web - интерфейс, реализующий симметричную систему шифрования текстовых файлов и
сообщений, основанный на самодостаточном протоколе безопасности и взаимном доверии
пользователей.

Вариант использования модуля:

1. Алиса и Боб используя закрытый канал связи определяют собственные секретные ключи и
подписи и обмениваются ими.

каждый пользователь имеет:
секретный ключ Алисы, Секретный ключ Боба, подпись Алисы, подпись Боба.

2. Во время сеанса связи Алиса:
- генерирует открытый сеансовый ключ и используя открытый канал связи отправляет его Бобу.
- генерирует закрытый сеансовый ключ, используя собственный закрытый ключ и сгенерированный ранее открытый сеансовый ключ.
- Создает сообщение, подписывает его, шифрует закрытым сеансовым ключем.
- отправляет Бобу сообщение.

Боб имеет:
Закрытая информация:
секретный ключ Алисы, Секретный ключ Боба, подпись Алисы, подпись Боба.
Открытая информация:
открытый сеансовый ключ, зашифрованное сообщение

3. Действия Боба:
- генерирует закрытый сеансовый ключ при помощи секретного ключа Алисы и открытого сеансового ключа. (таким образом проверяется авторство открытого сеансового ключа, который создан Алисой)
- При помощи полученного закрытого сеансового ключа Боб расшифровывает сообщение
- программа так же проверяет электронные подписи которые Боб вводит в поле при
расшифровке сообщения.
- отвечает Алисе на сообщение при помощи того же алгоритма, с использованием
собственного закрытого ключа и подписи.

Система будет взломана если злоумышленник получит секретный ключ одного из пользователей

либо закрытый сеансовый ключ.

web - interface that implements a symmetric encryption system for text files and
A message based on a self-contained security protocol and mutual trust
users.

The use of the module:

1. Alice and Bob using their private communication channel determine their own secret keys and
sign and exchange them.

each user has:
secret key of Alice, Secret key of Bob, Alice's signature, Bob's signature.

2. During the communication session, Alice:
- generates an open session key and uses an open channel
  communication sends it to Bob.
- Generates a private session key using its own private key
  and the previously generated public session key.
- Creates a message, signs it, encrypts it with a private session key.
- Sends a message to Bob.

Bob has:
Closed information:
secret key of Alice, Secret key of Bob, Alice's signature, Bob's signature.
Public information:
open session key, encrypted message.

3. Bob's actions:
- Generates a private session key using Alice's secret key and
  open session key. (thus verifying the authorship of the open
the session key that Alice created)
- With the help of the received private session key, Bob decrypts the message
- the program also checks the electronic signatures that Bob enters in the field when
  decoding of the message.
- Responds to Alice's message using the same algorithm, using
  own private key and signature.

The system will be hacked if the attacker receives the secret key of one of the users
or a private session key.