РЕФЕРАТ

Дипломну роботу виконано на 56 аркушах, вона містить 2 додатки та перелік посилань на використані джерела з 29 найменувань. У роботі наведено 6 рисунків та 3 таблиці. Метою даної дипломної роботи є виконання алгоритмів дискретного логарифмування для мультиплікативних груп простих полів GF(p) у хмарній моделі обчислень та оцінка дійсного розміру проблеми, яку можливо розв’язати з їх використанням за певний період часу та матеріальних витрат на цей розв’язок. Об’єктом дослідження є проблема дискретного логарифму у скінченних полях виду GF(p) . Предметом дослідження є процес виконання конкретних алгоритмів дискретного логарифмування у заданих полях на хмарних платформах. Проведено аналіз існуючих рішень проблеми дискретного логарифму, виконано їх порівняння з погляду швидкодії та легкості реалізації для паралельної моделі. Також проведено огляд існуючих систем хмарних обчислень та обрано ту, що дозволяє точніший контроль за загальною обчислювальною потужністю системи вузлів, з меншою ціною за рівних інших показниках. Був реалізований обраний алгоритм у паралельній моделі та проведено його виконання на обраній платформі. З результатів виконання зроблено аналіз оптимальних параметрів алгоритму та орієнтовного розміру модуля, розв’язок проблеми дискретного логарифму для якого можна отримати за календарний рік. Результати роботи можуть бути використані для оцінки вартості атаки на популярні асиметричні криптосистеми.

ДИСКРЕТНИЙ ЛОГАРИФМ, INDEX-CALCULUS, ПАРАЛЕЛЬНІ ОБЧИСЛЕННЯ, ХМАРНІ СИСТЕМИ