

**Софийски университет „Св. Кл. Охридски”**

Факултет по математика и информатика

специалност : „Защита на информацията в компютърните системи и мрежи“

**Дисциплина: Моделиране на защитени взаимодействия в компютърните системи**

**Курсова работа на тема “Описание на система за съхранение, проверка и генериране на сигурни пароли”**

*Автор:*

Иван Ивов Чучулски, фак. номер: 4MI3400043

*Ръководител:*

проф. д.т.н. Веселин Целков

летен семестър, 2021/2022г.

Съдържание

[**1.** **Въведение** 3](#_Toc106642902)

[**2.** **Описание на системата** 3](#_Toc106642903)

# **Въведение**

Целта на проекта е да бъдат формално описани взаимодействията в система за съхранение, проверка и генериране на сигурни пароли. С помощта на граф-схеми, е-мрежи ще бъдат представени основните функционални характеристики на системата и ще бъдат проверени условията за пълнота и непротиворечивост на алгоритмите.

Системата представлява клиент-сървър приложение, което позволява на потребителите да записват пароли за използвани от тях уеб сайтове или други услуги. Приложението ще възможност за генериране на сигурна парола за конкретна услуга, ако потребителите не желаят да измислят такава.

Клиентската част на системата ще поддържа два варианта – десктоп приложение с графичен потребителски интерфейс, което може да се изпълнява на всички основни операционни системи за персонални компютри, а вторият вариант на системата е с конзолен интерфейс, който изисква от потребителя въвеждане на текстови команди.

# **Описание на системата**

При съхранението на чувствителна информация като пароли за достъп е необходимо да се предприемат мерки за защита от неоторизиран достъп, модификация или кражба. За целта ще използваме концепциите за криптографска хеш функция и симетрично криптиране на данните.

Паролите, които потребителите подават при регистрация в системата ще преобразуваме с помощта на криптографска хеш функция и ще пазим в базата от данни резултата от пресмятането, който е поредица от байтовете на техния хеш. При опит за влизане в системата се пресмята хеша на въведената от потребителя парола и за успешен вход е необходимо той да съвпада с този в базата данни. Допълнителна сигурност ще ни донесе използването на т.нар. salt – това е поредица от байтове, която произволно генерираме при регистрация, долепяме към подадената парола и така пресмятаме хеша. По този начин се предпазваме от варианта, в който паролите за достъп на потребителите съвпадат и резултата от хеш функцията ще е еднакъв, а също така и на практика обезсмисляме много от brute-force атаките и атаките с rainbow таблици. Ще използваме 16-байтов salt и криптографската хеш функцията SHA-512.



Фигура 1 Хеширане на парола със salt

Тъй като приложението цели да предостави възможността на потребителите да могат да записват пароли за използвани от тях услуги е нужно записаната информация да бъде записана достатъчно сигурно, но да може да възстановена в явен вид. Това се постига с използването на симетрична криптографска функция, която използва един частен ключ, който трябва да остане таен за криптиране и декриптиране на информацията. За генерирането на този частен ключ ще изискваме от потребителя т.нар. “master” парола, която той трябва да въведе при регистрация. При нужда от добавяне или генериране на парола е необходимо потребителят да въведе своята “master” парола отново, като това добавя още едно ниво на сигурност и автентикация след влизането в системата.



Фигура 2. Симетрично криптиране

За образуването на частния ключ ще използваме алгоритъма “PBKDF2”, който дава възможност да добавим и случайно генерирана последователност от байтове(salt на ключа), тъй като отново съществува възможността “master” паролите на някои потребителите да съвпадат, както и правим по-трудни атака за отгатване на ключа, знаейки само “master” паролата. За самото криптиране използваме алгоритъма AES в режим CBC, като той изисква освен текста за криптиране да бъде подадена и случайно генерирана поредица от байтове, наречена инициализационен вектор(IV), която служи за подравняване на данните и увеличава силата на криптирането. В базата данни записваме криптирания текст, байтовете на salt-та за ключа и байтовете на инициализационен вектор.

При декриптиране потребителят въвежда своята “master” парола, която заедно с байтовете на salt-та за ключа формират тайния ключ. После ключа и инициализационен вектор участват в декриптирането на получаването на паролата в явен вид.