УДК 004.056:004.032:004.9 **doi: 10.26906/SUNZ.2025.2.66-73**

Є. О. Живило[1], Ю. В. Кучма[2]

[1] Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна
[2] ТОВ ПВНЗ «Університет сучасних технологій», Київ, Україна

ПРАКТИЧНЕ ЗАСТОСУВАННЯ ТА ВРАЗЛИВОСТІ HILL CIPHER У СУЧАСНОМУ КОНТЕКСТІ

Анотація. У статті досліджується шифр Хілла (Hill cipher) як класичний приклад застосування лінійної алгебри та модульної арифметики в криптографії. Розкрито математичні основи алгоритму: формування ключової матриці над скінченими полями, умови його оберненості та реалізація шифрування у вигляді множення векторів відкритого тексту на ключову матрицю. Показано, що цей підхід є своєрідним «з'єднанням між теорією і практикою», оскільки поєднує саме математичні конструкції з реальними механізмами захисту даних. Особливу увагу приділено вразливостям Hill cipher. Встановлено, що алгоритм є нестійким у сучасних умовах через лінійність перетворень та відсутність нелінійних компонентів. Наведено приклади криптоаналітичних атак, які дозволяють «розколоти шифр» навіть при мінімальній кількості пар «відкритий текст – шифротекст». Це робить очевидним, що в системах кібербезпеки XXI століття Hill cipher є лише «тінню своєї епохи» та не може слугувати повноцінним інструментом захисту. Разом із тим, підкреслено освітню та методологічну цінність шифру. Він дозволяє «побачити механізм зсередини», наочно продемонструвавши перехід від моноалфавітних шифрів до блокових перетворень. Зроблено акцент на тому, що Hill cipher відіграв роль «першої сходинки» у розвитку структур, які згодом втілилися в DES та AES, де використання блокових структур і матричних операцій стало основою сучасної криптографії.

Ключові слова: кібербезпека, кіберзагрози, штучний інтелект, машинне навчання, криптографія, криптоаналіз, шифр.

Вступ

Постановка проблеми. Сучасна криптографія функціонує на перетині високоточної теоретичної математики та актуальних практичних завдань у сфері кібербезпеки. З одного боку, новітні алгоритми спираються на складні обчислювальні задачі, що перевищують можливості навіть високопродуктивних обчислювальних систем. З іншого боку, класичні шифри, зокрема шифр Хілла (Hill cipher), продовжують виконувати роль ілюстративного матеріалу, демонструючи еволюцію методів захисту даних.

Шифр Хілла був одним із перших алгоритмів, що продемонстрував практичне застосування лінійної алгебри в криптографії. Використання матричних перетворень над скінченними полями стало математичною інновацією свого часу та проклало шлях до розвитку блокових шифрів. Водночас сьогодні цей метод має критичну вразливість – повну лінійність, яка робить його вразливим до криптоаналізу на основі систем лінійних рівнянь: наявність лише кількох пар «відкритий текст – шифротекст» достатня для повного відновлення ключа.

Таким чином, перед науковою спільнотою постає суперечливе завдання. З одного боку, шифр Хілла «не витримує випробування часом» і непридатний для практичного застосування в умовах сучасних кіберзагроз. Водночас його математична елегантність і методологічна прозорість дають змогу відстежувати фундаментальні ідеї криптографії, аналізувати обмеження лінійних моделей та моделювати принципи блокових перетворень.

У цьому контексті проблема полягає у формуванні системного бачення ролі Hill cipher не як застарілого інструмента, а як наукового та освітнього майданчика, що дозволяє поєднати історичний досвід, математичний аналіз і сучасні криптографічні виклики.

Аналіз останніх досліджень і публікацій. Новітня криптографія розвивається на перетині теоретичної математики та практичних завдань кібербезпеки, де алгоритми шифрування мають поєднувати високу стійкість до кібератак із ефективною реалізацією на апаратних платформах з обмеженими ресурсами.

У цьому контексті блокові шифри, такі як GFSPX, розроблений Xing Zhang, Chenyang Shao, Changda Wang та іші, у 2024 році, демонструють застосування поєднання операцій XOR, перестановок та циклічних зсувів, що дозволяє досягати високої криптографічної стійкості на мікропроцесорних платформах, водночас зберігаючи низьке енергоспоживання [1]. Цей підхід свідчить про прагнення забезпечити баланс між безпекою та практичною реалізацією, особливо у вбудованих системах.

Еволюція блокових шифрів тісно пов'язана з постквантовою криптографією, яка набирає актуальності у зв'язку з розвитком квантових обчислювальних технологій. У серпні 2024 року Національний інститут стандартів і технологій США (NIST) опублікував федеральні стандарти FIPS 203, FIPS 204 та FIPS 205, які визначають алгоритми CRYSTALS-Kyber, CRYSTALS-Dilithium та SPHINCS+ як стандарти постквантової криптографії [2]. Ці алгоритми базуються на складних математичних задачах, зокрема задачах на решітках, і забезпечують стійкість до атак з використанням квантових комп'ютерів. Інтеграція таких алгоритмів у сучасні системи дозволяє не лише підвищити безпеку, але й закладає основу для подальших наукових досліджень у сфері квантової стійкості.

Разом із розвитком алгоритмів зростає і використання новітніх методів криптоаналізу. Значна увага приділяється застосуванню машинного навчання для виявлення вразливостей у блокових шифрах. Дослідження, проведене Джиммі Дені, Каляном Наккою та

Нітешем Саксеною у 2024 році, представило нову атакувальну платформу MIND-Crypt, яка використовує глибоке навчання та трансферне навчання для порушення індетифіковуваності блокових шифрів, зокрема SPECK32/64 у режимі CBC, при атаках з відомим відкритим текстом [3]. Результати показали, що модель глибокого навчання досягає точності близько 99% при постійних криптографічних умовах, що свідчить про потенціал використання машинного навчання для криптоаналізу. Поряд із цим, увага наукової спільноти зосереджена на легких криптографічних алгоритмах для вбудованих систем, таких як ASCON, розроблений у рамках ініціативи NIST з стандартизації легких криптографічних алгоритмів. ASCON використовує 320-бітну перестановку, поділену на п’ять 64-бітних регістрів, що забезпечує 128-бітний рівень безпеки [4]. Завдяки оптимізованим матричним перестановкам та компактним ключовим структурам, ці алгоритми дозволяють реалізувати ефективне шифрування на апаратних платформах FPGA та ASIC, що особливо важливо для IoT-пристроїв та медичних сенсорів. У цьому контексті поєднання блокових шифрів, постквантових алгоритмів та легких криптографічних методів створює інтегровану основу для сучасних захищених систем.

Незважаючи на значні досягнення, сучасні дослідження також вказують на існування критичних вразливостей у реалізації алгоритмів. Наприклад, дослідження, проведене у 2024 році, виявило вразливість до атак з вибраним шифротекстом у реалізації CRYSTALS-Kyber, що може призвести до витоку секретної інформації [5]. Це підкреслює необхідність ретельного тестування та вдосконалення як алгоритмічних, так і апаратних компонентів систем шифрування. Зазначене створює умови для безперервного циклу наукового вдосконалення, а саме, дослідження у сфері криптографії не лише породжують нові алгоритми, але й стимулюють розвиток методів криптоаналізу, що, у свою чергу, формує підґрунтя для наступного покоління захищених систем.

Таким чином, аналіз останніх наукових публікацій демонструє, що сучасна криптографія розвивається як інтеграція теоретичних та практичних підходів, де класичні та легкі алгоритми, блокові шифри та постквантові методи взаємодіють для забезпечення високого рівня безпеки інформаційно-комунікаційних систем у різних прикладних контекстах [6].

Метою роботи є комплексне дослідження шифру Хілла у сучасному криптографічному контексті з визначенням його практичних можливостей та обмежень, а також аналізом вразливостей, що виявляються під впливом сучасних методів криптоаналізу.

Дослідження спрямоване на детальне вивчення алгоритму, оцінку його теоретичної витонченості та ролі у розвитку блокових шифрів, а також на визначення перспектив використання Hill cipher як навчального й експериментального інструмента для моделювання принципів сучасної інформаційної безпеки.

Основний матеріал

Важливим аспектом дослідження є розуміння історичної ролі Hill cipher у формуванні концептуальних засад сучасної криптографії. Саме цей алгоритм уперше на практиці продемонстрував можливість застосування методів лінійної алгебри та матричних перетворень у процесі шифрування, заклавши підґрунтя для майбутнього розвитку блокових структур. Попри очевидні обмеження, зокрема повну лінійність і відсутність механізмів, здатних протидіяти диференційному чи лінійному криптоаналізу Hill cipher засвідчив потенціал переходу від простих моноалфавітних підстановок до складніших багатовимірних перетворень.

У подальшому ця ідея знайшла розвиток у класичних промислових стандартах криптографії – Data Encryption Standard (DES) та Advanced Encryption Standard (AES). У DES, затвердженому NIST у 1977 р., було реалізовано принцип блочного шифрування з багатораундовою структурою та використанням S-блоків для нелінійності, що істотно підвищило стійкість до атак. AES, який замінив DES на початку XXI століття, розвинув цей підхід, інтегрувавши більш складні матричні перетворення над скінченими полями $GF(2^8)$, включаючи операції ShiftRows, MixColumns і SubBytes. У цьому сенсі AES можна розглядати як логічне продовження ідей, започаткованих Hill cipher, але з урахуванням сучасних вимог до криптостійкості та ефективності реалізації.

Шифр Хілла заданий ключовою матрицею: $K \in Mat_{n\times n}\left(\mathbb{Z}_m\right)$ і дією:

$$C = KP\left(\mathrm{mod}\, m\right), \tag{1}$$

де стовпчикові вектори P та C відповідно відповідають блокам відкритого тексту й шифротексту розмірності n. Для коректності дешифрування необхідно, щоб матриця K була оберненою в $\mathbb{Z}_m$, тобто $\gcd\left(\det K, m\right) = 1$, що гарантує існування оберненої матриці

$$K^{-1} \in Mat_{n\times n}\left(\mathbb{Z}_m\right). \tag{2}$$

З одного боку, ця компактна лінійна структура становить методологічну перевагу алгоритму, оскільки дозволяє наочно продемонструвати зв’язок криптографії з лінійною алгеброю та модульною арифметикою. Вона робить Hill cipher зручним освітнім інструментом для моделювання базових принципів блокового шифрування [7].

З іншого боку, саме лінійність усіх перетворень над кільцем $\mathbb{Z}_m$ формує фундаментальну вразливість алгоритму. Будь-які відношення між векторами відкритого тексту P відображаються на шифротекст C через лінійне відображення. Це означає, що на практиці навіть обмежений набір пар «відкритий текст – шифротекст» може бути використаний для відновлення ключової матриці шляхом розв’язання системи лінійних рівнянь у $\mathbb{Z}_m$. Саме ця властивість робить Hill cipher криптографічно нестійким у сучасних умовах, незважаючи на його історичну значущість.

Отже, щоб конкретизувати механізми цієї вразливості й показати її практичні наслідки, нижче роз-

глянуто окремі сценарії криптоаналізу, зокрема атаки з обраним і відомим відкритим текстом, статистичні методи при наявності лише шифротексту та комбіновані підходи із застосуванням побічних каналів реалізації:

1. Атака з обраним відкритим текстом (chosen-plaintext, CPA).

У моделі CPA атакувальник має можливість запитувати шифрування довільних блоків $P \in \mathbb{Z}_m^n$ і отримувати відповідні шифротексти C. Для Hill cipher, заданого ключовою матрицею $K \in Mat_{n\times n}(\mathbb{Z}_m)$ та дією (1), найпряміша й найбільш ефективна стратегія полягає у поданні стандартних одиничних (базисних) векторів $e_1,...,e_n$, де e_i має одиницю на i-й позиції й нулі в інших координатах. Для кожного такого запиту справедлива рівність

$$C^{(i)} = Ke_i \left(\mathrm{mod}\, m\right), \tag{3}$$

тобто вектор $C^{(i)}$ є i-м стовпцем матриці K (в модульній арифметиці). Отже, збір відповідей на запити $e_1,...,e_n$ дає пряму реконструкцію всієї ключової матриці:

$$K = \left[C^{(1)}C^{(2)}...C^{n} \right] \left(\mathrm{mod}\, m\right). \tag{4}$$

Алгоритмічна і інформаційна оцінки:

– кількість запитів. Для повної компрометації необхідно не більше n запитів (подавання n базисних векторів).

– обчислювальна складність. Збирання n векторів розмірності n дає складність зберігання $O(n^2)$ елементів $\mathbb{Z}_m$; сама реконструкція ключа за наявності прямого доступу до стовпців – операція конкатенації, тобто $O(n^2)$ за примірною кількістю операцій над елементами кільця.

– інформаційний внесок одного запиту. Кожен запит з одиничним вектором e_i повертає вектор довжини n над $\mathbb{Z}_m$, тобто надає $n^2 \log_2 m$ бітів інформації про секретний ключ. У сумі n таких запитів дають $n^2 \log_2 m$ бітів, що узгоджується з розмірністю простору можливих ключів (приблизно $\log_2 \left|GL\left(n,\mathbb{Z}_m\right)\right|$).

Припустимо, що якщо атакувальник не може подавати довільні вектори, а лише вектори з обмеженого підмножини $S \subseteq \mathbb{Z}_m^n$, то атака ускладнюється, але залишається реалістичною за багатьох практичних умов. Нехай атакувальник подає послідовність випадково обраних векторів із S. Для успішної реконструкції необхідно зібрати n лінійно незалежних блоків $P_1,...,P_n$ (тобто, щоб матриця $P = \left[P_1...P_n\right]$ мала ранг n у $\mathbb{Z}_m$).

У випадку, коли $S = \mathbb{Z}_q^n$ для поля $\mathbb{Z}_q$ (тобто $m = q$ просте), ймовірність того, що t випадкових векторів матимуть ранг n, швидко прямує до 1 при $t \gtrsim n$; очікувана кількість запитів для отримання n незалежних векторів – $O(n)$ (з малою додатковою константою, що залежить від q).

Якщо S структурований (наприклад, лише вектори з обмеженим набором шаблонів або з фіксованими полями заголовків), може знадобитися значно більше запитів – у найгіршому випадку до нескінченності, якщо $span(S)$ має ранг $< n$. Тому при практичному аналізі важливо враховувати модель доступності запитів та статистику структурованих повідомлень (заголовків, форматів).

Отже, поєднання CPA із side-channel інформацією (таймінги, потужність, помилки) або з можливістю інжекції помилок (fault injection) скорочує потрібну кількість запитів і знижує вимоги до незалежності блоків. Наприклад, певні неточні відповіді або додаткові виміри можуть надати часткові лінійні відомості про стовпці K, що значно полегшує відновлення ключа в реалістичних сценаріях.

Розглядаючи практичні контрзаходи й рекомендації, слід підкреслити, що оскільки CPA є фатальною для шифру Хілла, при проєктуванні систем і проведенні навчальних демонстрацій необхідно впроваджувати наступні технічні та процедурні заходи:

1. Обмежити можливість довільного шифрування шляхом введення автентифікації клієнтів і обмеження API, щоб виключити сценарії довільних запитів.

2. Використовувати протокольні елементи, що додають непередбачуваність, а саме IV/nonce, випадковий паддінг, сольові значення [8]; які перетворюють прямолінійний оператор у стан, залежний від випадкових параметрів.

3. Вводити конструктивну нелінійність: у блочних схемах це S-блоки і складні перестановки; у протоколах – комбінації підстановок і змішувань, що унеможливлюють просте лінійне відновлення.

4. Застосовувати автентифіковане шифрування (AEAD), щоб запобігти маніпуляціям і повторному використанню блоків [9].

5. Контролювати реалізаційні ризики, що забезпечить захист від побічних каналів і інжекції помилок, валідація вхідних параметрів (перевірка оберненості матриць, недопущення слабких ключів).

Підсумовуючи, CPA показує, що лінійність Hill cipher забезпечує атакувальнику простий шлях до відновлення ключа всього за n запитів. Навіть у обмежених моделях або з додатковими ускладненнями атака залишається здійсненною й може посилюватися побічними каналами. Тому Hill cipher доцільно розглядати лише як навчальний приклад, а не як засіб практичного захисту даних.

2. Атака при детермінованому (регулярно повторюваному) наборі відкритих блоків.

Нехай множина можливих блоків відкритого тексту обмежена підмножиною $S \subseteq \mathbb{Z}_m^n$. Позначимо її лінійний замик (над кільцем $\mathbb{Z}_m$) через $\mathrm{span}\left(S\right)$ і його модульну (або векторну, якщо m – просте)

щільність через $\dim \operatorname{span}(S) = r$. Тоді справедливі такі формальні спостереження.

Необхідна умова успіху. Якщо $r < n$, тобто *span*(*S*) є підпростором розмірності менше ніж порядок блоку, то жодна скінченна сукупність пар (P_j, C_j) із $P_j \in S$ не дасть матриці P повного рангу n. У такому випадку відновити повний ключ $K \in GL(n, \mathbb{Z}_m)$ у загальному вигляді неможливо, можна лише відновити його дію на підпросторі $\operatorname{span}(S)$.

Умова достатності. Якщо $r = n$ (тобто $\operatorname{span}(S) = \mathbb{Z}_m^n$), то існує набір n лінійно незалежних векторів $P_1, \ldots P_n \in S$. Наявність таких n незалежних пар (P_j, C_j) дозволяє побудувати матрицю $P = [P_1 \ldots P_n]$ з $\operatorname{rank}(P) = n$ і отримати ключ:

$$K = CP^{-1} \pmod m, \tag{5}$$

де $C = [C_1 \ldots C_n]$.

Практична схема атаки при детермінованих форматах. Нехай відкриті повідомлення мають регулярну структуру типу

$$P^{(t)} = u + B\, \mathcal{X}^{(t)}, \tag{6}$$

де u – фіксований вектор (наприклад, повторюваний заголовок), B – матриця, що відображає параметризовані поля (шаблони), а $X^{(t)}$ – вектор змінних полів. Якщо простір, породжений усіма можливими $X^{(t)}$, має розмірність r (відповідно $\dim span(S) = r$), то атакувальнику достатньо зібрати r лінійно незалежних спостережень, щоб визначити дію K на цей підпростір. Формально, якщо є підматриця $P_{\text{sub}} \in \mathbb{Z}_m^{n \times r}$ рангу r, то можна обчислити частковий оператор

$$K\big|_{\operatorname{span}(S)} \equiv C_{\text{sub}} P_{\text{sub}}^{+} \pmod m, \tag{7}$$

де P_{sub}^{+} – псевдообернена або обернена (за наявності) матриця на відповідному підпросторі. Якщо $r = n$, то P_{sub}^{-1} і відновлення повне.

Оцінка «швидкості» компрометації при випадкових зразках із S. У випадку, коли елементи P_j вибираються випадково з S за деяким розподілом, питання редуковане до отримання n лінійно незалежних векторів. Для алгебрично простих випадків (наприклад, $m = q$ просте і $S = \mathbb{F}_q^n$) ймовірність того, що t випадкових векторів дають повний ранг n, виражається через добуток

$$\mathrm{P_r}\left[\operatorname{rank}(P_t) = n\right] = \prod_{i=0}^{n-1} \left(1 - q^{i-t}\right) \tag{8}$$

тож очікувана кількість вибірок для досягнення рангу $n \in O(n)$. Для структурованих S ця оцінка змінюється відповідно до розміру $\dim span(S)$ і розподілу варіантів $\mathcal{X}^{(t)}$.

Алгоритмічна реалізація відновлення в умовах детермінованості. Процедура експлуатації вразливості:

– збирання пари (P_j, C_j) поки rank(P) зростає.

– за кожним новим спостереженням виконувати вставку стовпця й оновлення рангу (Gaussian elimination $\bmod m$).

– коли знайдено підматрицю P_{sub} рангу r достатнього розміру (рівного n або максимально можливого), обчислити відповідне K або $K\big|_{\operatorname{span}(S)}$ як $C_{\text{sub}} P_{\text{sub}}^{-1}$ (або за допомогою псевдооберненої для $r < n$).

Необхідно звернути увагу, що операційна складність – домінована обчисленням рангу та оберненням підматриці розміру r: $O(r^3)$ елементарних операцій над $\mathbb{Z}_m$.

Як приклад ситуації з регулярними заголовками можна навести наступне. Повідомлення складаються з фіксованого заголовка u (однаковий для всіх повідомлень) і невеликого поля $\mathcal{X}^{(t)}$ розмірності $k \ll n$, тобто $P^t = u + \left[B\mathcal{X}^{(t)} \right]$. Тоді $\dim \operatorname{span}(S) \le k+1$. Якщо $k+1 < n$, то повного ключа не отримати, але дія K на підпросторі розмірності $k+1$ відновлюється за $k+1$ незалежних прикладів що є достатньо, щоб дешифрувати всі змінні поля й компрометувати важливі частини структури повідомлення [10].

З огляду на зазначене можна підсумувати таке:

– якщо $\dim span(S) = n$, то повторювані/детерміновані формати не захищають від повної компрометації, необхідно очікувати $O(n)$ запитів;

– якщо $\dim \operatorname{span}(S) = r < n$, то атакувальник може відновити лише часткову дію $K\big|_{\operatorname{span}(S)}$, що все одно може бути достатньо для витоку конфіденційної інформації (зокрема заголовків, метаданих);

– рекомендовані захисні заходи: введення випадкових параметрів (IV/nonce, соль), шифрування змінних частин повідомлення окремими сесійними ключами, застосування AEAD; у навчальних експериментах – сувора ізоляція демонстрацій.

3. Атака за наявності лише шифротексту (ciphertext-only).

Нехай Hill cipher заданий ключовою матрицею $K \in GL(n, \mathbb{Z}_m)$ і перетворенням

$$C^t \equiv KP^t \pmod m, \quad t = 1, \ldots, T, \tag{9}$$

де $P^t \in \mathbb{Z}_m^n$ – послідовні блоки відкритого тексту,

$C^t \in \mathbb{Z}_m^n$ – відповідні блоки шифротексту, атакувальник має тільки набір спостережень $\left\{C^t\right\}_{t=1}^{T}$. У відсутності будь-яких пар «відкритий текст – шифротекст» завдання відновлення K є некласичною проблемою сліпого зворотного розв'язування лінійного оператора над кільцем $\mathbb{Z}_m$. Проте за певних припущень щодо статистики відкритого тексту або для малих параметрів *m, n* атака може бути практично здійсненною. Нижче наведено кілька формалізованих підходів.

– метод на основі перших і других моментів (метод моментів/кореляційний підхід).

Позначимо емпіричні середні та коваріації (розглядаємо підняття символів у інтервал $\{0, \dots, m\text{-}1\}$ і працюємо в $\mathbb{R}$ для статистичного оцінювання, з подальшим приведенням мод m):

$$\mu_C = \frac{1}{T}\sum_{t=1}^{T} C^t$$
$$\Sigma_{CC} = \frac{1}{T}\sum_{t=1}^{T}\left(C^{(t)} - \mu_C\right)\left(C^{(t)} - \mu_C\right)^T \quad . \quad (10)$$

Якщо атакувальник має апріорні знання або припущення про статистику відкритого тексту (середнє μ_P і коваріацію Σ_{PP} (інвертованої в $\mathbb{R}$) можна отримати оцінку

$$K = \Sigma_{CP}\ \Sigma_{PP}^{-1}, \quad (11)$$

де Σ_{CP} – крос-коваріація між C (спостережуваним) і P (оціночним, взятим із корпусу). Якщо атакувальник знає (або коректно оцінює) μ_P, Σ_{PP}, то оцінка K може бути хорошою початковою гіпотезою; вона переводиться в коректний ключ K шляхом проекції на $GL\left(n,\mathbb{Z}_m\right)$ (наприклад, округлення елементів і перевірка оберненості за модулем m).

Умови ефективності. Підхід працює краще при:

- достатньо великому T (статистична стійкість оцінок);
- точності апріорної моделі μ_P, Σ_{PP} (тобто коли текстова статистика корпусу близька до реальної);
- невеликих n і/або m, коли округлення та приведення до модульної арифметики мають менше неоднозначностей.

Обмеження. Якщо Σ_{PP} невироджена лише за модулем m (а не в $\mathbb{R}$), або якщо апріорні оцінки сильно відрізняються від реальних, то оцінка K може бути ненадійною.

– атака як задача «сліпого» лінійного розділення (BSS / ICA-подібний підхід).

Сутність полягає в тому, щоб знайти цілу невироджену матрицю $M \in GL\left(n,\mathbb{Z}_m\right)$ таку, що перетворення $P^{(t)} = M^{-1}C^{(t)}$ дає статистику, близьку до відомої статистики природної мови (наприклад, частоти букв, частоти біграм/мультіграм тощо). Формально, атакувальник вирішує оптимізаційну задачу

$$K = \arg\min_{K' \in GL\left(n,\mathbb{Z}_m\right)} D\left(\mathrm{Stat}\left(K'^{-1}C\right)\middle\|\mathrm{Stat}_{\mathrm{lang}}\right), \quad (12)$$

де $D\left(\cdot\middle\|\cdot\right)$ – міра нерівності (наприклад, Kullback-Leibler divergence або χ^2 – статистика), $\mathrm{Stat}\left(\cdot\right)$ – емпіричні частоти/мовні статистики відновленого тексту, $\mathrm{Stat}_{\mathrm{lang}}$ – еталонні статистики для мови. Підхід фактично перебирає (або оптимізує в просторі) кандидати з $GL\left(n,\mathbb{Z}_m\right)$ і вибирає ті, які «відновлюють» мовні шаблони.

Практичний аспект. Прямий перебір $GL\left(n,\mathbb{Z}_m\right)$ можливий лише при малих m, n. Для більших розмірів застосовують евристики:

- локальні пошуки/simulated annealing по простору ключів;
- градієнтоподібні методи на релаксації в дійсній області з подальшим проєктуванням на цілі матриці;
- комбінування з ML-методами (класифікатори, що оцінюють «мовність» декодованого тексту).

Оцінка. Для малих n (наприклад, $n = 2, 3$) і $m \le 26$ цей підхід часто успішний за наявності великого числа блоків T (тисячі – десятки тисяч блоків) і якісної мовної моделі.

– частотні та статистичні методи (класичний підхід для малих m, n).

У випадку, коли m і n невеликі, можна використовувати класичні частотні методи: аналіз розподілу символів (позиційні частоти), біграм/триграм та їх кореляцій. Формальна ідея:

- для кожної позиції блоку j оцінюється емпіричний розподіл $p_{C_j}(\alpha) = \Pr\left(C_j = \alpha\right)$ по всіх спостереженнях;
- внаслідок лінійного перетворення кожна компонента C_j є лінійною комбінацією компонент P; якщо припустити незалежність або малі кореляції між координатами P, можна побудувати систему лінійних співвідношень між емпіричними частотами, що дає підказки про елементи K.

Для оцінки елементів ключової матриці K доцільно шукати такі лінійні відношення, які максимізують узгодженість між компонентами шифротексту C_i та лінійними комбінаціями позицій відкритого тексту у межах мовної моделі. У практиці це реалізується через статистичні критерії – коефіцієнт кореляції, χ^2 та log-likelihood, що дозволяють відбирати ті кандидати ключа, які найкраще відтворюють характерні властивості природної мови.

Успіх методу істотно залежить від того, наскільки точно модель відкритого тексту (частоти, кореляції) відповідає реальній. Для природних мов з помітною нерівномірністю частот (наприклад, анг-

лійська) шанси на успіх вищі, ніж для рівномірних або ентропійно насичених джерел.

– алгоритмічна схема

- збір статистики: обчислити μ_C, Σ_{CC}, позиційні і n-грамні частоти з $\left\{C^{(t)}\right\}_{t=1}^{T}$.
- апріорні припущення: вибрати мовну/корпусну модель для μ_P, Σ_{PP} або частот $\mathrm{Stat}_{\mathrm{lang}}$.
- побудова кандидатів: (а) оцінка K методом моментів; (б) генерація кандидатів $K^{'} \in GL\left(n, \mathbb{Z}_m\right)$ евристично; (в) локальна оптимізація релаксованої задачі.
- оцінка кандидатів: для кожного $K^{'}$ обчислити $Stat\left(K^{'-1}C\right)$ і виміряти відстань $D\left(\cdot \| \mathrm{Stat}_{\mathrm{lang}}\right)$.
- верифікація: для найкращих кандидатів перевірити консистентність (наприклад, дешифрувати деякі блоки і оцінити лінгвістичну інформативність).

Обчислювальна складність є експоненційною при повному переборі, проте на практиці зводиться до поліноміальної чи евристичної залежно від обраної стратегії пошуку.

– оцінки ефективності та обмеження.

- малі m, n: атаки набагато реалістичніші; для $m = 26$, $\mathrm{n} \in \{2, 3\}$ – відомі практичні розв'язки із застосуванням частотного аналізу та пошуку.
- великий T: вимога великої статистичної вибірки – типово T має бути порядку кількох тисяч блоків для стабільних оцінок.
- апріорна інформація: наявність якісної мовної моделі або корпусу істотно підвищує шанси на успіх.
- наявність побічних каналів: з їх допомогою ciphertext-only сценарій легко перетворюється в гібридний (сильніше спрощує задачу).

– контрзаходи проти ciphertext-only атак.

- збільшення ентропії в блоку: використовувати рандомізовані IV/nonce і випадкові паддінги;
- впровадження нелінійності в трансформацію: S-блоки або інші нелінійні операції, які руйнують лінійні статистичні взаємозв'язки;
- обмеження експозиції шифротекстів: мінімізувати кількість доступних шифротекстних блоків для однієї ключової сесії;
- аутентифіковане шифрування (AEAD): запобігає маніпуляціям, повторному використанню блоків і робить збір корисних статистик менш ефективним.

Підсумовуючи можна зазначити, що ciphertext-only атака на Hill cipher є формально складною, проте за малих параметрів, достатньої кількості спостережень та використання мовних чи побічних статистик вона стає практично здійсненною, що підтверджує його непридатність для захисту даних навіть у режимі доступу лише до шифротекстів.

4. Комбінування з побічними каналами (side-channel).

Нехай шифрування блока P реалізовано апаратно й проміжний стан S (наприклад, вектор результату KP перед редукцією по модулю) є функцією від секретного ключа та вхідного блоку:

$$S = g\left(K, P\right), \tag{13}$$

де для Hill cipher $g\left(K, P\right) = KP$ (в інтерпретації апаратної реалізації – проміжні регістри перед модульною операцією). Побічний канал дає емпіричні вимірювання L (таймінг, потужність, електромагнітні випромінювання, помилкові відповіді), які моделюються як функція від проміжного стану з шумом:

$$L = l\left(S\right) + \eta, \tag{14}$$

де l – модель витоку (наприклад, Hamming-weight/Hamming-distance, лінійна або нелінійна функція від бітів S), η – шум (гаусівський або інший).

– Correlation/Template-style атаки (таймінг, power-analysis).

Якщо l дає хоча б часткову інформацію про компоненти вектора $S = KP$, то спостережувані L корелюють з лінійними функціями від рядків K_{i*}. Формально, для кожної позиції i можна розглядати гіпотезу про рядок k і обчислювати статистику кореляції

$$\rho\left(k\right) = Corr\left(L,\ h\left(k^{\mathrm{T}}P\right)\right), \tag{15}$$

де h – модель перетворення стану в вимір (наприклад, Hamming-weight). Максимум $k = \arg\ \max_k \rho\left(k\right)$ служить оцінкою K_{i*}. Для Hill cipher, оскільки $k^{\mathrm{T}}P$ – лінійна комбінація елементів P, навіть слабка кореляція дає значну інформацію про k, а накопичення кількох вимірів (для різних P) підвищує SNR і дозволяє невеликою кількістю профільних трас відновити рядки K. Таким чином CPA по витоку (Correlation Power Analysis) перетворює апаратну уразливість у лінійну систему про елементи ключа.

– Differential Fault Analysis (DFA/fault injection).

Припустимо, що атакувальник може інжектувати локальну помилку в обробку одного блоку P, отримавши некоректний шифротекст $C^{'} = C + \Delta C$. Для Hill cipher

$$C = KP\ \left(\mathrm{mod}\ m\right),\ C^{'} = K\left(P + \Delta P\right)\ \mathrm{mod}\ m, \tag{16}$$

тобто різниця

$$\Delta C = K\Delta P\ \left(\mathrm{mod}\ m\right). \tag{17}$$

Якщо ΔP – вектор з одиницею в одній позиції (або вектор, контрольований атакувальником), то ΔC дає прямі лінійні відношення для відповідних стовпців K. Навіть одинична цілеспрямована помилка (або відома форма помилки) перетворює атаку з диференціального виду на лінійний розв'язок для відповідних невідомих елементів K. Для прикладу:

якщо інжектовано $\Delta P = \delta e_j$ (де δ відома зміна), то

$$\Delta C = \delta K e_j = \delta \quad \text{j -й стовпець } K.$$

– комбінування джерел інформації та відновлення K.

Узгоджуючи статистичні оцінки від витоку $l(S)$ та лінійні рівняння, одержані через DFA, атакувальник вирішує узагальнену задачу оцінки в умовах шуму:

$$K = \arg \min_{K' \in GL(n, \mathbb{Z}_m)} \mathcal{J}K', \tag{18}$$

де, наприклад,

$$\mathcal{J}\left(K'\right) = \sum_{t=1}^{T} \| L^{(t)} - l\left(K' P^t\right) \|^2 + \lambda \sum_{u \in \mathcal{F}} \| \Delta C^u - K' \Delta P^u \|^2, \tag{19}$$

функція сумарної невідповідності, що включає вклад від power/timing трас $L^{(t)}$ та від диференціальних різниць $\Delta C^{(u)}$ отриманих через fault injection (параметр λ регулює показники впливу). Мінімізація цієї функції (через перебір, релаксації або евристичні методи) дає значно швидше відновлення ключа ніж класична KPA/CPA без побічних даних.

– практичні показники ефективності.

Ефективність side-channel-підсилених атак визначається SNR витоку, кількістю трас T і можливістю інжекції помилок. Типові емпіричні вимоги для успішної реконструкції рядка K_{i*} методом CPA: T порядку десятків-сотень трас при помірному SNR; для DFA достатньо кількох точково спрямованих інжекцій, якщо ΔP контролюється або має просту відому форму.

Щоб зменшити ризик компрометації через побічні канали та інжекцію помилок, необхідно поєднувати технічні, протокольні та організаційні контрзаходи [14]. Захист має руйнувати кореляції витоку, усувати залежність часу/потужності від секретів, виявляти і нейтралізовувати помилки та обмежувати експозицію шифротекстів і доступ до сервісів шифрування [11]. Ключовими складовими захисту є:

1. Маскування та рандомізація проміжних станів (randomized masking) для руйнування кореляцій.

2. Constant-time та детерміновані реалізації для усунення таймінгових каналів.

3. Детектування та запобігання інжекції помилок (контроль контрольних сум, дублювання обчислень, датчики напруги/температури).

4. Фізичний захист (екранування, захист від доступу до плат) та аудит апаратних інтерфейсів.

5. В рамках криптографічного дизайну необхідно уникати прямих лінійних залежностей у проміжних станах (вводити нелінійність, солі/IV, AEAD).

Отже, слід зазначити що поєднання побічної інформації з класичними методами криптоаналізу істотно знижує поріг успіху атак на Hill cipher: слабка лінійність, яка сама по собі робить алгоритм вразливим у CPA/KPA, стає практично нескладною для експлуатації, якщо реалізація видає навіть мінімальну побічну інформацію або піддається інжекції помилок. Тому оцінка безпеки повинна обов'язково включати аналіз реалізаційних ризиків та заходи проти side-channel і fault-атаки [12].

Підсумовуючи розглянуті сценарії криптоаналізу, можна виділити кілька основних висновків, що характеризують вразливості Hill cipher і практичні наслідки його лінійної структури:

по-перше, основною причиною вразливості Hill cipher є його лінійна структура, яка дозволяє відносно легко відновлювати ключ у моделях із доступом до відкритого тексту та значно спрощує статистичний аналіз у режимі лише шифротекстів;

по-друге, атаки з обраним або відомим відкритим текстом призводять до повної компрометації алгоритму за обмежену кількість запитів, що робить його непридатним для використання у продуктивних системах;

по-третє, навіть при обмеженому доступі до шифротекстів або за наявності статистичної інформації, ймовірність успішної атаки залишається достатньо високою, особливо для малих параметрів алгоритму.

Нарешті, використання побічних каналів (таймінг, енергоспоживання, помилкові інжекції) істотно полегшує атаки, знижуючи вимоги до спостережень і роблячи компрометацію ключа майже тривіальною.

Висновки

Проведене дослідження засвідчило, що шифр Хілла, хоча й став важливим кроком у становленні блокових шифрів та продемонстрував потужність застосування лінійної алгебри у криптографії, має фундаментальні вразливості, пов'язані з його повною лінійністю та відсутністю механізмів захисту від сучасних криптоаналітичних атак. У результаті цей алгоритм не відповідає вимогам безпеки XXI століття й не може розглядатися як практичний засіб захисту конфіденційних даних.

Водночас його простота, математична прозорість і наочність роблять Hill cipher цінним навчально-методичним інструментом, що дозволяє досліджувати основи криптографічних перетворень, відпрацьовувати базові моделі атак та моделювати перехід від класичних шифрів до сучасних блокових алгоритмів.

Таким чином, його доцільно розглядати виключно в освітньому та дослідницькому контексті як «першу сходинку» до розуміння архітектури безпечних шифрувальних систем.

СПИСОК ЛІТЕРАТУРИ

1. Zhang, X., Shao, C., Li, T. et al. GFSPX: an efficient lightweight block cipher for resource-constrained IoT nodes. J Supercomput 80, 25256–25282 (2024). https://doi.org/10.1007/s11227-024-06412-2
2. Announcing Issuance of Federal Information Processing Standards (FIPS) FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 204, Module-Lattice-Based Digital Signature Standard, and FIPS 205, Stateless

Hash-Based Digital Signature Standard. National Institute of Standards and Technology on 08/14/2024. Retrieved from https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved
3. Dani, J., Nakka, K. and Saxena, N. A Machine Learning-Based Framework for Assessing Cryptographic Indistinguishability of Lightweight Block Ciphers. 30 May 2024. Retrieved from https://arxiv.org/abs/2405.19683v1
4. Kaur, J., Canto, A. C., Kermani, M. M., Azarderakhsh, R. A Comprehensive Survey on the Implementations, Attacks, and Countermeasures of the Current NIST Lightweight Cryptography Standard, 2023. URL: https://arxiv.org/abs/2304.06222
5. Ni, Z., Khalid, A., Liu, W., & O'Neill, M. (2024). Bitstream Fault Injection Attacks on CRYSTALS Kyber Implementations on FPGAs. 1–6. Retrieved from https://doi.org/10.23919/date58400.2024.10546550
6. Zhyvylo Y. (2023). Exploring and Acquiring Modern Human Resource Competencies in Cybersecurity Amidst State Digital Transformation. Pressing Problems of Public Administration, 2(63), 111-127. https://doi.org/10.26565/1684-8489-2023-2-08
7. Zhyvylo , Y. O., & Zhyvylo , I. O. (2021). Joint training of the cyber security defense forces personnel in the conditions of total state defense. Theory and Practice of Public Administration, 2(73), 144-153. https://doi.org/10.34213/tp.21.02.16
8. Mahdi, Q. A., Zhyvotovskyi, R., Kravchenko, S., Borysov, I., Oleksandr, O., Panchenko, I., Zhyvylo, Y., Kupchyn, A., Koltovskov, D., Boholii, S. (2021). Development of a method of structural-parametric assessment of the object state. Eastern-European Journal of Enterprise Technologies, 5 (4 (113)), 34–44. doi: https://doi.org/10.15587/1729-4061.2021.240178
9. Koval M., Sova O., Orlov O., Zhyvylo Y., Zhyvylo I. Improvement of complex resource management of special-purpose communication systems // 5(9-119) (2022): Eastern-European Journal of Enterprise Technologies. P. 34–44;
10. S. Kashkevich, A. Shyshatskyi, O. Dmytriieva, Y. Zhyvylo, G. Plekhova, S. Neronov The development of management methods based on bio-inspired algorithms Information and control systems: modelling and optimizations: collective monograph. – Kharkiv: TECHNOLOGY CENTER PC, 2024. pp. 35-69. DOI: http://doi.org/10.15587/978-617-8360-04-7
11. Zhyvylo, Y.O. (2024). Methodology for developing a national cybersecurity strategy. State Formation, no. 2 (36), 307–321. DOI: https://doi.org/10.26565/1992-2337-2024-2-21
12. Живило Є. О. Оцінка ризиків кібербезпеки та контролю конфіденційності в інформаційних системах державного управління / Є. О. Живило, Д. Г. Шевченко // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. 2022. № 75. С. 66-77. URL: http://nbuv.gov.ua/UJRN/Znpviknu_2022_75_9
13. Живило Є.О., Черноног О.О. Стратегія кібероборони України, Збірник наукових праць ВІТІ № 4, 2017, С.30–37. URL: https://www.researchgate.net/publication/380979172_STRATEGIA_KIBEROBORONI_UKRAINI
14. Ігор Ромашко, Юлія Калашнікова, CISCO SECUREX ТА ZERO TRUST: СУЧАСНІ ПІДХОДИ ДО КІБЕРЗАХИСТУ, 2025. Retrieved from http://perspectives.pp.ua/index.php/nts/article/view/29469/29425.
15. Onyshchenko, S., Zhyvylo, Ye., Cherviak, A. and Bilko S. (2023), "Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security", //) (2023), Eastern-European Journal of Enterprise Technologies, vol. 5 (13 (125), pp. 65–76. DOI: https://doi.org/10.15587/1729-4061.2023.288175

Received (Надійшла) 11.08.2025
Accepted for publication (Прийнята до друку) 05.11.2025

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Живило Євген Олександрович – кандидат наук з державного управління, доцент, доцент кафедри комп'ютерних технологій та інформаційних систем, Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна;

Yevhen Zhyvylo – candidate of sciences in public administration, associate professor, associate professor of the department of computer technologies and information systems, National University "Poltava Polytechnic named after Yury Kondratyuk", Poltava, Ukraine;
e-mail: zhivilka@i.ua; ORCID Author ID: https://orcid.org/0000-0003-4077-7853;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57350779100.

Кучма Юрій – кандидат технічних наук, доцент, завідувач кафедри комп'ютерних систем, ТОВ «Університет сучасних технологій», Київ, Україна;

Yurii Kuchma – Candidate of Technical Sciences, Associate Professor, Head of the Bepartment of Computer Iystems of the University of Modern Technologies LLC,. Kyiv, Ukraine;
e-mail: krabatua@gmail.com; ORCID Author ID: https://orcid.org/0009-0002-5498-4271.

Practical application and vulnerabilities of Hill cipher in a modern context

Yevhen Zhyvylo, Yurii Kuchma

Abstract. The article examines the Hill cipher as a classical example of applying linear algebra and modular arithmetic in cryptography. It elucidates the mathematical foundations of the algorithm, including the formation of the key matrix over finite fields, the conditions for its invertibility, and the implementation of encryption as the multiplication of plaintext vectors by the key matrix. This approach is presented as a distinctive "bridge between theory and practice," combining formal mathematical constructions with practical data protection mechanisms. Particular attention is given to the vulnerabilities of the Hill cipher. It is shown that the algorithm is insecure in modern contexts due to the linearity of its transformations and the absence of nonlinear components. Examples of cryptanalytic attacks are provided, demonstrating that the cipher can be "broken apart" even with a minimal number of plaintext-ciphertext pairs. This makes it evident that, in the context of 21st-century cybersecurity, the Hill cipher is merely a "shadow of its era" and cannot serve as a fully reliable tool for data protection. At the same time, the educational and methodological value of the cipher is emphasized. It allows one to "see the mechanism from the inside," clearly illustrating the transition from monoalphabetic ciphers to block transformations. The article highlights that the Hill cipher played the role of a "first step" in the development of structures that later evolved into DES and AES, where the use of block structures and matrix operations became a fundamental element of modern cryptography.

Keywords: cyber security, cyber threats, artificial intelligence, machine learning, cryptography, cryptanalysis, cipher.