На правах рукопису

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут холоду,
кріотехнологій та екоенергетики
Факультет інформаційних технологій та кібербезпеки

XVII Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

Матеріали конференції. Частина 1

Одеса
19 квітня 2017 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XVII Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 19 квітня 2017 р. - Одеса, Видавництво ОНАХТ, 2017 р. - 88 с.

Збірник включає матеріали доповідей її учасників, які об'єднані по секціях кафедр: комп'ютерної інженерії (КІ), інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова – д.т.н., проф., **Єгоров Б.В.**, ректор ОНАХТ.

Співголови :

Поварова Н.М. – к.т.н., доц., проректор з наукової роботи,
Косой Б.В. – д.т.н., проф., в.о. директора ННІХКтаЕ ОНАХТ,
Котлик С.В. – к.т.н., доц., декан ФІТта КБ ОНАХТ,
Волков В.Е. – д.т.н., проф., директор НМАіР ОНАХТ,
Хобін В.А. – д.т.н., проф., завідувач кафедри АВП ОНАХТ,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри КІАтаМ ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ "Львівська політехніка",
Тарасенко В. П. – д.т.н., проф., завідувач кафедри СКС НТУУ «Київський політехнічний інститут»,
Жуков І. А. – д.т.н., проф., завідувач кафедри КСтаМ НАУ,
Сулімова Ю. – координатор IT–Cluster Odessa.

Члени оргокомітету:

Плотніков В. М. – д.т.н., проф., завідувач кафедри інформаційних технологій та кібербезпеки ОНАХТ,
Артеменко С.В. – д.т.н., проф., в.о. завідувача кафедри комп'ютерної інженерії ОНАХТ,
Князєва Н.О. – д.т.н., проф. кафедри комп'ютерної інженерії ОНАХТ,
Бойцова О.С. – заступник декана ФІТта КБ ОНАХТ,
Шамрай О.А. – к.т.н., доц. кафедри ТДтаВЕ ОНАХТ.

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Шамрай О.А.

(ВАТ «ІнфоТеКС»). Внесений Технічним комітетом зі стандартизації ТК 26 «Криптографічний захист інформації».

Новий шифр являє собою не точну мережу Фейстеля, а так звану SP-мережу: перетворення, що складається з декількох однакових раундів, при цьому кожен раунд складається з нелінійного та лінійного перетворень, а також операції накладення ключа. На відміну від мережі Фейстеля, при використанні SP-мережі перетворюється весь вхідний блок, а не його половина. Така структура іноді також називається AES-like (схожою на AES), проте, на відміну від останнього у «Коника» є ряд своїх переваг:

1. лінійне перетворення може бути реалізовано в за допомогою регістра зсуву;
2. ключова розгортка реалізована за допомогою мережі Фейстеля, в якій в якості опції використовуються раундові перетворення вихідного алгоритму.

Очікується, що новий блоковий шифр «Коник» буде стійкий до всіх видів атак на блокові шифри. Riham AlTawy та Amr M. Youssef описали атаку "зустрічі посередині" на 5 раундів шифру «Коник», що має обчислювальну складність 2140 і вимагає 2153 пам'яті і 2113 даних[3].

Як висновок, завдяки створенню теоретичної бази перевірки надійності шифру «Коник», показана неможливість заявленого взаємозв'язку ключів, але в той же час показано відповідність суті методу перевірки (сам метод пов'язаних ключів і правила вироблення шуканого ключа) всіма правилами алгоритму шифрування.

Слід зазначити, що розглянутий метод аналізу з використанням пов'язаних ключів малоймовірний при практичному застосуванні і часто може існувати лише через помилки протоколів безпеки або збоїв програм безпеки, отже, практичної цінності не має майже повністю, проте дуже корисний для вивчення криптографічних властивостей шифрів[4].

Список літератури

1. https://ru.wikipedia.org/wiki/Кузнечик_(шифр)
2. https://habrahabr.ru/post/266359/
3. http://tc26.ru/standard/gost/GOST_R_3412-2015.pdf
4. https://www.fundamental-research.ru/ru/article/view?id=41241

ANDROID-ДОДАТОК "BUCKET LIST"

Дурасов О., студент 343 гр., ОНАХТ, Одеса
Науковий керівник – Мітрофанова Н.Ф., ас. каф. ІТ та КБ, ОНАХТ, Одеса

Тайм-менеджмент є досить складним завданням для багатьох сучасних і активних людей. Швидкість плину часу і розвиток технологій роблять грамотний розподіл часу серйозною проблемою. Управління часом для сучасної лю-

дини – центральне поняття будь-якої системи особистої ефективності і продуктивності. Швидкий темп життя, особливо в великих містах і величезні масиви даних ускладнюють досягнення важливих для кожного з нас цілей.

Сьогодні тайм-менеджмент є необхідною складовою розвитку абсолютно будь-якого проекту так, як служить визначальним фактором при розрахунку його масштабу та часу, потрібного для його реалізації. Управління часом стосується не тільки сфери трудової діяльності або бізнесу, цей термін став розширюватися та включив в себе і різні аспекти особистої діяльності людини.

Електронними органайзерами користується все більша кількість людей, адже вони дозволяють організовувати діяльність у більш вузьких направленнях. Проаналізувавши потреби сучасних прогресивних людей, було вирішено створити органайзер "Bucket list", в який користувач може записати список своїх найзаповітніших бажань та мрій, встановити пріоритети виконання, розрахувати час та витрати на здійснення.

Створюваний програмний продукт надаватиме такі можливості як:

- створення списку бажань та розбиття на категорії;
- встановлення термінів виконання;
- розрахунок вартості обраних бажань;
- можливість прокладення маршруту до найближчих цілей;
- розміщення фото або відеоматеріалів про досягнення;
- можливість переносу інформації в соціальні мережі;
- нагадування про встановленні цілі;
- підрахунок витрачених грошей та залишку.

Метою розробки є створення android-додатку для організації вільного часу та розрахунку витрат коштів користувачів.

Список літератури:

1. Майер Рето Android 4. Программирование приложений для планшетных компьютеров и смартфонов // Эксмо. - 2013. - 816 с.
2. Медникс Зигард, Дорнин Лайрд, Мик Блэйк, Накамура Масуми Программирование под Android // Питер. - 2013. - 560 с.
3. Голощапов А. Google Android. Программирование для мобильных устройств // БХВ-Петербург. - Москва. - 2012. - 448 с .
4. Ed Brunette Hello Android 3e // Corvina Kiado - 2010. - 300 с.

РОЗРОБКА ІНФОРМАЦІЙНО-КЕРУЮЧОЇ СИСТЕМИ ДЛЯ АВТОВОКЗАЛУ

Єпур Л.І., студентка ТПА ОНАХТ
Керівник: Костиренко Т.П.

Сучасні умови для роботи з обслуговування клієнтів вже досягли того рівня, коли обслуговуюча система підприємства обробляє дані з дуже великою