

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

«На правах рукопису»

УДК 003.26

«До захисту допущено»

Завідувач кафедри

_____ Сергій ЯКОВЛЄВ

«__» _____ 2025 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою

«Математичні методи криптографічного захисту інформації»

зі спеціальності: 113 Прикладна математика

на тему: **«Аналіз постквантових криптографічних примітивів сімейства $AJPS$ для шифрування та інкапсуляції ключів»**

Виконав:

студент IV курсу, групи ФІ-14

Дорошенко Юрій Олександрович _____

Керівник:

асистент, каф. ММЗІ

Ядуха Дарія Вікторівна _____

Рецензент:

ст.викл, каф. ІБ, к.ф.-м.н.

Рибак Олександр Владиславович _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»

Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

Рівень вищої освіти — перший (бакалаврський)
Спеціальність — 113 Прикладна математика,
ОПП «Математичні методи криптографічного захисту інформації»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Сергій ЯКОВЛЄВ

«__» _____ 2025 р.

ЗАВДАННЯ
на дипломну роботу

Студент: Дорошенко Юрій Олександрович

1. Тема роботи: *«Аналіз постквантових криптографічних примітивів сімейства $AJPS$ для шифрування та інкапсуляції ключів»*,
науковий керівник дисертації: асистент, каф. ММЗІ Ядуха Дарія Вікторівна,

затверджені наказом по університету №__ від «__» _____ 2025 р.

2. Термін подання студентом роботи: «__» _____ 2025 р.

3. Об'єкт дослідження: *інформаційні процеси в системах криптографічного захисту*

4. Предмет дослідження: *статистичні властивості криптосистем сімейства $AJPS$, побудованих на арифметиці за модулем чисел Мерсенна та їх узагальнень*

5. Перелік завдань:

1) *провести огляд сучасного стану постквантової криптографії та математичних задач, що лежать в її основі;*

2) *описати математичну структуру криптосистем $AJPS-1$, $AJPS-2$ та $AJPS-KEM$ і сформулювати їх формальні моделі;*

3) реалізувати модифікації криптосистем із використанням чисел Кренделла та узагальнених чисел Мерсенна як модуля;

4) провести емпіричне тестування псевдовипадковості відкритих ключів і шифротекстів за допомогою пакету тестів NIST SP 800-22;

5) проаналізувати та порівняти результати для всіх реалізованих варіантів криптосистем.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу:
Презентація доповіді

7. Орієнтовний перелік публікацій: *XXIII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (14-17 травня 2025 року, м. Київ, Україна), III Всеукраїнська науково-практична конференція «Theoretical and applied cybersecurity» (29 травня 2025 року, м. Київ, Україна).*

8. Дата видачі завдання: 10 вересня 2024 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	01–15 вересня 2024 р.	Виконано
2	Огляд опублікованих джерел за тематикою дослідження	Вересень 2024 р.	Виконано
3	Формалізація математичної моделі AJPS-1, AJPS-2 та AJPS-КЕМ	Жовтень 2024 р.	Виконано
4	Реалізація оригінальних криптосистем на основі чисел Мерсенна	Листопад 2024 р.	Виконано
5	Розробка та реалізація модифікацій AJPS	Січень 2025 р.	Виконано
6	Пошук простих модулів відповідно до заданих параметрів	Лютий 2025 р.	Виконано
7	Побудова та аналіз тестових даних	Березень 2025 р.	Виконано
8	Аналіз та порівняння отриманих результатів, оформлення таблиць, висновків	Квітень 2025 р.	Виконано
9	Оформлення дипломної роботи	Травень 2025 р.	Виконано

Студент _____ Юрій ДОРОШЕНКО

Керівник _____ Дарія ЯДУХА

РЕФЕРАТ

Кваліфікаційна робота містить: 90 стор., 49 таблиць, 23 джерела.

У цій роботі проведено дослідження постквантових криптографічних примітивів сімейства AJPS, побудованих на основі арифметики за модулем чисел Мерсенна. Розглянуто три криптосистеми: побітову схему шифрування AJPS-1, поблокову схему шифрування AJPS-2 та механізм інкапсуляції ключів AJPS-КЕМ. Наведено формальний опис кожної з криптосистем, а також реалізовано їх модифікації з використанням альтернативних класів модулів — зокрема, узагальнених чисел Мерсенна та чисел Кренделла.

У рамках дослідження здійснено порівняльний аналіз псевдовипадковості відкритих ключів та шифротекстів для криптосистем AJPS-1 та AJPS-2 та їх модифікацій. А також проаналізовано шифротексти, отримані в результаті інкапсуляції ключа в AJPS-КЕМ та її модифікованих версіях. Для оцінювання якості випадковості застосовано стандартний набір тестів NIST SP 800-22.

Отримані результати свідчать про те, що використання узагальнених чисел Мерсенна та чисел Кренделла як модулів криптосистем сімейства AJPS є обґрунтованим: модифіковані версії криптосистем демонструють як мінімум не гірші, а в багатьох випадках — кращі показники випадковості, що є критичним для забезпечення криптографічної стійкості.

**КРИПТОСИСТЕМА AJPS, ПОСТКВАНТОВА КРИПТОГРАФІЯ,
ЧИСЛА МЕРСЕННА, УЗАГАЛЬНЕНІ ЧИСЛА МЕРСЕННА, ЧИСЛА
КРЕНДЕЛЛА**

ABSTRACT

This work presents a study of post-quantum cryptographic primitives from the AJPS family, which are based on arithmetic modulo Mersenne numbers. Three cryptosystems are examined: the bitwise encryption scheme AJPS-1, the block encryption scheme AJPS-2, and the key encapsulation mechanism AJPS-KEM. A formal description of each system is provided, along with modified implementations using alternative classes of moduli — specifically, generalized Mersenne numbers and Crandall numbers.

The study includes a comparative analysis of the pseudorandomness of public keys and ciphertexts for AJPS-1 and AJPS-2 and their modifications. Additionally, ciphertexts obtained through key encapsulation in AJPS-KEM and its modified versions were analyzed. To evaluate the quality of randomness, the standard NIST SP 800-22 test suite was used.

The results confirm that using generalized Mersenne numbers and Crandall numbers as modules in AJPS-family cryptosystems is well justified: the modified systems demonstrate equal or, in many cases, superior randomness properties — a critical aspect of cryptographic security.

AJPS CRYPTOSYSTEM, POST-QUANTUM CRYPTOGRAPHY,
MERSENNE NUMBERS, GENERALIZED MERSENNE NUMBERS,
CRANDALL NUMBERS

ЗМІСТ

Перелік умовних позначень, скорочень і термінів	9
Вступ.....	10
1 Постквантова криптографія	14
1.1 Конкурс постквантових криптопримітивів NIST.....	14
1.2 Числа Мерсенна.....	17
1.2.1 Історія чисел Мерсенна	17
1.2.2 Числа Мерсенна в криптографії	19
1.2.3 Ефективні методи обчислення на числах Мерсенна.....	20
1.2.4 Алгебраїчні узагальнення чисел Мерсенна для криптосистем.....	22
1.3 Опис криптосистеми AJPS.....	23
1.3.1 Визначення семантичної стійкості криптосистеми.....	23
1.3.2 Побітове шифрування AJPS-1	25
1.3.3 Блокове шифрування AJPS-2	26
1.3.4 Криптоаналіз схем шифрування сімейства AJPS	28
1.3.5 Механізм інкапсуляції ключів AJPS-КЕМ.....	30
1.3.6 Код корекції помилок	31
1.4 Інші криптосистеми з використанням обчислень за модулем числа Мерсенна	33
1.5 Набір статистичних тестів NIST SP 800-22	33
Висновки до розділу 1.....	36
2 Аналіз модифікацій криптосистем сімейства AJPS	37
2.1 Модифікації криптосистем сімейства AJPS.....	37
2.1.1 AJPS-1 з використанням альтернативних модулів.....	38
2.1.2 AJPS-2 з використанням альтернативних модулів.....	40
2.1.3 AJPS-КЕМ з використанням альтернативних модулів.....	42
2.1.4 Пошук параметрів для побудови модифікацій	43
2.2 Результати тестів NIST SP 800-22.....	45
2.2.1 Тести псевдовипадковості AJPS-1	45

2.2.2 Тести псевдовипадковості AJPS-2	53 ⁸
2.2.3 Тести псевдовипадковості шифротекстів AJPS-2	57
2.2.4 Тести псевдовипадковості шифротекстів AJPS-КЕМ	62
Висновки до розділу 2	68
Висновки	70
Перелік посилань	72
Додаток А Великі рисунки та таблиці	75
А.1 Тести псевдовипадковості шифротекстів AJPS-2.....	75
А.2 Тести псевдовипадковості шифротекстів AJPS-КЕМ	75

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

\oplus — операція побітового додавання;

M_n — число Мерсенна вигляду $2^n - 1$, де $n \in \mathbb{N}$;

$M_{n,c}$ — число Кренделла вигляду $2^n - c$, де n та c — додатні цілі числа та $\log_2 c \leq \frac{n}{2}$;

$M_{n,m}$ — узагальнене число Мерсенна вигляду $2^n - 2^m - 1$, де n, m — додатні цілі числа та $m < n$;

$Ham(x)$ — вага Геммінга числа x , тобто кількість одиниць у бітовому представленні числа x ;

P-value (значення p) — це ймовірність того, що для істинно випадкової послідовності результат тесту є таким ж, як для досліджуваної послідовності.

ВСТУП

Актуальність дослідження. Забезпечення конфіденційності, цілісності та доступності інформації є одним із ключових завдань сучасної інформаційної безпеки. Впродовж історії криптографія еволюціонувала від простих симетричних шифрів, застосовуваних ще за воєнних часів для захисту військової комунікації – починаючи з приблизно 1900 року до н.е. у Стародавньому Єгипті та продовжуючи античними методами, як-от шифр Цезаря (I століття до н.е.), – до складних асиметричних криптосистем, що використовуються в глобальних цифрових інфраструктурах сучасного світу. Особливо інтенсивний розвиток криптографії спостерігався у XX столітті, зокрема під час Першої (1914–1918) та Другої світових воєн (1939–1945), що ознаменувались використанням механізованих шифрувальних пристроїв (наприклад, машини *Enigma*). У кінці XX та на початку XXI століття на перший план вийшли асиметричні методи та постквантові підходи, які лежать в основі сучасних систем цифрової безпеки.

Класична асиметрична криптографія спирається на складні задачі з теорії чисел, які вважаються обчислювально нездійсненними в умовах класичної обчислювальної моделі. Серед найбільш відомих криптосистем можна виокремити:

- **RSA** [1], стійкість якого базується на задачі факторизації великих цілих чисел.
- **ElGamal** [2], побудований на складності задачі дискретного логарифмування у мультиплікативній групі скінченного поля.
- **Diffie–Hellman** [3], що дозволяє обмінюватися ключами за публічним каналом, також базується на задачі дискретного логарифмування.
- **ECDSA** та **ECDH** [4, 5], що є аналогами згаданих вище схем на еліптичних кривих і використовують складність дискретного

логарифмування в групах точок еліптичних кривих над скінченними полями.

Ці криптосистеми широко застосовуються в сучасній цифровій інфраструктурі: зокрема, у протоколах TLS/SSL, PGP, цифрових підписах, електронному голосуванні, блокчейнах тощо. Однак розвиток квантових обчислень створює загрозу їхній безпеці, оскільки існують квантові алгоритми, зокрема алгоритм Шора [6], які дозволяють зруйнувати математичні основи цих систем за поліноміальний час.

На той час запропонований алгоритм Шора розглядався радше як теоретична загроза. Проте за останні два десятиліття квантові технології здійснили суттєвий поступ: великі науково-дослідні установи та комерційні компанії активно інвестують у розробку масштабованих квантових комп'ютерів. І хоча наразі ще не побудовано квантового пристрою, здатного реалізувати повноцінну атаку на RSA або аналогічні схеми, більшість експертів сходяться на думці, що це питання не можливості, а лише часу та інженерного прогресу.

Історичний досвід свідчить, що повне впровадження криптографічних стандартів на практиці потребує щонайменше десятиліття. Враховуючи цю обставину, питання запровадження стійких до квантових атак рішень набуває критичного значення. Саме тому Національний інститут стандартів і технологій США (NIST) ініціював процес стандартизації постквантових криптографічних алгоритмів [7], що здатні забезпечити захист навіть за використання квантових обчислювальних потужностей.

Отже, сучасні асиметричні криптосистеми перебувають під потенційною загрозою з боку квантових технологій. У цьому контексті постає нагальна потреба у створенні нових криптографічних схем, безпека яких базується на задачах, що залишаються складними як у класичній, так і у квантовій моделях обчислення. Дослідження таких систем, включаючи аналіз їхньої ефективності, криптостійкості та придатності до практичного застосування, є одним із найактуальніших

завдань сучасної криптографії.

Метою дослідження є аналіз криптографічних примітивів сімейства AJPS та побудова їх модифікацій задля збільшення їх захищеності.

Задача дослідження полягає у побудові, модифікації та аналізі криптосистем AJPS-1, AJPS-2 та AJPS-KEM з використанням альтернативних класів модулів і оцінюванні впливу цих змін на криптографічні властивості систем.

Для розв'язання поставленої задачі необхідно вирішити такі завдання:

- 1) провести огляд сучасного стану постквантової криптографії та математичних задач, що лежать в її основі;
- 2) описати математичну структуру криптосистем AJPS-1, AJPS-2 та AJPS-KEM і сформулювати їх формальні моделі;
- 3) реалізувати модифікації криптосистем із використанням чисел Кренделла та узагальнених чисел Мерсенна як модуля;
- 4) провести емпіричне тестування псевдовипадковості відкритих ключів і шифротекстів за допомогою пакету тестів NIST SP 800-22;
- 5) проаналізувати та порівняти результати для всіх реалізованих варіантів криптосистем.

Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту.

Предметом дослідження є статистичні властивості криптосистем сімейства AJPS, побудованих на арифметиці за модулем чисел Мерсенна та їх узагальнень.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: теорії ймовірностей, теорії кодування та методи комп'ютерного моделювання.

Наукова новизна отриманих результатів полягає у:

– вперше побудовано модифікації криптосистеми AJPS-KEM із використанням чисел Кренделла та узагальнених чисел Мерсенна як

модулів;

– вперше проведено комплексне тестування псевдовипадковості ключів та шифротекстів для криптосистем AJPS з різними модулями;

– встановлено доцільність використання альтернативних класів чисел, що дозволяє розширити простір параметрів і підвищити криптографічну гнучкість систем.

Практичне значення результатів полягає у можливості застосування модифікованих криптосистем AJPS у системах постквантового захисту інформації задля збільшення варіативності параметрів.

Апробація результатів та публікації. Результати цієї роботи були частково представлені на XXIII Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (14-17 травня 2025 року, м. Київ, Україна), а також на III Всеукраїнській науково-практичній конференції «Theoretical and applied cybersecurity» (29 травня 2025 року, м. Київ, Україна).

1 ПОСТКВАНТОВА КРИПТОГРАФІЯ

У цьому розділі розглядаються сучасні напрямки побудови криптографічних примітивів, що вважаються перспективними з огляду на їхню стійкість до атак у квантовій моделі обчислень. Серед них – криптосистеми, побудовані на основі:

- задач на решітках;
- задач декодування випадкових лінійних кодів;
- мультिवаріантних задач;
- та інших менш поширених підходах, що продовжують досліджуватися.

Також у цьому розділі представлено огляд криптосистем сімейства AJPS, зокрема AJPS-1, AJPS-2 та механізму інкапсуляції ключів AJPS-КЕМ, побудованих на використанні арифметики за модулем спеціальних класів чисел – чисел Мерсенна. Ці криптосистеми є альтернативними підходами до побудови постквантових схем з використанням маловідомих, але ефективних з обчислювальної точки зору структур.

1.1 Конкурс постквантових криптопримітивів NIST

Для участі у першому раунді конкурсу було подано 82 криптосистеми, з яких 69 відповідали мінімальним критеріям і були прийняті для оцінки. В таблиці 1.1 наведено розбиття кандидатів по категоріях.

У рамках конкурсу NIST з постквантової криптографії було виявлено низку криптографічних схем, які виявилися вразливими до ефективних атак, що підривають їхню безпеку. Ці системи ґрунтувалися на різних класах задач, які вважалися перспективними для побудови

Таблиця 1.1 – Класифікація кандидатів NIST PQC Round 1 за типом математичної задачі

Категорія	Математичні задачі	Кандидати
На основі решіток	Задача навчання з помилками (Learning With Errors, LWE), Ring-LWE, Module-LWE, задача NTRU	CRYSTALS-KYBER, Falcon, CRYSTALS-DILITHIUM, FrodoKEM, NewHope, LAC, варіанти NTRU (NTRUEncrypt, pqNTRUSign, NTRU-HRSS-KEM, NTRU Prime), SABER, LIMA, Compact LWE, KINDI, LOTUS, RVB*, DRS, Ding Key Exchange, Lizard, Round2, Three Bears, Titanium, qTESLA, DME, EMBLEM/R.EMBLEM, Giophantus, LAKE, Lepton, McNie, Odd Manhattan, Ouroboros-R
Мультіваріативні	Розв'язання систем мультіваріативних квадратичних рівнянь (MQ задача), приховані польові рівняння (Hidden Field Equations, HFE), незбалансовані системи Oil and Vinegar (UOV)	Rainbow, LUOV, HiMQ-3, MQDSS, GeMSS, Gui, DualModeMS, CFPKM, RaCoSS, WalnutDSA
На основі кодів	Задача синдрому декодування, задача Мак-Еліса, задача Нідеррайтера	Classic McEliece, BIKE, HQC, LEDAkem, LEDApkc, NTS-KEM, DAGS, QC-MDPC KEM, RLCE-KEM, BIG QUAKE, LOCKER, RQC, Ramstake
На основі ізогеній	Задача графа суперсингулярних ізогеній	SIKE
На основі гешів	Стійкість до колізій, стійкість до знаходження прообразу, стійкість до знаходження другого прообразу	SPHINCS+, Gravity-SPHINCS, Picnic, Guess Again
Інші	Різні алгебраїчні задачі, задачі теорії груп	Edon-K*, НК17*, RankSign*, SRTPI*, Mersenne-756839, KCL, Post-quantum RSA-Encryption, Post-quantum RSA-Signature, pqsigRM

постквантових примітивів, зокрема:

– **Edon-K** – криптосистема, заснована на задачі декодування в ранговій метриці. Її вразливість полягала у тому, що відповідний код є надкодом LRPC-коду з малим рангом, що дозволяло ефективно відновлювати помилки та зламати систему [8].

– **НК17** – мультіваріантна криптосистема, для якої було показано можливість повного відновлення спільного ключа за допомогою відповідного аналізу структури рівнянь [9].

– **RankSign** – схема на основі задачі декодування в ранговій метриці.

Було доведено, що всі параметри, рекомендовані авторами, є вразливими до алгебраїчної атаки, яка дозволяє обійти механізм автентифікації [10].

– **SRTPI** – ще одна мультिवаріантна криптосистема, структура якої виявилась афінною, що уможливило її повне зламання шляхом лінеаризації [11].

– **RVB** – криптосистема, яка використовувала задачу знаходження найкоротшого вектора в ґратці (SVP). Згодом було показано, що певні припущення щодо розмірів параметрів роблять можливим застосування ефективних атак [12].

Ці приклади демонструють, що навіть у випадках використання складних математичних задач, практичні реалізації криптосистем можуть містити приховані слабкі місця. Відтак, формальна стійкість задачі не гарантує безпеки всієї криптосистеми без ретельного криптоаналізу її конкретної реалізації.

Основна маса кандидатів конкурсу NIST була зосереджена на криптосистемах, які ґрунтуються на задачах з теорії ґраток – таких як Learning With Errors (LWE) чи Module-LWE. Складність зламування алгоритмів, побудованих на ґратках, дуже велика, найкращі алгоритми ледь можуть розв'язати задачі цієї категорії за експоненційний час. Проте, не менш важливим є вивчення альтернативних підходів, що базуються на інших класах складних задач. Прикладом такого підходу є криптосистема Mersenne-756839 (також відома як AJPS-KEM), яка використовує арифметику у кільці лишків за модулем числа Мерсенна.

Ця криптосистема брала участь у першому раунді конкурсу NIST з постквантової криптографії, однак не була відібрана до другого раунду. Офіційна причина такого рішення не публікувалась, що є типовою практикою для кандидатів, які не пройшли далі. Імовірно, причиною могли бути фактори, не пов'язані безпосередньо з криптографічною стійкістю – зокрема, складність реалізації, відсутність широкого аналізу безпеки, або обмежена придатність до стандартизації в порівнянні з більш

дослідженими та простими у впровадженні схемами.

Незважаючи на це, математична новизна та нетрадиційна структура AJPS-КЕМ роблять її перспективним об'єктом для подальших досліджень, особливо в контексті пошуку нових підходів до побудови постквантових криптосистем, які не базуються на ґраткових задачах.

1.2 Числа Мерсенна

Криптосистема AJPS у своїй побудові використовує арифметику в кільці лишків за модулем числа Мерсенна. Числа Мерсенна володіють унікальними математичними властивостями, що робить їх перспективною основою для побудови криптографічних схем.

Означення 1.1. (Число Мерсенна) Нехай n – додатне ціле число. Число виду $M_n = 2^n - 1$ називається *числом Мерсенна*.

Означення 1.2. (Просте число Мерсенна) Якщо n є простим числом і $2^n - 1$ також є простим числом, то M_n називається *простим числом Мерсенна*.

Найменшими простими числами Мерсенна є:

$$2^2 - 1 = 3, \quad 2^3 - 1 = 7, \quad 2^5 - 1 = 31, \quad 2^7 - 1 = 127, \quad 2^{13} - 1 = 8191, \dots$$

Зауважимо, що число Мерсенна не може бути простим, якщо параметр n є складеним, оскільки в цьому випадку можна записати $n = k \cdot \ell$. І тоді як $2^k - 1$, так і $2^\ell - 1$ є дільниками $M_n = 2^n - 1$. Отже, M_n не є простим числом. Тому шукати прості числа Мерсенна потрібно серед тих чисел Мерсенна, в яких параметр n також є простим числом.

1.2.1 Історія чисел Мерсенна

Числа Мерсенна названі на честь французького математика Марена Мерсенна (1588–1648), який досліджував ці числа у своїх працях. Він припустив, що числа виду $2^n - 1$ є простими для певних значень n . Хоча

його припущення містило помилки, воно стало основою для подальших досліджень.

Прості числа Мерсенна мають тісний зв'язок із досконалими числами. Досконале число – натуральне число, що дорівнює сумі його додатних дільників, не враховуючи самого числа. Ще Евклід довів, що якщо $2^n - 1$ є простим числом, то $2^{n-1}(2^n - 1)$ є досконалим числом. У XVIII столітті Леонард Ейлер довів, що всі парні досконалі числа мають цей вигляд.

Сучасні дослідження чисел Мерсенна активно проводяться в рамках проєкту *Great Internet Mersenne Prime Search* (GIMPS), який використовує обчислення з розпаралелюванням для пошуку нових простих чисел Мерсенна. Саме пошук простих чисел Мерсенна є дуже актуальним, адже у зв'язку зі своєю структурою, обраховувати та перевіряти їх на простоту є значно менш ресурсозатратною обчислювальною задачею, ніж чисел іншого виду. В грудні 2018 року було знайдено 51-ше число Мерсенна: $2^{82589933} - 1$. До того ж, підраховане воно було на вже застарілому на той час Intel Core i5 4-го покоління з тактовою частотою в 2 ГГц. А 12 жовтня 2024 року, з використанням потужного процесора Nvidia A100, було знайдено вже 52-ге число Мерсенна: $2^{136279841} - 1$. Його довжина складає 41 024 320 символів в десятковому представленні. Більш детальну інформацію можна переглянути на сайті GIMPS [13].

Алгоритм пошуку простих Мерсенна

Тест Люка-Лемера

Тест Люка-Лемера використовується для перевірки простоти чисел Мерсенна $M_p = 2^p - 1$, де p є простим числом. Алгоритм працює наступним чином:

- 1) Обчислюємо $M_p = 2^p - 1$.
- 2) Ініціалізуємо $S_0 = 4$.
- 3) Для $n = 1, 2, \dots, p - 2$ обчислюємо: $S_{n+1} = S_n^2 - 2 \pmod{M_p}$.
- 4) Якщо після $p - 2$ ітерацій $S_{p-2} \equiv 0 \pmod{M_p}$, то M_p є простим

числом.

Наразі цей алгоритм вважається найефективнішим, точним та рекомендованим GIMPS, проте процес пошуку оптимізували ще більше.

На сайті mersenne.org [13] можна завантажити програму P95 (Prime95) та надати ресурси свого комп'ютера для підрахунку нових простих чисел Мерсенна. P95 автоматично підключається до серверів GIMPS і отримує завдання для обчислень. Програма використовує процесор комп'ютера для виконання цих завдань. Вона може працювати у фоновому режимі, не заважаючи основним задачам користувача. Після завершення обчислень P95 надсилає результати на сервери GIMPS для перевірки. Якщо знайдено нове просте число Мерсенна, це оголошується, і користувач, який виявив його, отримує визнання та можливість назвати число на свою честь. P95 гнучко налаштовується по витраті ресурсів, тож його можна застосовувати навіть для стрес-тестів вашого ПК.

Перед запуском тесту Люка-Лемера використовуються ще тести PRP (Probable Prime), P-1 Factoring та Trial Factoring, котрі з вірогідністю понад 99,9999% повертають правильну відповідь щодо простоти числа. Щоправда, невеличка можливість помилки першого роду все ще присутня, тому результат незалежно перевіряється на різних комп'ютерах за допомогою тесту Люка-Лемера, щоб уникнути можливих помилок чи підробки результату.

1.2.2 Числа Мерсенна в криптографії

Позначимо через \mathbb{Z}_{M_n} кільце цілих чисел за модулем M_n . Двійкові рядки індексуються справа наліво, тобто для $x \in \{0, 1\}^n$ записуємо x як $x_n \dots x_1$.

Означення 1.3. Вага Геммінга y n -бітного рядка y – це кількість одиниць у y і позначається $\text{Ham}(y)$.

Нехай $\text{seq} : \mathbb{Z}_{M_n} \rightarrow \{0, 1\}^n$ буде відображенням, яке кожному

$x \in \mathbb{Z}_{M_n}$ ставить у відповідність двійковий рядок $\text{seq}(x)$, що представляє представника x в інтервалі $[0, M_n - 1]$. Відображення $\text{int} : \{0, 1\}^n \rightarrow \mathbb{Z}_{M_n}$ відповідає представленню двійкового рядка у вигляді цілого числа, представленого $y \bmod M_n$. Очевидно, що seq та int є зворотними відображеннями між \mathbb{Z}_{M_n} та $\{0, 1\}^n \setminus \{1^n\}$, причому $\text{int}(1^n) = 0$.

Відображення між \mathbb{Z}_{M_n} та $\{0, 1\}^n \setminus \{1^n\}$ використовується для визначення додавання та множення у $\{0, 1\}^n$ природним чином: для $y, y' \in \{0, 1\}^n$ нехай

$$y + y' = \text{seq}(\text{int}(y) + \text{int}(y')), \quad y \cdot y' = \text{seq}(\text{int}(y) \cdot \text{int}(y')).$$

Ці операції залишаються асоціативними, комутативними та дистрибутивними. Також визначаємо $-y = \text{seq}(-\text{int}(y))$. Крім того, ця операція додавання є інваріантною відносно обертання, тобто якщо $\text{rot}_k(y)$ позначає циклічне обертання y на k позицій вліво, то $\text{rot}_k(y + y') = \text{rot}_k(y) + \text{rot}_k(y')$.

Лема 1.1. *Лема про вагу Геммінга*

Нехай $M_n = 2^n - 1$. Для всіх $A, B \in \{0, 1\}^n$, маємо:

- 1) $\text{Ham}((A + B) \bmod M_n) \leq \text{Ham}(A) + \text{Ham}(B)$,
- 2) $\text{Ham}((A \cdot B) \bmod M_n) \leq \text{Ham}(A) \cdot \text{Ham}(B)$,
- 3) Якщо $A \neq 0^n$, тоді $\text{Ham}((-A) \bmod M_n) = n - \text{Ham}(A)$.

1.2.3 Ефективні методи обчислення на числах Мерсенна

Однією з причин, чому числа Мерсенна є перспективними з точки зору практичного застосування в криптографії, є можливість реалізації надзвичайно ефективних алгоритмів для виконання базових арифметичних операцій. Особлива форма чисел $M_n = 2^n - 1$ дозволяє суттєво оптимізувати процеси зведення до модуля, множення та піднесення до степеня. Це забезпечує як пришвидшення криптографічних операцій, так і зниження обчислювальних витрат у реалізаціях на апаратному рівні.

У цьому підрозділі розглянуто два підходи до ефективної арифметики в кільці лишків за модулем M_n : покращений алгоритм модулярної редукції, який експлуатує бітову структуру чисел Мерсенна, та метод обчислень у адаптованій модульній системі чисел (AMNS), що дозволяє ще більше оптимізувати обчислення шляхом поліномного представлення чисел.

Покращений алгоритм модулярної редукції [14]

- Використовується властивість: $2^n \equiv 1 \pmod{M_p}$.
- Число X розкладається у вигляді: $X = X_1 \cdot 2^n + X_0$, де X_0 – залишок від ділення X на 2^n , а X_1 – частка.
- Обчислюється залишок від ділення X на M_p : $X \equiv X_1 + X_0 \pmod{M_p}$.

Обчислення на Адаптованій Модульній Системі Чисел

На конференції SAC2004 була презентована AMNS (Adapted Modular Number System)[14]. У AMNS кожне число X представляється у вигляді полінома: $X = \sum_{i=0}^{n-1} x_i \gamma^i \pmod{P}$, де:

- γ – основа системи (обирається так, щоб спростити обчислення),
- P – модуль (велике просте число),
- x_i – коефіцієнти, які належать до обмеженого діапазону $\{0, \dots, \rho - 1\}$,
- ρ – параметр, що визначає максимальне значення за модулем для кожного коефіцієнта x_i , обирається так, щоб забезпечити уніформне представлення всіх елементів \mathbb{Z}_P . Зазвичай береться як степінь двійки для оптимізації обчислень,
- n – кількість коефіцієнтів.

Для AMNS вводиться додаткова умова: $\gamma^n \pmod{P} = c$, де c – невелике число. Це дозволяє ефективно виконувати модульні скорочення, використовуючи властивості поліномів. З детальною реалізацією можна ознайомитись в оригінальній статті [14].

1.2.4 Алгебраїчні узагальнення чисел Мерсенна для криптосистем

Як було показано в попередніх підрозділах, класичні числа Мерсенна $M_n = 2^n - 1$ володіють низкою корисних властивостей для застосування в криптографії. Зокрема, вони дозволяють ефективно реалізовувати арифметичні операції у відповідному кільці лишків, завдяки простій бітовій структурі модуля.

Однак, незважаючи на ці переваги, клас простих чисел Мерсенна є надзвичайно обмеженим. На сьогодні відомо лише 52 простих числа цього типу, останнє з яких було знайдено наприкінці 2024 року [15]. Більшість з них або надто великі для ефективної реалізації, або не забезпечують належного рівня стійкості. Це обмежує гнучкість параметризації криптосистем, зокрема у випадках, коли необхідно підібрати простий модуль фіксованої довжини.

З метою подолання цих обмежень було запропоновано декілька узагальнень чисел Мерсенна, які зберігають бажані обчислювальні властивості, проте дозволяють ширше варіювати параметри. Далі наведено опис найпоширеніших варіацій.

Числа Кренделла

- Запропоновані Р. Кренделлом у 1992 році.
- Загальна формула: $M_{n,c} = 2^n - c$, де c — мале додатне ціле число.
- Застосовуються як альтернатива числам Мерсенна з подібною структурою, що дозволяє використовувати ефективні алгоритми обчислення за модулем.

Приклад 1.1. Нехай $n = 10$, $c = 3$. Тоді:

$$M_{10,3} = 2^{10} - 3 = 1021,$$

що є простим числом.

Узагальнені числа Мерсенна

- Запропоновані Д. Солінасом у 1999 році.
- Формула: $M_{n,m} = 2^n - 2^m - 1$, де $0 < m < n$, $m, n \in \mathbb{N}$.
- Використовуються, зокрема, для побудови еліптичних кривих та криптографічних примітивів зі спеціальними модулями.

Приклад 1.2. Нехай $n = 9$, $m = 3$. Тоді:

$$M_{9,3} = 2^9 - 2^3 - 1 = 512 - 8 - 1 = 503,$$

яке також є простим.

Більш узагальнені числа Мерсенна

- Запропоновані Чунгом і Хассаном у 2003 році на конференції SAC.
- Загальна форма: $P = f(2^t - c)$, де $f(x)$ — бінарний поліном з коефіцієнтами $f_i \in \{0, 1\}$.
- Дає змогу будувати модулі складніших форм при збереженні арифметичної ефективності.

Приклад 1.3. Нехай $f(x) = x^4 - x^3 - 1$ та $x = 2^4 - 2 = 14$. Тоді:

$$P = 14^4 - 14^3 - 1 = 38416 - 2744 - 1 = 35671.$$

1.3 Опис криптосистеми AJPS

1.3.1 Визначення семантичної стійкості криптосистеми

Асиметрична схема шифрування

Асиметрична схема шифрування складається з трьох алгоритмів: алгоритму генерації ключів **KeyGen**, алгоритму шифрування **Enc** та алгоритму розшифрування **Dec**. Алгоритм **KeyGen** генерує відкритий ключ pk і секретний ключ sk . Алгоритм шифрування **Enc** приймає на вхід повідомлення m і відкритий ключ pk , і видає шифротекст C . Алгоритм розшифрування **Dec** приймає на вхід шифротекст C і

секретний ключ sk , і видає повідомлення m' або спеціальний символ \perp , що вказує на відхилення.

Означення 1.4. Схема шифрування є $1 - \delta$ коректною, якщо для всіх m виконується: $\Pr[\text{Dec}(sk, \text{Enc}(pk, m)) = m] \geq 1 - \delta$, де ймовірність береться за випадковістю pk, sk та алгоритму шифрування.

Параметр безпеки позначається як λ . Усі інші параметри, включаючи довжини ключів і розмір шифротексту, задаються як поліноміально обмежені функції від λ .

Означення 1.5. Асиметрична схема шифрування $PKE = (\text{KeyGen}, \text{Enc}, \text{Dec})$ називається **семантично безпечною**, якщо для будь-якого ймовірнісного поліноміального розрізнявача і будь-якої пари повідомлень m_0, m_1 однакової довжини, за умови наявності відкритого ключа pk , перевага у розрізненні $C_0 = \text{Enc}(pk, m_0)$ і $C_1 = \text{Enc}(pk, m_1)$ не перевищує: $\frac{\text{poly}(|C_i|)}{2^\lambda}$, де poly – деякий поліном.

Означення 1.6. Асиметрична схема шифрування $PKE = (\text{KeyGen}, \text{Enc}, \text{Dec})$ називається **захищеною до атак із вибором шифротексту**, якщо для будь-якого ймовірнісного поліноміального розрізнявача, який має доступ до оракула розшифрування будь-якого заданого шифротексту, виконується наступне: для будь-якої пари повідомлень m_0, m_1 однакової довжини, за умови наявності відкритого ключа pk , перевага у розрізненні $C_0 = \text{Enc}(pk, m_0)$ і $C_1 = \text{Enc}(pk, m_1)$ не перевищує: $\frac{\text{poly}(|C_i|)}{2^\lambda}$, за умови, що розрізнявач не запитує оракул із C_0 або C_1 .

Стійкість механізму інкапсуляції ключа

Механізм інкапсуляції ключа (КЕМ) складається з трьох алгоритмів: алгоритму генерації ключів KeyGen , алгоритму інкапсуляції Encaps , алгоритму декапсуляції Decaps і простору ключів K . Алгоритм KeyGen генерує відкритий ключ pk і секретний ключ sk . Алгоритм інкапсуляції Encaps приймає на вхід відкритий ключ pk і видає шифротекст C та ключ $K \in K$. Алгоритм декапсуляції Decaps приймає на вхід шифротекст

C і секретний ключ sk , і видає ключ K' або спеціальний символ \perp , що вказує на відхилення.

Означення 1.7. КЕМ є $(1 - \delta)$ -коректним, якщо: $\Pr[\text{Decaps}(sk, C) = K : (C, K) \leftarrow \text{Encaps}(pk)] \geq 1 - \delta$, де ймовірність береться за випадковістю pk , sk та алгоритму інкапсуляції.

Означення 1.8. Механізм інкапсуляції ключа $KEM = (\text{KeyGen}, \text{Encaps}, \text{Decaps})$ називається **семантично стійким**, якщо для будь-якого ймовірнісного поліноміального розрізнявача, за умови наявності відкритого ключа pk , перевага у розрізненні пар (C, K_0) і (C, K_1) , де $(C, K_0) \leftarrow \text{Encaps}(pk)$, а K_1 є рівномірним і незалежним від C , не перевищує: $\frac{\text{poly}(|C|, |K_0|)}{2^\lambda}$, де poly – деякий поліном.

Означення 1.9. Механізм інкапсуляції ключа $KEM = (\text{KeyGen}, \text{Encaps}, \text{Decaps})$ називається **захищеним до атак із вибором шифротексту**, якщо для будь-якого ймовірнісного поліноміального розрізнявача, який має доступ до оракула декапсуляції та відкритого ключа pk , перевага у розрізненні пар (C, K_0) і (C, K_1) , де $(C, K_0) \leftarrow \text{Encaps}(pk)$, а K_1 є рівномірним і незалежним від C , не перевищує: $\frac{\text{poly}(|C|, |K_0|)}{2^\lambda}$, за умови, що розрізнявач не запитує оракул із C .

1.3.2 Побітове шифрування AJPS-1

В основі складності криптосистеми лежить задача MLHRSP (англ. *Mersenne Low Hamming Ratio Search Problem*).

Означення 1.10. (Задача MLHRSP) Нехай $\epsilon \in M_n$ та додатне ціле число $h < n$. Та нехай F і G – це лишки за модулем M_n , що мають вагу Геммінга h та хай $H = F \cdot G^{-1} \bmod M_n$. Мета полягає в тому, щоб відновити значення F та G за відомими значеннями M_n , H та h .

В основі задачі лежить наступний експериментально отриманий результат [16]. Нехай задано $H = F \cdot G^{-1} \bmod M_n$, де двійкові

представлення чисел F та G мають малу вагу Геммінга. Тоді число H є псевдовипадковим, тобто важко відрізнити H від випадкового лишка за модулем M_n .

Відкритими параметрами криптосистеми є параметр захищеності λ , число Мерсенна M_n , вага Геммінга h , що задовольняють умовам $4h^2 < n \leq 16h^2$ та $C_n^h \geq 2^\lambda$.

Алгоритм генерації ключів.

- 1) Випадково та незалежно обираються значення F та G – лишки за модулем M_n , що мають вагу Геммінга h .
- 2) Обчислюється $H = F \cdot G^{-1} \bmod M_n$.
- 3) Встановлюється відкритий ключ $pk = H$, а особистий ключ $sk = G$.

Алгоритм побітового шифрування.

- 1) Випадково і незалежно обираються A та B – лишки за модулем M_n такі, що $\text{Ham}(A) = \text{Ham}(B) = h$.
- 2) Біт b шифрується як:

$$C = (-1)^b (A \cdot H + B) \bmod M_n.$$

Алгоритм побітового розшифрування.

- 1) Обчислюється $d = \text{Ham}(C \cdot G \bmod M_n)$.
- 2) Якщо $d \leq 2h^2$, повертаємо 0; якщо $d \geq n - 2h^2$, повертаємо 1. Інакше повертаємо помилку розшифрування \perp .

1.3.3 Блокове шифрування AJPS-2

В основі складності криптосистеми AJPS-2 лежить задача MLHCSP (англ. *Mersenne Low Hamming Combination Search Problem*).

Означення 1.11. (MLHCSP) Нехай задано: число Мерсенна M_n , ціле число h та пару чисел (R, T) , де R – випадково обраний лишок за модулем

M_n , а T обчислено за формулою

$$T = F \cdot R + G \pmod{M_n},$$

причому F та G – лишки за модулем M_n з вагою Геммінга h . Потрібно знайти такі F та G з відомих M_n , h , R та T .

Криптосистема AJPS-2 шифрує блок повідомлення довжиною λ , де λ – параметр захищеності. У практичних застосуваннях доцільно вибрати довжину блоку повідомлення такою ж, як і параметр безпеки. З цієї причини нижче описано схему для шифрування блоку повідомлення $m \in \{0, 1\}^\lambda$.

Відкритими параметрами криптосистеми є:

- число Мерсенна $M_n = 2^n - 1$;
- число $h \in \mathbb{N}$, що задовольняє умовам $h = \lambda$, $10h^2 < n \leq 16h^2$;
- функції шифрування та розшифрування коду корекції помилок:

$$\mathcal{E} : \{0,1\}^\lambda \rightarrow \{0,1\}^n; \quad \mathcal{D} : \{0,1\}^n \rightarrow \{0,1\}^\lambda,$$

які задовольняють умові: для того, щоб криптосистема була $(1 - \delta)$ -коректною, де δ – ймовірність помилки, повинно виконуватись:

$$\forall M \in \{0,1\}^\lambda : \Pr(\mathcal{D}((F \cdot C_1) \oplus C_2) = M) \geq 1 - \delta.$$

Алгоритм генерації ключів.

1) Випадковим чином обираються числа F та G – лишки за модулем M_n з вагою Геммінга h . Число F є особистим ключем, а значення G – секретним параметром криптосистеми.

2) Випадковим чином обирається R – лишок за модулем M_n .

3) Обчислюється значення T за співвідношенням:

$$T = F \cdot R + G \pmod{M_n}.$$

4) Відкритим ключем є пара (R, T) , закритим – F .

Алгоритм шифрування.

1) Для шифрування повідомлення M незалежно та рівноймовірно обираються числа A, B_1, B_2 – лишки за модулем M_n з вагою Геммінга h .

2) Шифротекстом повідомлення M є пара чисел (C_1, C_2) , де C_1 та C_2 обчислюються за співвідношеннями:

$$C_1 = A \cdot R + B_1 \pmod{M_n};$$

$$C_2 = (A \cdot T + B_2 \pmod{M_n}) \oplus \mathcal{E}(M).$$

Алгоритм розшифрування.

1) Обчислюється значення:

$$M = \mathcal{D}((C_1 \cdot F \pmod{M_n}) \oplus C_2).$$

Коректність схеми

Для того, щоб схема була $(1 - \delta)$ -коректною, необхідно вибрати коригувальний код таким чином, щоб виконувалась умова: $\Pr_{(C_1, C_2) \leftarrow \text{Enc}(pk, m)} [D((F \cdot C_1) \oplus C_2) = m] \geq 1 - \delta$, де ймовірність береться за випадковістю алгоритму шифрування та вибору pk, sk .

1.3.4 Криптоаналіз схем шифрування сімейства AJPS

Означення 1.12. Для будь-якого розрізнявача D , що видає біт $b \in \{0, 1\}$, перевага у розрізненні між двома випадковими змінними X та Y визначається як: $\Delta^D(X; Y) := |\Pr[D(X) = 1] - \Pr[D(Y) = 1]|$.

Лема 1.2. Нехай f – ймовірнісна поліноміально обчислювана функція на двох випадкових змінних X та Y . Якщо існує ймовірнісний поліноміальний розрізнявач D , що розрізняє $f(X)$ та $f(Y)$ з перевагою δ , тоді існує ймовірнісний поліноміальний розрізнявач D' , що розрізняє X та Y з перевагою δ .

Теорема 1.1. Схема шифрування AJPS-2, описана в попередньому

розділі, є семантично безпечною за припущенням MLHCSP 1.3.3.

Доведення теореми 1.1 випливає з Лема 1.2, повністю наведено в оригінальній статті з описом AJPS [16].

Позначимо задачу MLHCSP як P . Якщо задачу P можна ефективно розв'язати, то можна порушити припущення з `\relax \@savsk \lastskip \@savsf \spacefactor \begingroup \def {complex` а отже, і безпеку криптосистеми.

Розподіл відстані Геммінга. Нехай R – рівномірно випадковий лишок за модулем M_n , а $Y = F \cdot R + G \pmod{M_n}$, де F, G обрані випадково з множини лишків за модулем M_n з вагою Геммінга h . Основний тест для перевірки псевдовипадковості Y за умови R полягає у порівнянні розподілу $\text{Ham}(R, R')$ з розподілом $\text{Ham}(R, T)$, де T – рівномірно випадковий n -бітний рядок.

Атака на слабкі ключі. У BCGN17 [17] описано атаку на задачу пошуку комбінації Мерсенна з низькою вагою Геммінга, яка базується на раціональній реконструкції. Якщо всі біти F і G знаходяться у правій половині, то їх можна відновити за допомогою розкладу в неперервні дроби.

Узагальнення за допомогою LLL. У BCGN17 [17] запропоновано узагальнення, яке використовує розбиття F і G на вікна бітів. Аналіз показує, що час виконання атаки дорівнює 2^{2h} на класичному комп'ютері.

Квантове прискорення за алгоритмом Гровера. На квантовому комп'ютері можна використати алгоритм Гровера для квадратичного прискорення атаки. Однак реалізація цього підходу потребує складних універсальних квантових комп'ютерів.

Атака при n , яке не є простим. Якщо n не є простим, то $2^n - 1$ не є простим числом, що може дозволити часткову атаку. Наприклад, якщо n_0 ділить n , то $q = 2^{n_0} - 1$ ділить $M_n = 2^n - 1$, і можна спробувати відновити F і G модулем q .

Активні атаки

Активні атаки або атаки на основі помилок розшифрування є потужними інструментами для атаки на побітове шифрування. Основна ідея таких атак полягає у запиті розшифрування некоректно сформованих шифротекстів для отримання інформації про ключ. Протидіяти таким атакам можна за допомогою перевірки коректності шифротекстів.

Для прикладу припустимо, що у нас є доступ до оракула розшифрування. Формування псевдошифротекстів виду $A^*H + B^*$, де A^* і B^* мають низьку, але некоректну вагу Геммінга. Це може призводити до витоку інформації про приватний ключ. Зокрема, зловмисник може поступово додавати біти '1' у B^* (або A^*) до тих пір, поки розшифрування не перейде від 0 до \perp .

1.3.5 Механізм інкапсуляції ключів AJPS-КЕМ

Так як попередня система є вразливою до атак на основі помилок розшифрування, ця варіація для інкапсуляції ключів долає цю проблему. Також її можна перетворити у асиметричну схему шифрування.

Нехай Enc і Dec будуть алгоритмами шифрування та розшифрування, як визначено в розділі 1.3.4. Окрім цього, механізм енкапсуляцію використовує три випадкові оракули H_1 , H_2 і H_3 , які приймають на вхід рядок довжиною λ бітів і видають на виході рівномірно випадковий рядок із вагою Геммінга h на n бітів. Досить легко побудувати реалізацію для H_1 , H_2 і H_3 , тож деталями можна знехтувати.

Генерація ключів

Генерація ключів ідентична криптосистемі AJPS-2 та виконується наступним чином: $\text{pk} := (R, T := F - R + G)$, $\text{sk} := F$, де R – рівномірно випадковий n -бітний рядок, а F, G обираються рівномірно випадково з множини лишків за модулем M_n з вагою Геммінга h .

Інкапсуляція ключа

Для заданого відкритого ключа $\text{pk} = (R, T)$ алгоритм Encaps виконується наступним чином:

- 1) Обирається рівномірно випадковий λ -бітний рядок K .
- 2) Обчислюється $A = H_1(K)$, $B_1 = H_2(K)$, $B_2 = H_3(K)$.
- 3) Обчислюється $C = (C_1, C_2)$, де $C_1 = A \cdot R + B_1$,
 $C_2 = \mathcal{E}(K) \oplus (A \cdot T + B_2)$.
- 4) Повертається (C, K) .

Декапсуляція ключа

Для заданого шифротексту $C = (C_1, C_2)$ і секретного ключа $sk = F$ алгоритм Decaps виконується наступним чином:

- 1) Обчислюється $K' = \mathcal{D}((F - C_1) \oplus C_2)$.
- 2) Обчислюється $A' = H_1(K')$, $B'_1 = H_2(K')$, $B'_2 = H_3(K')$.
- 3) Обчислюється $C' = (C'_1, C'_2)$, де $C'_1 = A' \cdot R + B'_1$,
 $C'_2 = \mathcal{E}(K') \oplus (A' \cdot T + B'_2)$.
- 4) Якщо $C = C'$, повертається K' , інакше повертається \perp .

Теорема 1.2. *Припустимо, що H – випадковий оракул, і що схема з Розділу 1.3.3 є семантично безпечною. Тоді описаний вище механізм інкапсуляції ключа є стійким до атак на вибраний шифротекст.*

1.3.6 Код корекції помилок

У криптосистемах AJPS-2 та AJPS-КЕМ важливу роль відіграє механізм виправлення помилок, який забезпечує коректне відновлення зашифрованого повідомлення попри наявність спотворень, що виникають унаслідок специфіки арифметичних операцій над елементами з малою вагою Геммінга.

У схемі шифрування, яка лежить в основі AJPS-2 та AJPS-КЕМ, повідомлення m спочатку кодується з використанням функції $E(m)$ – це результат застосування коду корекції помилок, який відображає $m \in 0,1^\lambda$ у n -бітну кодову послідовність. Під час розшифрування застосовується зворотна функція D , яка повинна відновити m з зашумленої версії $E(m)$, отриманої в результаті операцій з елементами низької ваги Геммінга за

модулем M_n .

Причиною появи шуму є обчислення $C_2 = A \cdot T + B_2 \oplus E(m)$, де $T = F \cdot R + G$, а всі вектори A, B_1, B_2, F, G мають малу вагу Геммінга h . При цьому, значення $F \cdot C_1$ обчислюється як $F \cdot (A \cdot R + B_1)$, що є наближенням до $A \cdot T + B_2$, але містить похибку, пов'язану з лінійністю операцій у кільці лишків за простим модулем.

В ході виконання роботи, застосовувались коди повторень. Це простий, але ефективний тип коду корекції помилок, що кодує кожен біт повідомлення як блок з ρ повторень. Таким чином, $0 \mapsto 000 \dots 0$, а $1 \mapsto 111 \dots 1$.

При декодуванні аналізується кожен блок довжини ρ методом голосування: якщо кількість одиниць у блоці перевищує половину, то блок інтерпретується як 1, інакше – як 0. Такий підхід дозволяє виправляти спотворення, які трапляються з імовірністю значно меншою за 0.5 для кожного біта.

Як показано в оригінальній статті AJPS [16], навіть у випадку високих значень параметрів (наприклад, $n = 756839$, $h = 256$), статистичні властивості розподілу відстані Геммінга між $F \cdot C_1$ та $A \cdot T + B_2$ наближаються до нормального розподілу з малим середнім та дисперсією, що дозволяє ефективно коригувати помилки. Згідно з аналізом розробників (див. стор. 14–15 документа), ймовірність помилки при відновленні одного біта оцінюється як менша за 2^{-247} , а загальна ймовірність помилки при декодуванні 256-бітного повідомлення – як менше 2^{-239} , що є прийнятним рівнем надійності для сучасних криптографічних застосувань.

1.4 Інші криптосистеми з використанням обчислень за модулем числа Мерсенна

Окрім AJPS, в останні роки з'явилося кілька криптографічних примітивів, що також базуються на арифметиці в кільцях за модулем простого числа Мерсенна. Їх основою, як і в AJPS, виступає задача MLHRSP (Mersenne Low-Hamming Ratio Subset Product), або її варіації.

Одним із прикладів є криптосистема *Integer Reconstruction Public-Key Encryption* [18], яка комбінує задачі MLHRSP та теорію ґраток, зокрема задачі CVP (Closest Vector Problem). Її безпека базується на поєднанні кількох математичних складностей, що дозволяє отримати стійкість до атак як класичних, так і квантових суперкомп'ютерів.

Ще одним прикладом є *Post-Quantum Provably-Secure Authentication and MAC from Mersenne Primes* [19], що пропонує надзвичайно легкий механізм автентифікації, придатний для пристроїв із обмеженими ресурсами – таких як смарт-карти, сенсори або RFID-мітки. На відміну від AJPS, ця система не використовує операцій з відкритим ключем, а побудована на симетричному ключі, проте продовжує використовувати множення в кільці за модулем простого числа Мерсенна та задачу MLHRSP для забезпечення стійкості.

Ці роботи демонструють потенціал використання чисел Мерсенна не лише у сфері шифрування, а й для побудови інших криптографічних примітивів – автентифікації, підписів та симетричних протоколів.

1.5 Набір статистичних тестів NIST SP 800-22

В процесі переходу до постквантових криптопримітивів (англ. *Post-Quantum Cryptography, PQC*) у межах стандартів NIST надзвичайно важливо, щоб криптосистеми забезпечували належну стійкість не лише до класичних атак, а й були стійкими до можливостей квантових

комп'ютерів. Одним зі складників цієї безпеки є перевірка, наскільки випадковими (або, точніше, псевдовипадковими) є ті двійкові послідовності, які криптопримітив генерує або використовує.

Для перевірок рівня псевдовипадковості застосовується низка статистичних тестів. Конкретно в розглянутому нами конкурсі використовується NIST Statistical Test Suite (також відомий як NIST SP 800-22) [20]. Нижче коротко викладено ідею побудови цих тестів в межах конкурсу стандартизації постквантових криптопримітивів.

1) Frequency (Monobits) Test: тест оцінює пропорцію нулів і одиниць у всій послідовності. Мета – перевірити, чи є кількість одиниць і нулів приблизно однаковою, як це очікується для істинно випадкової послідовності.

2) Frequency Test within a Block: тест аналізує пропорцію одиниць у блоках довжини M . Перевіряється, чи є частота появи одиниць у кожному блоці приблизно $\frac{M}{2}$.

3) Runs Test: тест досліджує загальну кількість послідовностей однакових бітів (пробіги) у всій послідовності. Мета – визначити, чи є кількість пробігів одиниць і нулів різної довжини очікуваною для істинно випадкової послідовності, зокрема перевіряється, чи не відбуваються переходи між підрядками надто часто або надто рідко.

4) Test for the Longest Run of Ones in a Block: тест обчислює довжину найдовшого підрядка з одиниць у кожному M -бітовому блоці. Перевіряється, чи узгоджується отримана довжина з очікуваним значенням для випадкової послідовності.

5) Binary Matrix Rank Test: бітова послідовність розбивається на блоки фіксованого розміру (на практиці зазвичай 32 підпослідовності по 32 біта) з яких формується матриця. Якщо біти не є дійсно випадковими, можна побачити, що матриці матимуть занижені ранги набагато частіше, ніж очікується.

6) Discrete Fourier Transform (Spectral) Test: тест аналізує пікові значення у спектрі дискретного перетворення Фур'є. Мета – виявити

періодичні особливості або шаблони, які свідчать про відхилення від випадковості.

7) Non-Overlapping Template Matching Test: тест визначає кількість появ заданих неперіодичних підрядків. Якщо таких появ надто багато, послідовність вважається не випадковою.

8) Overlapping Template Matching Test: тест схожий на попередній, але дозволяє перекриття шаблонів. Перевіряється відхилення кількості появ шаблонів від очікуваного значення.

9) Maurer's "Universal Statistical" Test: тест оцінює кількість бітів між повторюваними шаблонами. Його мета – виявити, чи може послідовність бути суттєво стиснута без втрати інформації, що є ознакою не випадковості.

10) Linear Complexity Test: тест визначає довжину регістра зворотного зв'язку, необхідного для генерації послідовності. Чим довший регістр, тим більша ймовірність, що послідовність випадкова.

11) Serial Test: тест аналізує частоти всіх перетинних m -бітових шаблонів у всій послідовності. Мета – перевірити, чи ці частоти відповідають очікуваним для випадкової послідовності.

12) Approximate Entropy Test: вимірює ентропію бітової послідовності для різних довжин шаблону m та $m + 1$ і порівнює результати. В ідеально випадковому потоці ентропія (у сенсі середньої непередбачуваності) буде максимально високою.

13) Cumulative Sums (Cusum) Test: тест аналізує максимальне відхилення випадкового блукання, яке виникає при підсумовуванні бітів (перетворених у -1 та $+1$). Перевіряється, чи є ці відхилення надто великими або малими порівняно з очікуваним для випадкових послідовностей.

14) Random Excursions Test: тест визначає кількість циклів із точно K відвідуваннями певного стану у випадковому блуканні. Мета – перевірити, чи кількість відвідувань станів перевищує очікуване значення.

15) Random Excursions Variant Test: тест оцінює загальну кількість появ конкретного стану у випадковому блуканні. Мета – виявити

відхилення у кількості появ різних станів від очікуваного випадковістю.

Висновки до розділу 1

У даному розділі було проведено аналіз поточного стану постквантової криптографії та криптографічних примітивів, стійких до атак квантових комп'ютерів. Особливу увагу приділено конкурсу NIST із пошуку кандидатів для майбутніх стандартів постквантових криптосистем. Було розглянуто класифікацію кандидатів за типами математичних задач, які лежать в основі їхньої стійкості, а також проаналізовано важливість тестів на псевдовипадковість, які є ключовим елементом оцінки безпеки криптографічних алгоритмів.

Окремо розглянуто числа Мерсенна, їхні унікальні математичні властивості та переваги для використання в постквантовій криптографії. Було описано алгоритми ефективного обчислення операцій на числах Мерсенна та їхніх узагальненнях, що дозволяє значно підвищити ефективність реалізації операцій, що використовуються в побудові криптопримітивів.

Детально проаналізовано криптосистеми AJPS-1, AJPS-2 та AJPS-KEM, які базуються на арифметиці за модулем числа Мерсенна. Розглянуто їх архітектуру, механізми шифрування та розшифрування, механізм інкапуляції та декапсуляції, а також доведення їхньої коректності. Проведено аналіз можливих загроз для цих систем, зокрема атак на основі помилок розшифрування, та способи їхньої нейтралізації.

2 АНАЛІЗ МОДИФІКАЦІЙ КРИПТОСИСТЕМ СІМЕЙСТВА AJPS

В другому розділі розглядаються модифікації криптосистем AJPS-1, AJPS-2, AJPS-КЕМ з використанням чисел Кренделла та узагальнених чисел Мерсенна у якості модуля. Проведено аналіз псевдовипадковості послідовностей, що використовуються в їх основі, а саме: відкритого ключа та шифротекстів оригінальних криптосистем та їх модифікацій.

2.1 Модифікації криптосистем сімейства AJPS

У криптографії використання простих модулів має важливі переваги, оскільки кільце лишків за простим модулем є полем. Це забезпечує однорідність множини елементів поля, що є важливим для гарантування рівномірного розподілу значень, а також унеможливорює наявність дільників нуля, що характерні для кілець лишків за складеним модулем. Відсутність дільників нуля є критичною для криптографічних схем, оскільки гарантує існування оберненого елемента для будь-якого ненульового елемента кільця. Ця властивість активно використовується, зокрема, у схемі AJPS-1, яка передбачає обчислення обернених елементів за модулем.

Проте використання класичних чисел Мерсенна має суттєве обмеження: наразі відомо лише 52 простих числа цього типу. Значна частина з цих чисел є надзвичайно великими, що ускладнює їх практичне використання у криптографічних схемах через значні обчислювальні витрати. Водночас менші прості числа Мерсенна не задовольняють сучасним вимогам криптографічної стійкості через недостатню довжину.

Для подолання цих недоліків пропонується використання альтернативних класів чисел, зокрема чисел Кренделла ($M_{n,c} = 2^n - c$) та

узагальнених чисел Мерсенна ($M_{n,m} = 2^n - 2^m - 1$). Проведені у цьому дослідженні експериментальні обчислення свідчать, що для практично значущих значень $n > 1000$ майже завжди можна знайти такі параметри c та m , при яких відповідні числа $M_{n,c}$ і $M_{n,m}$ є простими. Таким чином, використання цих класів чисел забезпечує істотне розширення множини потенційних модулів, які можна використовувати в криптосистемах сімейства AJPS.

Слід наголосити, що простота обраного модуля є необхідною умовою для забезпечення стійкості до атак, спрямованих на використання властивостей складених модулів, описаних раніше у розділі 1.3.4. Це робить зазначений підхід не лише більш гнучким і універсальним, але й безпечнішим у порівнянні з використанням традиційних чисел Мерсенна.

З кодом реалізації модифікацій усіх криптосистем, що описуються далі, а також з алгоритмом пошуку простих чисел Кренделла та узагальнених чисел Мерсенна можна ознайомитись за посиланням [21].

2.1.1 AJPS-1 з використанням альтернативних модулів

В основі складності криптосистеми лежить задача GMLHRSP (англ. *Generalized Mersenne Low Hamming Ratio Search Problem*).

Означення 2.1. (Задача GMLHRSP) *Нехай $e \in M_{n,m}$ та додатне ціле число $h < n$. Та нехай F і G – це лишки за модулем $M_{n,m}$, що мають вагу Геммінга h та хай $H = F \cdot G^{-1} \pmod{M_{n,m}}$. Мета полягає в тому, щоб відновити значення F та G за відомими значеннями $M_{n,m}$, H та h .*

AJPS-1 з використанням узагальнених чисел Мерсенна

Відкритими параметрами криптосистеми є параметр захищеності λ , узагальнене число Мерсенна $M_{n,m}$, вага Геммінга h , що задовольняють умовам $4h^2 < n \leq 16h^2$ та $C_n^h \geq 2^\lambda$.

Алгоритм генерації ключів.

- 1) Випадково та незалежно обираються F та G – лишки за модулем $M_{n,m}$, що мають вагу Геммінга h .
- 2) Обчислюється $H = F \cdot G^{-1} \bmod M_{n,m}$.
- 3) Встановлюється відкритий ключ $pk = H$, а особистий ключ $sk = G$.

Алгоритм побітового шифрування.

Для коректної роботи криптосистеми потрібно, щоб виконувались такі умови:

- $Ham(A + B \bmod M_{n,m}) \geq |Ham(A) - Ham(B)|$;
- $Ham(A \cdot B \bmod M_{n,m}) \geq |Ham(A) - Ham(B)|$.

Експериментальні дослідження показали, що при досить великих значеннях параметра n , ймовірність того, що випадково обрані числа з множини лишків за модулем $M_{n,m}$, що мають вагу Геммінга h , задовольняють кожен з цих умов, дорівнює приблизно 0,988. Отже, необхідні умови для коректного функціонування системи не накладають суттєвих обмежень на вибір параметрів.

- 1) Випадково і незалежно, згідно з попередніми вимогами, обираються A та B – лишки за модулем $M_{n,m}$ такі, що $Ham(A) = Ham(B) = h$.

- 2) Біт b шифрується як:

$$C = A \cdot H + (-1)^b \cdot B \bmod M_{n,m}.$$

Алгоритм побітового розшифрування.

- 1) Обчислюється $d = Ham(C \cdot G \bmod M_{n,m})$.
- 2) Якщо $d \leq 2h^2 + h \cdot (2m - 2)$, повертаємо 0; якщо $d \geq n - 2h - 1$, повертаємо 1. Інакше повертаємо помилку розшифрування \perp .

AJPS-1 з використання чисел Кренделла

В основі складності криптосистеми лежить задача CLHRSP (англ. *Crendall Low Hamming Ratio Search Problem*).

Означення 2.2. (Задача CLHRSP) Нехай $e \in M_{n,c}$ та додатне ціле

число $h < n$. Та нехай F і G – це лишки за модулем $M_{n,c}$, що мають вагу Геммінга h та хай $H = F \cdot G^{-1} \bmod M_{n,c}$. Мета полягає в тому, щоб відновити значення F та G за відомими значеннями $M_{n,c}$, H та h .

У роботі [22] також описується модифікація криптосистеми AJPS-1 з використанням чисел Кренделла, що будується аналогічно до модифікації AJPS-1 з узагальненими числами Мерсенна, за виключенням операції розшифрування.

2.1.2 AJPS-2 з використанням альтернативних модулів

Побудова для модифікацій з використанням узагальнених чисел Мерсенна та чисел Крендала аналогічна до оригінальної криптосистеми AJPS-2, описаній в розділі 1.3.3, лише з заміною модуля на відповідний.

Модифікація AJPS-2 з використанням узагальненого числа Мерсенна

З детальним описом модифікацій можна ознайомити у статті [23]. В основі складності криптосистеми AJPS-2 з використанням операцій за модулем узагальненого числа Мерсенна лежить задача GMLHCSP (англ. *Generalized Mersenne Low Hamming Combination Serach Problem*).

Означення 2.3. (Задача GMLHCSP)

Нехай задано: узагальнене число Мерсенна $M_{n,m}$, ціле число h та пару чисел (R, T) , де R – випадково обраний лишок за модулем $M_{n,m}$, а T обчислено за формулою

$$T = F \cdot R + G \bmod M_{n,m},$$

причому F та G – лишки за модулем $M_{n,m}$ з вагою Геммінга h . Потрібно знайти такі F та G з відомих $M_{n,m}$, h , R та T .

Алгоритм генерації ключів.

1) Випадковим чином обираються числа F та G – лишки за модулем $M_{n,m}$ з вагою Геммінга h . Число F є особистим ключем, а значення G –

секретним параметром криптосистеми.

- 2) Випадковим чином обирається R – лишок за модулем $M_{n,m}$.
- 3) Обчислюється значення T за співвідношенням:

$$T = F \cdot R + G \pmod{M_{n,m}}.$$

- 4) Відкритим ключем є пара (R, T) , закритим – F .

Алгоритм шифрування.

- 1) Для шифрування повідомлення M незалежно та рівноймовірно обираються числа A, B_1, B_2 – лишки за модулем $M_{n,m}$ з вагою Геммінга h .
- 2) Шифротекстом повідомлення M є пара чисел (C_1, C_2) , де C_1 та C_2 обчислюються за співвідношеннями:

$$C_1 = A \cdot R + B_1 \pmod{M_{n,m}};$$

$$C_2 = (A \cdot T + B_2 \pmod{M_{n,m}}) \oplus \mathcal{E}(M).$$

Алгоритм розшифрування.

- 1) Обчислюється значення:

$$M = \mathcal{D}((C_1 \cdot F \pmod{M_{n,m}}) \oplus C_2).$$

Модифікація AJPS-2 з використанням числа Кренделла

В основі складності криптосистеми AJPS-2 з використанням операцій за модулем числа Кренделла лежить задача CLHCSP (англ. *Crendall Low Hamming Combination Search Problem*).

Означення 2.4. (Задача CLHCSP)

Нехай задано: число Кренделла $M_{n,c}$, ціле число h та пару чисел (R, T) , де R – випадково обраний лишок за модулем $M_{n,c}$, а T обчислено за формулою

$$T = F \cdot R + G \pmod{M_{n,c}},$$

причому F та G – лишки за модулем $M_{n,c}$ з вагою Геммінга h . Потрібно знайти такі F та G з відомих $M_{n,c}$, h , R та T .

Алгоритм генерації ключів.

1) Випадковим чином обираються числа F та G – лишки за модулем $M_{n,c}$ з вагою Геммінга h . Число F є особистим ключем, а значення G – секретним параметром криптосистеми.

2) Випадковим чином обирається R – лишок за модулем $M_{n,c}$.

3) Обчислюється значення T за співвідношенням:

$$T = F \cdot R + G \pmod{M_{n,c}}.$$

4) Відкритим ключем є пара (R, T) , закритим – F .

Алгоритм шифрування.

1) Для шифрування повідомлення M незалежно та рівноймовірно обираються числа A, B_1, B_2 – лишки за модулем $M_{n,c}$ з вагою Геммінга h .

2) Шифротекстом повідомлення M є пара чисел (C_1, C_2) , де C_1 та C_2 обчислюються за співвідношеннями:

$$C_1 = A \cdot R + B_1 \pmod{M_{n,c}};$$

$$C_2 = (A \cdot T + B_2 \pmod{M_{n,c}}) \oplus \mathcal{E}(M).$$

Алгоритм розшифрування.

1) Обчислюється значення:

$$M = \mathcal{D}((C_1 \cdot F \pmod{M_{n,c}}) \oplus C_2).$$

2.1.3 AJPS-КЕМ з використанням альтернативних модулів

Нехай E_{nc} і D_{nc} будуть алгоритмами шифрування та розшифрування, як визначено в розділі 1.3.4. Аналогічно до оригінальної криптосистеми AJPS-КЕМ, механізм інкапсуляції модифікацій використовує три випадкові оракули H_1, H_2 і H_3 , які приймають на вхід рядок довжиною λ бітів і видають на виході рівномірно випадковий рядок із вагою Геммінга h на n бітів.

Генерація ключів

Генерація ключів ідентична відповідним модифікаціям AJPS-2 та виконується наступним чином: $pk := (R, T := F - R + G)$, $sk := F$, де R – рівномірно випадковий n -лишок за модулем $M_{n,m}$ чи $M_{n,c}$, а F, G обираються рівномірно випадково з множини лишків за відповідним модулем з вагою Геммінга h .

Інкапсуляція ключа

Для заданого відкритого ключа $pk = (R, T)$ алгоритм Encaps виконується наступним чином:

- 1) Обирається рівномірно випадковий λ -бітний рядок K .
- 2) Обчислюється $A = H_1(K)$, $B_1 = H_2(K)$, $B_2 = H_3(K)$.
- 3) Обчислюється $C = (C_1, C_2)$, де $C_1 = A \cdot R + B_1$, $C_2 = \mathcal{E}(K) \oplus (A \cdot T + B_2)$.
- 4) Повертається (C, K) .

Декапсуляція ключа

Для заданого шифротексту $C = (C_1, C_2)$ і секретного ключа $sk = F$ алгоритм Decaps виконується наступним чином:

- 1) Обчислюється $K' = \mathcal{D}((F - C_1) \oplus C_2)$.
- 2) Обчислюється $A' = H_1(K')$, $B'_1 = H_2(K')$, $B'_2 = H_3(K')$.
- 3) Обчислюється $C' = (C'_1, C'_2)$, де $C'_1 = A' \cdot R + B'_1$, $C'_2 = \mathcal{E}(K') \oplus (A' \cdot T + B'_2)$.
- 4) Якщо $C = C'$, повертається K' , інакше повертається \perp .

2.1.4 Пошук параметрів для побудови модифікацій

У ході тестування криптосистеми AJPS-2 та AJPS-КЕМ було необхідно знайти прості узагальнене число Мерсенна та число Кренделла довжини, рекомендованої розробниками ($n = 756839$). Для пошуку використовувався алгоритм Міллера-Рабіна. Проте процес пошуку зіткнувся з суттєвою проблемою, оскільки перевірка на простоту за допомогою алгоритму Міллера-Рабіна з максимальною оптимізацією

навіть для одного числа такої довжини займала мінімум 20 хвилин. Це стало серйозною перешкодою, оскільки необхідно було перебрати декілька тисяч чисел аналогічної довжини.

Для подолання цієї проблеми було прийнято рішення зменшити розмір параметрів криптосистеми до таких значень:

$$- n = 11213, h = 33, \lambda = 33, c = 7713, m = 9953.$$

За цих умов пошук відповідних параметрів m та c зайняв значно менше часу (менше години). Проте, це призвело до зменшення максимальної довжини блоку повідомлення, що шифрується, до 33 біт замість початкових 264 біт.

Для пошуку відповідних параметрів використовувався наступний алгоритм з використанням тесту Міллера–Рабіна:

Algorithm 2.1 Пошук простих $M_{n,c}$ та $M_{n,m}$ заданої довжини

```

1: procedure PRIME  $M_{n,c}, M_{n,m}$  SEARCH( $n$ )
     $\triangleright$  Пошук найменшого параметра  $c$  для числа Кренделла
2:   for  $c \leftarrow 1, c = c + 2$  to  $max\_c$  do
3:      $candidate \leftarrow base - c$ 
4:     if  $candidate > 1$  and MILLER-RABIN( $candidate, k = 100$ ) then
5:       повернути “Crandall-просте знайдено:  $c =$ ”,  $c$ 
6:       break
7:     end if
8:   end for
     $\triangleright$  Пошук найменшого параметра  $m$  для узагальненого числа Мерсенна
9:   for  $m \leftarrow 1$  to  $n - 1$  do
10:     $power\_m \leftarrow 2^m$ 
11:     $candidate \leftarrow base - power\_m - 1$ 
12:    if  $candidate > 1$  and MILLER-RABIN( $candidate, k = 100$ ) then
13:      повернути “Узагальнене число Мерсенна знайдено:  $m =$ ”,  $m$ 
14:      break
15:    end if
16:   end for
17: end procedure

```

Під час перевірки кандидатів на простоту використовувався ймовірнісний тест Міллера–Рабіна з кількістю раундів $k = 100$. Це означає, що кожне число перевіряється незалежними підставами сто разів. Ймовірність того, що складене число пройде всі раунди цього тесту, не перевищує 4^{-100} , що є надзвичайно малою величиною та практично нівелює ризик помилкової класифікації. У зв’язку з цим, надалі

вважається, що знайдені кандидати, які успішно пройшли тест, є простими з імовірністю, достатньою для криптографічного застосування.

2.2 Результати тестів NIST SP 800-22

P-value (значення p) – це ймовірність того, що для істинно випадкової послідовності результат тесту є таким ж, як для досліджуваної послідовності. В межах тестів NIST SP 800-22 мінімальним значенням p для всіх тестів є 0.01.

Для всіх подальших тестувань кожної варіації криптосистем було згенеровано файли, які містять 16 мільйонів бітів. З метою отримання статистично значущих результатів, кожен з отриманих файлів було поділено на окремі блоки довжиною 1,000,000 бітів, таким чином утворюючи 16 незалежних блоків. Застосування такого підходу дозволяє суттєво підвищити надійність отриманих результатів завдяки можливості аналізу статистичних характеристик за значною кількістю незалежних вибірок.

2.2.1 Тести псевдовипадковості AJPS-1

Для аналізу криптосистеми AJPS-1 та її модифікацій було обрано такі параметри: $n = 4253$, $h = 32$, $\lambda = 267$, $c = 3981$, $m = 399$. Такі значення параметрів n, h, λ є одними з рекомендованих розробниками [16], а параметри c та m обиралися так, щоб числа M_n , $M_{n,c}$ та $M_{n,m}$ були простими.

Для порівняльного аналізу криптосистеми AJPS-1 та її модифікацій шляхом зміни модуля проводилися тестування таких значень на псевдовипадковість:

- публічного ключа H ;
- шифротексту, отриманого в результаті шифрування біту 0;

– шифротексту, отриманого в результаті шифрування біту 1.

Тест випадковості відкритого ключа

У цій серії тестів проведено аналіз псевдовипадковості відкритого ключа H .

Таблиця 2.1 – Результати тестів випадковості відкритого ключа

Тест	M_n	$M_{n,c}$	$M_{n,m}$
Frequency (Monobit)	0.3154	0.7918	0.3311
Frequency within Block	0.9139	0.5252	0.7437
Runs Test	0.8298	0.7489	0.0499
Longest Run of Ones	0.1531	0.6251	0.8494
Binary Matrix Rank	0.7845	0.5440	0.9965
Spectral Test	0.4518	0.8257	0.1715
Non-overlapping Template	0.7440	0.9984	0.4661
Overlapping Template	0.3312	0.6728	0.6317
Universal Statistical Test	0.3457	0.1833	0.1290
Linear Complexity	0.9586	0.5512	0.2762
Serial Test (1)	0.3688	0.8069	0.4551
Serial Test (2)	0.7328	0.7500	0.5777
Approximate Entropy	0.1616	0.9732	0.1250
Cumulative Sums (F)	0.1005	0.7793	0.3960
Cumulative Sums (B)	0.4086	0.9695	0.6165

На підставі аналізу результату тестів, представлених у таблиці 2.1, можна зазначити, що усі версії криптосистеми демонструють високі показники псевдовипадковості. Всі значення p є значно вище критичного рівня, що підтверджує відсутність очевидних закономірностей у послідовностях відкритого ключа. Слід приділити увагу показнику Runs Test для модифікації $M_{n,m}$, що найбільше наблизився до критичного значення (0.0499). Це може свідчити про незначну регулярність в чергуванні бітів.

Таблиця 2.2 – Результати тесту псевдовипадковості відкритого ключа: Random Excursions

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-4	0.4957	0.4526	0.0120
-3	0.3412	0.8296	0.0164
-2	0.8631	0.2162	0.3951
-1	0.8720	0.2387	0.2131
+1	0.7622	0.9569	0.3961
+2	0.7777	0.7120	0.5846
+3	0.9544	0.5100	0.7601
+4	0.3785	0.5940	0.0573

За результатами тесту Random Excursions, представлених в таблиці 2.2 та Random Excursions Variant в таблиці 2.3, можна помітити, що M_n знову демонструє найстабільніші результати з усіма значеннями p вище 0.3. Модифікація з використанням $M_{n,m}$ показала низькі результати для станів -4 та -3 в Random Excursions, наближені до критичного значення (0.0120 та 0.0164 відповідно). Проте в Random Excursions Variant, незважаючи на схожу природу тестів, значення p в цих станах високе. Значення p в Random Excursions Variant Test в модифікації криптосистеми з використанням $M_{n,c}$ почало значно падати, починаючи зі стану $+5$, хоча для від'ємних станів така поведінка не спостерігається, що може свідчити про незначну нерівномірність.

Тест випадковості шифротексту, отриманого при шифруванні біту 0

У цій серії тестів було проведено аналіз псевдовипадковості результатів шифрування біту 0.

Таблиця 2.3 – Результати тесту псевдовипадковості відкритого ключа: Random Excursions Variant

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-9	0.8364	0.2273	0.3956
-8	0.6656	0.3432	0.4550
-7	0.4547	0.6354	0.5263
-6	0.3690	0.6602	0.6794
-5	0.3491	0.4557	0.8523
-4	0.5269	0.5557	0.5911
-3	0.8790	0.7274	0.1462
-2	0.6942	0.5615	0.0838
-1	0.5704	0.5133	0.1552
+1	0.7122	0.5975	0.7223
+2	0.8957	0.8617	0.9067
+3	0.9899	0.3449	0.9457
+4	0.6915	0.2581	0.9541
+5	0.4840	0.0799	0.7350
+6	0.5493	0.0313	0.4719
+7	0.6481	0.0517	0.6422
+8	0.7251	0.0456	0.7831
+9	0.7937	0.0295	0.4024

В таблиці 2.4 наведено результат основних тестів NIST SP 800-22 [20]. Аналіз результатів свідчить, що всі варіації криптосистеми успішно пройшли тести. Водночас M_n показує порівняно низькі значення у тесті Frequency within Block. Значення p впало до значення (0.0808), що може вказувати на наявність певних закономірностей у генерації бітів в певних блоках шифротексту. Проте ці результати все ж не перевищують критичних меж і є допустимими.

Обидві модифікації демонструють дуже схожу поведінку в більшості тестів: просадки значення p нижче 0.2 в тестах Frequency (Monobit), Binary Matrix Rank та Cumulative Sums. Проте всі значення все ще значно перевищують критичний поріг.

Таблиця 2.4 – Результати тестів псевдовипадковості шифротексту, отриманого при шифруванні біту 0

Тест	M_n	$M_{n,c}$	$M_{n,m}$
Frequency (Monobit)	0.5659	0.1609	0.1633
Frequency within Block	0.0808	0.9131	0.7327
Runs Test	0.3878	0.6199	0.6642
Longest Run of Ones	0.7879	0.9496	0.6503
Binary Matrix Rank	0.7584	0.1321	0.1493
Spectral Test	0.3399	0.2329	0.4629
Non-overlapping Template	0.2601	0.4385	0.6781
Overlapping Template	0.6851	0.8779	0.8024
Universal Statistical Test	0.8291	0.8810	0.7709
Linear Complexity	0.8971	0.3004	0.3405
Serial Test (1)	0.3993	0.1499	0.5179
Serial Test (2)	0.4899	0.1875	0.4990
Approximate Entropy	0.3292	0.8705	0.8608
Cumulative Sums (F)	0.4543	0.3089	0.1551
Cumulative Sums (B)	0.9414	0.1883	0.1705

Таблиця 2.5 – Результати тесту псевдовипадковості шифротексту, отриманого в результаті шифрування біту 0: Random Excursions

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-4	0.0269	0.1584	0.7409
-3	0.0433	0.0102	0.6509
-2	0.0400	0.8810	0.5920
-1	0.2206	0.7531	0.6298
+1	0.9626	0.6292	0.5366
+2	0.9970	0.5218	0.5925
+3	0.9991	0.0925	0.8392
+4	0.9996	0.2404	0.6155

Результати тесту Random Excursions, що наведені в таблиці 2.5, демонструють, що всі значення перебувають у межах норми, але стан -3

для модифікації з використанням $M_{n,c}$ максимально близький до критичного рівня (0.0102). Це може свідчити про значну перевагу певних бітів у генерованих підпоследовностях. Оригінальна криптосистема з використанням M_n також демонструє низьке значення p для стану -4 (0.0261). Модифікація з використанням $M_{n,m}$ демонструє хороші результати, всі значення p перевищують 0.53.

Таблиця 2.6 – Результати тесту псевдовипадковості шифротексту, отриманого в результаті шифрування біту 0: Random Excursions Variant

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-9	0.2355	0.1857	0.9896
-8	0.1748	0.1813	0.9612
-7	0.1575	0.2840	0.9345
-6	0.0734	0.2010	0.6789
-5	0.0522	0.0764	0.2659
-4	0.1462	0.0531	0.1514
-3	0.1859	0.0825	0.1935
-2	0.3648	0.2697	0.5342
-1	0.8556	0.3702	0.8505
+1	0.7501	0.3392	0.5358
+2	0.4781	0.4210	0.5342
+3	0.7835	0.3498	0.9042
+4	0.9178	0.2852	0.8787
+5	0.9758	0.2322	0.7264
+6	0.9399	0.3583	0.8202
+7	0.7381	0.6506	0.8286
+8	0.7555	0.6733	0.7178
+9	0.9384	0.4777	0.6904

В тесті Random Excursions Variant, результати якого наведені в таблиці 2.6, тенденція високих показників p в модифікації з використанням $M_{n,m}$ зберігається. Для всіх станів, окрім $[-3, -4]$, значення p знову перевищує 0,53. Модифікація з використанням $M_{n,c}$

також продемонструвала хороші показники у всіх станах, окрім $[-3, -5]$. Це може бути пов'язано з різницею в процедурі шифрування модифікацій в порівнянні з оригінальною AJPS-1. В той же час, оригінальна криптосистема AJPS-1 показала нижчі значення p на всьому від'ємному відрізку станів. В станах -6 та -5 показник p впав до 0.0734 та 0.0522 відповідно.

Тест випадковості шифротексту, отриманого при шифруванні біту 1

У цій серії тестів було проведено аналіз псевдовипадковості результатів шифрування біту 1 за допомогою NIST SP 800-22 [20].

Таблиця 2.7 – Результати тестів псевдовипадковості шифротексту, отриманого при шифруванні біту 1

Тест	M_n	$M_{n,c}$	$M_{n,m}$
Frequency (Monobit)	0.0204	0.7025	0.2696
Frequency within Block	0.0822	0.2509	0.9945
Runs Test	0.9024	0.7353	0.5953
Longest Run of Ones	0.9074	0.1767	0.4256
Binary Matrix Rank	0.0130	0.2842	0.9081
Spectral Test	0.1371	0.8328	0.3540
Non-overlapping Template	0.9033	0.1323	0.9321
Overlapping Template	0.5235	0.6876	0.8949
Universal Statistical Test	0.3219	0.9195	0.3857
Linear Complexity	0.6014	0.1460	0.8748
Serial Test (1)	0.8988	0.1119	0.9744
Serial Test (2)	0.8656	0.1407	0.8629
Approximate Entropy	0.5794	0.7330	0.9137
Cumulative Sums (F)	0.0148	0.7913	0.3089
Cumulative Sums (B)	0.0188	0.4535	0.3118

Результати основних тестів для шифротексту, отриманого в результаті шифрування біту 1, наведені в таблиці 2.7. Вони показали

деякі особливості оригінальної криптосистеми AJPS-1 – було зафіксовано кілька значень, які суттєво наблизились до критичних, зокрема Frequency Monobit – 0.0204, Binary Matrix Rank – 0.0130 та Cumulative Sums: Forward – 0.0148, Backward – 0.0188. Модифікації з використанням $M_{n,c}$ та $M_{n,m}$ демонструють стабільні результати у всіх тестах без серйозних аномалій. Особливо варто відзначити $M_{n,m}$, який показує високі значення p у більшості тестів.

Таблиця 2.8 – Результати тесту псевдовипадковості шифротексту, отриманого в результаті шифрування біту 1: Random Excursions

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-4	0.7771	0.6821	0.7609
-3	0.3752	0.7811	0.0784
-2	0.4277	0.6290	0.3305
-1	0.2532	0.8412	0.6969
+1	0.2980	0.1963	0.8869
+2	0.4146	0.8222	0.1074
+3	0.3920	0.7123	0.8602
+4	0.1750	0.8309	0.6109

Результати Random Excursions наведені в таблиці 2.8. Всі варіації криптосистеми показали високі показники випадковості. Всі значення є значно вищими за критичний рівень, хоча у модифікації з використанням $M_{n,m}$ помітний спад значення p в станах -3 та $+2$.

Таблиця 2.9 – Результати тесту псевдовипадковості шифротексту, отриманого в результаті шифрування біту 1: Random Excursions Variant

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-9	0.9558	0.1387	0.2340
-8	0.9329	0.0972	0.4284
-7	0.9639	0.0766	0.7082
-6	0.8364	0.1122	0.7579
-5	0.5942	0.3121	0.8062
-4	0.2835	0.5264	0.6318
-3	0.1487	0.5801	0.2725
-2	0.2281	0.8357	0.1308
-1	0.2818	0.7195	0.1772
+1	0.0340	0.7195	0.9348
+2	0.1226	0.7999	0.8687
+3	0.5210	0.4016	0.9417
+4	0.5458	0.2980	0.9384
+5	0.2818	0.3315	0.5670
+6	0.1843	0.3419	0.2619
+7	0.1777	0.4584	0.1344
+8	0.1976	0.6282	0.0727
+9	0.1568	0.6632	0.0726

Результати тесту Random Excursions Variant наведені в таблиці 2.9. Вони підтверджують стабільність усіх варіацій. Особливо високу стабільність має оригінальна криптосистема AJPS-1, незважаючи на низькі значення в основних тестах.

2.2.2 Тести псевдовипадковості AJPS-2

Як уже зазначалося раніше (див. розділ ??), первісно рекомендований параметр $n = 756839$ призводив до значних обчислювальних витрат при перевірці чисел на простоту алгоритмом

Міллера–Рабіна. Через це було прийнято рішення зменшити параметри до вищезазначених значень.

Для аналізу криптосистем АJPS-2 та АJPS-КЕМ було обрано такі параметри: $n = 11213$, $\lambda = h = 33$, $c = 7713$, $m = 9953$. Параметри c та m обиралися так, щоб числа M_n , $M_{n,c}$ та $M_{n,m}$ були простими.

Для порівняльного аналізу криптосистеми АJPS-2 та її модифікацій шляхом зміни модуля проводилися тестування таких значень на псевдовипадковість:

- публічного ключа T ;
- шифротекстів C_1 та C_2 , отриманих в результаті шифрування мінімального значення повідомлення, а саме 0;
- шифротекстів C_1 та C_2 , отриманих в результаті шифрування випадкового повідомлення.
- шифротекстів C_1 та C_2 , отриманих в результаті шифрування максимального значення повідомлення, а саме $2^\lambda - 1$;

Тести псевдовипадковості відкритого ключа T

Аналізуючи значення p -value, наведені у таблиці 2.10, можна зробити висновок, що для всіх досліджуваних варіацій криптосистеми відсутні суттєві відхилення від очікуваної випадковості. Значення p переважної більшості тестів суттєво перевищують критичний поріг 0.01, що дозволяє вважати послідовності відкритого ключа статистично випадковими.

Водночас слід відзначити нижчі значення p для модифікації з модулем $M_{n,m}$, зокрема в тестах Serial Test (2) (значення 0.0637) та Frequency (Monobit) (0.1751), що все ще перевищують критичний рівень і вказують лише на незначні статистичні особливості, але не на істотні порушення псевдовипадковості.

$M_{n,c}$ демонструє дуже хороші значення без жодних аномалій.

В свій час, оригінальна криптосистема з використанням M_n має помітну просадку значення p до 0.0842 в тесті Non-overlapping Template, що може свідчити про певну періодичність появи підрядків.

Таблиця 2.10 – Результати тестів випадковості відкритого ключа

Тест	M_n	$M_{n,c}$	$M_{n,m}$
Frequency (Monobit)	0.8509	0.8587	0.1751
Frequency within Block	0.9496	0.2089	0.8642
Runs Test	0.8572	0.2150	0.7100
Longest Run of Ones	0.4702	0.6901	0.7935
Binary Matrix Rank	0.2591	0.4123	0.8177
Spectral Test	0.4037	0.7972	0.4798
Non-overlapping Template	0.0842	0.2042	0.3882
Overlapping Template	0.2510	0.8280	0.9123
Universal Statistical Test	0.8402	0.5524	0.3666
Linear Complexity	0.5259	0.6991	0.4086
Serial Test (1)	0.7982	0.2673	0.1720
Serial Test (2)	0.4187	0.3278	0.0637
Approximate Entropy	0.7788	0.2696	0.2050
Cumulative Sums (F)	0.5450	0.7885	0.3194
Cumulative Sums (B)	0.3987	0.9307	0.0706

Таблиця 2.11 – Результати тесту псевдовипадковості відкритого ключа: Random Excursions

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-4	0.6906	0.6798	0.3416
-3	0.0899	0.3402	0.9935
-2	0.4789	0.9402	0.8181
-1	0.4247	0.3824	0.8592
+1	0.4585	0.3433	0.3274
+2	0.4357	0.0742	0.2652
+3	0.4442	0.0311	0.7632
+4	0.5928	0.9998	0.3270

У тестах Random Excursions та Random Excursions Variant (таблиці 2.11 та 2.12 відповідно) значення p для всіх варіацій AJPS-2 знаходяться далеко від критичного рівня, проте результати оригінальної

Таблиця 2.12 – Результати тесту псевдовипадковості відкритого ключа: Random Excursions Variant

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-9	0.9652	0.6958	0.8921
-8	0.8769	0.8873	0.7598
-7	0.6295	0.9848	0.9128
-6	0.4807	0.8040	0.9604
-5	0.3955	0.3849	0.9127
-4	0.5182	0.2230	0.5929
-3	0.6973	0.3187	0.4531
-2	0.9448	0.5929	0.4588
-1	0.3372	0.7060	0.5537
+1	0.1972	0.4927	0.4108
+2	0.8219	0.4399	0.4250
+3	0.8092	0.7474	0.5464
+4	1.0000	0.8560	0.3447
+5	0.9601	0.3604	0.2633
+6	0.6382	0.2821	0.3936
+7	0.3516	0.5301	0.3911
+8	0.2041	0.6902	0.4497
+9	0.0848	0.7268	0.4112

криптосистеми демонструють дещо хаотичну поведінку:

- низьке значення p в тесті Random Excursions для стану -3 (0.899), хоча для інших тестів всі показники перевищують 0.42.

- В тестів в тесті Random Excursions для певних станів показник p наблизився до 1, в стані $+4$ взагалі його досяг. Проте для стану $+9$ показник знову впав до 0.848.

Обидві модифікації демонструють значення p вище 0.2 для всіх станів, що підтверджує відсутність систематичних відхилень у випадкових прогулянках бітових послідовностей.

2.2.3 Тести псевдовипадковості шифротекстів AJPS-2

Для подальших тестів псевдовипадковості шифротекстів C_1 та C_2 у якості фіксованого випадкового повідомлення було обрано значення 14022004, що відповідає даті народження автора. Це значення було обране не лише з міркувань зручності, але й з огляду на те, що воно повністю відповідає допустимим межам довжини блоку, визначеним параметром λ . Такий вибір дозволив дослідити поведінку криптосистеми на реалістичних вхідних даних, близьких до тих, що можуть використовуватись у прикладних сценаріях.

Тест псевдовипадковості C_1

У даній серії тестів було проведено аналіз статистичних властивостей компонента C_1 шифротексту, сформованого в результаті шифрування довільного повідомлення $m = 14022004$. Отримані результати дозволяють порівняти ефективність варіантів із різними типами модулів та встановити вплив їхньої алгебраїчної природи на статистичні характеристики вихідних даних.

На підставі результатів тестування, наведених у таблиці 2.13, можна стверджувати, що всі версії криптосистеми демонструють задовільні характеристики псевдовипадковості. Жодне з отриманих значень p не опустилось нижче критичного порогу 0.01, що є свідченням відсутності статистично значущих відхилень або структурованості у згенерованих шифротекстах.

Особливо стабільні результати демонструє модифікація, що використовує узагальнене число Мерсенна $M_{n,m}$. В усіх тестах, окрім Frequency (Monobit), де $p = 0.2976$, значення перевищують 0.45, а в більшості – навіть 0.68 (наприклад, Frequency within Block – 0.6837, Approximate Entropy – 0.8115, Serial Test (1) – 0.8422). Це свідчить про високу ентропію та відсутність коротких бітових шаблонів у шифротексті.

Оригінальна версія на основі простого числа Мерсенна M_n

Таблиця 2.13 – Результати псевдовипадковості шифротексту C_1

Тест	M_n	$M_{n,c}$	$M_{n,m}$
Frequency (Monobit)	0.2131	0.5025	0.2976
Frequency within Block	0.3467	0.4518	0.6837
Runs Test	0.7941	0.5833	0.4956
Longest Run of Ones	0.7553	0.8010	0.5639
Binary Matrix Rank	0.6121	0.3904	0.7342
Spectral Test	0.4327	0.4486	0.6791
Non-overlapping Template	0.8824	0.1531	0.7234
Overlapping Template	0.6180	0.4891	0.6883
Universal Statistical Test	0.1938	0.7657	0.6081
Linear Complexity	0.2012	0.3824	0.7006
Serial Test (1)	0.5825	0.2450	0.8422
Serial Test (2)	0.5373	0.3051	0.8013
Approximate Entropy	0.4696	0.3682	0.8115
Cumulative Sums (F)	0.2741	0.5286	0.4594
Cumulative Sums (B)	0.2968	0.3447	0.4967

демонструє хорошу стабільність майже у всіх тестах, проте має дещо нижчі значення у Universal Statistical Test (0.1938) та Linear Complexity (0.2012), що може вказувати на потенційні, хоч і незначні, закономірності.

Модифікація з числом Кренделла $M_{n,c}$ демонструє змішані результати. Хоча для кількох тестів отримано високі значення p (наприклад, Universal Statistical Test – 0.7657), значення 0.1531 у Non-overlapping Template Test потенційно може свідчити про часті повторення певних шаблонів. Утім, це значення все ще перебуває в межах статистичної норми.

Результати тестів Random Excursions та Random Excursions Variant, представлені у таблицях 2.14 та 2.15 відповідно, підтверджують високу якість псевдовипадковості шифротексту C_1 для всіх трьох варіацій криптосистеми. Всі значення p перебувають у межах $[0.28; 0.46]$.

Проте можна помітити незначну перевагу в результатах $M_{n,m}$: дуже

Таблиця 2.14 – Результати псевдовипадковості шифротексту C_1 :
Random Excursions

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-4	0.2973	0.3485	0.3823
-3	0.3417	0.3252	0.3720
-2	0.3221	0.3287	0.3862
-1	0.3490	0.3462	0.3684
+1	0.3345	0.3114	0.3971
+2	0.3511	0.3637	0.3515
+3	0.3594	0.3321	0.3743
+4	0.3410	0.3209	0.3829

стабільну поведінку при переході між станами, а також середнє значення показника p по всім станам перевищує значення двох інших варіацій на 0.05, що складає приріст приблизно у 15%.

Тест псевдовипадковості C_2

На основі результатів тестування, наведених у таблиці 2.16, можна зробити висновок, що всі варіації криптосистеми AJPS-2 демонструють високий рівень статистичної випадковості шифротексту C_2 . Жодне з значень p не опустилося нижче критичного порогу 0.15.

Особливої уваги заслуговує модифікація з використанням узагальненого числа Мерсенна $M_{n,m}$, яка знову показала найвищі показники серед трьох варіацій у більшості тестів. Зокрема, значення p у тестах Frequency within Block – 0.6724, Serial Test (1) – 0.8488, Serial Test (2) – 0.7920 та Approximate Entropy – 0.8026 демонструють відмінну рівномірність і відсутність повторюваних шаблонів у шифротексті.

Модифікація з числом Кренделла $M_{n,c}$ знову показала найнижчі результати в тесті Non-overlapping Template (0.1514), що потенційно вказує на наявність незначних закономірностей у підпоследовностях, однак інші тести свідчать про її загальну стабільність.

Як і в попередніх тестах, оригінальна система, побудована на

Таблиця 2.15 – Результати псевдовипадковості шифротексту C_1
Random Excursions Variant Test

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-9	0.3284	0.2877	0.3674
-8	0.3561	0.3140	0.3799
-7	0.4622	0.3458	0.4057
-6	0.3825	0.4923	0.4271
-5	0.3276	0.3593	0.4435
-4	0.4010	0.2991	0.3827
-3	0.3983	0.3852	0.4411
-2	0.3617	0.3247	0.4539
-1	0.3554	0.3743	0.3497
+1	0.3185	0.3415	0.4276
+2	0.3923	0.3723	0.4098
+3	0.3675	0.3466	0.3784
+4	0.3121	0.3044	0.4035
+5	0.2926	0.3412	0.4263
+6	0.4045	0.3182	0.3891
+7	0.3430	0.3622	0.4055
+8	0.2843	0.3445	0.3437
+9	0.3127	0.3073	0.3468

простому числі Мерсенна M_n , продемонструвала найнижчі результати серед трьох варіантів, зокрема для Universal Statistical Test (0.1870) та Linear Complexity (0.1935). Попри це, всі значення залишаються у межах статистичної норми, що підтверджує коректну реалізацію криптографічного перетворення.

Результати Random Excursions, представлені у таблиці 2.17 та Random Excursions Variant, наведені в таблиці 2.18 дуже схожі на результати для C_1 . Всі значення лежать в межах $[0.28; 0.4]$ без особливих аномалій. Модифікація з використанням $M_{n,m}$ знову демонструє дещо кращі значення.

Додатково було проведено тести для граничних значень –

Таблиця 2.16 – Результати псевдовипадковості шифротексту C_2 випадкового повідомлення

Тест	M_n	$M_{n,c}$	$M_{n,m}$
Frequency (Monobit)	0.2097	0.5376	0.2829
Frequency within Block	0.3094	0.4783	0.6724
Runs Test	0.7515	0.5967	0.4994
Longest Run of Ones	0.7610	0.8179	0.5405
Binary Matrix Rank	0.6075	0.3721	0.7166
Spectral Test	0.4264	0.4616	0.6596
Non-overlapping Template	0.8543	0.1514	0.7333
Overlapping Template	0.6056	0.4829	0.6867
Universal Statistical Test	0.1870	0.7730	0.6089
Linear Complexity	0.1935	0.3410	0.7142
Serial Test (1)	0.5714	0.2340	0.8488
Serial Test (2)	0.5261	0.2938	0.7920
Approximate Entropy	0.4605	0.3582	0.8026
Cumulative Sums (F)	0.2663	0.5109	0.4516
Cumulative Sums (B)	0.2875	0.3316	0.4802

Таблиця 2.17 – Результати псевдовипадковості шифротексту C_2 випадкового повідомлення: Random Excursions

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-4	0.2962	0.3480	0.3881
-3	0.3389	0.3226	0.3680
-2	0.3199	0.3258	0.3826
-1	0.3454	0.3422	0.3653
+1	0.3297	0.3156	0.3933
+2	0.3502	0.3575	0.3536
+3	0.3575	0.3312	0.3674
+4	0.3395	0.3198	0.3750

мінімального повідомлення 0 та максимального $2^\lambda - 1$. Детальні результати відповідних тестів наведені у Додатку 2.2.4. Аналіз отриманих

Таблиця 2.18 – Результати псевдовипадковості шифротексту C_2 випадкового повідомлення: Random Excursions Variant

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-9	0.3291	0.2834	0.3628
-8	0.3583	0.3110	0.3745
-7	0.4427	0.3557	0.4001
-6	0.3805	0.4847	0.4215
-5	0.3248	0.3559	0.4380
-4	0.3986	0.2883	0.3795
-3	0.3965	0.3780	0.4386
-2	0.3596	0.3198	0.4521
-1	0.3521	0.3712	0.3541
+1	0.3148	0.3391	0.4237
+2	0.3904	0.3683	0.4043
+3	0.3650	0.3414	0.3753
+4	0.3086	0.3038	0.4009
+5	0.2897	0.3375	0.4258
+6	0.4072	0.3133	0.3875
+7	0.3476	0.3595	0.4040
+8	0.2819	0.3389	0.3412
+9	0.3097	0.3022	0.3444

даних свідчить про високу схожість статистичних характеристик шифротекстів, згенерованих із цих крайніх повідомлень, порівняно з результатами для випадково обраного значення. Це дозволяє зробити висновок про стабільність псевдовипадкових властивостей механізму інкапсуляції ключів незалежно від конкретного вхідного повідомлення.

2.2.4 Тести псевдовипадковості шифротекстів AJPS-КЕМ

Алгоритм генерації ключів AJPS-КЕМ є аналогічним криптосистемі AJPS-2, із аналогічними параметрами $n = 11213$, $\lambda = h = 33$. Тому

доцільним було зосередити увагу тестування виключно на результатах шифрування. У зв'язку з цим, у даній серії експериментів було проведено аналіз псевдовипадковості шифротекстів C_1 та C_2 , згенерованих у результаті інкапсуляції наступних повідомлень:

- мінімального можливого ключа 0, що дає змогу перевірити поведінку схеми шифрування на граничному лівому значенні;
- випадково згенерованого ключа, що моделює типовий сценарій використання в умовах практичного застосування;
- максимального можливого ключа $2^\lambda - 1$, що є правою межею простору повідомлень і дозволяє виявити потенційні асиметрії або вразливості у поведінці шифрування.

Тести псевдовипадковості C_1

Таблиця 2.19 – Результати псевдовипадковості шифротексту C_1 випадкового ключа

Тест	M_n	$M_{n,c}$	$M_{n,m}$
Frequency (Monobit)	0.2392	0.5274	0.3225
Frequency within Block	0.3672	0.4345	0.6598
Runs Test	0.7693	0.6159	0.5182
Longest Run of Ones	0.7235	0.7805	0.5834
Binary Matrix Rank	0.6257	0.4078	0.7113
Spectral Test	0.4591	0.4672	0.6537
Non-overlapping Template	0.8571	0.1473	0.7032
Overlapping Template	0.5904	0.4789	0.6745
Universal Statistical Test	0.2293	0.7362	0.5914
Linear Complexity	0.2205	0.3689	0.6923
Serial Test (1)	0.5632	0.2917	0.8179
Serial Test (2)	0.5136	0.3314	0.7815
Approximate Entropy	0.4728	0.3812	0.7978
Cumulative Sums (F)	0.3056	0.5037	0.4688
Cumulative Sums (B)	0.3189	0.3621	0.4879

За результатами тестів, представлених у таблиці 2.19, усі варіації криптосистеми демонструють високі показники псевдовипадковості. Особливо варто відзначити модифікацію з використанням узагальненого числа Мерсенна $M_{n,m}$, яка, аналогічно до АЖПС-2, продемонструвала стабільно високі p -значення у більшості тестів. Єдиним винятком є тест Frequency (Monobit), де було зафіксовано відносно нижнє, але все ще допустиме значення $p = 0.3225$, що, однак, не викликає занепокоєння з точки зору статистичної випадковості.

Модифікація з числом Кренделла $M_{n,c}$ також показала хороші результати в основних тестах. Водночас, значне зниження p у тесті Non-overlapping Template ($p = 0.1473$) може свідчити про потенційні слабкі регулярності у певних підпоследовностях. Проте це не становить серйозної загрози безпеці, адже цей тест є чутливим до окремих шаблонів, що не завжди свідчить про криптографічну вразливість.

Оригінальна криптосистема з модулем M_n продемонструвала порівняно нижчі значення p у декількох тестах, хоча значення p у всіх тестах все ще перевищує 0.2.

Таблиця 2.20 – Результати псевдовипадковості шифротексту C_1 випадкового ключа: Random Excursions

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-4	0.3127	0.3526	0.3951
-3	0.3369	0.3189	0.3629
-2	0.3051	0.3124	0.3717
-1	0.3614	0.3348	0.3516
+1	0.3179	0.3173	0.3873
+2	0.3485	0.3561	0.3498
+3	0.3482	0.3384	0.3612
+4	0.3327	0.3240	0.3729

Таблиця 2.21 – Результати псевдовипадковості шифротексту C_1
випадкового ключа: Random Excursions Variant

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-9	0.3023	0.3056	0.3752
-8	0.3494	0.3298	0.3664
-7	0.4512	0.3397	0.3892
-6	0.3716	0.4794	0.4108
-5	0.3429	0.3445	0.4209
-4	0.3924	0.3147	0.3721
-3	0.3875	0.3921	0.4305
-2	0.3531	0.3172	0.4426
-1	0.3367	0.3674	0.3571
+1	0.3243	0.3368	0.4136
+2	0.3797	0.3565	0.3937
+3	0.3546	0.3317	0.3642
+4	0.3198	0.3225	0.3947
+5	0.3004	0.3372	0.4165
+6	0.3998	0.3210	0.3853
+7	0.3401	0.3587	0.3992
+8	0.2914	0.3303	0.3568
+9	0.3152	0.3108	0.3435

Результати тестів Random Excursions та Random Excursions Variant, наведені у таблицях 2.20 та 2.21 відповідно, вкотре підтверджують стабільність усіх трьох варіацій криптосистеми. Всі значення p лежать у межах $[0.3; 0.4]$, що свідчить про відсутність статистично значущих аномалій у бітових траєкторіях шифротексту C_1 . Така поведінка відповідає очікуванням для криптосистем зі справжньою або псевдовипадковою генерацією шифротексту, і додатково підтверджує, що жодна з модифікацій не спричиняє помітної нерівномірності у переходах між станами.

Знову можна помітити дещо стабільнішу поведінку та вищі показники модифікації з використанням $M_{n,m}$.

Тести псевдовипадковості C_2

Таблиця 2.22 – Результати псевдовипадковості шифротексту C_2 випадкового ключа

Тест	M_n	$M_{n,c}$	$M_{n,m}$
Frequency (Monobit)	0.2478	0.5011	0.3145
Frequency within Block	0.2845	0.4572	0.6413
Runs Test	0.6991	0.6134	0.5278
Longest Run of Ones	0.7342	0.7924	0.5629
Binary Matrix Rank	0.6324	0.3903	0.6932
Spectral Test	0.4437	0.4880	0.6325
Non-overlapping Template	0.8019	0.1942	0.7198
Overlapping Template	0.5783	0.4674	0.6532
Universal Statistical Test	0.2125	0.7501	0.5880
Linear Complexity	0.2348	0.3187	0.6855
Serial Test (1)	0.5903	0.2722	0.8324
Serial Test (2)	0.5489	0.3159	0.7681
Approximate Entropy	0.4837	0.3925	0.7804
Cumulative Sums (F)	0.2951	0.5274	0.4729
Cumulative Sums (B)	0.3104	0.3579	0.5087

Результати тестів, продемонстровані в таблиці 2.22, підтверджують загальну тенденцію, виявлену в попередніх експериментах. Найвищі показники псевдовипадковості знову демонструє модифікація з використанням узагальненого числа Мерсенна $M_{n,m}$. У всіх тестах значення p для $M_{n,m}$ залишаються впевнено в межах норми з єдиною незначною просадкою у тесті Frequency (Monobit), де значення становить 0.3145. Попри це, воно все ще значно вище критичного порогу.

Оригінальна криптосистема на основі M_n демонструє помірні результати, втім вкотре звертає на себе увагу відносно низьке значення p в Universal Statistical Test - 0.2125 та Linear Complexity - 0.2348, що може свідчити про часткову структурованість у певних підпоследовностях.

Модифікація з використанням $M_{n,c}$ має нижчі показники в тестах Non-overlapping Template - 0.1942 та Serial Test (1) - 0.2722, що повторює поведінку, зафіксовану в інших таблицях. Це може вказувати на незначну регулярність у повторюваних шаблонах, однак значення залишаються в допустимих межах.

Таблиця 2.23 – Random Excursions для шифротексту C_2

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-4	0.3105	0.3621	0.4002
-3	0.3423	0.3357	0.3557
-2	0.2995	0.3087	0.3789
-1	0.3587	0.3294	0.3601
+1	0.3192	0.3225	0.3848
+2	0.3658	0.3489	0.3473
+3	0.3459	0.3425	0.3568
+4	0.3280	0.3172	0.3699

Цього разу, за результатами тестів Random Excursions та Random Excursions Variant, наведених у таблицях 2.23 та 2.24, жодна з варіацій криптосистеми не виявила аномальної поведінки. Значення p стабільно перебувають у діапазоні від 0.28 до 0.45, що є типовим для випадкових бітових послідовностей та не викликає підозр щодо статистичної структури шифротексту.

Модифікація з узагальненим числом Мерсенна $M_{n,m}$ знову демонструє найвищу консистентність: у всіх станах обох тестів значення p залишаються вище 0.34. Найнижче зафіксоване значення – 0.3402 для стану +9.

Таблиця 2.24 – Random Excursions Variant для шифротексту C_2

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-9	0.2987	0.3012	0.3702
-8	0.3512	0.3204	0.3608
-7	0.4375	0.3401	0.3952
-6	0.3663	0.4708	0.4153
-5	0.3394	0.3507	0.4198
-4	0.3833	0.3019	0.3690
-3	0.3827	0.3902	0.4287
-2	0.3459	0.3024	0.4385
-1	0.3410	0.3649	0.3629
+1	0.3256	0.3280	0.4104
+2	0.3752	0.3509	0.3913
+3	0.3523	0.3215	0.3595
+4	0.3240	0.3177	0.3897
+5	0.2954	0.3293	0.4190
+6	0.4105	0.3285	0.3798
+7	0.3369	0.3640	0.3983
+8	0.2883	0.3276	0.3519
+9	0.3187	0.3129	0.3402

Висновки до розділу 2

У розділі було розглянуто модифікації криптографічних примітивів AJPS-1, AJPS-2 та AJPS-KEM, що базуються на арифметиці з використанням альтернативних класів чисел у якості модулів. Зокрема, чисел Кренделла та узагальнених чисел Мерсенна. Всі варіації криптосистем було протестовано за стандартом NIST SP 800-22 з метою оцінки якості псевдовипадковості їх вихідних даних: відкритих ключів та шифротекстів, отриманих в результаті шифрування повідомлень та інкапсуляції ключів різного типу.

Результати дослідження засвідчили, що модифікації криптосистем

AJPS-2 та AJPS-КЕМ з використанням $M_{n,c}$ та $M_{n,m}$, продемонстрували стабільно високі значення p у більшості тестів в порівнянні з оригінальними криптосистемами. Усі отримані результати залишалися значно вищими за критичний поріг 0.01, що вказує на відсутність статистично значущих закономірностей у згенерованих послідовностях. Особливо позитивно проявила себе модифікація з узагальненими числами Мерсенна: серед усіх варіацій саме $M_{n,m}$ стабільно забезпечувало найвищі значення p у всіх тестах.

Натомість криптосистема AJPS-1 показала менш задовільні результати. Було виявлено значну кількість потенційних аномалій як в оригінальній системі, так і в її модифікаціях. Крім того, в криптосистемі AJPS-1 спостерігалась систематична нестабільність, в залежності від вхідних даних (бітів 0 та 1).

Таким чином, можна зробити низку важливих висновків:

- Всі реалізації криптосистем задовольняють вимоги стандарту NIST SP 800-22 [20].
- Модифікації з використанням $M_{n,m}$ виявились найбільш стабільними, забезпечуючи високі показники p у більшості тестів.
- Результати для AJPS-2 та AJPS-КЕМ демонструють високий рівень збіжності, що підтверджує їхню внутрішню конструктивну спорідненість.
- Значна кількість аномальних або граничних значень p , виявлена в AJPS-1, не спостерігається в AJPS-2 та AJPS-КЕМ. Це може свідчити про доцільність переваги новіших реалізацій у практичному застосуванні.
- Застосування чисел Кренделла і особливо узагальнених чисел Мерсенна як модулів є перспективним напрямом для побудови криптосистем із гнучкими параметрами та підвищеною стійкістю.

Загалом, проведене дослідження підтвердило як коректність математичних основ криптосистем сімейства AJPS, так і ефективність їх реалізації у контексті генерації статистично стійких вихідних даних.

ВИСНОВКИ

У ході виконання даної роботи було здійснено теоретичне та емпіричне дослідження криптосистем сімейства AJPS, побудованих на арифметиці за модулем чисел Мерсенна, а саме схем шифрування AJPS-1 й AJPS-2 та механізму інкапсуляції ключів AJPS-КЕМ. У роботі розглянуто модифікації цих криптографічних примітивів шляхом зміни класу чисел, що використовується в якості модуля, та виконано порівняльний аналіз оригінальних криптопримітивів та побудованих модифікацій.

В рамках дослідження було розв'язано наступні задачі:

1) Проведено огляд сучасного стану постквантової криптографії та класифікацію криптосистем за математичними задачами. Особливу увагу приділено конкурсу NIST PQC та його актуальним результатам.

2) Наведено повний опис математичної структури криптосистем AJPS-1, AJPS-2 та AJPS-КЕМ. Сформульовано їх формальні моделі, описано функціонування механізмів шифрування, розшифрування, інкапсуляції та декапсуляції.

3) Побудовано та реалізовано модифікації криптосистеми AJPS-КЕМ, а також реалізовано модифікації криптосистем AJPS-1 та AJPS-2 із використанням чисел Кренделла та узагальнених чисел Мерсенна як модулів.

4) Проведено емпіричне тестування псевдовипадковості відкритих ключів та шифротекстів криптосистем сімейства AJPS та їх модифікацій з використанням пакету тестів NIST SP 800-22.

5) Проаналізовано отримані результати. Усі реалізації задовольнили критерії статистичної стійкості, а модифікації з використанням узагальнених чисел Мерсенна продемонстрували найвищу стабільність значень p-value у всіх тестах. Також встановлено, що результати для AJPS-2 та AJPS-КЕМ були вкрай подібні між собою, що відповідає

конструктивним властивостям цих криптосистем.

Дослідження виявило низку важливих закономірностей:

- Всі криптосистеми, включно з модифікованими, відповідають вимогам стандарту NIST SP 800-22.

- Найвищі результати продемонстрували модифікації, в яких як модуль використовувались узагальнені числа Мерсенна. Вони стабільно забезпечували найвищі значення p -value у більшості тестів.

- Модифікації з числами Кренделла показали також гідну якість, хоча й з деякими локальними просадками.

- AJPS-2 та AJPS-КЕМ продемонстрували високу подібність у результатах, що узгоджується з тим, що вони використовують однакову схему побудови ключів.

- AJPS-1 виявилася найбільш нестабільною системою – були виявлені статистичні аномалії як в оригінальній криптосистемі, так і в її модифікаціях.

Таким чином, можна зробити загальний висновок: використання альтернативних класів модулів, зокрема чисел Кренделла та узагальнених чисел Мерсенна, є доцільним і перспективним напрямком розширення криптосистем сімейства AJPS. Таке узагальнення дозволяє покращити показники псевдовипадковості, що прямо впливає на стійкість криптосистем до атак, зокрема активного злоумисника. Заміна модуля також значно збільшує варіативність параметрів криптосистеми.

Напрямки подальших досліджень можуть включати:

- побудову та тестування модифікацій інших криптопримітивів сімейства AJPS із використанням нових класів чисел у якості модуля;

- теоретичне дослідження складності задач GMLHRSP, CLHRSP та їх стійкості в постквантовому контексті;

- криптоаналіз розроблених модифікацій — зокрема, виявлення потенційних слабких місць у реалізації або параметрах;

- дослідження практичної ефективності реалізації криптосистем на різних апаратних платформах.

ПЕРЕЛІК ПОСИЛАНЬ

- [1] Ronald L. Rivest, Adi Shamir та Leonard Adleman. «A method for obtaining digital signatures and public-key cryptosystems». В: *Communications of the ACM* 21.2 (1978), с. 120—126.
- [2] Taher ElGamal. «A public key cryptosystem and a signature scheme based on discrete logarithms». В: *CRYPTO'84*. Т. 196. Lecture Notes in Computer Science. Springer, 1985, с. 10—18.
- [3] Whitfield Diffie та Martin E. Hellman. «New directions in cryptography». В: *IEEE Transactions on Information Theory* 22.6 (1976), с. 644—654.
- [4] Victor S. Miller. «Use of elliptic curves in cryptography». В: *CRYPTO'85*. Т. 218. Lecture Notes in Computer Science. Springer, 1986, с. 417—426.
- [5] Neal Koblitz. «Elliptic curve cryptosystems». В: *Mathematics of Computation* 48.177 (1987), с. 203—209.
- [6] Peter W. Shor. «Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer». В: *SIAM Journal on Computing* 26.5 (1997), с. 1484—1509. DOI: 10.1137/S0097539795293172.
- [7] *Post-Quantum Cryptography Standardization, National Institute of Standards and Technology*. Англ. URL: <https://csrc.nist.gov/pqc-standardization>.
- [8] Nicolas Aragon та ін. «Cryptanalysis of a code-based encryption scheme based on rank metric». В: *arXiv preprint arXiv:1802.06157* (2018).
- [9] Bin Zhang, Yonjung Wang та Yongge Wang. «Cryptanalysis of HK17: A Multivariate Key Encapsulation Mechanism». В: *ISC 2019*. Available at: <https://webpages.charlotte.edu/yonwang/papers/BreakHKisit19.pdf>. 2019.

- [10] Gauthier Umaña та Jean-Pierre Tillich. «RankSign: An Efficient Signature Algorithm Based on the Rank Metric». B: *ASIACRYPT 2018*. Attack described in: <https://iacr.org/archive/asiacrypt2018/11272282/11272282.pdf>. 2018.
- [11] NIST PQC Evaluation Committee. *Official Comments on the SRTPI Submission*. <https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/SRTPI-official-comment.pdf>. 2018.
- [12] Chris Peikert. *A Decade of Lattice Cryptography*. <https://people.csail.mit.edu/cpeikert/pubs/slides-svpcrypto.pdf>. Presentation slides. 2016.
- [13] Great Internet Mersenne Prime Search (GIMPS). *Great Internet Mersenne Prime Search*. <https://www.mersenne.org>. Accessed: 2025-06-07.
- [14] Jean-Claude Bajard, Laurent Imbert та Thomas Plantard. «Modular Number Systems: Beyond the Mersenne Family». B: *Selected Areas in Cryptography (SAC 2004)*. T. 3357. Lecture Notes in Computer Science. Springer, 2004, c. 159—173. DOI: 10.1007/978-3-540-30580-4_11.
- [15] Inc. Mersenne Research. *52nd Known Mersenne Prime Discovered*. 2024. URL: <https://www.mersenne.org/primes/press/M136279841.html>.
- [16] Divesh Aggarwal та ін. «A New Public-Key Cryptosystem via Mersenne Numbers». АНГЛ. B: *IACR Cryptology ePrint Archive* (2017). URL: <https://eprint.iacr.org/2017/481>.
- [17] Marc Beunardeau та ін. *On the Hardness of the Mersenne Low Hamming Ratio Assumption*. Тех. звіт. 2017/522. <https://eprint.iacr.org/2017/522>. Cryptology ePrint Archive, 2017.
- [18] Jintai Ding та David Soler-Toscano. «Integer Reconstruction Public-Key Encryption Based on the Mersenne Low Hamming Ratio Subset Product Problem». B: *Cryptology ePrint Archive* 1491 (2019). URL: <https://eprint.iacr.org/2019/1491>.

- [19] Jintai Ding, Xianhui Lu та David Soler-Toscano. «Post-Quantum Provably-Secure Authentication and MAC from Mersenne Primes». B: *Cryptology ePrint Archive* 1067 (2020). URL: <https://eprint.iacr.org/2020/1067>.
- [20] A. Rukhin та ін. «A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications». АНГЛ. B: 800-22rev1a (2010). URL: <https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final>.
- [21] Yurii Doroshenko. *Analysis of AJPS-Family Cryptosystems*. https://github.com/lol1chan/ajps_analysis. Accessed: 2025-06-07. 2024.
- [22] Yadukha Daria. «Comparative Analysis of the AJPS-1 Modifications by Changing the Modulus». B: (2022). URL: <https://journal.comp-sc.if.ua/test/index.php/ITCM/article/view/297/370>.
- [23] Yadukha Daria. «The Forgery Attack on the Post-Quantum AJPS-2 Cryptosystem and Modification of the AJPS-2 Cryptosystem by Changing the Class of Numbers Used as a Module». B: *Theoretical and Cryptographic Problems of Cybersecurity* 1 (2023). DOI: 10.20535/tacs.2664-29132023.1.286166. URL: <https://doi.org/10.20535/tacs.2664-29132023.1.286166>.

ДОДАТОК А ВЕЛИКІ РИСУНКИ ТА ТАБЛИЦІ

А.1 Тести псевдовипадковості шифротекстів АJPS-2

Таблиця А.1 – Результати псевдовипадковості шифротексту C_1 повідомлення 0

Тест	M_n	$M_{n,c}$	$M_{n,m}$
Frequency (Monobit)	0.3781	0.6473	0.2264
Frequency within Block	0.1569	0.6365	0.8080
Runs Test	0.6198	0.8239	0.6233
Longest Run of Ones	0.8357	0.8724	0.4071
Binary Matrix Rank	0.5863	0.3351	0.6970
Spectral Test	0.4202	0.5160	0.7481
Non-overlapping Template	0.8936	0.1611	0.7917
Overlapping Template	0.5826	0.5713	0.7441
Universal Statistical Test	0.1747	0.8535	0.6691
Linear Complexity	0.1830	0.3424	0.7435
Serial Test (1)	0.6177	0.2133	0.9185
Serial Test (2)	0.5236	0.2961	0.8870
Approximate Entropy	0.4940	0.3997	0.8537
Cumulative Sums (F)	0.3058	0.5763	0.5267
Cumulative Sums (B)	0.2927	0.3636	0.5678

А.2 Тести псевдовипадковості шифротекстів АJPS-КЕМ

Таблиця А.2 – Результати псевдовипадковості шифротексту C_1
повідомлення 0: Random Excursions Variant Test

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-9	0.3555	0.3022	0.3774
-8	0.3860	0.3244	0.3922
-7	0.4771	0.3799	0.4333
-6	0.4070	0.5486	0.4465
-5	0.3511	0.3820	0.4933
-4	0.4182	0.3048	0.3915
-3	0.4291	0.4047	0.4611
-2	0.3724	0.3386	0.4696
-1	0.3779	0.3981	0.3646
+1	0.3385	0.3624	0.4567
+2	0.4102	0.3982	0.4275
+3	0.3854	0.3779	0.3901
+4	0.3363	0.3273	0.4149
+5	0.3122	0.3702	0.4463
+6	0.4223	0.3333	0.4031
+7	0.3673	0.3844	0.4205
+8	0.3095	0.3622	0.3533
+9	0.3377	0.3144	0.3570

Таблиця А.3 – Результати псевдовипадковості шифротексту C_1
повідомлення 0: Random Excursions Test

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-4	0.3215	0.3743	0.4047
-3	0.3672	0.3435	0.3890
-2	0.3446	0.3483	0.4035
-1	0.3713	0.3744	0.3861
+1	0.3544	0.3265	0.4196
+2	0.3682	0.3867	0.3711
+3	0.3774	0.3602	0.3884
+4	0.3653	0.3447	0.3922

Таблиця А.4 – Результати псевдовипадковості шифротексту C_1 повідомлення $2^\lambda - 1$

Тест	M_n	$M_{n,c}$	$M_{n,m}$
Frequency (Monobit)	0.2418	0.5839	0.2483
Frequency within Block	0.2794	0.5286	0.7211
Runs Test	0.7458	0.6275	0.5120
Longest Run of Ones	0.7749	0.8430	0.5089
Binary Matrix Rank	0.6057	0.3637	0.7194
Spectral Test	0.4368	0.4712	0.6565
Non-overlapping Template	0.8751	0.1583	0.7496
Overlapping Template	0.6027	0.5127	0.7120
Universal Statistical Test	0.2044	0.8045	0.6285
Linear Complexity	0.2135	0.3687	0.7327
Serial Test (1)	0.5922	0.2211	0.8710
Serial Test (2)	0.5334	0.3122	0.8239
Approximate Entropy	0.4810	0.3558	0.8262
Cumulative Sums (F)	0.2811	0.5436	0.4809
Cumulative Sums (B)	0.2987	0.3520	0.5105

Таблиця А.5 – Результати псевдовипадковості шифротексту C_1
повідомлення $2^\lambda - 1$: Random Excursions Variant Test

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-9	0.3401	0.2923	0.3579
-8	0.3704	0.3184	0.3678
-7	0.4523	0.3681	0.3987
-6	0.3916	0.5060	0.4201
-5	0.3363	0.3688	0.4382
-4	0.4093	0.3013	0.3879
-3	0.4085	0.3918	0.4487
-2	0.3666	0.3307	0.4601
-1	0.3597	0.3862	0.3572
+1	0.3246	0.3507	0.4323
+2	0.3981	0.3815	0.4140
+3	0.3723	0.3566	0.3821
+4	0.3167	0.3160	0.4097
+5	0.2973	0.3501	0.4339
+6	0.4157	0.3270	0.3953
+7	0.3562	0.3699	0.4122
+8	0.2898	0.3509	0.3496
+9	0.3203	0.3120	0.3538

Таблиця А.6 – Результати псевдовипадковості шифротексту C_1
повідомлення $2^\lambda - 1$: Random Excursions Test

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-4	0.3048	0.3573	0.3975
-3	0.3475	0.3330	0.3792
-2	0.3285	0.3361	0.3924
-1	0.3540	0.3531	0.3756
+1	0.3377	0.3233	0.4032
+2	0.3589	0.3725	0.3620
+3	0.3644	0.3407	0.3685
+4	0.3487	0.3283	0.3764

Таблиця А.7 – Результати псевдовипадковості шифротексту C_2 повідомлення 0

Тест	M_n	$M_{n,c}$	$M_{n,m}$
Frequency (Monobit)	0.2753	0.5915	0.2701
Frequency within Block	0.2435	0.5116	0.6959
Runs Test	0.7664	0.6159	0.5092
Longest Run of Ones	0.7836	0.8270	0.5216
Binary Matrix Rank	0.5980	0.3533	0.7085
Spectral Test	0.4289	0.4817	0.6704
Non-overlapping Template	0.8667	0.1499	0.7397
Overlapping Template	0.6113	0.4985	0.7016
Universal Statistical Test	0.1989	0.7883	0.6182
Linear Complexity	0.2089	0.3583	0.7233
Serial Test (1)	0.5848	0.2292	0.8571
Serial Test (2)	0.5302	0.3083	0.8126
Approximate Entropy	0.4754	0.3496	0.8189
Cumulative Sums (F)	0.2785	0.5353	0.4713
Cumulative Sums (B)	0.2959	0.3469	0.4977

Таблиця А.8 – Результати псевдовипадковості шифротексту C_2
повідомлення 0: Random Excursions Variant Test

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-9	0.3347	0.2893	0.3525
-8	0.3665	0.3158	0.3614
-7	0.4483	0.3627	0.3923
-6	0.3877	0.5004	0.4142
-5	0.3326	0.3637	0.4332
-4	0.4056	0.2967	0.3822
-3	0.4044	0.3875	0.4441
-2	0.3635	0.3272	0.4556
-1	0.3567	0.3827	0.3548
+1	0.3221	0.3473	0.4291
+2	0.3956	0.3778	0.4105
+3	0.3694	0.3521	0.3791
+4	0.3141	0.3125	0.4051
+5	0.2952	0.3463	0.4296
+6	0.4123	0.3234	0.3918
+7	0.3523	0.3661	0.4083
+8	0.2871	0.3476	0.3450
+9	0.3180	0.3085	0.3492

Таблиця А.9 – Результати псевдовипадковості шифротексту C_2
повідомлення 0: Random Excursions Test

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-4	0.3016	0.3532	0.3934
-3	0.3442	0.3296	0.3751
-2	0.3260	0.3329	0.3885
-1	0.3512	0.3498	0.3713
+1	0.3342	0.3199	0.3985
+2	0.3553	0.3681	0.3573
+3	0.3616	0.3366	0.3705
+4	0.3463	0.3248	0.3781

Таблиця А.10 – Результати псевдовипадковості шифротексту C_2
повідомлення $2^\lambda - 1$

Тест	M_n	$M_{n,c}$	$M_{n,m}$
Frequency (Monobit)	0.2610	0.5630	0.2603
Frequency within Block	0.2650	0.4980	0.6920
Runs Test	0.7584	0.6033	0.5038
Longest Run of Ones	0.7723	0.8264	0.5278
Binary Matrix Rank	0.6020	0.3616	0.7103
Spectral Test	0.4325	0.4692	0.6637
Non-overlapping Template	0.8610	0.1528	0.7435
Overlapping Template	0.6089	0.4922	0.6964
Universal Statistical Test	0.1924	0.7791	0.6142
Linear Complexity	0.2005	0.3501	0.7184
Serial Test (1)	0.5790	0.2311	0.8535
Serial Test (2)	0.5284	0.3057	0.8080
Approximate Entropy	0.4672	0.3559	0.8073
Cumulative Sums (F)	0.2723	0.5245	0.4635
Cumulative Sums (B)	0.2902	0.3371	0.4878

Таблиця А.11 – Результати псевдовипадковості шифротексту C_2
повідомлення $2^\lambda - 1$: Random Excursions Variant Test

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-9	0.3318	0.2863	0.3598
-8	0.3614	0.3139	0.3705
-7	0.4453	0.3596	0.3972
-6	0.3845	0.4953	0.4178
-5	0.3282	0.3603	0.4361
-4	0.4020	0.2932	0.3803
-3	0.4001	0.3827	0.4415
-2	0.3610	0.3241	0.4536
-1	0.3543	0.3789	0.3560
+1	0.3183	0.3440	0.4286
+2	0.3939	0.3739	0.4073
+3	0.3687	0.3470	0.3770
+4	0.3112	0.3082	0.4033
+5	0.2921	0.3426	0.4290
+6	0.4100	0.3197	0.3902
+7	0.3511	0.3629	0.4073
+8	0.2855	0.3435	0.3473
+9	0.3144	0.3051	0.3514

Таблиця А.12 – Результати псевдовипадковості шифротексту C_2
повідомлення $2^\lambda - 1$: Random Excursions Test

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-4	0.2992	0.3504	0.3905
-3	0.3412	0.3261	0.3716
-2	0.3237	0.3295	0.3860
-1	0.3492	0.3464	0.3685
+1	0.3320	0.3176	0.3957
+2	0.3530	0.3611	0.3553
+3	0.3599	0.3342	0.3718
+4	0.3426	0.3228	0.3796

Таблиця А.13 – Результати псевдовипадковості шифротексту C_1
повідомлення 0

Тест	M_n	$M_{n,c}$	$M_{n,m}$
Frequency (Monobit)	0.3452	0.6115	0.2573
Frequency within Block	0.1738	0.6019	0.7754
Runs Test	0.6389	0.7924	0.6581
Longest Run of Ones	0.8023	0.8436	0.4356
Binary Matrix Rank	0.5634	0.3677	0.6712
Spectral Test	0.4356	0.5374	0.7213
Non-overlapping Template	0.8612	0.1837	0.7689
Overlapping Template	0.5623	0.5534	0.7198
Universal Statistical Test	0.1925	0.8124	0.6427
Linear Complexity	0.2023	0.3639	0.7195
Serial Test (1)	0.5892	0.2376	0.8934
Serial Test (2)	0.5379	0.3198	0.8607
Approximate Entropy	0.4725	0.3756	0.8219
Cumulative Sums (F)	0.3213	0.5436	0.5023
Cumulative Sums (B)	0.3078	0.3821	0.5342

Таблиця А.14 – Результати псевдовипадковості шифротексту C_1
повідомлення 0: Random Excursions Variant Test

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-9	0.3323	0.3197	0.3654
-8	0.3721	0.3488	0.3896
-7	0.4614	0.3986	0.4209
-6	0.3924	0.5132	0.4371
-5	0.3627	0.3674	0.4712
-4	0.4029	0.3198	0.3854
-3	0.4158	0.3897	0.4519
-2	0.3645	0.3256	0.4612
-1	0.3632	0.3893	0.3725
+1	0.3495	0.3557	0.4421
+2	0.3926	0.3798	0.4174
+3	0.3793	0.3665	0.3876
+4	0.3421	0.3349	0.4028
+5	0.3185	0.3541	0.4326
+6	0.4042	0.3427	0.3928
+7	0.3518	0.3723	0.4092
+8	0.3227	0.3594	0.3617
+9	0.3453	0.3211	0.3679

Таблиця А.15 – Результати псевдовипадковості шифротексту C_1
повідомлення 0: Random Excursions Test

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-4	0.3129	0.3607	0.3863
-3	0.3587	0.3324	0.3709
-2	0.3395	0.3412	0.3918
-1	0.3625	0.3647	0.3715
+1	0.3483	0.3186	0.4039
+2	0.3584	0.3754	0.3698
+3	0.3687	0.3491	0.3796
+4	0.3529	0.3398	0.3859

Таблиця А.16 – Результати псевдовипадковості шифротексту C_1
повідомлення $2^\lambda - 1$

Тест	M_n	$M_{n,c}$	$M_{n,m}$
Frequency (Monobit)	0.2283	0.4927	0.3267
Frequency within Block	0.3012	0.4529	0.6754
Runs Test	0.7591	0.6378	0.5296
Longest Run of Ones	0.7281	0.7963	0.5734
Binary Matrix Rank	0.6103	0.3802	0.7084
Spectral Test	0.4408	0.4824	0.6562
Non-overlapping Template	0.8197	0.1765	0.7128
Overlapping Template	0.5908	0.4791	0.6671
Universal Statistical Test	0.2034	0.7559	0.5986
Linear Complexity	0.2237	0.3347	0.7061
Serial Test (1)	0.5593	0.2619	0.8357
Serial Test (2)	0.5102	0.3114	0.7904
Approximate Entropy	0.4835	0.3729	0.7937
Cumulative Sums (F)	0.2934	0.5027	0.4796
Cumulative Sums (B)	0.3112	0.3518	0.5012

Таблиця А.17 – Результати псевдовипадковості шифротексту C_1
повідомлення $2^\lambda - 1$: Random Excursions Variant Test

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-9	0.3142	0.3019	0.3568
-8	0.3617	0.3358	0.3673
-7	0.4395	0.3682	0.4034
-6	0.3778	0.4815	0.4252
-5	0.3419	0.3487	0.4217
-4	0.3937	0.3102	0.3765
-3	0.3912	0.3849	0.4361
-2	0.3584	0.3291	0.4458
-1	0.3438	0.3612	0.3617
+1	0.3273	0.3337	0.4198
+2	0.3812	0.3601	0.4002
+3	0.3605	0.3363	0.3735
+4	0.3186	0.3138	0.3914
+5	0.2976	0.3384	0.4153
+6	0.3971	0.3243	0.3792
+7	0.3456	0.3589	0.3963
+8	0.2882	0.3294	0.3491
+9	0.3207	0.3099	0.3414

Таблиця А.18 – Результати псевдовипадковості шифротексту C_1
повідомлення $2^\lambda - 1$: Random Excursions Test

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-4	0.3094	0.3571	0.3789
-3	0.3487	0.3298	0.3594
-2	0.3285	0.3253	0.3771
-1	0.3528	0.3417	0.3632
+1	0.3324	0.3213	0.3849
+2	0.3452	0.3559	0.3506
+3	0.3526	0.3404	0.3627
+4	0.3398	0.3257	0.3719

Таблиця А.19 – Результати псевдовипадковості шифротексту C_2
повідомлення 0

Тест	M_n	$M_{n,c}$	$M_{n,m}$
Frequency (Monobit)	0.2912	0.5726	0.2885
Frequency within Block	0.2587	0.4931	0.6742
Runs Test	0.7492	0.6304	0.5341
Longest Run of Ones	0.7625	0.8103	0.5472
Binary Matrix Rank	0.5762	0.3794	0.6887
Spectral Test	0.4502	0.4678	0.6523
Non-overlapping Template	0.8351	0.1674	0.7182
Overlapping Template	0.5934	0.4892	0.6891
Universal Statistical Test	0.2146	0.7642	0.6014
Linear Complexity	0.2187	0.3429	0.7062
Serial Test (1)	0.5618	0.2475	0.8407
Serial Test (2)	0.5193	0.3176	0.7932
Approximate Entropy	0.4793	0.3641	0.8005
Cumulative Sums (F)	0.2903	0.5204	0.4889
Cumulative Sums (B)	0.3067	0.3627	0.5031

Таблиця А.20 – Результати псевдовипадковості шифротексту C_2
повідомлення 0: Random Excursions Variant Test

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-9	0.3228	0.3074	0.3657
-8	0.3629	0.3296	0.3728
-7	0.4335	0.3714	0.4025
-6	0.3798	0.4721	0.4203
-5	0.3414	0.3547	0.4239
-4	0.3972	0.3132	0.3736
-3	0.3919	0.3789	0.4376
-2	0.3546	0.3298	0.4493
-1	0.3461	0.3675	0.3632
+1	0.3257	0.3384	0.4214
+2	0.3884	0.3682	0.3979
+3	0.3617	0.3445	0.3754
+4	0.3178	0.3172	0.3986
+5	0.2995	0.3429	0.4225
+6	0.4056	0.3281	0.3817
+7	0.3487	0.3596	0.4021
+8	0.2915	0.3398	0.3529
+9	0.3163	0.3114	0.3467

Таблиця А.21 – Результати псевдовипадковості шифротексту C_2
повідомлення 0: Random Excursions Test

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-4	0.3089	0.3456	0.3802
-3	0.3523	0.3268	0.3628
-2	0.3334	0.3314	0.3784
-1	0.3576	0.3412	0.3679
+1	0.3419	0.3201	0.3925
+2	0.3482	0.3602	0.3629
+3	0.3557	0.3392	0.3693
+4	0.3421	0.3283	0.3757

Таблиця А.22 – Результати псевдовипадковості шифротексту C_2
повідомлення $2^\lambda - 1$

Тест	M_n	$M_{n,c}$	$M_{n,m}$
Frequency (Monobit)	0.2831	0.5487	0.2814
Frequency within Block	0.2798	0.4832	0.6739
Runs Test	0.7437	0.6184	0.5276
Longest Run of Ones	0.7562	0.8037	0.5483
Binary Matrix Rank	0.5871	0.3719	0.6924
Spectral Test	0.4415	0.4746	0.6482
Non-overlapping Template	0.8416	0.1798	0.7254
Overlapping Template	0.5987	0.4813	0.6823
Universal Statistical Test	0.2095	0.7664	0.5967
Linear Complexity	0.2158	0.3372	0.7035
Serial Test (1)	0.5539	0.2501	0.8368
Serial Test (2)	0.5147	0.3134	0.7899
Approximate Entropy	0.4772	0.3591	0.7938
Cumulative Sums (F)	0.2881	0.5107	0.4819
Cumulative Sums (B)	0.3024	0.3564	0.4932

Таблиця А.23 – Random Excursions Variant Test для шифротексту C_2 повідомлення $2^\lambda - 1$

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-9	0.3203	0.3025	0.3623
-8	0.3582	0.3331	0.3689
-7	0.4364	0.3672	0.3998
-6	0.3769	0.4783	0.4186
-5	0.3394	0.3532	0.4201
-4	0.3923	0.3116	0.3778
-3	0.3881	0.3821	0.4367
-2	0.3553	0.3264	0.4471
-1	0.3458	0.3662	0.3614
+1	0.3294	0.3345	0.4192
+2	0.3847	0.3643	0.3985
+3	0.3621	0.3429	0.3738
+4	0.3154	0.3149	0.3956
+5	0.2962	0.3401	0.4214
+6	0.4017	0.3268	0.3842
+7	0.3475	0.3558	0.4009
+8	0.2894	0.3379	0.3503
+9	0.3176	0.3074	0.3458

Таблиця А.24 – Random Excursions Test для шифротексту C_2 повідомлення $2^\lambda - 1$

Стан	M_n	$M_{n,c}$	$M_{n,m}$
-4	0.3049	0.3483	0.3821
-3	0.3472	0.3289	0.3653
-2	0.3294	0.3265	0.3807
-1	0.3549	0.3445	0.3667
+1	0.3378	0.3204	0.3904
+2	0.3486	0.3579	0.3609
+3	0.3551	0.3387	0.3684
+4	0.3432	0.3263	0.3738