Захист інформації в автоматизованих системах шляхом шифрування даних з використанням стандарту «IDEA»

Демчик С.Л.[1]

[1]студентка кафедри кібернетики та інженерії, Житомирський військовий інститут імені С. П. Корольова
проспект Миру, 22, м. Житомир, Україна, Angelachek@mail.ru

***Анотація*— Обґрунтовано застосування методу захисту інформації в автоматизованих системах шляхом шифрування даних з використанням міжнародного стандарту шифрування. Запропоновано реалізацію нового методу захисту інформації від несанкціонованого доступу шляхом створення програмного комплексу, що проводить шифрування інформації перед її передачею відкритими каналами. Представлено реалізацію міжнародного стандарту шифрування даних «IDEA». Розроблено модель системи, алгоритм функціонування та схему проектованого програмного забезпечення. Отримані результати теоретичного аналізу криптостійкості системи.**

Ключові слова: захист інформації, автоматизована система, шифрування даних, відкрита інформація.

Information protection in automated systems by encrypting data using standards «idea»

Demchyk S.L.[1]

[1]Student., Department of of Cybernetics and Engineering, S.P. Korolyov Zhytomyr Military Institute
pr. Mira, 22, Zhytomyr, Ukraine, Angelachek@mail.ru

***Abstract* — Application of the method of protection of information in automated systems by encrypting data using the international standard encryption. An implementation of a new method to protect information from unauthorized access by creating a software system that conducts encryption before transferring it to the open channels. Presented by implementing the international standard data encryption «IDEA». The model system algorithm of the scheme and the designed software. The results of the theoretical analysis of the reliability of the system.**

Keywords: information protection, automated system, data encryption, public information.

Вступ

Швидке вдосконалення інформатизації, проникнення її в усі сфери життєво важливих інтересів зумовило, крім безперечних переваг, і появу низки стратегічних проблем. Збільшення небезпеки несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем змушує розробляти нові методи захисту інформації. Одним з таких методів є шифрування відкритої інформації технологіями, що не перебувають у відкритому доступі. Таким чином, є необхідність у розробці автоматизованих технічних та програмних засобів, що допоможуть у короткий строк передати інформацію у зашифрованому вигляді.

Найкращим способом забезпечення критеріїв конфіденційності, цілісності та доступності для програм є верифікація та валідація результатів розробленого програмного продукту на кожному етапі життєвого циклу з виключенням можливості проникнення сторонніх програмних додатків всередину системи.

Для усунення можливості модифікації програмного комплексу слід застосувати інструменти криптографічного захисту шляхом перетворення інформації з використанням спеціальних даних з метою приховування змісту інформації, цілісності, авторства. Важливим є захист інформації від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення [1].

Серед засобів захисту відкритої інформації одним з найважливіших є криптографічний. Такий захист даних здійснюється за допомогою відповідної криптографічної системи. Конкретні вимоги до засобів криптографічного захисту інформації залежать від її правового режиму.

Так, для захисту інформації в автоматизованих системах доцільним буде розроблення програмного засобу шифрування відкритої інформації за допомогою міжнародного стандарту шифрування даних IDEA.

Генерування ключів для шифрування даних з використанням стандарту IDEA

Алгоритм IDEA (англ. International Data Encryption Algorithm) є симетричним блоковим шифром, в якому процес розшифрування даних аналогічний процесу їх зашифрування, тому структурна схема алгоритму розшифрування даних відповідає схемі алгоритму зашифрування.

Алгоритм розгортання ключа визначає порядок отримання раундових ключів із початкового ключа шифрування *K*. Раундові ключі виходять із ключа шифрування за допомогою алгоритму вироблення ключів. Він містить два компоненти: розширення ключа шифрування *K*; вибір раундових ключів.

Основний принцип алгоритму полягає в тому, що ключ шифрування *K* розширюється в розширений ключ K_P, при чому кількість бітів кожного раундового ключа дорівнює довжині підблока даних, а кількість раундових ключів визначається з розрахунку шести ключів на кожний раунд зашифрування або розшифрування даних (*48* ключів, кожний завдовжки *16* бітів) і чотири ключі на кінцеве перетворення даних (кожний завдовжки також *16* бітів). Разом має бути створено п'ятдесят два *16*-бітових раундових ключі.

На рис. 1 наведено процес отримання розширення ключа зашифрування

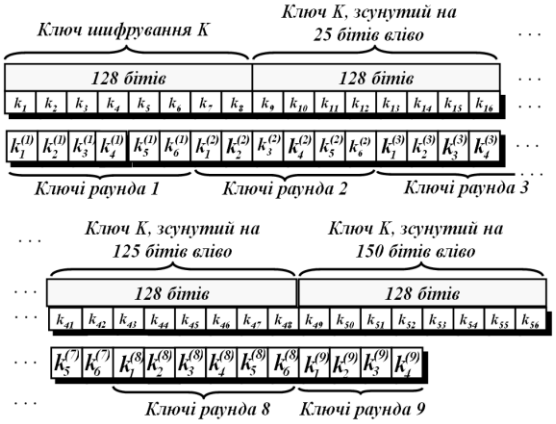

Рисунок 1 – Схема отримання раундових ключів зашифрування

Розширення ключа шифрування *K* здійснюється таким чином: ключ шифрування *K* поділяється на вісім частин по *16* бітів кожна. Як результат виходять перші вісім ключів для зашифрування даних, які позначимо як k_1, k_2, ..., k_8, при цьому ключ k_1 дорівнює першим *16* бітам ключа шифрування *K*, k_2 дорівнює наступним *16* бітам ключа *K* і так далі. Потім відбувається циклічний зсув ключа шифрування *K* вліво на *25* бітів. Отримана *128*-розрядна послідовність також поділяється на вісім частин по *16* бітів кожна. Як результат виходять другі вісім ключів для зашифрування даних, які позначимо як k_8, k_9, ..., k_{17}. Ця процедура повторюється до тих пір, поки не буде створено *56* ключів. Останні чотири ключі (k_{53}, k_{54}, k_{55} і k_{56}) у шифрі *IDEA* не використовуються і вони просто відкидаються.

Хоча в кожному раунді за винятком першого й восьмого використовуються тільки 96 бітів ключа шифрування *K*, множина бітів цього ключа на кожній ітерації не перетинаються, і не існує відношення простого зсуву між ключами різних раундів. Це відбувається, тому що в кожному раунді використовується тільки шість раундових ключів, тоді як при кожній ротації ключа виходить вісім ключів розширеного ключа K_P.

ПРОЦЕС ШИФРУВАННЯ ДАНИХ З ВИКОРИСТАННЯМ СТАНДАРТУ IDEA

Алгоритм шифрування має два входи: незашифрований блок і ключ. У даному випадку незашифрований блок має довжину 64 біти, ключ має довжину 128 бітів.

Алгоритм IDEA складається з восьми раунді. Блок даних поділяється на чотири 16-бітові підблоки. Кожний раунд отримує на вході чотири 16-бітові підблоки та створює чотири 16-бітові вихідні підблоки, тобто всього в алгоритмі використовується 52 раундових ключа.

На рис. 2 наведено структура алгоритму IDEA

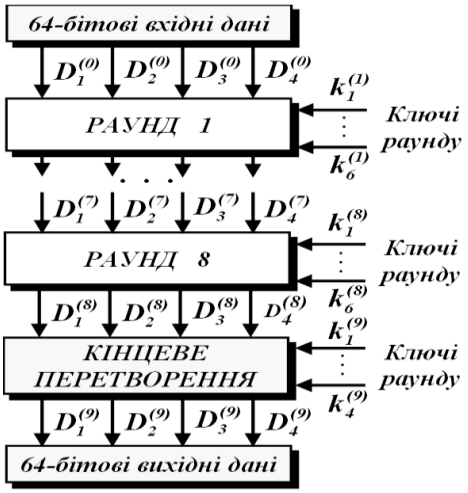

Рисунок 2 – Структура алгоритму *IDEA*

Раунд починається з перетворення, яке комбінує чотири вхідні підблоки даних: $D_1^{(i)}$, $D_2^{(i)}$, $D_3^{(i)}$ і $D_4^{(i)}$ кожний довжиною *16* бітів з чотирма раундовими ключами: $k_1^{(i)}$, $k_2^{(i)}$, $k_3^{(i)}$ і $k_4^{(i)}$ кожний довжиною також *16* бітів, використовуючи операції складання та множення.

Одним з основних елементів алгоритму, що забезпечують дифузію, є структура *MA* — множення/складання. Ця структура повторюється в алгоритмі вісім разів, забезпечуючи високоефективну дифузію.

Чотири вихідних блоки цього перетворення комбінуються, використовуючи операцію *xor* для формування двох *16*-бітових підблоків, які є входами *MA* структури. Крім того, *MA* структура має на вході ще два раундових ключі і створює два *16*-бітові підблоки виходу.

На рис. 3 наведено структуру пристрою *MA*

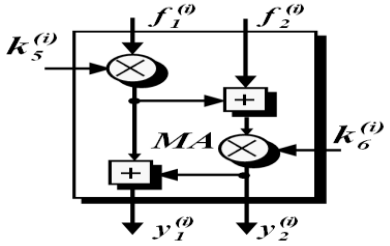

Рисунок 3 – Структура пристрою *MA*

На вхід цієї структури подаються два *16*-бітові значення ($f_1^{(i)}$ і $f_2^{(i)}$) і два *16*-бітових раундових ключа ($k_1^{(i)}$ і $k_2^{(i)}$), на виході створюються два *16*-бітових значення ($y_1^{(i)}$ і $y_2^{(i)}$).

Вичерпна комп'ютерна перевірка показує, що кожний біт виходу цієї структури залежить від кожного біта входів незашифрованого блоку даних і від кожного біта раундових ключів. Ця структура повторюється в алгоритмі вісім разів, забезпечуючи високоефективну дифузію.

Генерування псевдовипадкових чисел

Для створення експертної системи з шифрування відкритої інформації для передачі відкритими каналами було обрано міжнародний алгоритм шифрування даних IDEA.

Безперечною перевагою алгоритму є те, що довжина ключа є досить великою для того, щоб запобігти можливості простого перебору ключа. За довжини ключа 128 бітів IDEA вважається досить безпечним. Довжина блока має достатні розміри, щоб приховати всі статистичні характеристики початкового повідомлення. З іншого боку, складність реалізації криптографічної функції зростає експоненціально відповідно до розміру блока. Якщо розбиття на блоки по 64 біт неможливо, останній блок доповнюється різними способами певною послідовністю біт. Для уникнення витоку інформації про кожному окремому блоці використовуються різні режими шифрування.

Проаналізувавши алгоритм зашифрування даних з використанням алгоритму IDEA, було встановлено, що алгоритм IDEA безпечний алгоритм. Алгоритм IDEA має 128-бітовий ключ, що забезпечує його криптостійкість. Внутрішня структура алгоритму IDEA забезпечує кращу стійкість до криптоаналізу. При шифруванні закодований текст має ту ж довжину, що й вихідний.

Проте, істотним недоліком цього алгоритму є те, що він запатентований, а це перешкоджає його вільному поширенню. IDEA не передбачає збільшення довжини ключа, а також не всі роботи з криптоаналізу були опубліковані, тобто цілком можливо, що шифр буде зламаний в майбутньому.

Зашифровані дані однозначно залежать від ключа складним і запутаним способом. Кожний біт початкових даних впливає на кожний біт зашифрованих даних. Поширення одного незашифрованого біта на велику кількість зашифрованих бітів приховує статистичну структуру початкових даних. Визначити, як статистичні характеристики зашифрованих даних залежать від статистичних характеристик початкових даних, досить не просто. IDEA з цього погляду є дуже ефективним алгоритмом.

ВИСНОВКИ

Проведений аналіз алгоритму генерації раундових ключів для зашифрування/ розшифрування даних з використанням алгоритму IDEA. В результаті чітко сформовані уявлення про роботу проектованого додатку, його функціональні можливості та інтерфейсну частину, щодо формування ключів.

Проведений аналіз алгоритму зашифрування/розшифрування даних з використанням алгоритму IDEA. Розроблено модель системи, алгоритм функціонування та схему класів проектованого програмного забезпечення. Детального розроблено та вирішено задачі, що складають функціонал програмного забезпечення.

Впровадження в програму інструментів криптографічного захисту посилює безпеки при несанкціонованому втручанні в роботу комп'ютерних, інформаційних і телекомунікаційних систем, а значить будь-який зловмисник не зможе отримати доступ до інформаційної системи.

Отримані результати теоретичного аналізу доводять, що з допомогою розглянутої методики стала кращою криптостійкість програми та інформаційної системи в цілому.

ЛІТЕРАТУРА REFERENCES

[1] Комич Б.М.Основні принципи діяльності із захисту інформації. Захист інформації в інформаційних системах. – 2012. – № 2 (22). – С. 216-230., Корченко О.Г., Сіденко В.П., Дрейс Ю.О. Прикладна криптологія: системи шифрування // К.: ДУТ,2014. – С. 245-269.

[2] [Электронный ресурс] - Олег Зензин — Режимы шифрования, раздел Накопление ошибок в различных режимах шифрования - Режим доступа: - http://citforum.ru/security/cryptography/rejim_shifrov/

[3] С.Г.Баричев, Р.Е.Серов "Основы современной криптографии