УДК 004.056.55

О. Г. Суверток

ПОШУК НАЙЕФЕКТИВНІШОГО МЕТОДУ АСИМЕТРИЧНОГО ШИФРУВАННЯ ЩОДО ПІДВИЩЕННЯ ШВИДКОДІЇ КРИПТОПЕРЕТВОРЕНЬ

[1] Вінницький національний технічний університет;

Анотація

Використавши порівняльний аналіз криптоалгоритмів з відкритим ключем аналізуємо, швидкості шифрування і дешифрування даних, які передаються, яка обумовлена їх класичною асиметричною структурою. Дана методика експертної оцінки асиметричних криптоалгоритмів дозволила оцінити їх якість з позиції рівня реалізованих функцій.

Ключові слова: асиметричні шифри, порівняльний метод Сааті

Abstract

Using a comparative analysis of open source cryptographic algorithms, we analyze the speed of encryption and decryption of transmitted data, which is due to their classical asymmetric structure. This method of expert estimation of asymmetric cryptographic algorithms allowed to evaluate their quality from the standpoint of the level of reactive functions.

Keywords: asymmetric ciphers, comparative Saati method.

Вступ

Використання криптографічних методів стала особливо актуальною в даний час у зв'язку з передачею у відкритій мережі Інтернет великих обсягів інформації державного, військового, комерційного і приватного характеру. У зв'язку з високою вартістю збитків від втрат, розголошення і спотворення інформації, що зберігається в базах даних і передаються по локальних мережах, в сучасних ІС рекомендується зберігати і передавати інформацію в зашифрованому вигляді.

Метою даної роботи є пошук найефективнішого методу асиметричного шифрування щодо підвищення швидкості криптоперетворень.

Результати дослідження

Для оціночного порівняння обраних криптоалгоритмов проведиться їх порівняльний аналіз за допомогою методу Сааті. Трохи нижче відображені вибрані критерії, на підставі яких буде проводитися процедура оцінки:

A1 — Криптостійкість (MIPS);

A2 — Розмір генерованого ключа (до 4096 біт);

A3 — Призначення (шифрування і цифровий підпис);

A4 — Швидкість шифрування (при довжині модуля в 1024 біта);

A5 — Швидкість дешифрування (при довжині модуля в 1024 біта).

Використовуючи аналітично-ієрархічну процедуру Сааті, встановимо для кожного критерію якості його вагу.

Правила заповнення матриці парних порівнянь представлені в таблиці 1.

Таблиця 1.

Значення коефіцієнтів матриці парних порівнянь

Xij	Значення
1	і-ий критерій практично рівноцінний j-му
3	і-ий критерій у меншій мірі важливіше j-го
5	і-ий критерій важливіше j-го
7	і-ий критерій більшою мірою важливіше j-го
9	і-ий критерій набагато важливіше j-го

Матриця парних порівнянь, ваги критеріїв і середні геометричні занесені в таблицю 2.

Таблиця 2.

Матриця парних порівнянь, середні геометричні і ваги критеріїв

	A1	A2	A3	A4	A5	Середнє геометричне	Важелі критеріїв
A1	1	3/1	7/1	5/1	5/1	3,5	0,49
A2	1/3	1	5/1	5/1	5/1	2,11	0,29
A3	1/7	1/5	1	3/1	3/1	0,76	0,11
A4	1/5	1/5	1/3	1	1	0,42	0,06
A5	1/5	1/5	1/3	1	1	0,42	0,06

На рисунку 1. зображена створена на підставі даних таблиці 2. діаграма вагових коефіцієнтів критеріїв для A1, A2, A3, A4 і A5

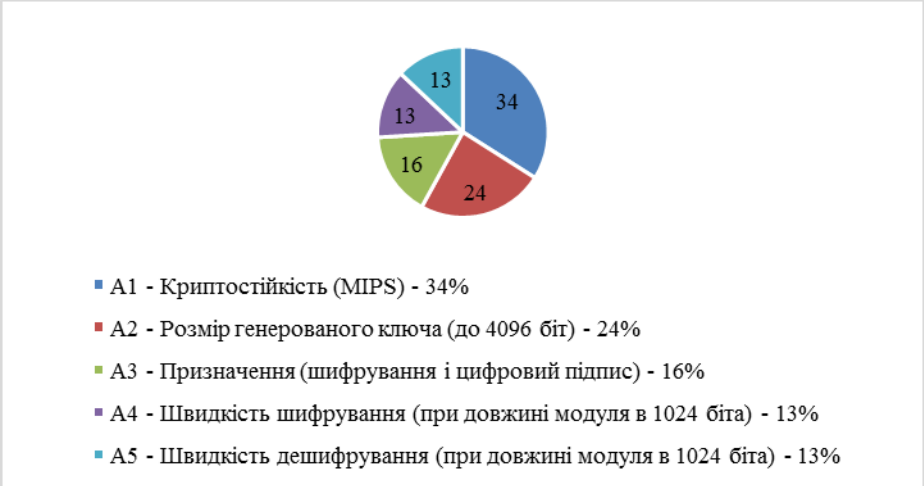

Рис. 1. Діаграма вагових коефіцієнтів критеріїв для A1, A2, A3, A4 і A5

Після цього обчислимо додаткову величину L, підсумувавши вагові коефіцієнти і добутки сум стовпців матриць: L = 5,45.

Таким чином, індекс узгодженості ІУ = (L-N)/(N-1) = 0,113.

Отже, величина випадкової узгодженості для розмірності матриці парних порівнянь: ВУ = 1,24.

Відношення узгодженості ВУ=ІУ/ВУ = 0,09 не перевищує 0,2, а значить, додаткове уточнення матриці парних порівнянь не вимагається.

Використовуючи обчислені коефіцієнти, знайдемо інтегральний показник якості для наступних асиметричних алгоритмів шифрування даних: RSA, DSA, шифросистеми Ель-Гамаля, обміну ключами Діффі-Хелмана, протоколу Аншеля-Гольдфельда.

Встановимо категоріальну шкалу від нуля до семи (де 0 - якість не задовільна, а 7 - гранично досяжний рівень якості) для встановлення функціональних можливостей обраних криптоалгоритмів.

Значення вагових коефіцієнтів a_i, що відповідають функціональним можливостям аналогів:

Криптостійкість (MIPS): a1 = 0.34;

Розмір генерованого ключа (до 4096 біт): a2 = 0.24;
Призначення (шифрування і цифровий підпис): a3 = 0.16;
Швидкість шифрування (при довжині модуля в 1024 біта): a4 = 0.13;
Швидкість дешифрування (при довжині модуля в 1024 біта): a5 = 0.13;
де $\sum a_i = 1$. За обраною шкалою визначимо кількісні значення функціональних можливостей Xij (таблиця 2.3) і обчислимо інтегральні показники якості для обраних асиметричних алгоритмів шифрування:

Таблиця 3.

Інтегральні показники якості

Критерії	**Вагові коефіцієнти**	**Асиметричні алгоритми**					**Базові значення**
		RSA	DSA	Шифросистема Ель-Гамаля	Обмін ключами Діффі-Хелмана	Протокол Аншеля - Гольдфельда	
Криптостійкість (MIPS)	0,49	7	7	7	5	5	6,2
Розмір генерованого ключа (до 4096 біт)	0,29	5	3	7	3	5	4,6
Призначення (шифрування і цифровий підпис)	0,11	7	7	7	3	3	5,45
Швидкість шифрування (при довжині модуля в 1024 біта)	0,06	7	7	3	5	3	4,95
Швидкість дешифрування (при довжині модуля в 1024 біта)	0,06	3	3	7	3	3	3,8
Інтегральні показники якості Q		6,25	5,67	6,83	4,13	4,59	5,49

Де $Q_j = \sum a_i * X_{ij}$ - інтегральний показник якості для j-го криптоалгоритма.
Значення характеристик функціональних можливостей (критеріїв) представлена у вигляді пелюсткової діаграми на рисунку 2.

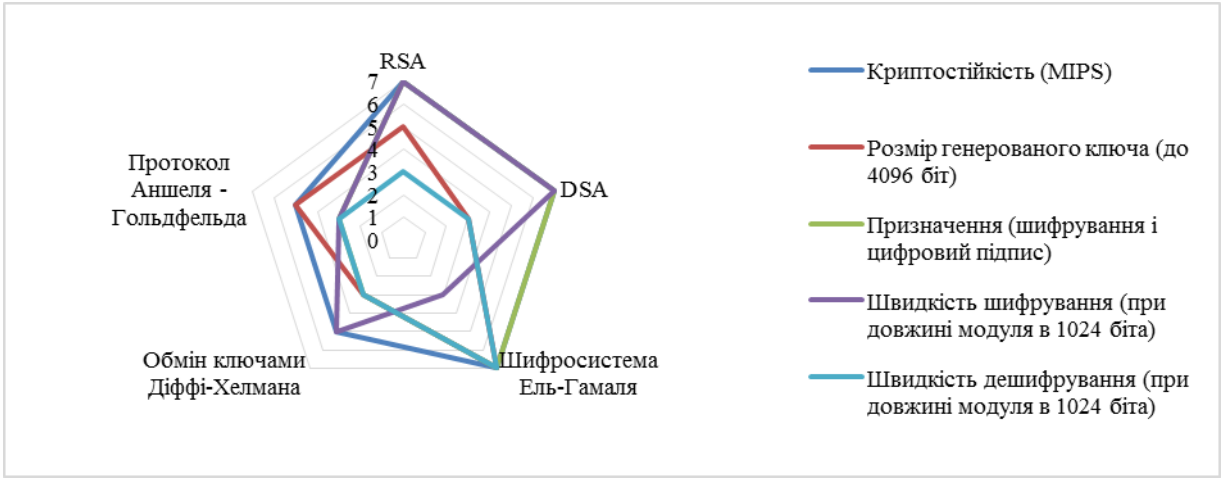

Рис. 2. Значення характеристик функціональних можливостей (критеріїв)

Висновки

Порівняльний аналіз криптоалгоритмів з відкритим ключем показав, що з усіх представлених аналогів ні один не має максимально високого показника по всім заявленим параметрам, особливо розглянуті криптоалгоритми страждають від низької швидкості шифрування і дешифрування даних, які передаються, яка обумовлена їх класичною асиметричною структурою. Дана методика експертної оцінки асиметричних криптоалгоритмів дозволила оцінити їх якість з позиції рівня реалізованих функцій. Якщо розглядати алгоритми з позиції швидкості шифрування то із проаналізованих алгоритмів лідуючі позиції зайняли два алгоритми – RSA та DSA.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Рыбанов А. Определение весовых коэффициентов сложности тем учебного курса на основе алгоритма Саати // Педагогические измерения. 2014. № 4. С. 21-28.

2. Ростовцев, А. Г. Методы криптоанализа классических шифров / А. Г. Ростовцев, Н. В. Михайлова. – М.: Наука, 2012. – 208 с.

3. Адигеев М.Г. Введение в криптографию. Часть 1. Основные понятия, задачи и методы криптографии. - Ростов-на-Дону: Ростовский гос. ун-т, 2002. - 35 с.

Суверток Олексій Геннадійович — студент групи УБ-14б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: Suvlex97@gmail.com

Науковий керівник: ***Яремчук Юрій Євгенович*** — доктор технічних наук, професор, директор Центру інформаційних технологій і захисту інформації, голова секції «Управління інформаційною безпекою», Вінницький національний технічний університет, м. Вінниця

Suvertok Oleksii — student group UB-14b, Faculty of Management and Information Officer, Vinnytsia National Technical University, Vinnytsia, e-mail: Suvlex97@gmail.com

Supervisor: ***Yaremchuk Yuriy*** — Doctor of Technical Sciences, Professor, Director of the Center for Information Technology and Information Protection, Head of the Section "Information Security Management", Vinnytsia National Technical University, Vinnytsya