УДК 004.7.056.5

АНАЛІЗ ІСНУЮЧИХ АЛГОРИТМІВ ЗАХИСТУ ІНФОРМАЦІЇ, ЯКА ПЕРЕДАЄТЬСЯ В КОМП'ЮТЕРНИХ МЕРЕЖАХ, ТА ВИЗНАЧЕННЯ НАПРЯМКІВ ЇХ ВДОСКОНАЛЕННЯ

І. І. Когут

Івано-Франківський національний технічний університет нафти і газу
(76019, Україна, м. Івано-Франківськ, Карпатська 15,ksm@nung.edu.ua)

Захист інформації, що передається в комп'ютерних мережах з кожним роком набуває все більшого значення [1, 2].

Кожний вид інформації має свої специфічні особливості, що суттєво впливають на вибір методів її шифрування. Велике значення відіграють об'єм та необхідна швидкість передачі даних [3,4].

Потреба вирішення проблеми захисту електронної інформації обумовлює актуальність розробки шифрів, як одного із видів криптографічних перетворень, що використовують для захисту інформації в комп'ютерних системах та мережах. В таблиці 1 наведені результати проведеного аналізу існуючих алгоритмів захисту інформації.

Таблиця 1 – Результати аналізу криптографічних алгоритмів

Алгоритм	Переваги	Недоліки
DES	Високий рівень захисту даних проти дешифрування і можливої модифікації даних; високий ступінь складності, що робить його розкриття дорожче одержуваного при цьому прибутку; економічний в реалізації і ефективний в швидкодії	Занадто малий розмір ключа, орієнтований на апаратну реалізацію, а тому є уразливим
ДГСТ 28147-89	Відсутність недоліків алгоритму DES і володіння всіма його перевагами	Дуже складна програмна реалізація, низька швидкодія
MARS	Симетричність	Складна структура, високі затрати пам'яті, погана розпаралелюваність
TEA	Стійкий до диференціального криптоаналізу	Найбільш вразливий до "атак на зв'язаних ключах", наявність еквівалентних ключів
XTEA	Менша вразливість до "атак на зв'язаних ключах" порівняно з TEA	Менш стійкий до диференціального аналізу порівняно з TEA
RSA	Асиметричність, можливість змінювати як відкритий, так і закритий ключ	Досить повільний
ECDSA	Криптостійкість і швидкість роботи більші, ніж в RSA	Кожен підпис потребує кілька випадкових або непередбачуваних даних в якості вхідних

В результаті проведених досліджень встановлено, що значними перевагами по відношенню до інших володіють алгоритми RSA і ECDSA. В даних алгоритмах закладені властивості програмної реалізації, обміну повідомленнями по незахищених каналам зв'язку, досягнення необхідної крипостійкості. Проте, алгоритми RSA і ECDSA мають невисоку швидкість роботи. В зв'язку з вищевказаним подальші дослідження потрібно спрямувати на підвищення продуктивності вказаних алгоритмів захисту інформації.

Літературні джерела

1 Бабчук С. М. Класифікація спеціалізованих комп'ютерних мереж для автоматизації систем життєзабезпечення будівель / С. М. Бабчук // Научные труды Sworld. 2014. т.11. №3. с. 33-35.

2 Бабчук С. М. Спеціалізована експертна комп'ютерна система ідентифікації кадмію / С. М. Бабчук, Л. Р. Бабчук // Восточно-Европейский журнал передовых технологий. 2013. т.2. №10(62). с. 18-20.

3 Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф. 2002. - 610 с.

4 Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии / Ф. Бауэр. – М.: Мир, 2007. - 550 с.

УДК 622.691.002.51

УДОСКОНАЛЕННЯ УЛЬТРАЗВУКОВОГО МЕТОДУ КОНТРОЛЮ ДЕФОРМАЦІЇ ТРУБНИХ СТАЛЕЙ

Р.О. Тімков, М.Б. Маритчак, О.В. Гойсан, А.А. Сєвєрова, З.П. Лютак

Івано-Франківський національний технічний університет нафти і газу

У недеформованому металі важаємо, що швидкість ультразвуку в усіх напрямках однакова. При деформації металу змінюється структура металу (розтяг, стиск) і швидкість ультразвуку змінюється як в напрямку дії сили, так і в перпендикулярному напрямках.

$$\sigma = \mu \cdot \varepsilon \qquad (1)$$

де σ – напруження

μ – модуль Юнга

ε – деформація

Знаючи зміну швидкості поширення ультразвуку і механічні константи досліджуваного металу, тобто, модуль Юнга, коефіцієнт Пуассона можна визначити механічні властивості матеріалу.

$$\varepsilon = k \cdot \left(\frac{c_1 - c_2}{c_1}\right) \qquad (2)$$

де, k – механічний коефіцієнт