Руководство пользователя LATEBRA LIGHT

1 ПЕРВИЧНЫЕ УСТАНОВКИ 2

1.1 ГЕНЕРАЦИЯ КРИПТО-КЛЮЧА ПРИЛОЖЕНИЯ 2

1.1.1 ИСПОЛЬЗУЕМЫЕ АЛФАВИТЫ 2

1.1.2 УРОВЕНЬ ЗАЩИТЫ 2

1.1.3 КОДОВОЕ СЛОВО 2

1.1.4 КРИПТО КЛЮЧ ПРИЛОЖЕНИЯ 2

1.2 ПОДКЛЮЧЕНИЕ АККАУНТА 3

2 РАБОТА С СООБЩЕНИЯМИ  3

2.1 РЕДАКТОР  4

2.1.1 ШИФРОВАНИЕ СООБЩЕНИЙ 4

2.1.2 ДЕШИФРОВКА СООБЩЕНИЙ 4

2.1.3 СОХРАНИТЬ ЧЕРНОВИК 5

2.1.4 ОТКРЫТЬ ЧЕРНОВИК 5

2.1.5 ПОСЛАТЬ СООБЩЕНИЕ 5

2.1.6 АДРЕСНАЯ СТРОКА 5

2.1.7 РАБОТА С СООБЩЕНИЯМИ В РЕЖИМЕ COPY&PASTE 5

3 НАСТРОЙКА  6

ВВЕДЕНИЕ

Latebra Light– приложение для конфиденциальной переписки. Только тот, у кого есть Latebra или Latebra Light сможет читать Ваши письма. В приложении используются оригинальные алгоритмы шифрования для шифрования/дешифрования всех типов сообщений: E-mail/ SMS/ MMS сообщений. Шифрование осуществляется крипто-ключом Приложения, который необходимо отослать вместе с сообщением, чтобы его расшифровать. Можно синхронизовать крипто-ключи у нескольких пользователей, создав общий ключ Приложений и в этом случае можно обойтись без пересылки крипто-ключа вместе с сообщением.
В профессиональной версии Latebra предоставляются более надежные и удобные средства криптозащиты. В частности, в профессиональной версии обеспечивается возможность генерации персональных крипто-ключей и приписывание их к данным, содержащимся в «Контактах». Благодаря данной возможности нет необходимости дополнять сообщение крипто-ключом, достаточно это сделать один раз. Это, безусловно, поднимет уровень криптозащиты.

1 ПЕРВИЧНЫЕ УСТАНОВКИ

1.1 ГЕНЕРАЦИЯ КРИПТО-КЛЮЧА ПРИЛОЖЕНИЯ

Работа с Latebra Light начинается с генерации крипто-ключа Приложения, который используется для шифрования/дешифрования сообщений. Для генерации крипто-ключа Приложения необходимо определить используемые алфавиты, установить требуемый уровень защиты, придумать и ввести кодовое слово.

1.1.1 ИСПОЛЬЗУЕМЫЕ АЛФАВИТЫ

По умолчанию, алгоритм шифрования Latebra Light предназначен для английского языка и языка локализации мобильного устройства (смартфон или планшет). Если Вы пишете сообщения на других языках, Вам нужно расширить список используемых языков, отметив соответствующие чек-боксы. В противном случае, буквы, которые Вы используете в сообщениях, и которые отсутствуют в отмеченных алфавитах, не будут зашифровываться.

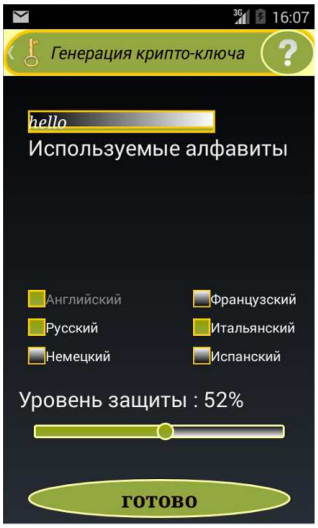


Рис. 1.1 Генерация крипто-ключа.

1.1.2 УРОВЕНЬ ЗАЩИТЫ

Существует возможность управления уровнем криптозащиты, которая определяется в %. Изменение уровня защиты осуществляется с помощью перемещения ползунка. Чем выше уровень защиты будет установлен, тем больше будет криптобезопасность, но тем медленнее будет происходить процесс шифрования/дешифрования. 99% соответствует максимальному уровню защиты в Latebra Light.

1.1.3 КОДОВОЕ СЛОВО

При генерации крипто-ключа Приложения необходимо ввести кодовое слово. Это слово будет паролем для входа в Latebra Light и его нужно запомнить.

Кодовое слово обеспечивает персонификацию крипто-ключей. Чем более длинное слово будет введено, тем более длинный крипто-ключ будет сгенерирован. Максимальная длина кодового слова составляет 10 символов.
Кодовое слово обеспечит не только доступ в приложение, но и поможет восстановить крипто-ключ, поэтому при замене крипто-ключа Приложения желательно сохранить старое кодовое слово, оно необходимо, если понадобится дешифровать те сообщения, которые Вы забыли дешифровать перед заменой крипто-ключа Приложения.
Кодовое слово должно содержать исключительно латинские буквы без диакритики и цифры, но последний символ не может быть цифровым.

1.1.4 КРИПТО КЛЮЧ ПРИЛОЖЕНИЯ

После выбора используемых алфавитов, определения уровня защиты, ввода кодового слова и двойного клика кнопки «Готово» крипто ключ Приложения будет сгенерирован.

После генерации крипто-ключа Приложения предлагается определить режим использования кодового слова в виде пароля. А именно запрашивать его при каждом входе в Приложение или нет.
!!!! Не рекомендуется использовать второй режим, кроме как для тестирования.
Существует возможность, заменить ранее созданный крипто-ключ Приложения, крипто-ключом присланным Вашим абонентом. Получив от своего абонента сообщение с крипто-ключом, подготовьте ответное сообщение, воспользовавшись для шифрования присланным ключом. На выходе из режима «Работа с сообщениями» Вам будет предложено присланный ключ сделать крипто-ключом вашего Приложения. Когда Вы согласитесь заменить свой крипто-ключ Приложения на присланный крипто-ключ, Вы тем самым синхронизируете свой крипто-ключ с крипто-ключом Приложения вашего абонента.
После синхронизации Вам будет предложено запомнить кодовое слово, использованное вашим абонентом при генерации этого крипто-ключа. В дальнейшем Вы должны будете использовать это слово как пароль. Такая синхронизация даёт Вам возможность переписки с этим абонентом без пересылки ключей.

1.2 ПОДКЛЮЧЕНИЕ АККАУНТА

После генерации крипто-ключа Приложения желательно подключить Ваши E-mail аккаунты к Latebra Light. Это обеспечит возможность удобной работы с E-mail сообщениями, когда Latebra Light будет использоваться как E-mail клиент с функцией шифрования/дешифрования.
Для подключения необходимо ввести E-mail адрес, пароль, кликнуть «Сохранить» и в заключение «Готово». После этого Latebra Light можно будет использовать как E-mail клиента.
В настоящий момент, в Latebra Light поддерживается работа только с двумя E-mail сервисами: Gmail и Yandex. С другими E-mail сервисами придется работать в режиме copy&paste. В дальнейшем планируется расширить список поддерживаемых сервисов.
Если E-mail аккаунты не подключать, то в Latebra Light непосредственно можно будет работать только с SMS/MMS сообщениями, а с E-mail придётся работать исключительно методом copy&paste.
На этом первичные установки завершены. После завершения этой части работы можно непосредственно приступить к использованию Latebra Light.

Рис 1.3 Диалог подключения аккаунта

Первичные установки всегда можно поменять в «Настройке»  , где обеспечена возможность управления E-mail аккаунтами а также восстановления и замены крипто-ключа Приложения.

2 РАБОТА С СООБЩЕНИЯМИ 

С E-mail сообщениями наиболее эффективно и удобно работать пользователям Gmail и Yandex, т.к. для них Latebra Light становится E-mail клиентом с функцией шифрования/дешифрования.

Клик по кнопке «Сообщения» вызовет диалоговое меню, где нужно будет выбрать, с каким типом сообщений планируется работать: SMS/MMS и/или E-mail, любые или только шифрованные сообщения. Например, отметив «SMS/MMS» и «только шифрованные сообщения» Вы получите список только шифрованных SMS/MMS сообщений.
После того, как выбран тип сообщений и дважды кликнута кнопка «Готово» будет загружен список сообщений в соответствие с выбранным фильтром. Клик на сообщении выделит его для последующих действий: во-первых, вторым кликом его можно загрузить в Latebra Light Редактор для просмотра,

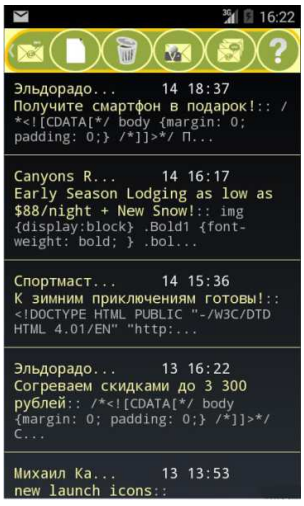


Рис 2.1 Фильтр при загрузке сообщений

Рис 2.2 Список сообщений

дешифрования и подготовки ответного сообщения ;

во-вторых, просмотреть переписку с данным контактом по всем его адресам и в-третьих, удалить , выделенное сообщение (только для SMS).

При работе с подключённым E-mail сервисом доступна функция управления аккаунтами .
Если возникнет необходимость создать и отослать новое сообщение, то нужно только кликнуть кнопку «Новое» и вызвать Редактор, где выполнить все необходимые действия.

2.1 РЕДАКТОР

Подготовка и отсылка новых или ответных сообщений осуществляется с помощью Редактора. Вызов Редактора осуществляется тремя возможными способами.
1) Клик по выделенному сообщению загрузит это сообщение в Редактор.

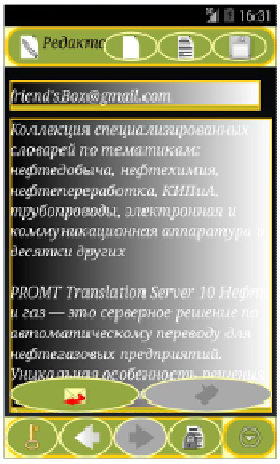
2) Клик кнопки «Новое».

3) Клик кнопки «Редактор» основного окна Приложения .
Редактор обеспечивает следующую функциональность при работе с сообщениями:
1) просмотр, создание и редактирование; 2) шифрование/дешифрование; 3) сохранение; 4) отсылка; 5) выход в Интернет по web-ссылкам из текста;

2.1.1 ШИФРОВАНИЕ СООБЩЕНИЙ

Для обеспечения конфиденциальности переписки необходимо перед отправкой зашифровать подготовленное сообщение, кликнув по кнопке «Шифровать» . Следует помнить, что у Вашего корреспондента на мобильном устройстве также должен быть Latebra или Latebra Light.
Шифрование сообщения будет осуществляться либо вашим крипто-ключом Приложения либо крипто-ключом из присланного Вам сообщения. Воспользоваться присланным ключом можно только в режиме ответного сообщения, т.е. кликнув по кнопке «Ответить» .

Рис 2.3 Окно редактора с шифрованным сообщением



2.1.2 ДЕШИФРОВКА СООБЩЕНИЙ

Если получено шифрованное сообщение, то оно дешифруется кликом по кнопке «Дешифровать» в Редакторе. Сообщение будет дешифровано крипто-ключом, присланным вместе с сообщением в один клик или вашим крипто-ключом Приложения.
Получив крипто-ключ вместе с сообщением, Вы можете заменить свой крипто-ключ Приложения присланным. Если Вы согласитесь, то это будет означать, что крипто ключи у Вас и у вашего абонента синхронизированы.
В этом случае с данным абонентом Вы можете в дальнейшем переписываться, не посылая крипто-ключ.

Рис 2.4 Окно редактора с дешифрованным сообщением

Однако, в отличие от Latebra, где создается «экосистема», в которой обеспечивается возможность конфиденциальной переписки без пересылки крипто-ключей с неограниченным количеством абонентов, в версии Latebra Light такая возможность может быть реализована только с одним абонентом.
Следует иметь в виду, что эта возможность наиболее удобно реализуется для SMS/MMS сообщений или, если идет речь об E-mail, только для сервисов Gmail или Yandex, для которых Latebra Light становится E-mail клиентом с функцией шифрование/дешифрование.

2.1.3 СОХРАНИТЬ ЧЕРНОВИК

Подготовленное сообщение с адресом из адресной строки Редактора (или с пустой адресной строкой) можно сохранить как черновик  . Следует помнить, что при сохранении черновика предыдущий черновик с данным адресом будет заменен этим. Новый черновик без адреса также заменяет старый без адреса.

2.1.4 ОТКРЫТЬ ЧЕРНОВИК

Клик на кнопке «Открыть»  откроет черновик с адресом, который в данный момент находится в адресной строке Редактора. Если адресная строка пустая, то откроется последний сохраненный черновик без адреса или новое сообщение, если безадресных черновиков нет.

2.1.5 ПОСЛАТЬ СООБЩЕНИЕ

Сообщение будет послано по адресу, указанному в адресной строке, если кликнуть по кнопке «послать сообщение»  . Отсылаемое сообщение может быть как зашифрованным, так и нет. При отсылке зашифрованного сообщения будет предложено дополнить сообщение Вашим крипто-ключом Приложения. Если Вы не пошлете крипто-ключ, то читать Ваше сообщение может только абонент, у которого крипто-ключ Приложения синхронизирован с вашим.

2.1.6 АДРЕСНАЯ СТРОКА

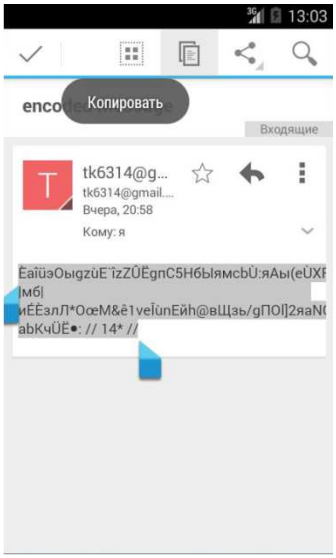
При вводе адреса в Адресной Строке работает подсказка, использующая данные «Контактов». Если адресат отсутствует в «Контактах», его адрес придется набирать вручную. Допускается поиск, как по имени адресата, так и непосредственно по адресу или телефону.

Рис 2.5 Окно редактора с подсказкой

Рис 2.6 Окно редактора с подсказкой, предлагающей выбрать телефон или E-mail

2.1.7 РАБОТА С СООБЩЕНИЯМИ В РЕЖИМЕ COPY&PASTE

Пользователям отличных от Gmail и Yandex сервисов придется пользоваться режимом copy&paste. В этом случае Latebra Light уже не будет E-mail клиентом, а будет только редактором с функцией шифрования/дешифрования. В частности, у подобных пользователей не будет возможности шифровать/дешифровать E-mail в один клик.



При получении шифрованного сообщения в соответствующем E-mail клиенте нужно будет его полностью скопировать и вставить в Редактор Latebra Light , где, используя присланный крипто-ключ, расшифровать.

Рис 2.7 Стандартный E-mail сервис, копирование сообщения

Рис 2.8 Окно редактора с сообщением, вставленным из стандартного E-mail сервиса

3 НАСТРОЙКА

Вы всегда можете изменить параметры Latebra Light выбранные изначально, используя кнопку «Настройка» . В режиме «Настройка» Вы можете:

1) проверить уже введенные данные или подключить новые почтовые аккаунты (только Gmail и Yandex); 2) сгенерировать новый крипто-ключ Приложения; 3) восстановить один из старых крипто-ключей Приложения.

Следует помнить, что после смены крипто-ключа Приложения ВСЁ ранее зашифрованное этим ключом нельзя будет дешифровать новым крипто-ключом Приложения. Настоятельно рекомендуется перед сменой крипто-ключа Приложения дешифровать ВСЁ ранее им зашифрованное.

Если же Вы, все-таки, забудете дешифровать ВСЁ ранее им зашифрованное, то Вы сможете временно восстановить предыдущие крипто-ключи Приложения, зная кодовые слова, используемые при их генерации, и приблизительное время, когда они были созданы.