УДК 004.422

О. О. Булда

ПРОГРАМНИЙ ЗАСІБ ДЛЯ ЗАХИСТУ ФАЙЛІВ НА WINDOWS 10 MOBILE

Вінницький національний технічний університет

Анотація: *У статті представлено дослідження Windows app platform та Windows 10 mobile, обґрунтовано необхідність захисту файлів на даній операційній системі. Запропоновано і реалізовано протокол для шифрування і можливість перенесення даного додатку на настільну версію ОС Windows.*

Ключові слова: *шифрування, Windows, WAP, AES, захист файлів.*

Abstract: *The paper presents the research Windows app platform 10 and Windows mobile, the necessity of protecting files on this operating system. Proposed and implemented a protocol for encryption and the ability to transfer this application on the desktop version of Windows.*

Keywords: *encryption, windows, WAP, AES, file protection .*

У наше століття науково-технічного прогресу дуже складно уявити собі життя і побут сучасного суспільства без використання мобільних пристроїв. Прискорюється ритм життя, разом з ним прискорюється процес створення суспільством технічних новинок для своєї зручності. Взяти, приміром, мобільні телефони. Ми користуємося ними всюди – вдома, у потягу, на роботі, на відпочинку. Це зручно і, можна навіть сказати, комфортно. Мобільний телефон є у кожного – і у бізнесмена, і у школяра, він несподівано увірвався, але міцно осів і закріпився в нашому житті.

Якщо на зорі свого розвитку телефони намагалися зробити компактними і дешевими, то сьогодні, досягнувши в цьому пристойних показників, мобільні телефони роблять універсальним пристроєм, який може замінити диктофон, фотоапарат, і навіть комп'ютер.

Це ставить задачу захисту файлів, які зберігаються та передаються на мобільних пристроях, адже втрачений або вкрадений пристрій може зберігати в собі конфіденційну інформацію, банківські данні, особисті файли та ін. В цьому приходить на допомогу шифрування та стеганографії, що набагато збільшує, або не уможливлює доступ до даних.

Універсальність мобільних пристроїв досягається завдяки новим можливостям операційних систем, які розвиваються разом з самими апаратними можливостями. Успіх мобільного пристрою в більшій мірі залежить від того, яка операційна система на ньому встановлена.

Платформа Microsoft покриває широкий спектр пристроїв – від смартфонів і планшетів до настільних комп'ютерів та ігрової приставки Xbox One, і цілком природно, що розробнику хочеться мінімізувати зусилля при створенні додатків під усі форм-фактори (рис. 1). На конкуруючих платформах існує величезна різниця між настільними і мобільними додатками, оскільки вони працюють під управлінням різних операційних систем [1].

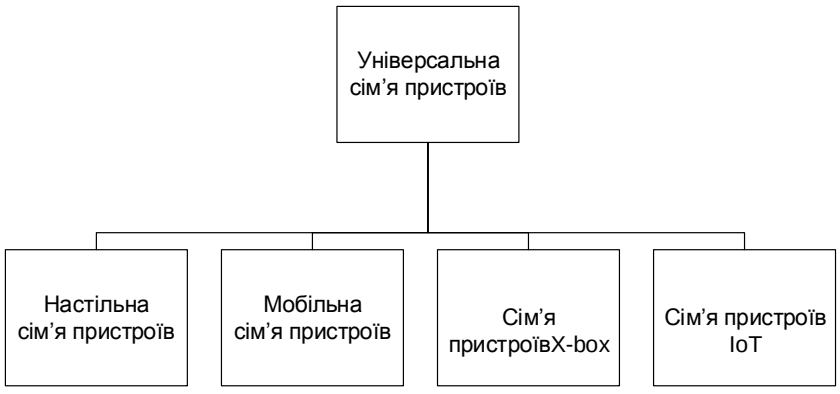

Рисунок 1 – Сімейство універсальних додатків

На даний момент корпорація Microsoft впритул підійшла до того, щоб уніфікувати всі платформи (Windows Phone, Windows 8, Xbox One) з точки зору API, і дозволити програмістам максимально використовувати загальний код при створенні додатків будь-яких додатків [2]. При цьому постає проблема малої кількості програм, що дозволяють захистити файли, які зберігаються або передаються на мобільній версії цієї ОС та недовіра до тих, які уже створені.

Для шифрування запропоновано використовувати AES. Стандарт AES (Advanced Encryption Standard) є стандартом шифрування США, прийнятим в 2000-му році. Він специфікує алгоритм Rijndael. Цей алгоритм є симетричним блоковим шифром, який працює з блоками даних довжиною 128 біт та використовує ключі довжиною 128, 192 і 256 біт (версії AES-28; AES-192 і AES-256) (рис. 2). Сам алгоритм може працювати і з іншими довжинами блоків даних і ключів, але ця можливість в стандарт не увійшла. При використанні 128-бітного ключа для злому шифрування, за заявою уряду США, буде потрібно 149 трильйонів років [3].

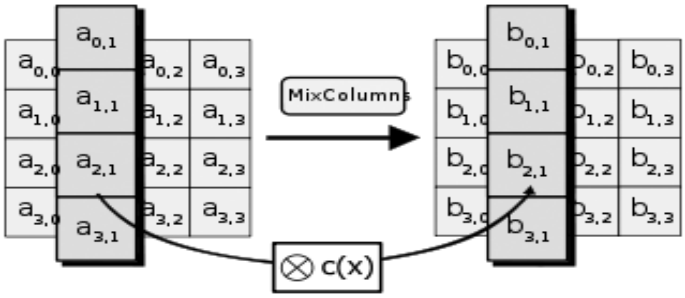

Рисунок 2 – Схема шифрування AES

Rijndael став новим стандартом шифрування даних завдяки цілому ряду переваг перед іншими алгоритмами. Насамперед, він забезпечує високу швидкість шифрування на всіх платформах: як при програмній, так і при апаратній реалізації. Його відрізняють незрівнянно кращі можливості розпаралелювання обчислень у порівнянні з іншими алгоритмами, представленими на конкурс. Крім того, вимоги до ресурсів для його роботи мінімальні, що важливо при використанні в пристроях, що володіють обмеженими обчислювальними можливостями.

Недоліком алгоритму можна вважати лише властиву йому нетрадиційну схему. Справа в тому, що властивості алгоритмів, заснованих на мережі Фейстеля, добре досліджені, а Rijndael, на відміну від них, може містити приховані уразливості, які можуть виявитися лише через деякий час з моменту початку його широкого розповсюдження [4].

Розроблений програмний засіб дозволить виконувати шифрування на операційній системі Windows 10 mobile будь-яких файлів та матиме можливість перенесення коду майже без змін на настільну версію, що підвищить рівень захисту та не уможливить доступ до захищених файлів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Универсальные приложения для Windows и Windows Phone [Електронний ресурс] // habrahabr.ru. – 2014. – Режим доступу до ресурсу: https://habrahabr.ru/company/microsoft/blog/218441/.

2. Пугачев С. Разработка приложений для Windows 8 на языке C# / С. Пугачев, А. Шериев, К. Кичинский. – Санкт-Петербург: БХВ-Петербур, 2013. – 416 с.

3. Бензин О. С. Стандарт криптографической защиты – AES / О. С. Бензин, М. А. Иванов. – Москва: КУДИЦ-ОБРАЗ, 2002. – 176 с.

4. Семенов Ю. А. Алгоритм шифрования AES [Електронний ресурс] / Ю. А. Семенов. – 2010. – Режим доступу до ресурсу: http://book.itep.ru/6/aes.htm.

Булда Олександр Олександрович, факультет інформаційних технологій так комп'ютерної інженерії, студент групи БС-14МС, Вінницький національний технічний університет, Вінниця, bulda.alex@gmail.com.

Каплун Валентина Аполінаріївна, ст. викл. кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, valuka8379@gmail.com.

Bulda Alexander, Faculty of Information Technology and Computer Engineering, student group BS-14MS, Vinnytsia National Technical University, Vinnytsia, olegskavun@mail.ru.

Kaplun Valentina Apolinariyvna, Vinnytsia National Technical University, Vinnytsia, valuka8379@gmail.com.