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.

Для цього потрібно розуміти що і на яких веб-ресурсах говорять про підприємство. При використанні ручного пошуку кожного разу необхідно підбирати ключові слова, фільтрувати недостовірні джерела оминати рекламу, яка на даний момент в інтернеті повсюди, та ще й розбиратися зі структурою сайті з яких отримуватимуться данні. Весь моніторингу є доволі труд ємким і якщо користувач не має потрібних навичок то скоріш за все пошук спеціалізованої вузько-направленої інформації займе багато часу.

На даний момент існує маса продуктів які дозволили б автоматизувати цей процес, проте переважна більшість з них платними та складними у використанні для простого користувача. Виходячи з вище перерахованих деталей можна зрозуміти що реалізація додатку, який дозволив би автоматизувати процес пошуку інформації пов’язаної з ОНАХТ і був би простим у використанні є дуже доречною. Дана робота покликана:

1) автоматизувати процес пошуку новин пов’язаних з ОНАХТ;
2) підвищити ефективність роботи та зекономити затрачений час на моніторинг веб-ресурсів;
3) забезпечити впорядкування, структуризацію та зручний доступ до знадних даних.

Список літератури:

1. «Парсеры сайтов -программы для парсинга» http://obzor-tyt.ru/parsery-sajtov-programmy-dlya-parsinga-statya-1/

ОГЛЯД БЛОЧНОГО ШИФРУ «КОНИК»

Дубовка В.С., студент 334 групи ОНАХТ, Одеса
Науковий керівник – Болтач С. В., ас. Каф. ІТтаКБ, ОНАХТ, Одеса

Необхідність в більш надійній криптографічній системі захисту інформації стала поштовхом до створення нового блочного шифру, який був представлений у вигляді міжнародного стандарту, що об'єднує в собі більшу частину переваг блокових шифрів.

Метою дослідження є огляд нововведення нового стандарту блокового шифру «Коник».

В основі коду симетричний алгоритм блочного шифрування з розміром блоку 128 біт і довжиною ключа 256 біт який використовує для генерації раундових ключів мережу Фейстел.

Даний шифр затверджений як стандарт ГОСТ Р 34.12-2015 «Інформаційна технологія. Криптографічний захист інформації. Блокові шифри» наказом від 19 червня 2015 року № 749-ст.. Стандарт вступив в дію з 1 січня 2016 року[1;2].

Шифр розроблений Центром захисту інформації та спеціального зв'язку ФСБ Росії за участю ВАТ «Інформаційні технології та комунікаційні системи»

(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-