Техническое задание к продукту

“Криптографический чат”

Содержание

1. Общие положения

Команда разработчиков, роли

Гайков Сергей - разработчик, дизайнер, тестировщик

2. Предназначение и формулировка целей

Целевая аудитория

Физические лица, заинтересованные в обмене личными сообщениями в среде с повышенным уровнем безопасности.

Цели

Главные цели этого документа следующие:

- Четкий и полный список функциональных требований;
- Список проектных рисков связаные с плановыми работами и применяемыми стратегиями.

Не цели

Процесс реализации и использования продукта экспертными пользователями, технологии, тонкости коммуникаций не являются целями данного документа.

Терминология

Пользователь - лицо или организация, которое использует действующую систему для выполнения конкретной функции.

Личный кабинет - это особый раздел сайта, который позволяет клиенту определенной компании получить доступ к данным о состоянии и статистической информации лицевого счета, деталям заказа, ведущимся про проекту работам и т.д.

DES - алгоритм для симметричного шифрования, разработанный фирмой IBM и утверждённый правительством США в 1977 году как официальный стандарт (FIPS 46-3).

Caesar - это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите.

AES - симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES.

RSA - криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

MD5 - 128-битный алгоритм хеширования, разработанный профессором Рональдом Л. Ривестом из Массачусетского технологического института (Massachusetts Institute of Technology, MIT) в 1991 году.

ГОСТ Р 34.10-2012 (полное название: «ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и

проверки электронной цифровой подписи») — российский стандарт, описывающий алгоритмы формирования и проверки электронной цифровой подписи.

ECDSA (Elliptic Curve Digital Signature Algorithm) — алгоритм с открытым ключом для создания цифровой подписи, аналогичный по своему строению DSA, но определённый, в отличие от него, не над кольцом целых чисел, а в группе точек эллиптической кривой.

3. Функциональные требования

1.1 Домашняя страница

- **R 1.1.1** На домашней странице авторизированного пользователя находится список зарегистрированных пользователей системы в виде кнопок, позволяющих перейти в комнату(скоуп) для общения тет-а-тет.
  - **R 1.1.1.1** Кнопки располагаются в вертикальном порядке.
  - **R 1.1.1.2** Цвет кнопок задается произвольным образом.

1.2 Страница личного кабинета пользователя

- **R 1.2.1** На странице личного кабинета пользователь может производить редактирование параметров шифрования текстовых сообщений, параметров цифровой подписи.
- **R 1.2.2** В системе присутствуют способы шифрования текстовых сообщений : Caesar, DES, DES CBC, AES CTR, RSA.
- **R 1.2.2.1** Для шифра Caesar на форме определено текстовое поле “The number of letters shifted”, устанавливающее количество сдвигов в латинском алфавите для шифрации и дешифрации сообщений.
- **R 1.2.2.2** Для алгоритма DES опередeлено тестовое поле “128-bit key”, представляющее собой 128-битный ключ в виде hex-строки.
- **R 1.2.2.3** Для алгоритма DES CBC используется тот же ключ, который определен в R 1.2.2.2.
- **R 1.2.2.4** Для алгоритма AES (CTR mode) определены текстовые поля : “Either 128,192 or 256-bit key” (отражающее 128- , 192- или 256-битный ключ в виде hex-строки), “Either 128,192 or 256-bit counter” (отражающее 128- , 192- или 256-битный дополнительный счетчик в виде hex-строки).
- **R 1.2.2.5** Для алгоритма RSA определены поля : “1024-bit modulus” (1024-битный модуль в виде hex-строки), “Public key exponent” (открытая экспонента в виде hex-строки), “Private key exponent(hex)” (приватная экспонента), “First prime number(hex)” (первое простое число), “Second prime number(hex)” (второе простое число), “d mod (p-1)(hex)”, “d mod (q-1)(hex)”, “1/q mod p(hex)”.
- **R 1.2.3** Способ шифрации/дешифрации сообщений, описанный в R 1.2.2. устанавливается при помощи drop-down-меню.
- **R 1.2.4** В системе присутствуют способы валидации загружаемых/скачиваемых файлов : MD5, GOST 3410, ECDSA.
  - **R 1.2.4.1** Для алгоритма GOST 3410 на форме определены текстовые поля : "prime number 'p'(hex)" (простое число ‘p’), "prime number 'q'(hex)" (простое число ‘q’), "elliptic curve's coefficient 'a'(hex)" (коэффициент/инвариант эллиптической кривой ‘a’), "elliptic curve's coefficient ‘b'(hex)" (коэффициент/инвариант эллиптической кривой ‘b’), "'x' coordinate of base point(hex)" (координата ‘x’ базовой точки), "'y' coordinate of base

point(hex)” (координата ‘y’ базовой точки), "private key(hex)" (приватный ключ для генерации подписи), "public key's 'x' coordinate(hex)" (координата ‘x’ открытого ключа – для проверки подлинности подписи), "public key's ‘y' coordinate(hex)" (координата ‘x’ открытого ключа – для проверки подлинности подписи).

- **R 1.2.4.2.** Для алгоритма ECDSA определены поля : "prime number ‘p'(hex)" (простое число ‘p’), "elliptic curve's coefficient 'a'" (коэффициент/инвариант эллиптической кривой ‘a’), "elliptic curve's coefficient ‘b'(hex)" (коэффициент/инвариант эллиптической кривой ‘b’), "'x' coordinate of base point(hex)" (координата ‘x’ базовой точки), "'y' coordinate of base point(hex)” (координата ‘y’ базовой точки), "random number in [1,n-1] (hex)" (случайное число из промежутка [1,n-1], где n - порядок одной из циклических подгрупп группы точек эллиптической кривой), "secret multiplier(hex)" (секретный множитель), "order of base point(hex)" (порядок одной из циклических подгрупп группы

- **R 1.2.5** Проверка файлов производится одновременно тремя алгоритмами, описанными в R 1.2.4.

1.3 Страница чат-комнаты

- R 1.3.1 На странице чат-комнаты находятся (в вертикальном порядке) : индикатор статуса “online”/”offline” собеседника, окно с историей сообщений, форма для загрузки файла и его аттачинга к сообщению, кнопка “Отправить” сообщение.
- R 1.3.2 Индикатор статуса “online”/”offline” показывает авторизирован ли в данным момент собеседник в системе, если да – “online” , нет – “offline”.
- R 1.3.3 Окно с историей сообщений отображается сообщения в формате : “[пользователь] – [дата отправки] : [сообщение]”. Под текстовым сообщением находится кнопка для скачивания загруженного файла, если таковой был приаттачен во время отправки сообщения.
- R 1.3.4 Форма для загрузки файла позволяет выбрать произвольный файл на компьютере и загрузить его при отправке сообщения; таким образом, собеседнику можно передать абсолютно любой файл, с максимальным размером, установленным при инициализации системы.
- R 1.3.5 При нажатии на кнопку “Отправить” сообщение шифруется и отправляется собеседнику. Если у собеседника установлены корректные параметры для используемого отправителем типа шифрования, то сообщение автоматически дешифруется на выходе у собеседника. При наличии загружаемого файла происходит его загрузка, подсчет MD5-хэша, подписывание цифровой подписью при помощи алгоритма ГОСТ 3410, подписывание цифровой подписью при помощи алгоритма ECDSA. Собеседник или отправитель сообщения сможет загрузить файл к себе на компьютет из системы только, если все три алгоритма проверки файла сработали положительно, в противном случае файл не загружается.

1.4 Страница смены пароля

- R 1.4.1 На этой странице пользователь может сменить свой пароль от личного кабинета на новый.

1.5 Дополнительные требования

- R 1.5.1 Язык, при помощи которого отображаются все опции в личном кабинете – “Английский”.
- R 1.5.2 В процессе разработки функциональность может быть дополнена и расширена.

4 Проект-план

No п/п	Описание этапа	Оценка даты завершения этапа
1	Разработка технического задания.	30.09
2	Реализация аутентификации пользователей.	10.10
3	Реализация Домашней страницы.	18.10
4	Реализация страницы Личного кабинета.	24.10
5	Реализация страницы Смены пароля.	28.10
6	Реализация страницы Чат-комнаты.	7.11
7	Тестирование и устранение ошибок, завершение разработки проекта, сдача заказчику.	16.12