Завдання: для дослідження пропонуються дві багатомірні булеві функції: f (x) = x ^ N mod p(x) та g(x) = x ^ M mod p(x), де x – елемент простору GF(2^n) , N та M – задані натуральні числа, а всі обчислення виконуються у полі GF(2^n), побудованому за допомогою полінома-генератора p(x) . Відповідно, обидва досліджувані перетворення є (n,n) -булевими функціями.

Згідно варіанту, n = 17, N = 131070, M = 131069.

В якості полінома-генератора використовується такий поліном: p(x) = x ^ 17 + x ^ 3 + 1.

Для функцій f (x) та g(x) було визначено криптографічні властивості, що занесені до таблиці. Оскільки результати виявились однаковими, то результати занесено до однієї таблиці.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Результати обчислень для f(x) та g(x) | | | | |
| № координатної функції | Дисбаланс | Нелінійність | Алгебраїчний степінь | Рівень кореляційного імунітету |
| 1 | 0 | 65174 | 16 | 0 |
| 2 | 0 | 65174 | 16 | 0 |
| 3 | 0 | 65174 | 16 | 0 |
| 4 | 0 | 65174 | 16 | 0 |
| 5 | 0 | 65174 | 16 | 0 |
| 6 | 0 | 65174 | 16 | 0 |
| 7 | 0 | 65174 | 16 | 0 |
| 8 | 0 | 65174 | 16 | 0 |
| 9 | 0 | 65174 | 16 | 0 |
| 10 | 0 | 65174 | 16 | 0 |
| 11 | 0 | 65174 | 16 | 0 |
| 12 | 0 | 65174 | 16 | 0 |
| 13 | 0 | 65174 | 16 | 0 |
| 14 | 0 | 65174 | 16 | 0 |
| 15 | 0 | 65174 | 16 | 0 |
| 16 | 0 | 65174 | 16 | 0 |
| 17 | 0 | 65174 | 16 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Таблиця коефіцієнтів розповсюдження помилок координатних функцій по кожній змінній для f(x) | | | | | | | | | | | | | | | | | |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| **F[1]:** | 65344 | 65456 | 65364 | 65584 | 65384 | 65288 | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 |
| **F[2]:** | 65456 | 65364 | 65584 | 65384 | 65288 | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 | 65792 |
| **F[3]:** | 65364 | 65584 | 65384 | 65288 | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 | 65792 | 65312 |
| **F[4]:** | 65584 | 65384 | 65288 | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 | 65792 | 65312 | 65792 |
| **F[5]:** | 65384 | 65288 | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 | 65792 | 65312 | 65792 | 65216 |
| **F[6]:** | 65288 | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 | 65792 | 65312 | 65792 | 65216 | 65312 |
| **F[7]:** | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 | 65792 | 65312 | 65792 | 65216 | 65312 | 65236 |
| **F[8]:** | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 | 65792 | 65312 | 65792 | 65216 | 65312 | 65236 | 65792 |
| **F[9]:** | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 | 65792 | 65312 | 65792 | 65216 | 65312 | 65236 | 65792 | 65600 |
| **F[10]:** | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 | 65792 | 65312 | 65792 | 65216 | 65312 | 65236 | 65792 | 65600 | 65216 |
| **F[11]:** | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 | 65792 | 65312 | 65792 | 65216 | 65312 | 65236 | 65792 | 65600 | 65216 | 65792 |
| **F[12]:** | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 | 65792 | 65312 | 65792 | 65216 | 65312 | 65236 | 65792 | 65600 | 65216 | 65792 | 65312 |
| **F[13]:** | 65584 | 65504 | 65504 | 65588 | 65792 | 65792 | 65312 | 65792 | 65216 | 65312 | 65236 | 65792 | 65600 | 65216 | 65792 | 65312 | 65552 |
| **F[14]:** | 65504 | 65504 | 65588 | 65792 | 65792 | 65312 | 65792 | 65216 | 65312 | 65236 | 65792 | 65600 | 65216 | 65792 | 65312 | 65552 | 65236 |
| **F[15]:** | 65712 | 65388 | 65504 | 65344 | 65456 | 65364 | 65584 | 65384 | 65288 | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 |
| **F[16]:** | 65388 | 65504 | 65344 | 65456 | 65364 | 65584 | 65384 | 65288 | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 |
| **F[17]:** | 65504 | 65344 | 65456 | 65364 | 65584 | 65384 | 65288 | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 |
| Таблиця відносного відхилення коефіцієнтів розповсюдження помилок координатних функцій по кожній змінній для f(x) | | | | | | | | | | | | | | | | | |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| **F[1]:** | 0,293 | 0,122 | 0,262 | 0,073 | 0,232 | 0,378 | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 |
| **F[2]:** | 0,122 | 0,262 | 0,073 | 0,232 | 0,378 | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 |
| **F[3]:** | 0,262 | 0,073 | 0,232 | 0,378 | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 | 0,342 |
| **F[4]:** | 0,073 | 0,232 | 0,378 | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 | 0,342 | 0,391 |
| **F[5]:** | 0,232 | 0,378 | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 | 0,342 | 0,391 | 0,488 |
| **F[6]:** | 0,378 | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 | 0,342 | 0,391 | 0,488 | 0,342 |
| **F[7]:** | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 | 0,342 | 0,391 | 0,488 | 0,342 | 0,458 |
| **F[8]:** | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 | 0,342 | 0,391 | 0,488 | 0,342 | 0,458 | 0,391 |
| **F[9]:** | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 | 0,342 | 0,391 | 0,488 | 0,342 | 0,458 | 0,391 | 0,098 |
| **F[10]:** | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 | 0,342 | 0,391 | 0,488 | 0,342 | 0,458 | 0,391 | 0,098 | 0,488 |
| **F[11]:** | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 | 0,342 | 0,391 | 0,488 | 0,342 | 0,458 | 0,391 | 0,098 | 0,488 | 0,391 |
| **F[12]:** | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 | 0,342 | 0,391 | 0,488 | 0,342 | 0,458 | 0,391 | 0,098 | 0,488 | 0,391 | 0,342 |
| **F[13]:** | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 | 0,342 | 0,391 | 0,488 | 0,342 | 0,458 | 0,391 | 0,098 | 0,488 | 0,391 | 0,342 | 0,024 |
| **F[14]:** | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 | 0,342 | 0,391 | 0,488 | 0,342 | 0,458 | 0,391 | 0,098 | 0,488 | 0,391 | 0,342 | 0,024 | 0,458 |
| **F[15]:** | 0,269 | 0,226 | 0,049 | 0,293 | 0,122 | 0,262 | 0,073 | 0,232 | 0,378 | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 |
| **F[16]:** | 0,226 | 0,049 | 0,293 | 0,122 | 0,262 | 0,073 | 0,232 | 0,378 | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 |
| **F[17]:** | 0,049 | 0,293 | 0,122 | 0,262 | 0,073 | 0,232 | 0,378 | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Таблиця коефіцієнтів розповсюдження помилок координатних функцій по кожній змінній для g(x) | | | | | | | | | | | | | | | | | |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| **F[1]:** | 65564 | 65860 | 65724 | 65780 | 65528 | 65680 | 65804 | 65388 | 65344 | 65364 | 65384 | 65712 | 65456 | 65288 | 65584 | 65504 | 65792 |
| **F[2]:** | 65344 | 65456 | 65364 | 65584 | 65384 | 65288 | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 |
| **F[3]:** | 65860 | 65724 | 65780 | 65528 | 65680 | 65804 | 65388 | 65344 | 65364 | 65384 | 65712 | 65456 | 65288 | 65584 | 65504 | 65792 | 65312 |
| **F[4]:** | 65456 | 65364 | 65584 | 65384 | 65288 | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 | 65792 |
| **F[5]:** | 65724 | 65780 | 65528 | 65680 | 65804 | 65388 | 65344 | 65364 | 65384 | 65712 | 65456 | 65288 | 65584 | 65504 | 65792 | 65312 | 65216 |
| **F[6]:** | 65364 | 65584 | 65384 | 65288 | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 | 65792 | 65312 |
| **F[7]:** | 65780 | 65528 | 65680 | 65804 | 65388 | 65344 | 65364 | 65384 | 65712 | 65456 | 65288 | 65584 | 65504 | 65792 | 65312 | 65216 | 65236 |
| **F[8]:** | 65584 | 65384 | 65288 | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 | 65792 | 65312 | 65792 |
| **F[9]:** | 65528 | 65680 | 65804 | 65388 | 65344 | 65364 | 65384 | 65712 | 65456 | 65288 | 65584 | 65504 | 65792 | 65312 | 65216 | 65236 | 65600 |
| **F[10]:** | 65384 | 65288 | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 | 65792 | 65312 | 65792 | 65216 |
| **F[11]:** | 65680 | 65804 | 65388 | 65344 | 65364 | 65384 | 65712 | 65456 | 65288 | 65584 | 65504 | 65792 | 65312 | 65216 | 65236 | 65600 | 65792 |
| **F[12]:** | 65288 | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 | 65792 | 65312 | 65792 | 65216 | 65312 |
| **F[13]:** | 65804 | 65388 | 65344 | 65364 | 65384 | 65712 | 65456 | 65288 | 65584 | 65504 | 65792 | 65312 | 65216 | 65236 | 65600 | 65792 | 65552 |
| **F[14]:** | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 | 65792 | 65792 | 65312 | 65792 | 65216 | 65312 | 65236 |
| **F[15]:** | 65388 | 65504 | 65344 | 65456 | 65364 | 65584 | 65384 | 65288 | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 |
| **F[16]:** | 65644 | 65564 | 65860 | 65724 | 65780 | 65528 | 65680 | 65804 | 65388 | 65344 | 65364 | 65384 | 65712 | 65456 | 65288 | 65584 | 65504 |
| **F[17]:** | 65504 | 65344 | 65456 | 65364 | 65584 | 65384 | 65288 | 65712 | 65504 | 65456 | 65584 | 65288 | 65504 | 65584 | 65504 | 65504 | 65588 |
| Таблиця відносного відхилення коефіцієнтів розповсюдження помилок координатних функцій по кожній змінній для g(x) | | | | | | | | | | | | | | | | | |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| **F[1]:** | 0,043 | 0,494 | 0,287 | 0,372 | 0,012 | 0,22 | 0,409 | 0,226 | 0,293 | 0,262 | 0,232 | 0,269 | 0,122 | 0,378 | 0,073 | 0,049 | 0,391 |
| **F[2]:** | 0,293 | 0,122 | 0,262 | 0,073 | 0,232 | 0,378 | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 |
| **F[3]:** | 0,494 | 0,287 | 0,372 | 0,012 | 0,22 | 0,409 | 0,226 | 0,293 | 0,262 | 0,232 | 0,269 | 0,122 | 0,378 | 0,073 | 0,049 | 0,391 | 0,342 |
| **F[4]:** | 0,122 | 0,262 | 0,073 | 0,232 | 0,378 | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 |
| **F[5]:** | 0,287 | 0,372 | 0,012 | 0,22 | 0,409 | 0,226 | 0,293 | 0,262 | 0,232 | 0,269 | 0,122 | 0,378 | 0,073 | 0,049 | 0,391 | 0,342 | 0,488 |
| **F[6]:** | 0,262 | 0,073 | 0,232 | 0,378 | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 | 0,342 |
| **F[7]:** | 0,372 | 0,012 | 0,22 | 0,409 | 0,226 | 0,293 | 0,262 | 0,232 | 0,269 | 0,122 | 0,378 | 0,073 | 0,049 | 0,391 | 0,342 | 0,488 | 0,458 |
| **F[8]:** | 0,073 | 0,232 | 0,378 | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 | 0,342 | 0,391 |
| **F[9]:** | 0,012 | 0,22 | 0,409 | 0,226 | 0,293 | 0,262 | 0,232 | 0,269 | 0,122 | 0,378 | 0,073 | 0,049 | 0,391 | 0,342 | 0,488 | 0,458 | 0,098 |
| **F[10]:** | 0,232 | 0,378 | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 | 0,342 | 0,391 | 0,488 |
| **F[11]:** | 0,22 | 0,409 | 0,226 | 0,293 | 0,262 | 0,232 | 0,269 | 0,122 | 0,378 | 0,073 | 0,049 | 0,391 | 0,342 | 0,488 | 0,458 | 0,098 | 0,391 |
| **F[12]:** | 0,378 | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 | 0,342 | 0,391 | 0,488 | 0,342 |
| **F[13]:** | 0,409 | 0,226 | 0,293 | 0,262 | 0,232 | 0,269 | 0,122 | 0,378 | 0,073 | 0,049 | 0,391 | 0,342 | 0,488 | 0,458 | 0,098 | 0,391 | 0,024 |
| **F[14]:** | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 | 0,391 | 0,391 | 0,342 | 0,391 | 0,488 | 0,342 | 0,458 |
| **F[15]:** | 0,226 | 0,049 | 0,293 | 0,122 | 0,262 | 0,073 | 0,232 | 0,378 | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 |
| **F[16]:** | 0,165 | 0,043 | 0,494 | 0,287 | 0,372 | 0,012 | 0,22 | 0,409 | 0,226 | 0,293 | 0,262 | 0,232 | 0,269 | 0,122 | 0,378 | 0,073 | 0,049 |
| **F[17]:** | 0,049 | 0,293 | 0,122 | 0,262 | 0,073 | 0,232 | 0,378 | 0,269 | 0,049 | 0,122 | 0,073 | 0,378 | 0,049 | 0,073 | 0,049 | 0,049 | 0,079 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № координатної функції | Коефіцієнти розповсюдження помилок по кожній змінній для | Відносне відхилення коефіцієнтів розповсюдження помилок по кожній змінній для , % | Коефіцієнти розповсюдження помилок по кожній змінній для | Відносне відхилення коефіцієнтів розповсюдження помилок по кожній змінній для , % |
| [1] | 1113160 | 0,085 | 1114608 | 0,045 |
| [2] | 1112952 | 0,104 | 1114468 | 0,032 |
| [3] | 1113152 | 0,086 | 1114200 | 0,008 |
| [4] | 1113440 | 0,06 | 1113944 | 0,015 |
| [5] | 1113888 | 0,02 | 1113436 | 0,061 |
| [6] | 1113744 | 0,033 | 1113508 | 0,054 |
| [7] | 1114172 | 0,005 | 1113436 | 0,061 |
| [8] | 1113804 | 0,028 | 1113164 | 0,085 |
| [9] | 1113732 | 0,034 | 1113160 | 0,085 |
| [10] | 1113680 | 0,039 | 1113152 | 0,086 |
| [11] | 1113760 | 0,032 | 1113888 | 0,02 |
| [12] | 1113856 | 0,023 | 1114172 | 0,005 |
| [13] | 1113616 | 0,045 | 1113732 | 0,034 |
| [14] | 1113824 | 0,026 | 1113760 | 0,032 |
| [15] | 1113848 | 0,024 | 1113616 | 0,045 |
| [16] | 1113896 | 0,019 | 1113848 | 0,024 |
| [17] | 1113548 | 0,051 | 1113548 | 0,051 |

ВИСНОВКИ