sssnike

0.1

Создано системой Doxygen 1.9.1

Глава 1

Список файлов

1.1 Файлы

Полный список файлов.

Глава 2

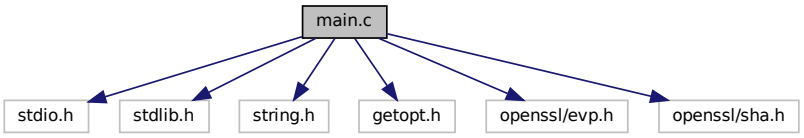
Файлы

2.1 Файл main.c

Основной и единственный файл.

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <getopt.h>
#include <openssl/evp.h>
#include <openssl/sha.h>
```

Граф включаемых заголовочных файлов для main.c:



Макросы

- #define KEY_LENGTH 32
- #define IV_LENGTH 16

Функции

- void print_usage (const char *prog_name)

  Выводит сообщение о способе использования программы.
- int derive_key_iv (const char *password, unsigned char *key, unsigned char *iv)

  Вычисляет ключ и вектор инициализации на основе пароля. Используется SHA512, иначе длинна ключа+вектора инициализации вылезет за границу массива и в расшивированном сообщении будет мусор.
- int encrypt_file (const char *in_filename, const char *out_filename, const char *password)

  Шифрует входной файл и записывает данные в выходной файл.
- int decrypt_file (const char *in_filename, const char *out_filename, const char *password)

  Расшифровывает входной файл и записывает данные в выходной файл.
- int main (int argc, char *argv[])

  Главная функция программы, обрабатывает аргументы командной строки и выполняет шифрование или расшифровку.

2.1.1 Подробное описание

Основной и единственный файл.

2.1.2 Макросы

2.1.2.1 IV_LENGTH

```
#define IV_LENGTH 16
```

2.1.2.2 KEY_LENGTH

```
#define KEY_LENGTH 32
```

2.1.3 Функции

2.1.3.1 decrypt_file()

```
int decrypt_file (
                const char * in_filename,
                const char * out_filename,
                const char * password )
```

Расшифровывает входной файл и записывает данные в выходной файл.

Аргументы

in_filename	Путь к зашифрованному файлу.
out_filename	Путь к выходному файлу.
password	Пароль для расшифровки.

Возвращает

Возвращает 0 при успешном расшифровании, иначе 1.

2.1.3.2 derive_key_iv()

```
int derive_key_iv (
                const char * password,
                unsigned char * key,
                unsigned char * iv )
```

Вычисляет ключ и вектор инициализации на основе пароля. Используется SHA512, иначе длинна ключа+вектора инициализации вылезет за границу массива и в расшиврованном сообщении будет мусор.

Аргументы

password	Пароль для выработки ключа.
key	Буфер для хранения ключа.
iv	Буфер для хранения вектора инициализации.

Возвращает

Возвращает 0 при успешном выполнении.

2.1.3.3 encrypt_file()

```
int encrypt_file (
                const char * in_filename,
                const char * out_filename,
                const char * password )
```

Шифрует входной файл и записывает данные в выходной файл.

Аргументы

in_filename	Путь к входному файлу.
out_filename	Путь к выходному файлу.
password	Пароль для шифрования.

Возвращает

Возвращает 0 при успешном шифровании, иначе 1.

2.1.3.4 main()

```
int main (
                int argc,
                char * argv[] )
```

Главная функция программы, обрабатывает аргументы командной строки и выполняет шифрование или расшифровку.

Аргументы

argc	Количество аргументов командной строки.
argv	Массив строк аргументов командной строки.

Возвращает

Возвращает 0 при успешном выполнении, иначе 1.

2.1.3.5 print_usage()

```
void print_usage (
                const char * prog_name )
```

Выводит сообщение о способе использования программы.

Аргументы

prog_name	Имя исполняемого файла программы.

Предметный указатель