Вы можете увидеть в Интернете форумы с ложными вопросами: как я могу зашифровать всю папку (перенести содержимое в ZIP-файл и затем зашифровать ZIP!), PDF-файл, как я могу зашифровать DOC-файл и т.д.? Это ложная проблема, любой документ - это не более чем последовательность n байтов, поэтому единственное, что имеет значение - это получить зашифрованный файл, в котором

байт (n) + алгоритм = зашифрованный байт (n)

и что вы можете получить оригинал документа обратно с

зашифрованный байт (n) - алгоритм = байт (n)

Каким бы ни был тип документа, он снова становится доступным для приложений, которые его используют, со своим содержимым и оригинальным именем.

# ШИФРОВАНИЕ ДОКУМЕНТОВ

Вы можете дать зашифрованным документам любое имя.

Имя исходного файла хранится в зашифрованном файле, поэтому при расшифровке документа ему автоматически присваивается исходное имя без необходимости запоминать, к какому документу относится данный конкретный файл.

**ШИФРОВАНИЕ ТЕКСТА**

То, что вы набираете с клавиатуры, напрямую шифруется, это удобно для написания коротких заметок.

После расшифровки содержимое хранится в файле MESSAGE.TXT

**АУТЕНТИФИКАЦИЯ**

Каждый зашифрованный документ содержит неповторяющийся идентификационный код (**NIDE**), который исключает любую возможность манипуляции и надежно удостоверяет личность отправителя.

Система шифрования на самом деле такова, что один и тот же документ, зашифрованный одним и тем же ключом n раз, создает n всегда разных зашифрованных файлов и, следовательно, n разных **NIDE.**

**NIDE** показывается в конце шифрования, проверяется системой перед расшифровкой каждого документа и в любом случае может быть проверена в любое время с помощью специальной функции, и поэтому отправитель и получатель могут гарантировать подлинное происхождение зашифрованного документа и его целостность.

В дополнение к коду NIDE указываются следующие данные:

* дата создания
* имя используемого ключа
* кто зашифровал документ
* название оригинального документа

**ключевой файл quankeys**

quankeys зашифрован с помощью **ключа KEY.OF.THE.KEYFILE (KOK).**

**Это ключ, который вы должны выбрать при первом использовании системы и который**

**вы должны предоставлять каждый раз при входе в систему.**

Это единственный ключ, который вам нужно запомнить, но вы ДОЛЖНЫ его запомнить, иначе вы

никогда не сможете восстановить уже зашифрованные файлы, потому что

**только те, кто знает КЛЮЧ может работать в системе.**

quankeys содержит все пользовательские ключи в форме:

KEYNAME (открытое, любой может его увидеть) + KEY (который можете увидеть только вы, так как он зашифрован с помощью KOK)

Поэтому, как только имя ключа, который будет использоваться, известно, он извлекается из quankeys, и система

расшифровывает его с помощью KOK и разрешает его использование.

Имя / ссылка, относящаяся к ключу, хранится в зашифрованных файлах, поэтому ключи должен быть

используемые для расшифровки, будут взяты без необходимости предоставления какой-либо информации.

**КЛЮЧИ**

Их можно сгенерировать с помощью специальной функции 7 программы, а затем присвоить им желаемое имя. Вы можете создать ключ для обмена с вашим корреспондентом, используя процесс обмена ключами 8, предусмотренный системой.

### Процесс проходит в 2 этапа:

A ---- отправляет данные " B, который генерирует ключK

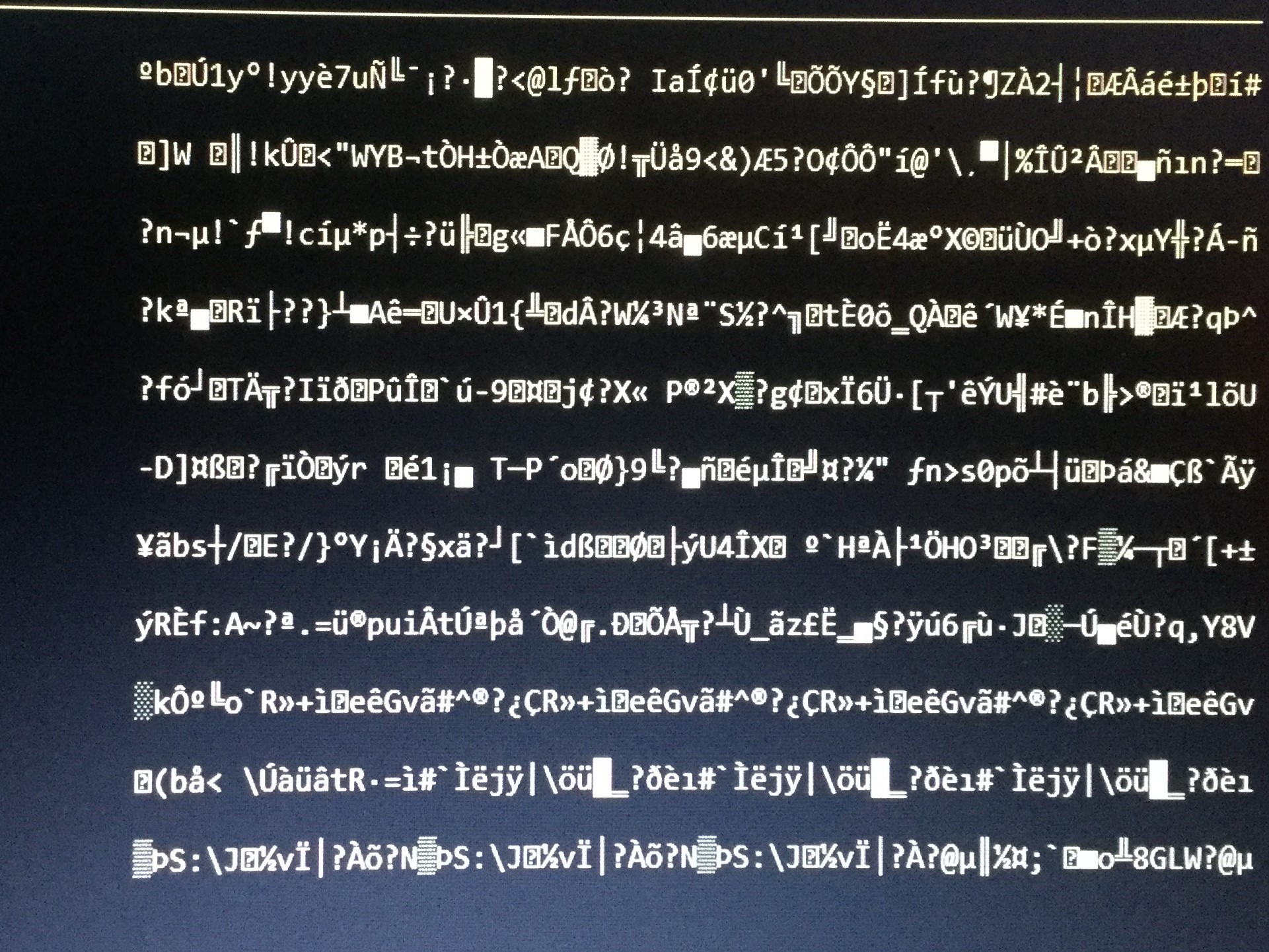
B --- отправляет обратно данные " A, который генерирует ключ =K

Имя ключа - это имя пользователя корреспондента, оно присваивается автоматически и позволяет обоим правильно расшифровывать свои сообщения, так как на каждом зашифрованном файле, который они отправляют, стоит имя, с которым общий ключ хранился в их файлах quankeys.

Программа показывает, какая фаза находится в процессе. Вам нужно только договориться, кто начинает фазу 1.

Описание может быть связано с созданными ключами для облегчения идентификации корреспондента.

Вы можете сгенерировать ключ в других системах и импортировать его в QCRYPTO через файл с именем KIMPEXP, который должен иметь следующий формат: имя ключа (24) + имя пользователя (24) + ключ (64).

Функция, генерирующая ключи, позволяет экспортировать сгенерированный ключ в файл KIMPEXP. Используя программу камуфляжа **CAMO,** вы можете произвести с его помощью достаточно безопасный обмен ключами (см. ниже).

Функция 10 перечисляет все клавиши (некоторые специальные символы, которые не могут быть представлены, заменяются на ?)

**ВАЖНО**: Никогда не вводите новый ключ, название которого совпадает с вашим псевдонимом. **Как выглядят сгенерированные ключи.**

**БОЛЬШЕ**

В папке вы найдете еще две программы, запускаемые отдельно от QCRYPTO :

**CAMO (**camouflage) позволяет спрятать любой файл в любой другой документ (hosts) и при необходимости извлечь его оттуда (decamouflage). Запустите программу и прочитайте справку, чтобы узнать, какие расширения файлов разрешены в качестве хостов.

**UTIL** позволяет вам :

- разбить любой файл на части длиной n, а затем перестроить его

- можете изменить язык на QCRYPTO

- отменить (физически) любой файл?

**Иметь хорошую планировку:**

* **создать ярлык Qcrypto на рабочем столе**
* **щелкните правой кнопкой мыши на значке**
* **свойства / расположение**
* **в размерах окна установить 30 по высоте и 102 по ширине**