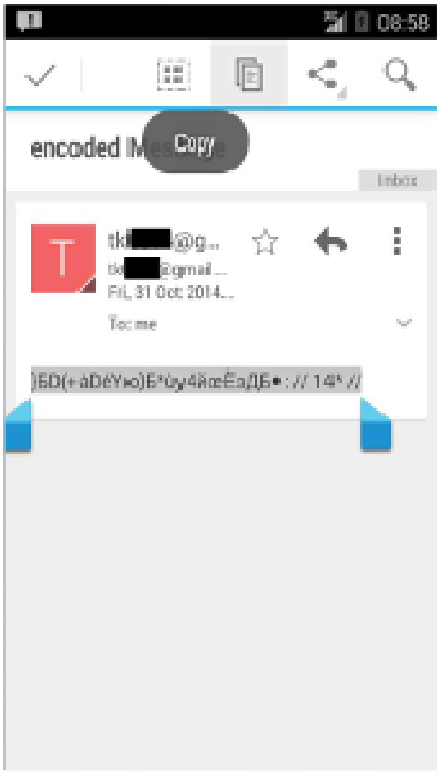


Figure 3.7 Copied message in standard E-mail client

3.1.8 Work with E-mail Services Using Copy&Paste

If you didn’t use Gmail or Yandex and use another E-mail services the functionality of Latebra will be restricted for you, you cannot use Latebra as Email client with possibility encryption/decryption in one click. You have to use copy&paste for message exchanging between Latebra and another E-mail clients.
You will be forced to copy encrypting E-mail message and paste it by click the button in Latebra Editor. If this E-mail message included crypto-key it can be decrypted it in one click. If not, more typically, you will have to copy and paste sender's address (or type it manually) to address input line to identify copied address with a contact from “Address book”. Only in this case Latebra will know which crypto-key has to be used for decryption (this key preliminary must be assigned to the sender of this E-mail).

4 Settings

Initial setup in any time can be changed by click on the button “Settings”  . Settings provide following functionalities:
1) checking connected E-mail account parameters or creating a new connection;
2) generation a new App crypto-key;
3) restoring previous App crypto-key if you remember previous codeword and approximate time of generation.
Item 1) can be fulfilled only if you are Gmail or Yandex user.

Remember: after App crypto-key changing all things earlier encrypted are impossible to decrypt. We recommend decrypting all before App crypto-key changing.
If you forgot these recommendations you can temporary restore App crypto-key by using corresponding codeword and then decrypt all things needful.