УДК 004.056.55:004.021

СИНТЕЗ КРИПТОГРАФІЧНИХ СИСТЕМ НА ПРИКЛАДІ DES І RSA АЛГОРИТМІВ

Марініч К. Ю.
Науковий керівник – професор катедри ПІ, к.т.н. Бондарєв В. М.
Харківський національний університет радіоелектроніки, каф. ПІ,
м. Харків, Україна
тел. +38-(099)-788-18-24, e-mail: kseniia.marinich@nure.ua.

The purpose of this work is to identify types of cryptographic systems, analyse and compare them. Determine the difference between symmetric and asymmetric cryptographic systems on examples of DES and RSA algorithms. In thesis were considered principles of working both of these methods.

З кожним роком питання безпеки та секретності стає все більш і більш актуальним. Потужності комп'ютерів посилюються, швидкість обробки даних зростає, тож і можливості дешифрування стають ширше. Тому задля забезпечення секретності повідомлень користувачів використовують різні системи та алгоритми шифрування.

Яким чином взагалі відбувається шифрування і дешифрування інформації? Шифрування передбачає перетворення даних у зашифровану форму так, що будь-яка сторона, яка перехоплює, не може прочитати та зрозуміти їх, крім отримувача, якому вони призначені. Процес шифрування стає можливим завдяки криптографічним ключам в поєднанні з різними математичними алгоритмами. На наш час існує дві системи шифрування: симетрична (symmetric cryptographic system) та асиметрична (asymmetric cryptographic system). Розглянемо кожну окремо.

Симетрична криптосистема, що містить алгоритми, які виконуються на одному наборі параметрів. Симетричний шифр, тобто шифр, що є симетричною криптографічною системою, використовує один й той самий ключ як для шифрування, так і для розшифровки, або ж різні, але такі, що з одного легко можна знайти інший. Найбільш розповсюдженим алгоритмом з закритим ключом є DES (Data Encryption Standard) алгоритм.

Принцип його заснований на мережі Фейстиля, і має таку структуру: шифрує текст 64-бітними блоками, з одного кінця алгоритму вводиться 64-бітний блок відкритого тексту, з іншого виводиться 64-бітний блок шифротексту. Ключ – 56-бітне число, що псевдорандомно генерується і може бути змінене в будь-який момент часу. На першому рівні алгоритм – це лише комбінація двох основних методів шифрування: зміщення та перестановки. Фундаментальною частиною DES э застосування до тексту одиничної комбінації цих методів (спочатку зміщення, потім – дифузія), що залежить від ключа. Такий блок називається раундом, DES складається з 16 таких раундів. В алгоритмі використовується лише стандартна арифметика 64-бітових чисел та булеві операції, а достаток

повторень робить його ідеальним для реалізації в спеціалізованій мікросхемі.

Асиметрична криптосистема – це така система, що містить алгоритми, набори параметрів яких різняться і є такими, що по одному з них неможливо обчислювально знайти інші. RSA (абревіатура від прізвищ Rivest, Shamir й Adleman) є найбільш популярним шифруванням з відкритим ключом.

Ці криптосистеми використовують односторонні функції, що мають такі властивості:

- якщо x відомо, то f(x) знайти досить просто;
- якщо відомо y = f(x), то для знаходження x немає ефективного шляху.

В основу RSA покладено складність задачі факторизації добутку двох простих великих чисел. Для шифрування використовується піднесення до степеню за модулем великого числа. Для дешифрування необхідно за реальний час вирахувати функцію Ейлера від даного великого числа.

Генерація простого та секретного ключів виконується за таким алгоритмом:

1. Оберемо два простих великих числа p й q;
2. Нехай n – результат їх множення, n=p*q;
3. Оберемо довільне число d, d є взаємно простим до (p-1)*(q-1);
4. Визначимо таке число e, для якого є правдивим співвідношення (e*d) mod ((p-1)*(q-1))=1.
5. Тоді відкритим ключом буде пара (e, n), а секретним (d,n)

Аби зашифрувати текст ми маємо розбити його на блоки, кожний з яких може бути представлений у вигляді числа M(i) = 1, 2, …, n-1 і зашифрувати за формулою $c = m^e \bmod n$.

У 2010 році група вчених зуміла дешифрувати RSA шифротекст довжиною в 768 біт, тож зараз в якості надійної системи шифрування розглядається лише RSA-ключі довжиною від 1024 біт. Деякі компанії не підтримують шифрування менше ніж 2048 біт.

RSA шифрування, як і будь який інший алгоритм з відкритим ключом, є в рази повільнішим, аніж буть-який із симетричним шифруванням. Також системи з відкритим ключом потребують меншу довжину ключа для забезпечення потрібної стійкості шифру, що спрощує реалізацію алгоритму. Але асиметричні системи можуть використовуватись у E2EE методі – шифрування і дешифрування відбувається на сторонах, через що сервер не має доступу до даних, що передаються.

Список використаних джерел:

1. Акопов Д. О. (2014). Криптографія - історія, методи та стандарти. *Вісник Київського інституту бізнесу та технологій.*
2. Zubov A. Y. (2008). Authentication encryption based on authentication code with secrecy. *Prikladnaya diskretnaya matematika*.