Міністерство освіти і науки, молоді та спорту України
Вінницький національний технічний університет
Харківський національний економічний університет
Об'єднаний інститут проблем інформатики НАН Білорусі
Азербайджанська державна нафтова академія
Бєлгородський державний університет, Росія
Гірничо-металургійна академія AGH, Польща
Новий університет Лісабона, Португалія
Університет ЛІОН 2 ім. Люм'єра, Франція
Інститут інженерів з електротехніки та електроніки (IEEE), Українська секція

Тези доповідей Тертьої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації»

м. Вінниця, Україна
20-22 квітня 2011 року

Тезисы докладов Третьей Международной научно-практической конференции «Методы и средства кодирования, защиты и сжатия информации»

г. Винница, Украина
20-22 апреля 2011 года

ВНТУ 2011

УДК 004+681.3+621.3
М54

Відповідальний редактор В. А. Лужецький

Матеріали статей опубліковані в авторській редакції

Методи та засоби кодування, захисту й ущільнення
М54 інформації. Тези доповідей Третьої Міжнародної науково-практичної конференції. м. Вінниця, 20-22 квітня 2011 року. – Вінниця: ВНТУ, 2011. – 231 с.
ISBN 978-966-641-406-2

Збірка містить матеріали доповідей третьої Міжнародної науково-практичної конференції з сучасних проблем кодування, захисту й ущільнення інформації за п'ятьма основними напрямками: методи та засоби кодування інформації; методи та засоби криптографічного захисту інформації; інформаційна безпека комп'ютерних систем; методи та засоби ущільнення інформації; методи та засоби перетворення форм інформації.

УДК 004+681.3+621.3

ISBN 978-966-641-406-2

УДК 681.3.06

ДОСЛІДЖЕННЯ СТРУКТУРИ ДАНИХ ДЕКАРТОВЕ ДЕРЕВО

В. А. Лужецький, д.т.н., професор;
О. С. Стах, студент
Вінницький національний технічний університет

Важливість структур даних важко переоцінити. Адже правильно організоване зберігання даних в пам'яті дає змогу значно пришвидшити роботу програм. Виходячи з цих міркувань можна зробити висновок, що використання структур даних для захисту інформації є актуальною задачею.

Існує досить багато структур даних, які можна поділити на 2 основні групи: лінійні (стек, масив), нелінійні (логарифмічні: куча, дерево).

Перевагою лінійних структур даних є можливість виконання деяких операцій зі складністю $O(1)$ (наприклад, індексація для масиву). Проте деякі операції виконуватимуться зі складністю $O(n)$ (видалення елементу).

Логарифмічні структури забезпечують зменшення складності при виконанні певних операцій над даними, хоча не кожна з них може бути виконана на логарифмічних структурах.

Наприклад, при реалізації бінарного дерева пошуку чи кучі не можна швидко знайти суму на підмасиві даних чи розвернути частину масиву. Також проблемою подібних структур є можливе розбалансування, при якому висота структури може стати лінійною. В такому випадку зручно використовувати декартове дерево. Це вид бінарного дерева, вузол якого, крім посилань на ліве та

праве піддерева містить два ключі – x (ключ) та y (пріоритет). По x – це двійкове дерево пошуку, по y – двійкова куча. Така організація дозволяє виконувати дві основні операції – поділ дерева по ключу та злиття двох дерев – зі складністю $O(\log_2 n)$, де n – висота дерева. Будь-які операції над деревом зводяться до двох даних операцій. Єдина умова, що накладається на злиття дерев – ключі лівого дерева повинні бути меншими за ключі правого дерева. Тому різновидом декартового дерева є дерево по неявному ключу – аналог масиву чисел. Тобто при злитті двох дерев ми передаємо їх як параметри в такому порядку, в якому нам потрібно їх розташування у вихідному масиві. Пріоритети (y) використовуються лише для балансування декартового дерева та задаються випадковим чином.

У доповіді розглядається такий алгоритм захисту даних.

1. Розбиття повідомлення на n блоків, нумерація їх у природному порядку.
2. Завдання n пріоритетів у випадковому порядку.
3. Побудова декартового дерева розмірності n по пріоритетам та заданим блокам даних.
4. Генерування індексів [st; fin] за допомогою генератора псевдовипадкових чисел.
5. Виконання інверсії даних на підвідрізку [st; fin]
6. Виконання п. 2-5 задану кількість разів, яка забезпечує необхідну стійкість шифрування.
7. Перебудування повідомлення згідно з результуючої нумерацією блоків.
8. Накладання на дані гами для виключення можливості здійснення атаки нав’язуванням тексту.

Таким чином ми добились захищеності даних.