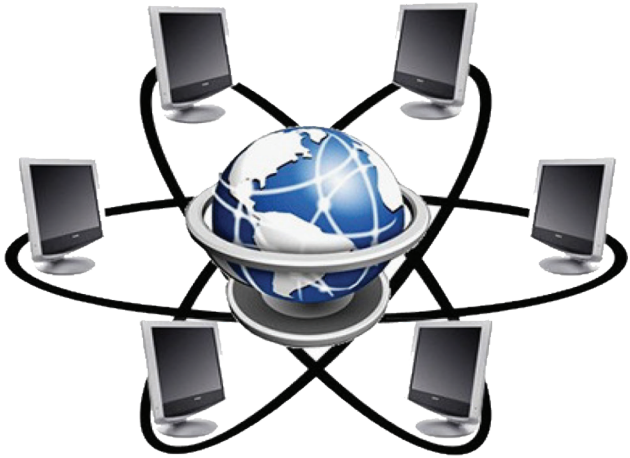
Одеський національний політехнічний університет; Київський національний університет ім. Т. Г. Шевченка; Харківський національний університет радіоелектроніки; Національний авіаційний університет; Державний університет морського та внутрішнього мореплавства ім. адмірала С. О. Макарова; Одеський національний університет ім. І. І. Мечникова; Сумський державний університет; Національний університет суднобудування ім. адмірала С. О. Макарова; Лодзінський технічний університет



МАТЕРІАЛИ 9-ї МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«Інформаційні управляючі системи та технології (ІУСТ–2020)»

24–26 вересня 2020 р.

Одеса — 2020
«Екологія»

ЗМІСТ

Секція 1 Інформаційні системи управління

Рассчитывая поверхность распределения вероятностей взлома одноуровневых защит в соответствие с формулами (1), (2) и (3), получим реальное распределение вероятности взлома комбинированной многоуровневой защиты. На рис.1 представлены расчеты поверхностей распределения реальной вероятности взлома (светлая поверхность) и распределения вероятности взлома комбинированной многоуровневой технической защиты информации (темная поверхность), которые определяются формулами (2) и $P(m)=1/m$ соответственно. Из рис.1 видно, что реальный взлом ТЗИ наиболее вероятен для направления по линии 1 в точке $m1=4$ и $t1=3$ и для направления по линии 2 в точке $m2=4$ и $t2=6$.

В работе предложен способ определения реальной защищенности информации по направлению процесса и распределению вероятности взлома комбинированной ТЗИ. В этом случае по построенным поверхностям вероятностей взлома можно определять реальную надежность ТЗИ для любых направлений взлома.

Литература

1. Журиленко Б.Е. Вероятностная надежность защиты информации в зависимости от направления взлома/ Журиленко Б.Е., Николаева Н.К.//Захист інформації, 2018. – №3(20). – С. 174-179. DOI:10.18372/2410-7840.20.13073

УДК 681.3.05:004.056.5

КРИПТОГРАФІЧНИЙ КООПЕРАТИВНИЙ ПРОТОКОЛ УЗГОДЖЕННЯ ІЗОМОРФНО ПРЕДСТАВЛЕНОГО СПІЛЬНОГО СЕКРЕТНОГО МАТРИЧНОГО КЛЮЧА-ПЕРЕСТАНОВКИ ВЕЛИКОЇ РОЗМІРНОСТІ

К.т.н. Красиленко В.Г.[0000-0001-6528-3150], Нікітович Д.В.[0000-0002-8907-1221]
E-mail:krasvg@i.ua

CRYPTOGRAPHIC COOPERATIVE PROTOCOL FOR HARMONIZATION AN ISOMORPHICALLY PRESENTED JOINT SECRET MATRIX-PERMUTATION KEY OF LARGE DIMENSION

Ph.D. Krasilenko V.G., Nikitovich D.V.

Анотація. Розглядається кооперативний протокол узгодження ізоморфно представленого спільного секретного матричного ключа-перестановки великої розмірності, наведені результати моделювання.

Ключові слова*:* протокол узгодження ключа-перестановки, захист.

Abstract. The cooperative negotiation protocol of large dimension secret key-permutation is considered. The simulation results are given.

Keywords: key negotiation protocol, cryptography, permutations, defense.

Вступ. Захист інформаційних об'єктів (ІО) забезпечують методи та засоби криптографії. Одним з ключових питань їх застосування є процеси узгодження електронним шляхом спільних секретних ключів чи низки похідних від них під-ключів. Проте, більшість протоколів, наприклад, Діффі-Хелмана, MTI, STS, тощо, як і більшість методів криптографічних перетворень (КП) ІО, зорієнтовані на суто скалярні ключі та послідовну обробку блоків. Навіть для стандартів AES, IDEA, довжини блоків і ключів не перевищують 512 бітів, за винятком хіба-що FEAL, RC6 та деяких нових, для яких ці довжини можуть обмежуватись 1К-2К бітами. Темпи розвитку методів крипто-аналізу, обчислювальних засобів спонукають до збільшення довжин ключів (ДК), тому актуальним є пошук нових концепцій, що зорієнтовані на паралельні матричні процесори та моделі матричного типу (МТ) [1-3]. Необхідність виконання КП над великорозмірними багатовимірними ІО, зображеннями (З) також потребує не лише матрично-алгебраїчних моделей (МАМ) КП, але і секретних матричних ключів (МК) [4, 5].

Аналіз останніх досліджень і публікацій. У роботах [1-3] були показані переваги МАМ МТ КП З та узагальнених матричних афінних і афінно-перестановочних шифрів (МАПШ), МАМ RSA, модифікації яких дозволили створити покращені електронні цифрові підписи (ЕЦП), сліпі ЕЦП [1], блокові параметричні багатофункціональні та багатосторінкові моделі КП з перевіркою цілісності криптограм [2-5]. Поява таких МАМ спричинила необхідність створення і відповідних МК. Стосовно МК 1-ого типу у вигляді випадкового (шумового) З, який був позначений нами як МК_З (від «зображення»), то нами ще в 2008р. було запропоновано узагальнення протоколу Діффі-Хелмана на матричний випадок і метод формування МК_З. Удосконаленню таких матричних протоколів за рахунок застосування покращених методів організації прискорених обчислень на основі паралельної матричної логіки присвячені роботи [3, 4], в яких були підтверджені низкою експериментів переваги багатокрокових, багатоступеневих протоколів узгодження секретного МК_З. Для МАПШ необхідно мати МК і 2-го типу, а саме, набір бінарних матриць перестановок [1-4], позначимо тут їх як МК_П.

Питання щодо їх формувань і застосувань частково розглядались в [1-3], і лише в [5] запропоновано протокол узгодження МК типу МК_П.

Проте в ній не розглядались протоколи для випадків узгодження МК_П спільного для учасників групи, що бажає створити свій кооперативний груповий МК**.** На відміну від протоколів з [3, 4], у [6] був розглянутий, так званий авторами, кооперативний протокол, але стосовно МК_З. Тому **метою роботи** є розробка, моделювання та дослідження криптографічного кооперативного протоколу узгодження ізоморфно представленого спільного секретного МК_П для МАМ КП.

Виклад основних результатів. Моделювання протоколу для випадку піднесення МК_П у випадкові, відомі лише сторонам обміну, степені, показано на рис.1. Навіть знання МК_П – основи при значній потужності множини перестановок (N!, де N - розмірність МК_П) не дає можливості без перехоплення обох створених сторонами МК_П взнати ключ. Результати моделювання кооперативного протоколу для випадку трьох сторін показані на рис. 2-4. Протокол виконується так.

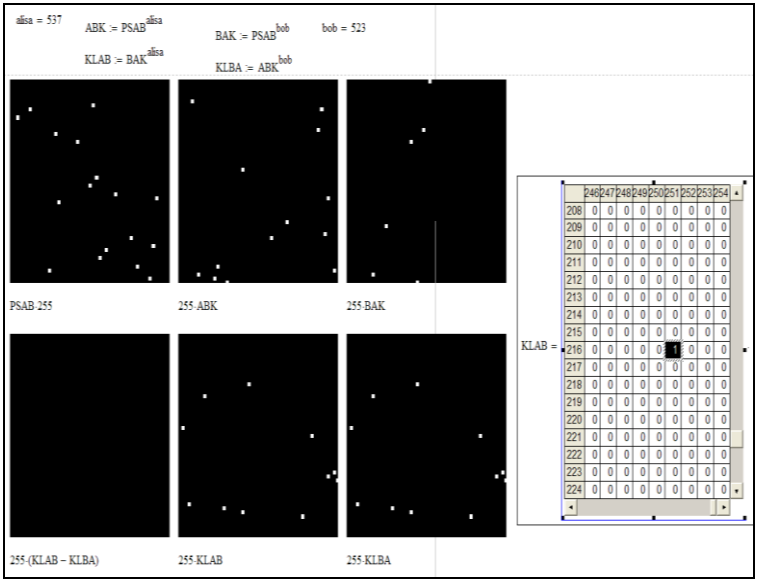


Рис. 1 – *Фрагмент вікна Mathcad з верифікацією модифікації протоколу Діффі-Хелмана для випадку піднесення у степені (537 та 523) МК_П, як основи. Вигляд основи (матриця PSAB 256*256), проміжних МК_П (ABK, BAK), що ними обмінюються сторони, та утворених ключів (KLAB, KLBA), які однакові*

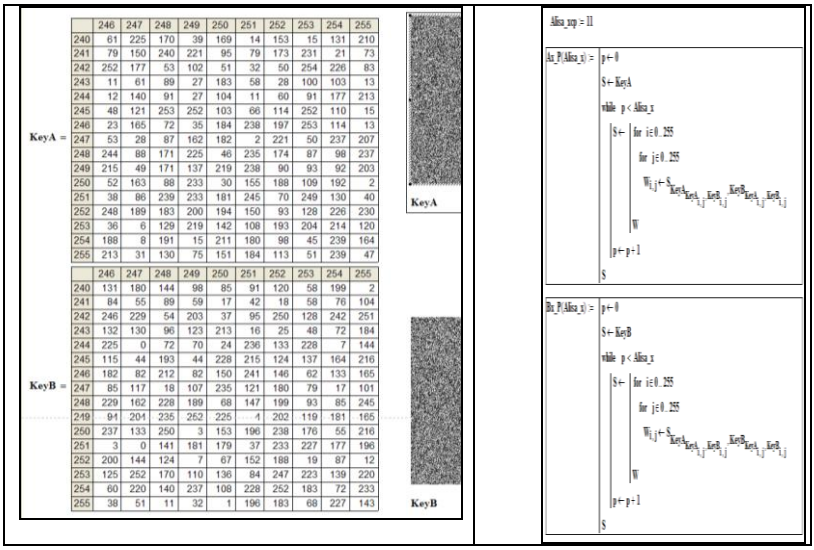


Рис. 2 – *Вікно Mathcad з вибраною МК_П значної розмірності, ізоморфно представленою її складовими (KeyA, KeyB) у цифровому та візуальному вигляді, (ліворуч) та програмним модулем для багаторазових перестановок (праворуч)*

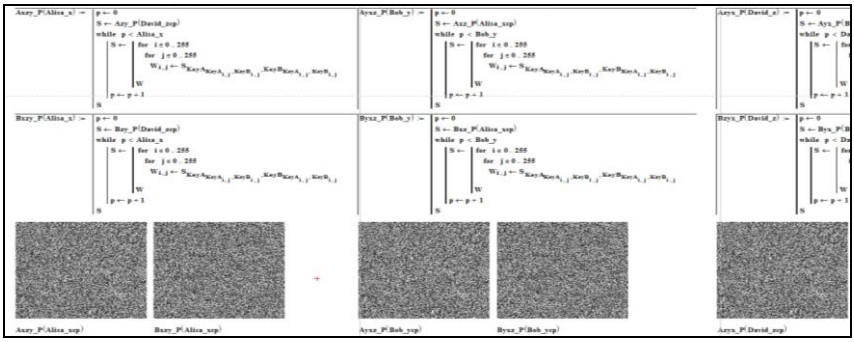


Рис. 3 – *Вид інтерфейсу Mathcad з процедурами утворення секретного МК_П трьома сторонами (Alisa, Bob, David): модулі для перестановок, вигляд ключів*

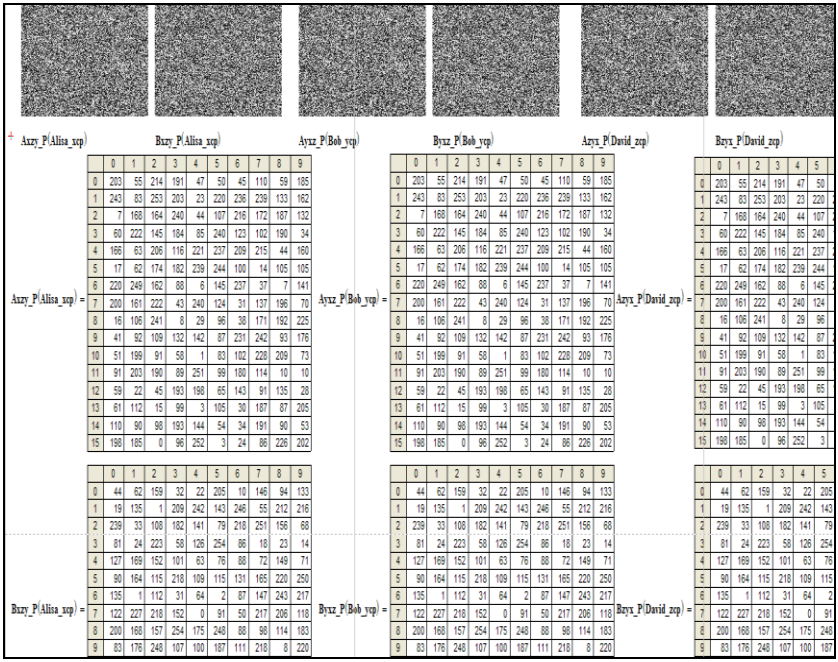


Рис. 4 – *Вид інтерфейсу Mathcad з утвореними трьома сторонами рівними секретними ключами МК_П у вигляді їх ізоморфних двох складових*

Кожна з сторін x, y, z (Alisa, Bob, David) вибирають за основу спільну МК_П, ізоморфно представлену її складовими (KeyA, KeyB) та шлях послідовних передач між собою утворених на кожному кроці ними проміжних МК_П, що утворюються як степені основи в залежності від вибраних таємних ідентифікаторів-чисел: Alisa_x, Bob_y, David_z за допомогою модуля перестановок, що на рис.2.

Утворені МК_П (дві матриці по 256*256 байтів сторони передають сусідам по шляху, а потім підносять отримані МК знову у свої степені, дивись рис.3-4.

Результатом є тотожні ключі, таємний МК_П, рівність якого очевидна (рис.4), забезпечена для всіх n сторін без знання їх ідентифікаторів.

Література

1. Красиленко В. Г. Матричні афінно-перестановочні алгоритми для шифрування та дешифрування зображень / В. Г. Красиленко, С. К. Грабовляк // Системи обробки інформації, 2012. – Вип. 3(2) . – С. 53-61. – Режим доступу: http://nbuv.gov.ua/UJRN/soi_2012_2_3_15

2. Красиленко В.Г. Моделювання та дослідження криптографічних перетворень зображень на основі їхньої матрично-бітовозрізової декомпозиції та матричних моделей перестановок з верифікацією цілісності / В.Г. Красиленко, Д.В. Нікітович // Електроніка та інформаційні технології. – Львів: ЛНУ, 2016. – Вип. 6. – С 111-127. – Режим доступу: http://elit.lnu.edu.ua/pdf/6_12.pdf

3. Красиленко В.Г. Моделювання протоколів узгодження секретного матричного ключа для криптографічних перетворень та систем матричного типу / В.Г. Красиленко, Д.В. Нікітович // Системи обробки інформації, 2017. – Вип. 3 (149). – С 151-157.

4.Красиленко В. Г. Моделювання багатокрокових та багатоступеневих протоколів узгодження секретних матричних ключів / В. Г. Красиленко, Д. В. Нікітович // Комп'ютерно-інтегровані технології: освіта, наука, виробництво, 2017. – № 26. – С. 111-120.

5. Красиленко В.Г. Протоколи узгодження секретних ключів у вигляді матричних перестановок значної розмірності для криптографічних перетворень / В.Г. Красиленко, Д.В. Нікітович // Тези доповідей XI МНТК «ІКТ – 2020», м. Житомир, 9-11 квітня 2020 р., 2020. – С. 39-49.

6. Красиленко В.Г. Кооперативний протокол узгодження спільного секретного матричного ключа // В.Г. Красиленко, Д.В. Нікітович // Матеріали VII МНПК (ІУСТ), 17 – 18 вересня 2018 р., Одеса / ОНПУ; ред. кол: В.В. Вичужанін. – Одеса, 2018. – С. 122–127.

УДК 004.42

АЛГОРИТМ АВТОМАТИЧЕСКОГО РАСПОЗНАВАНИЯ ОБЪЕКТОВ НА МОРСКОЙ ИЛИ РЕЧНОЙ ГЛАДИ

Шипунов И.С.[0000-0002-3864-9716], Ильина А.А.
E-mail: mr-shis@yandex.ru

ALGORITHM FOR AUTOMATIC RECOGNITION OF OBJECTS ON THE SEA OR RIVER SURFACE

Shipunov I.S., Ilina A.A.

Аннотация. Рассматривается алгоритм автоматического распознавания объектов на морской или речной глади, который возможно применить на безэкипажных судах.

Ключевые слова: *техническое зрение, безэкипажное судоходство, детектор Кэнни.*