можливості придбання книг у ролі клієнта. У ході проведення роботи було виділено основні завдання сайту, важливі особливості цільової аудиторії та вивчені основні функції інтернет-магазинів, на основі яких створювався програмний засіб.

Список літературних джерел

1. Поняття клієнт-серверних систем [Електронний ресурс]. Режим доступу: http://bourabai.kz/dbt/client1.htm . Дата доступу: 29.09.2020
2. Django підручник: Використання моделей [Електронний ресурс]. Режим доступу:https://developer.mozilla.org/ru/docs/Learn/Serverside/Django/Models Дата доступу: 14.10.2020
3. SQLite. [Електронний ресурс]. Режим доступу: https://habr.com/ru/post/149356/ Дата доступу: 14.10.2020
4. Мережеве програмування [Електронний ресурс]. Режим доступу: https://www.ibm.com/developerworks/ru/library/l-python_part_10/index.html Дата доступу: 10.10.2020
5. DB-API 2.0 interface for SQLite databases [Електронний ресурс]. Режим доступу: https://docs.python.org/3/library/sqlite3.html Дата доступу: 29.09.2020

УДК 004.4(043.2)

Сеник І.О., студент 4 курсу спеціальності 122 «Комп'ютерні науки»
Римар П.В., старший викладач кафедри комп'ютерних наук та інформаційних технологій

ЗАСТОСУВАННЯ ПРОСТИХ КРИПТОСИСТЕМ У ПОВСЯКДЕННОМУ ЖИТТІ

Донецький національний університет імені Василя Стуса, м. Вінниця

Криптосистема – це реалізація криптографічних методів і супутньої їм інфраструктури для надання послуг інформаційної безпеки. Криптосистема також називається системою шифрування.

Шифрування і пов'язані з ним технології широко і часто використовуються як засіб забезпечення безпеки інформації, а їх важливість зростає при все більш широкому використані інтернету. Використання шифрування можна простежити до 3000 року до н.е. в вавилонську епоху. Технології шифрування розвивалися в міру їх застосування у військових і політичних умовах, але в результаті недавнього широкого використання Інтернету і різкого збільшення кількості інформації в яких використовуються технології шифрування застосовуються і впроваджені, збільшилися, і тепер вони використовуються всюди в нашому повсякденному житті. Історія шифрування –

це історія «конкурсу дотепності» між розробниками шифрування і шифрувальними кодами. Кожного разу, коли створюється новий алгоритм шифрування, він розшифровується і, в свою чергу, призводить до створення нового алгоритму шифрування, а цикли створення і дешифрування алгоритмів повторюються і до цього дня [1].

Компоненти криптосистеми містять в собі:

Простий текст. Це дані, які повинні бути захищені під час передачі.

Алгоритм шифрування. Це математичний процес, який створює зашифрований текст для будь-якого заданого відкритого тексту та ключа шифрування. Це криптографічний алгоритм, який приймає відкритий текст і ключ шифрування в якості вхідних даних і створює зашифрований текст.

Гіпертекст. Це зашифрована версія відкритого тексту, створеного алгоритмом шифрування з використанням спеціального ключа шифрування. Зашифрований текст не охороняється, тече по загальнодоступному каналу. Він може бути перехоплений або скомпрометований будь-яким, хто має доступ до каналу зв'язку.

Алгоритм дешифрування. Це математичний процес, який створює унікальний відкритий текст для будь-якого заданого шифротексту та ключа дешифрування. Це криптографічний алгоритм, який приймає зашифрований текст і ключ дешифрування в якості вхідних даних і виводить відкритий текст. Алгоритм дешифрування, по суті, звертає алгоритм шифрування і, таким чином, тісно пов'язаний з ним.

Ключ шифрування. Це значення, яке відоме відправнику. Відправник вводить ключ шифрування в алгоритм шифрування разом з відкритим текстом, щоб обчислити зашифрований текст.

Ключ розшифровки. Це значення, яке відоме одержувачу. Ключ дешифрування пов'язаний з ключем шифрування, але не завжди ідентичний йому. Приймач вводить ключ дешифрування в алгоритм дешифрування разом із зашифрованим текстом для обчислення відкритого тексту.

В залежності від типу шифрування ключа, криптосистеми можуть бути з симетричним або асиметричним шифруванням. Основна відмінність між цими криптосистемами полягає в зв'язку між шифруванням і ключем дешифрування. Логічно, що в будь-якій криптосистемі обидва ключа тісно пов'язані. Розшифрувати зашифрований текст практично неможливо за допомогою ключа, не пов'язаного з ключем шифрування.

Принцип Кірхгофа. Він застосовується практично у всіх сучасних алгоритмах шифрування, таких як DES, AES і т. Д. Ці загальнодоступні алгоритми вважаються повністю безпечними. Безпека зашифрованого повідомлення залежить виключно від безпеки секретного ключа шифрування.

Зберігання алгоритмів в секреті може служити істотною перешкодою для криптоаналізу. Однак зберігати алгоритми в секреті можливо тільки тоді, коли вони використовуються в строго обмеженому колі.

У сучасну епоху криптографія повинна обслуговувати користувачів, які підключені до Інтернету. У таких випадках використання секретного алгоритму

нездійсненно, тому принципи Кірхгофа стали важливими керівними принципами для розробки алгоритмів в сучасній криптографії[2].

Криптографічний захист каналів передачі даних може бути реалізован на наступних рівнях, для кожного з яких характерне використання певних засобів захисту і протоколів:

фізичний рівень – специфічна форма шифрування, яка реалізується апаратно і застосовується тільки на фізичному рівні, є захист передачі (захист по ширині частотного спектра);

мережевий рівень – шифрування переданого між вузлами трафіку (наприклад, протокол IPSec);

рівень представлення – шифрування даних, що передаються між віддаленими програмами (наприклад, протоколи SSL і TLS);

прикладний рівень – самостійне шифрування даних додатками.

Крім того, криптографічні методи і засоби можуть використовуватися для вирішення завдань під час аутентифікації сторін для обміну інформацією, забезпечення автентичності та недоторканості джерела даних і цілісності переданих даних.

Список літератури:

1. Електронний ресурс. Режим доступу: https://proverkassl.com/book_ssl_history.html
2. Електронний ресурс. Режим доступу: https://coderlessons.com/tutorials/akademicheskii/izuchite-kriptografiiu/kriptosistemy

УДК 004.4(043.2)

Пивовар І.І., студентка 4 курсу спеціальності 122 «Комп'ютерні науки»
Єпік М.О., к.т.н., доцент, доцент кафедри комп'ютерних наук та інформаційних технологій

ВЕБ-РЕСУРС «ЕКЗОТИЧНІ ФРУКТИ»

Донецький національний університет імені Василя Стуса, м. Вінниця

Метою даної роботи є розробка веб-ресурсу, що призначений для продажу і покупки екзотичних фруктів. Так як у сучасному світі стає все популярнішим вживати корисні екзотичні фрукти у раціоні харчування – ця тема є актуальною.

Веб-ресурс призначений для широкого кола користувачів, не залежно від віку та фаху і може використовуватися з пристрою, що підключений до мережі інтернет за умов перенесення його на хостинг.