DOI 10.15276/imms.v15.no1.24
УДК 621.37

Informatics and Mathematical Methods in Simulation
Vol.15 (2025), No. 1, pp. 24-38

ЗАСТОСУВАННЯ ХАОСУ В АЛГОРИТМАХ ГЕНЕРАЦІЇ КЛЮЧІВ

О.В. Агаджанян, А.Р. Агаджанян, О.А. Сиропятов

Національний університет «Одеська політехніка»
1, Шевченка пр., м.Одеса, 65044, Україна
Emails: o.v.ahadzhanian@op.edu.ua, 7985798@op.edu.ua, o.a.syropiatov@op.edu.ua

Сучасні вимоги до безпеки інформаційних систем акцентують увагу на новітніх методах генерації криптографічних ключів, одним із яких є використання властивостей хаотичних систем, що робить їх перспективними джерелами ентропії для криптографії. Мета дослідження: проаналізувати можливості застосування хаотичних динамічних систем, зокрема автогенераторів, для генерації криптографічних ключів у системах захисту інформації. Наукова та практична значущість роботи полягає в обґрунтуванні ефективності хаотичних генераторів для формування високоентропійних псевдовипадкових послідовностей і їх застосування в створенні захищених систем генерації ключів відповідно до сучасних вимог безпеки.Методологія дослідження включає теоретичний аналіз хаотичних динамічних систем, вивчення режимів автогенераторів на прикладі атрактора Лоренца, а також статистичний і ймовірнісний аналіз сигналів із оцінкою їх розподілів і кореляцій. Основні результати і висновки: визначено, що біфуркації є критичними точками переходу системи до хаотичного режиму, що породжує сигнали з високою ентропією; показано, що хаотичні генератори здатні працювати як генератори шуму та автогенератори, змінюючи характеристики розподілу вихідних сигналів; підтверджено, що вихідні послідовності є аперіодичними та можуть мати безперервний спектр, що є ключовою властивістю для криптографічної стійкості; наведено обґрунтування доцільності використання хаосу в алгоритмах формування шумових послідовностей для захисту інформації. Цінність дослідження – робота внесла вагомий внесок у розуміння ролі хаотичних систем у криптографії, зокрема у створенні нових алгоритмів генерації ключів із високим ступенем ентропії, що розширює спектр засобів забезпечення інформаційної безпеки. Практичне значення – отримані результати можуть бути використані при розробці апаратних і програмних генераторів криптографічних ключів на основі хаотичних систем, що підвищить захищеність інформаційних систем від несанкціонованого доступу та атак.

Ключові слова: хаос, генерація ключів, криптографія, автогенератор, ентропія, аттрактор Лоренца, псевдовипадкові послідовності

Вступ. Сучасні вимоги до безпеки інформаційних систем дедалі більше орієнтуються на нестандартні підходи до генерації криптографічних ключів. Одним із перспективних напрямів є використання властивостей хаотичних систем. Теорія хаосу — це розділ математики, що досліджує поведінку нелінійних динамічних систем, які за певних умов можуть демонструвати складну, на перший погляд випадкову, але детерміновану поведінку. Таке явище отримало назву динамічний (детермінований) хаос. Особливістю подібних систем є надзвичайна чутливість до початкових умов, що робить їх складнопередбачуваними та ідеальними для криптографічних застосувань.

Однією з технічних реалізацій хаотичних систем є генератори шуму, які створюють електричні сигнали у заданому частотному діапазоні. Вони вже мають застосування у пристроях захисту інформації від несанкціонованого доступу. Проте, як буде показано в подальшому, за певних умов генератор хаосу може виконувати роль автогенератора — пристрою з самозбудженням, здатного до стійкої генерації сигналів без зовнішнього збурення.

Автогенератори широко застосовуються в системах формування сигналів, і в контексті інформаційної безпеки вони можуть виступати як джерело

псевдовипадкових, але керованих послідовностей. Завдяки зворотному зв'язку, що забезпечує перевищення коефіцієнта підсилення над одиницею, такі системи можуть працювати в різних режимах — м’якому або жорсткому — в залежності від умов запуску та стійкості коливань. У результаті формується сигнал, властивості якого визначаються характеристиками самої системи і можуть бути використані для генерації криптографічних ключів з високим ступенем ентропії.

На сьогодні існує широкий спектр методів генерації криптографічних ключів, серед яких все більшої популярності набувають підходи, засновані на використанні хаотичних систем. Хаос у фізичних та електронних системах характеризується складною, але детермінованою динамікою, що є ідеальним джерелом високої ентропії для формування ключів. У науковій літературі описано численні реалізації таких генераторів — як апаратних, так і програмних. Наприклад, у роботі Rahman et al. (2022) [1] представлено метод генерації ключів на основі логістичного відображення для шифрування AES у системах IoT. У дослідженні Pellicer-Lostao & Lopez-Ruiz (2008) [2] показано, що двовимірні хаотичні карти здатні генерувати криптографічно стійкі псевдовипадкові біти. Вітчизняні дослідники, зокрема Дмітрієв О.С., Єфремов Є.В., Максимов Н.А. та Панас А.І., також розглядали використання автогенераторів зі специфічними схемами включення для формування хаотичних шумових коливань, придатних до застосування у системах захисту інформації.

Попри те, що класичні криптографічні стандарти, такі як NIST SP 800-90A [3], прямо не використовують хаос як джерело ентропії, сучасні дослідження демонструють, що хаотичні генератори можуть успішно відповідати вимогам до криптографічно стійких генераторів псевдовипадкових чисел (CSPRNG). Наприклад, Nguyen et al. (2021) [4] запропонували гіперхаотичну систему на основі п’яти змінних, яка демонструє високу швидкість генерації та проходить тести NIST SP 800-22, Diehard та TestU01. А в новітній роботі Song et al. (2025) [5] розроблено гібридну криптографічну систему "CryptoChaos", що поєднує кілька хаотичних карт із сучасними хеш-функціями (SHA-3) та алгоритмами постквантового шифрування (X25519). Такий підхід дозволяє створювати стійкі, адаптивні та незалежні системи захисту, що базуються на фізичних властивостях нелінійної динаміки.

Метою цієї статті є дослідження можливостей застосування хаотичних динамічних систем, реалізованих у вигляді автогенераторів, в алгоритмах генерації ключів для інформаційних систем захисту.

Основний розділ. Після детального вивчення підходів формування хаотичних коливань було віддано перевагу саме методам отримання хаосу за допомогою Атракторів. Такі схеми реалізують чисельне рішення диференційних рівнянь. Для побудови експерименту та отримання необхідних результатів нашу увагу привернув метод формування хаосу за Лоренцом [6].

Атрактор Лоренца в свою чергу описує, як стан нелінійної тривимірної динамічної системи змінюється з плином часу хаотичним чином. Атрактор був спочатку відкритий Едом Лоренцем, який вивів його зі спрощеної моделі конвекційних валів в земній атмосфері. Однак він також виникає в лазерах і динамо.

Дифференціальні рівняння (1), які визначають атрактор Лоренца [6, 7]:

$$\begin{aligned} dx / dt &= Sigma * (yx) \\ dy / dt &= (Rho-z) * x – y \\ dz / dt &= x * y - Beta * z, \end{aligned} \qquad (1)$$

де Sigma згадується як число Прандтля, Rho називають числом Релея, а бета - геометричним фактором. У Micro-Cap такі диференціальні рівняння можна моделювати за допомогою поведінкових моделей, доступних в розділі "Макро". Схема аттрактора Лоренца представлена нижче [8, 9].

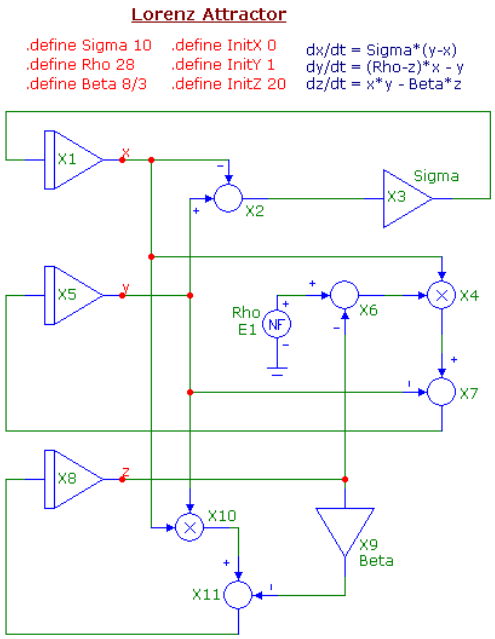


Рис. 1. – Аттрактор Лоренца в програмі Microcap

Вузли x, y і z обчислюють напруги, еквівалентні їх відповідним змінним в наведених вище рівняннях. Змінна x обчислюється за допомогою макросу Int, макросу Sub і макросу Amp. Допоміжний макрос (X2) забирає напругу в вузлі y на напругу в вузлі x. Потім різниця передається в макрос підсилювача (X3), параметр gain якого встановлений на Sigma. Вихідні дані макросу Amp потім вводяться в макрос Int (X1), який обчислює інтеграл для отримання x.

Змінна y обчислюється за допомогою макросу Int, двох макросів Sub, макросу Mul і джерела функції NFV. Джерело функції NFV (E1) видає напругу, еквівалентну Rho. Допоміжний макрос (X6) віднімає значення Rho на напругу в вузлі z. Потім різниця вводиться в макрос Mul (X4), де вона множиться на напругу в вузлі x. Потім цей продукт подається в інший допоміжний макрос (X7), де він віднімається з напруги в вузлі y. Потім ця різниця вводиться в макрос Int (X5), який обчислює інтеграл для отримання y.

Змінна z обчислюється за допомогою макросу Int макросу Mul, макросу Amp і макросу Sub. Напруги в вузлах x і y множаться за допомогою макросу Mul (X10). Напруга в вузлі z масштабується коефіцієнтом Beta за допомогою макросу Amp (X9). Ці два продукти вводяться в допоміжний макрос (X11). Потім різниця вводиться в макрос Int (X8), який обчислює інтеграл для отримання z.

Значення Sigma, Rho і Beta встановлюються за допомогою операторів define.

Наступні три оператори визначення також присутні на схемі:

define InitX 0, .define InitY 1 .define InitZ 20

Ці оператори визначення встановлюють початкові значення для змінних x, y і z. InitX, InitY і InitZ використовуються для визначення параметра VINIT для макросів X1, X5 і X8 Int відповідно. Параметр VINIT макросу Init встановлює початкову напругу на виході інтегратора. Аналогічно з іншими хаотичними системами атрактор Лоренца дуже чутливий до початкових умов, навіть невелика зміна призведе до іншого сюжету.

Загальні налаштування для відображення хаотичної поведінки з атрактором Лоренца - це встановити Sigma на 10, Rho на 28 і Beta на 8/3 [6]. З використанням цих значень виконується 200-секундний перехідний аналіз, який дає класичний графік "метелик", коли V (Z) будується в залежності від V (X), як показано на рис.2.

Біфуркація - це якісна зміна поведінки динамічної системи при нескінченно

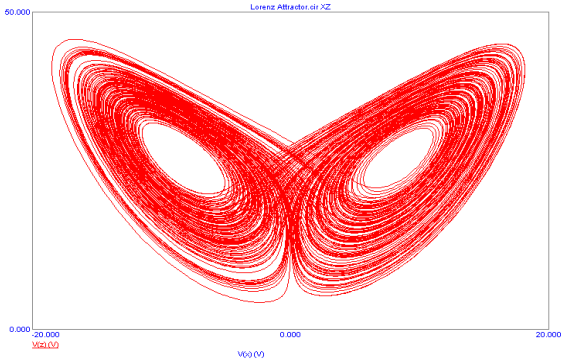


Рис. 2. – Бифуркації при Rho = 28

малій зміні її параметрів. Також для проведення дослідження для нас важливо таке поняття як «ентропія».

Ентропія зазвичай застосовується для опису рівноважних (оборотних) процесів.

У статистичній фізиці ентропія характеризує ймовірність здійснення будь-якого макроскопічного стану. Крім фізики, термін широко вживається в математиці: теорії інформації та математичної статистики. У цих областях знання ентропія визначається статистично і називається статистичною або інформаційною ентропією [6].

Розглянемо зміни в поведінці рішення системи Лоренца при різних значеннях параметра Rho. Rho < 1 – атрактором є початок координат, інших стійких точок немає.

1 < Rho < 13,927 – траєкторії спірально наближаються (це відповідає наявності загасаючих коливань) до двох точок.

Ці точки визначають стан стаціонарного режиму конвекції, коли в шарі формується структура з обертових валів рідини.

Rho ≈ 13,927 – якщо траєкторія виходить з початку координат, то, зробивши повний оборот навколо однієї зі стійких точок, вона повернеться назад в початкову точку -виникають дві гомоклінічні петлі. Поняття гомоклінічної траєкторії означає, що вона виходить і приходить в одне і те ж положення рівноваги.

Rho > 13,927 – залежно від напрямку траєкторії, приходить до однієї з двох стійких точок. Гомоклінічні петлі перероджуються в нестійкі граничні цикли, також виникає сімейство складно влаштованих траєкторій, що не є атрактором, а скоріше навпаки, що відштовхує від себе траєкторії. Іноді за аналогією ця структура називається «дивним репеллером».

Rho ≈ 24,06 – траєкторії тепер ведуть не до стійких точок, а асимптотично наближаються до нестійких граничних циклів – виникає власне аттрактор Лоренца. Однак обидві стійкі точки зберігаються до значень Rho ≈ 24,74.

Rho ≈ 28 – класичне значення параметра, розглянуте у статті Лоренца.

Всі три стани рівноваги нестійкі і траєкторії з їх околиць притягуються до хаотичного (локального) атрактору (який, таким чином, самозбуджуємо по відношенню до всіх станів рівноваги). Хаотичний атрактор має дробову ляпуновську розмірність, для якої аналітична оцінка зверху може бути отримана аналітично через форму ляпуновської розмірності глобального атрактора, а оцінка знизу може бути отримана аналітично.

При великих значеннях параметра Rho траєкторія зазнає серйозних змін. Шильников і Каплан показали, що для великих Rho система перетворюється на режим автоколивань, у якій, якщо зменшувати параметр, спостерігатиметься перехід до хаосу через послідовність подвоєння періоду коливань.

Нижче наведемо рисунки моделювання атрактора у програмі Microcap.

На початку будуть наведені біфуркації X, Y та Z, також графік сигналу, функція

розподілу та щільність ймовірності при Rho=28 та початкових умовах x=0, y=1, z=20 (рис 3).

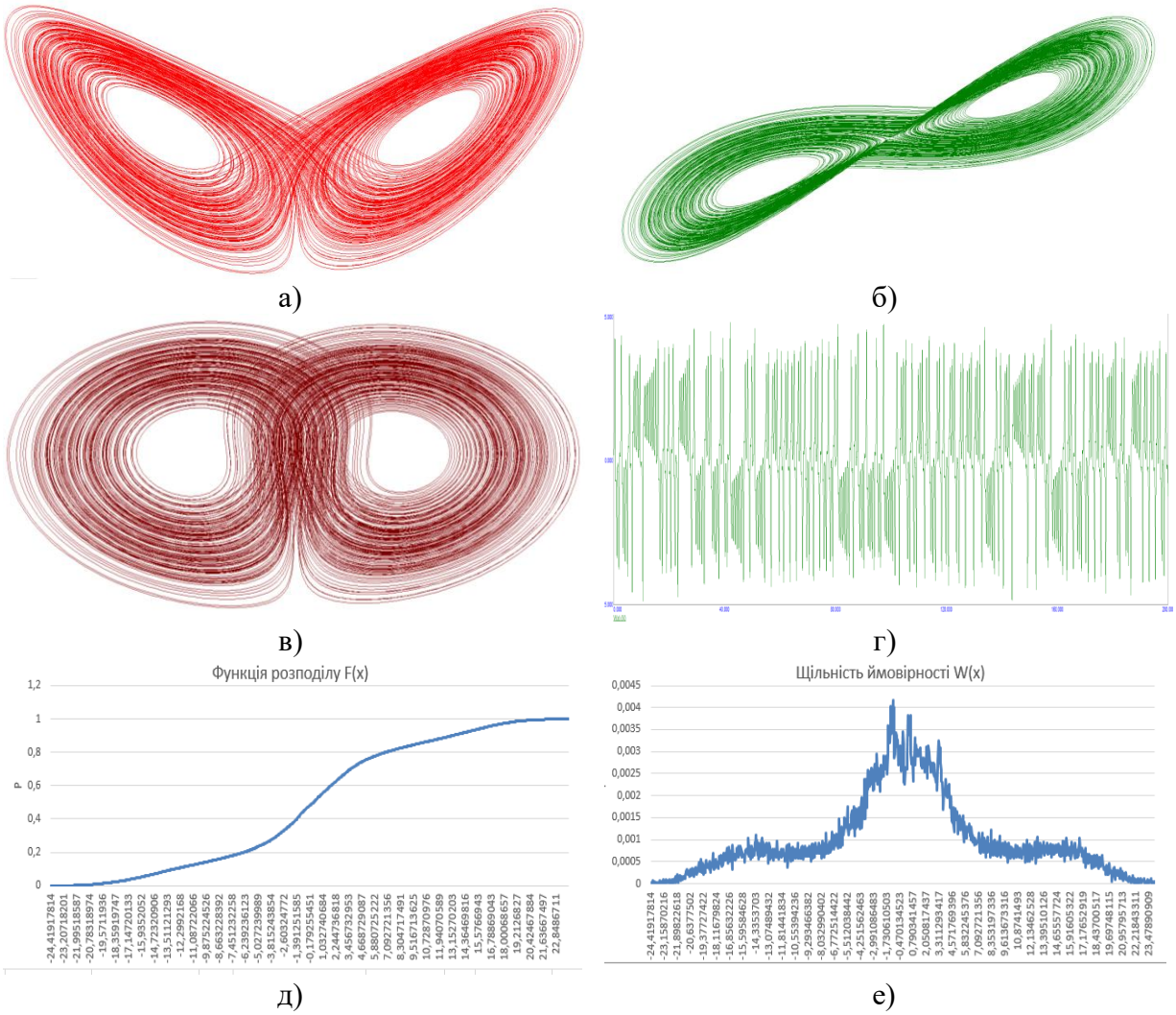


Рис. 3. – Результати моделювання схеми Атрактора Лоренца з наступними параметрами: Rho = 28, x = 0, y = 1, z = 20, де: (а) - XZ; (б) – XY; (в) – YZ; (г) – Сигнал; (д) - Функція розподілу; (е) - Щільність ймовірності

На рис. 3 (е) наведено розрахунок щільності ймовірності за наступними числовими характеристиками: сер. значення – a = 0.150363519; дисперсія – σ^2 = 81.53201942, медіана – m = 0.147919755. Отримання йомовірнісних характеристи віпадкової величини взято за допомгою відведення у. Зроблено усереднення за часом та обрано частотний метод визначення йомовірності за допомогою аналізу 40000 значень відгуку атрактору Лоренца.

В загальному вигляді систему рівнянь руху системи можливо викласти у вигляді (2) згідно [6]:

$$V_i(\vec{x}) = \frac{dx_i}{dt},\ i = 1, 2, \ldots, N. \qquad (2)$$

Заповнення фазового простору системи відбувається шляхом численного інтегрування системи рівнянь Лоренца, яка є несиметрична за часом (3):

$$-\sigma x - \sigma y = \frac{dx}{dt};\ rx - y - xz = \frac{dy}{dt};\ -bz + xy = \frac{dz}{dt}. \qquad (3)$$

Всі величини, які входять до рівняння 3 разом з часом (t) беруться у безрозмірному вигляді.

X, Y та Z – це змінні пропорційні відповідно швидкості конвективного руху. Sigma та Beta – це константи, відповідно 10 та 8/3. Параметр Rho може бути аналогічний (для генераторів іншого типу) параметру збудження. Фазову траєкторію використовують за алгоритмом подвійної апроксимації (4).

$$X_{i,\,n+1} = x_{in} + \frac{1}{2}[V_i(x_n, y_n, z_n) + V_i(x_{n+1}, y_{n+1}, z_{n+1})]\Delta t. \qquad (4)$$

Виявилося, що фазова траєкторія затягується в область (атрактор Лоренца), що представляє собою два «вихори», які мають своїми центрами дві різні нерухомі точки. Траєкторія потрапляє в околиці однієї з них, здійснює біля неї деяку кількість оборотів і потім, віддаляючись від неї, переміщається в околицю другої нерухомої точки, описує тепер уже у неї якусь кількість оборотів, віддаляється, потрапляє в околиці першої нерухомої точки тощо.

Це доводить, що такі фазові траєкторії системи нестійкі. Це проявляється в сильній залежності розрахункової траєкторії від початкових умов (від вибору початкової точки), так що неможливо передбачити заздалегідь, ні в околицю з яких нерухомих точок виявиться в перший раз затягнутою дана траєкторія, ні яке число оборотів вона зробить в кожній окремій серії. Як нестійкий і обмежений у фазовому просторі, рух даної системи виявляється стохастичним і має чітко виражену турбулентну структуру.

Надалі атрактор Лоренца піддався всебічному вивченню. Була досліджена його структура для різних значень параметра Rho.

Виявилося, що тут має місце своєрідний гістерезис: якщо ми збільшуємо Rho, то конвективний (регулярний) потік зривається в турбулентний (стохастичний) при Rho — 24,74, якщо ж, навпаки, зменшуємо Rho, то турбулентний рух переходить в конвективний при Rho = 24,06. У вузькій області значень 24,06 < Rho < 24,74 в системі Лоренца існують три атрактори, два з яких відповідають регулярному руху, а третій — стохастичному. Виявилося також, що перехід до стохастичного руху відбувається в ній через ряд біфуркацій.

У тому, що рівняння Лоренца несиметричні за часом, легко переконатися безпосередньо. Таким чином, цей динамічний хаос, що виникає в даній системі, є незворотнім.

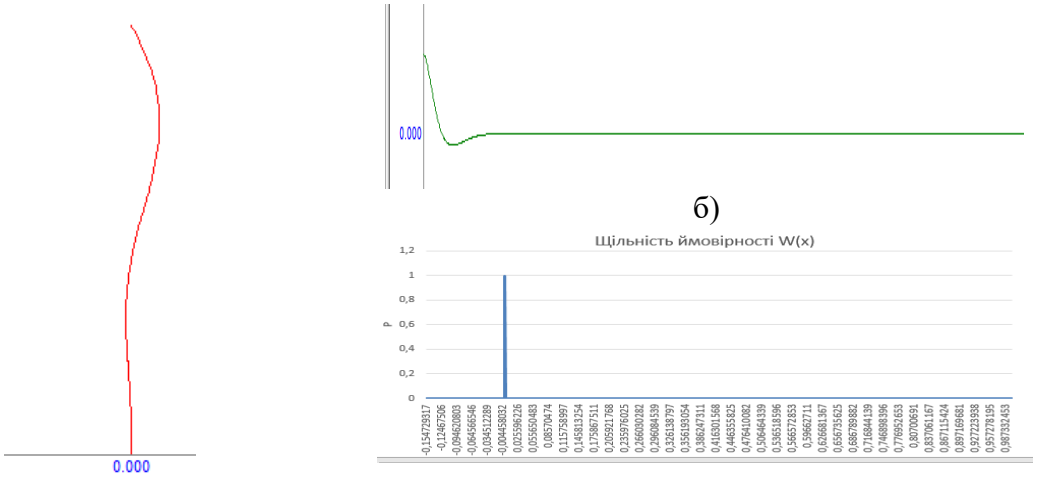
Це зумовлює особливу топологічну природу атрактора Лоренца, яка кардинально відрізняє його від стохастичних атракторів, що виникають в оборотних (реверсивних) динамічних системах. Аттрактор Лоренца є класичним прикладом детермінованого хаосу, де хаотична поведінка виникає з абсолютно детермінованих рівнянь руху без зовнішніх випадкових впливів. Його топологічні властивості характеризуються фрактальною структурою та складною геометрією, що забезпечує високу чутливість до початкових умов і складність прогнозування подальшого розвитку системи.

У противагу цьому, стохастичні атрактори формуються під впливом випадкових процесів і шумів у системах із зворотністю динаміки, що призводить до статистично описуваної поведінки.

Такий різний характер атракторів визначає їхнє застосування у моделюванні різноманітних фізичних, біологічних і технічних процесів, зокрема у сфері генерації псевдовипадкових послідовностей для криптографії.

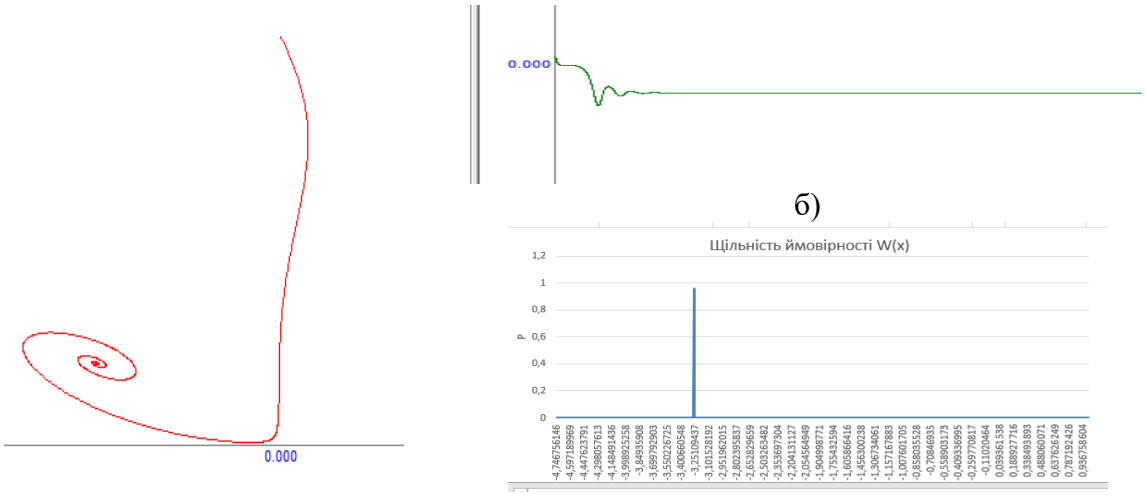
Далі наведені результати моделювання лише найважливіших параметрів дослідного алгоритму формування хаотичних послідовностей за схемою атрактора Лоренца. Показані біфуркації (XZ), вигляд хаотичного сигналу у часовому просторі. Визначені щільності розподілу ймовірності для аналізу саме у площині застосування алгоритму для формування ключів.

Варіації параметрів показані на рис. 4-9.



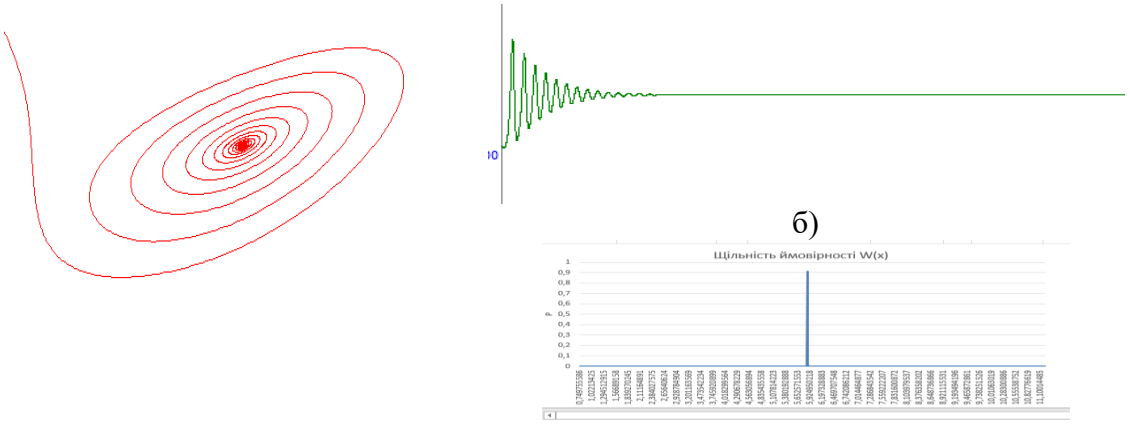
а) б) в)

Рис. 4. - Результати моделювання схеми Атрактора Лоренца з наступними параметрами: Rho = 0.5, x = 0, y = 1, z = 20, де: (а) - XZ; (б) – Сигнал; (в) - Щільність ймовірності. Параметри: a = 0.000337217; дисперсія – σ^2 = 0.000436894, медіана m = 0



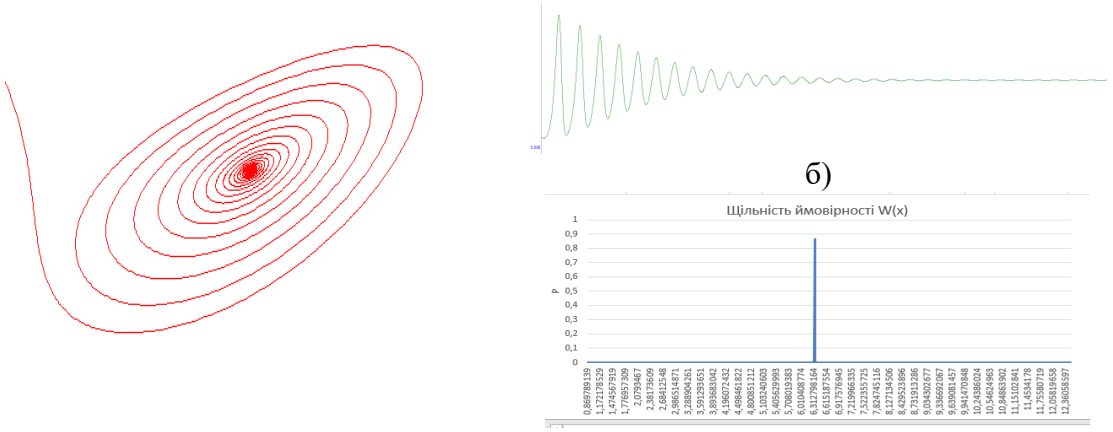
а) б) в)

Рис. 5. - Результати моделювання схеми Атрактора Лоренца з наступними параметрами: Rho = 5, x = 0, y = 1, z = 20, де: (а) - XZ; (б) – сигнал; (в) - щільність ймовірності. a = -3.230049362; дисперсія – σ^2 = 0.118095236, медіана m = -3.26598665



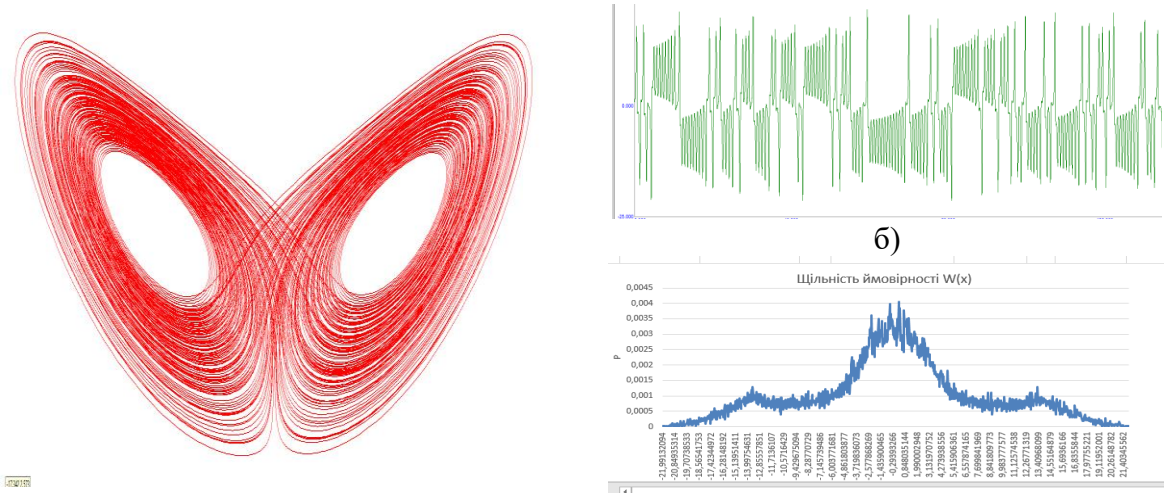
а) в)

Рис. 6. - Результати моделювання схеми Атрактора Лоренца з параметрами: Rho = 13.927, x = 0, y = 1, z = 20.a = 5.851226298; σ2 = 0.179453846, m = 5.871287205



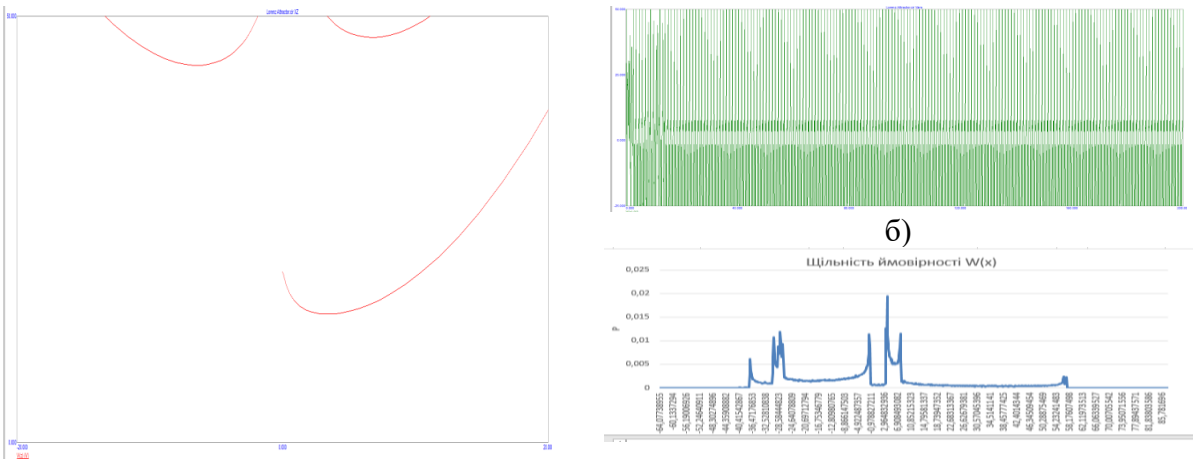
а) в)

Рис. 7. - Результати моделювання схеми Атрактора Лоренца з наступними параметрами: Rho = 16, x = 0, y = 1, z = 20, де: (а) - XZ; (б) – Сигнал; (в) - Щільність ймовірності.
Параметри: a = 6.300076775; дисперсія – σ2 = 0.271385236, медіана – m = 6.324556591



а) в)

Рис. 8. - Результати моделювання схеми Атрактора Лоренца з наступними параметрами: Rho = 24.06, x = 0, y = 1, z = 20, де: (а) - XZ; (б) – Сигнал; (в) - Щільність ймовірності.
Параметри: a = 0.156394423; дисперсія – σ2 = 65.72242363, медіана – m = –0.176483671



а) в)

Рис. 9. - Результати моделювання схеми Атрактора Лоренца з параметрами: Rho = 100, x = 0, y = 1, z = 20. a = -4.229658168; σ^2 = 504.443928, m = -3.800248801

Далі приведемо результати моделювання при стандартному Rho = 28, але різних початкових умовах. На рис. 10-18 наведені щільності розподілу ймовірності за різними критеріями. На рис. 19 визначено коваріаційну функцію для хаотичної послідовності.

Рис. 10. - Щільність ймовірності схеми атрактора з параметрами: Rho = 28, x = 10, y = 1, z = 20

Рис. 11. Щільність ймовірності схеми атрактора з параметрами: Rho = 28, x = 50, y = 1, z = 20

Рис. 12. - Щільність ймовірності схеми атрактора з наступними параметрами: Rho = 28, x = 100, y = 1, z = 20

Рис. 13. - Щільність ймовірності схеми атрактора з наступними параметрами: Rho = 28, x = 0, y = 10, z = 20

Рис. 14. - Щільність ймовірності схеми атрактора з наступними параметрами: Rho = 28, x = 0, y = 50, z = 20

Рис. 15. - Щільність ймовірності схеми атрактора з наступними параметрами: Rho = 28, x = 0, y = 100, z = 20

Рис. 16. - Щільність ймовірності схеми з параметрами: Rho = 28, x = 0, y = 1, z = 200

Рис. 17. - Щільність ймовірності схеми з параметрами: Rho = 28, x = 0, y = 1, z =

Рис. 18. - Щільність ймовірності схеми Атрактора з наступними параметрами: Rho = 28, x = 0, y = 1, z = 2000

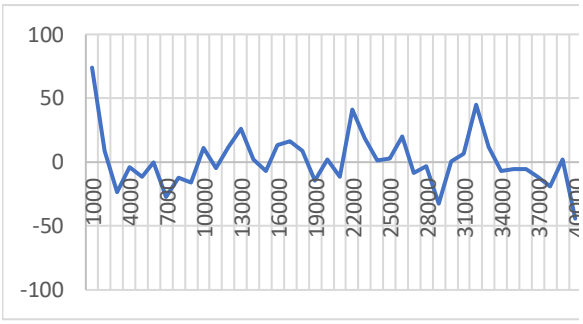


Рис. 19. - Коваріаційна функція реалізації сигналу з наступними параметрами: Rho = 28, x = 0, y = 1, z = 2000

До завершення визначень статистичних параметрів атрактора побудовано коваріаційну функцію вихідного сигналу на відведенні y (рис. 19) відповідно до [7]. Коваріаційна функція побудована у границі від 1 до 1000 значень, другий масив було взято зі збільшенням значення +1000. Таким чином у вихідні послідовності (y) було проаналізовано першу 1000 значень та порівняно з наступними 1000 значень масиву через 1000 значень. Отримано 40 значень функції коваріації.

Особлива топологічна природа атрактора Лоренца, зокрема його складна фрактальна структура, впливає на характер динаміки системи, що значно відрізняє його від стохастичних атракторів у оборотних системах. Ці властивості визначають специфіку переходів у системі від регулярного до хаотичного режиму, що знаходить своє відображення у змінах ймовірнісних характеристик випадкових процесів, які описують поведінку системи. Аналіз цих характеристик дозволяє глибше зрозуміти природу хаосу і вплив параметрів системи на формування статистичних властивостей генерованих сигналів.

Значення біфуркацій в теорії динамічного хаосу визначається тією обставиною, що саме з ними пов'язаний перехід системи від регулярного руху до стохастичного, при якому фазова траєкторія, змінюючи свою топологію, перестає бути гладкою лінією. Аналіз ймовірнісних характеристик випадкових процесів (дискретного випадкового сигналу) показав наступне: такі характеристики, як щільність розподілу ймовірності, змінюються залежно від режиму роботи атрактора. Характер функції щільності ймовірностей варіюється від нормального розподілу (коли спостерігаються нерівномірні зміни ймовірностей в області ±3σ (рис. 18) до розподілу Парето (рис. 4(e)), що характеризується концентрацією ймовірності у локалізованій області значень, а також до гамма-розподілу, який відзначається несиметричністю лівої та правої частин функції розподілу (рис. 3(e)). Відповідно до властивостей коваріаційної функції можна зробити висновок, що у вихідній послідовності навіть у малих вікнах існує невеликий статистичний взаємозв’язок.

Далі розглянемо порівняльний статистичний аналіз криптоалгоритмів, що дозволить оцінити практичні наслідки описаних теоретичних результатів. Результати статистичних випробувань алгоритмів DES, СКЗД, а також GAMMA 4, проведеного на ЕОМ, є перевірка на випадковість шифртексту і ключового потоку при різних варіантах формування ключової послідовності і вихідного тексту.

Узагальненою характеристикою випадковості будь-якої сукупності чисел, в тому числі і досліджуваних двійкових послідовностей, є ентропія:

$$H = \sum_{i=0}^{N-1} P_i * \log_2 P_i. \qquad (5)$$

Ентропія максимальна для рівноймовірних випадкових послідовностей, коли:

$$P_i = 1/N_1 = const, \qquad \mathrm{H}_{max} = \log_2 N^{-1} \text{ [біт]}. \tag{6}$$

Аналізу підлягає байтова структура шифртексту, тоді $N^{-1} = 2^8$.

$\mathrm{H}_{max} = 8$, якщо в експерименті ентропія H близька до H_{max}. Таким чином, дана характеристика свідчить про близькість експериментально одержуваних вибіркових розподілів ймовірності шифртексту і шифрограм до рівноймовірних розподілів для ключів всіх досліджених довжин і відкритих текстів будь-яких типів. У статистиці більше за інших використовують розподіл у вигляді χ^2

У нашому випадку приймаємо гіпотезу рівноймовірного розподілу досліджуваної послідовності, і тоді:

$$P_i = 1/N_1 = 1/2^8 \text{ [біт]} \tag{7}$$

При $\mathrm{E} > 30$ ($\mathrm{E} = N^{-1} - 1 = 255$ – розподіл степенів свободи) розподіл величини:

$$\chi_{\text{ср.}} = \sqrt{2\chi^2} - \sqrt{2E},$$
$$\chi^2 = \sum_{i=0}^{N^1-1} \frac{(v_i - N_1 * P_i)^2}{N_1 P_i}, \text{ при (7) має вигляд: } \chi^2 = \sum_{i=0}^{255} \frac{(v_i - N_1 2^{-8})^2}{N_1 2^{-8}} \tag{8}$$

близько до нормального з нульовим математичним очікуванням і одиничною дисперсією.

Для перевірки правдоподібності гіпотези про равновероятном розподілі досліджуваних послідовностей шифртексту і шифргамми проводяться наступні дії:

1. Обчислюється величина χ^2 для прийнятого в експерименті обсягу вибірки $N_1 = 2^{13} = 8192$ байту, то отримуємо:

$$\chi^2 = \sum_{i=0}^{255} \frac{(v_i - 32)^2}{32} \tag{9}$$

2. Обчислюємо величину $\chi_{\text{ср.}}$

Оскільки розподіл величини $\chi_{\text{ср.}}$може вважатися практично нормальним (10) (число ступенів свободи E = 255) з нульовим математичним очікуванням і одиничною дисперсією, то відхилення $\chi_{\text{ср.}}$ від математичного очікування не більше ніж на три одиниці гарантує високу значимість гіпотези про рівномовірному розподілі.

$$\chi_{\text{ср.}} = \sqrt{2\chi^2} - \sqrt{510} = \sqrt{2\chi^2} - 22{,}583179 \tag{10}$$

Для дослідження двійкової послідовності зашифрованих даних (шифртексту) і двійкової послідовності шифргаммі (ключового потоку) складається, так звана, маркувальна таблиця, яка, незалежно від довжини тестових файлів, являє собою таблицю об'ємом 28 осередків. Досліджувана двійкова послідовність розбивається на 8-розрядні байти і кожен байт розглядається як одне з 256 чисел. Таким чином, непересічні восьмиграми досліджуваної двійкової послідовності представляються як трирозрядні десяткові числа. На перетині відповідного рядка і стовпця у маркувальній таблиці записано кількість випадків, у яких дане число зустрілося серед N чисел у досліджуваній послідовності.

На основі маркувальних таблиць отримують наступні статистичні характеристики:

- значення максимального елемента таблиці Max;
- значення мінімального елемента таблиці Min;
- відхилення $\chi_{\text{ср.}}$ від математичного очікування;
- квадрата відхилення χ^2;
- ентропії H;

$$\mathrm{H} = -\sum_{i=0}^{255} \left(\frac{v_i}{N}\right)_i * \log_2 \left(\frac{v_i}{N}\right),$$

- полюсності за формулою (10)

$$P = (2N_1 - N)/\sqrt{N}, \qquad (10)$$

де: N_1 – кількість одиниць у послідовності. Якщо кількість одиниць рівна кількості нулів у дослід жувальній послідовності, то P=0.

Результат та обговорення. Вочевидь, що статистичні характеристики шифртексту повинні залежати від статистичних характеристик відкритого тексту і його довжини, а також і від вихідного значення ключового регістра. При цьому, чим вище ентропія відкритого тексту, тим більш високе значення ентропії слід очікувати в шифртексту. Цей же результат, в загальному випадку, найбільш вірогідний при збільшенні довжини відкритого тексту. Структура змісту ключового регістра найчастіше призводить до збільшення ентропії шифртексту у випадках, коли кількість одиничних символів приблизно дорівнює числу нульових символів. Незалежно від конкретного криптоалгоритму найменше значення ентропії шифртексту слід очікувати в разі такої структури відкритого тексту, що складається, наприклад, тільки з нульових або тільки з одиничних двійкових символів. Аналогічний висновок щодо ентропії можна зробити і для такої структури секретного ключа, що складається, наприклад, тільки з нульових або тільки з одиничних двійкових символів. Очевидно, поєднання цих двох умов в одному експерименті ставить криптоалгоритм в найбільш складне становище, тому значення наведених вище статистичних характеристик слід досліджувати саме для таких поєднань відкритих текстів і ключових послідовностей.

Об'єктом дослідження в процесі випробувань кожного криптоалгоритму були, перш за все, статистичні характеристики шифртексту. Однак, для потокових адитивних шифрів, до яких відноситься криптоалгоритм GAMMA 4, не менший інтерес представляють статистичні характеристики шифргамми (або ключової послідовності), тому за програмою обчислювалися статистичні характеристики послідовності, що являє собою порозрядну логічну суму шифртексту і відкритого тексту. Подібні обчислення статистичних характеристик аналогічної послідовності проводилися і для обох стандартних криптоалгоритмів.

Час обробки (шифрування) кожного файлу фіксувався вбудованими електронними годинами ПЕОМ з точністю до однієї сотої частки секунди. При цьому в інтервалі часу шифрування процесор не мав додаткових завдань. В якості секретних ключів для статистичних випробувань криптоалгоритмів використовувалися двійкові послідовності довжини:

- 56 біт для криптоалгоритму DES;
- 60 біт для криптоалгоритма GAMMA 4;
- 256 біт для кріптоалгоритма по ГОСТ 28147-89, що складаються:
- з одних двійкових символів"0";
- з одних двійкових символів "1";
- з випадкової (або псевдовипадкової) послідовності двійкових символів "0" або "1";

Як випадкові (або псевдовипадкові) синхросилки для статистичних випробувань криптоалгоритмів використовувалися двійкові послідовності довжини. Такі синхросилки формувались алгоритмом атрактора Лоренца:

- 56 біт для криптоалгоритму DES;
- 60 біт для криптоалгоритма GAMMA 4;
- 256 біт для кріптоалгоритма по ГОСТ 28147-89, що складаються:
- з одних двійкових символів " 0 " з одиницею в молодшому розряді;
- з одних двійкових символів " 0 " з одиницею в старшому розряді.

В якості тестових використовувалися файли довжини 8192 байта:

файл null_8.pas, що складається з 65536 двійкових символів “0”;

файл edin_8.pas, що складається з 65536 двійкових символів “1”;

файл teks_8.pas, що складається з 65536 двійкових символів "0" і " 1 " звичайного текстового документа.

Таким чином, використані в процесі випробувань сукупності тестових вхідних файлів і секретних ключів займають весь діапазон можливих структур даних і ключів від одного граничного положення до іншого, включаючи найчисленніші проміжні варіанти, що дозволяє судити про діапазон представлення вхідних даних програмних моделей.

Результати статистичних випробувань трьох алгоритмів захисту інформації наведені на рис. 20.

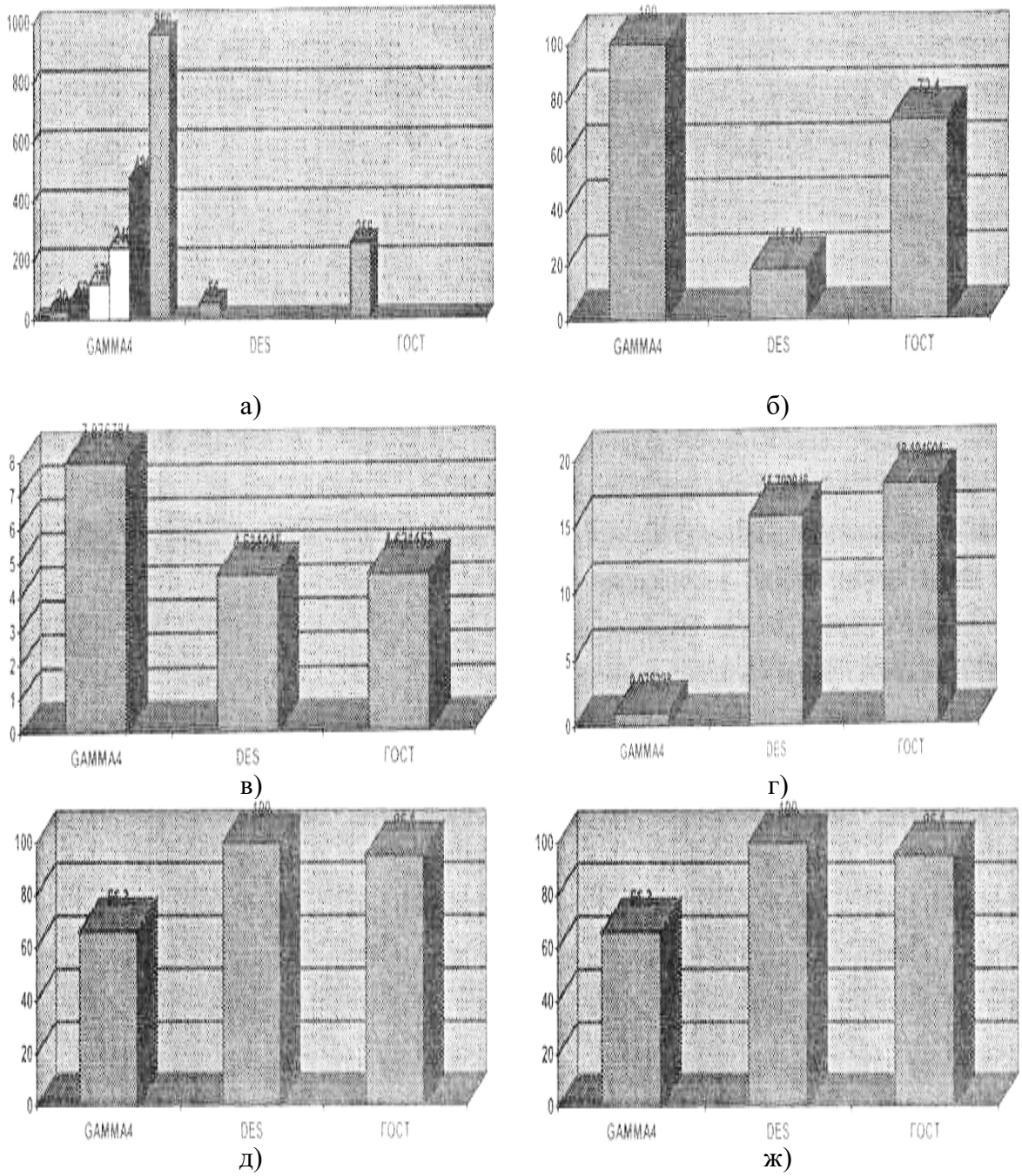


Рис. 20. - Результати статистичних випробувань, де: (а) – довжина ключа (практична стійкість), двійкових розрядів, (б) – швидкодія, %, (в) – ентропія шифртексту (ідеальне значення – 8.0), (г) – полюсність шифртексту (ідеальне значення – 0), (д)) - складність реалізації (відносний обсяг пам'яті для розміщення процедури шифрування), (ж) - середнє значення різниці елементів маркувальних таблиць (граничне значення = 0)

Отримані результати свідчать про досить високу ефективність алгоритму захисту GAMMA 4. Однак алгоритм GAMMA 4 в даний час не сертифікований і отже

може розглядатися лише як ефективний алгоритм цифрового маскування.

Основні висновки. Біфуркації у теорії динамічного хаосу відіграють ключову роль, оскільки саме вони визначають перехід системи від регулярного, детермінованого руху до хаотичного, стохастичного режиму. При цьому фазова траєкторія системи втрачає гладкість і змінює свою топологію, що є ознакою виникнення хаосу.

Аналіз коваріаційної функції показав, що навіть у малих часових вікнах вихідна послідовність має невеликий, але стійкий статистичний взаємозв'язок, що свідчить про певну структуру хаотичного сигналу.

Ймовірнісні характеристики випадкових процесів змінюються залежно від режиму роботи атрактора і можуть набувати вигляду різних функцій розподілу — від нормального до розподілу Парето та гамма-розподілу, що вказує на складність та різноманітність статистичних властивостей таких сигналів.

Підтверджено, що хаотична динаміка породжує аперіодичні послідовності з безперервним спектром, що є важливою властивістю для використання у системах захисту інформації.

Використання генераторів хаосу для формування шумових послідовностей у криптографічних алгоритмах дозволяє підвищити рівень скритності та стійкості систем, особливо в контексті активного зашумлення.

Атрактор Лоренца демонструє дві режимні поведінки — як генератор шуму та як автогенератор — при зміні параметра Rho, що змінює характер розподілу вихідних сигналів і робить його потенційно корисним у системах зв'язку, де шумова складова зазвичай оцінюється нормальним розподілом.

Хоча фрактальні розмірності атракторів є важливим параметром для кількісної оцінки складності систем, у цій роботі основна увага приділялась аналізу вихідних послідовностей, а не безпосередньому визначенню фрактальних розмірностей.

Всі досліджені атрактори є фрактальними множинами, що підтверджується графіками біфуркацій у фазовому просторі, а фрактальна самоподібність атрактора Лоренца базується на гіпотезі Пуанкаре, доведеній Григорієм Перельманом.

Список літератури

1. Rahman M., Hossain M., Hoque M. Chaos and Logistic Map Based Key Generation Technique for AES-driven IoT Security. *IEEE Access*. 2022. Vol. 10. P. 78150–78163. DOI: 10.1109/ACCESS.2022.3190076.
2. Pellicer-Lostao C., Lopez-Ruiz R. Pseudo-random bit generation based on 2D chaotic maps // *Computers & Mathematics with Applications*.– 2008. Vol. 59(10). P. 3258–3268. DOI: 10.1016/j.camwa.2009.08.036.
3. SP 800-90A Rev. 1. *Recommendation for Random Number Generation Using Deterministic Random Bit Generators* / National Institute of Standards and Technology (NIST). – Gaithersburg, MD, 2015. 76 p.
4. Nguyen V.H., Ha N.D., Nguyen T.T. Designing a Pseudo-Random Bit Generator with a Novel 5D Hyperchaotic System. *Applied Sciences*. – 2021. – Vol. 11(14). Article 6394. DOI: 10.3390/app11146394.
5. Song K., Li Y., Zhang H. A Hybrid Chaos-Based Cryptographic Framework for Post-Quantum Secure Communications. *IEEE Trans. on Information Forensics and Security*. – 2025 (in press). Preprint: arXiv:2403.12345.
6. Дмитрієв А.С. *Генерація хаосу* / А.С. Дмитрієв. М.: Техносфера, 2012. 424 с.
7. Філіпський Ю.К. *Випадкові процеси в радіо колах: навч. посібник* . Ю.К. Філіпський. – Одеса: Наука і техніка, 2012. 176 с.
8. Опис програмного забезпечення MICRO–CAP [Електронний ресурс]. Режим доступу: http://www.spectrum-soft.com/index.shtm
9. Логвинов В.В., Фриск В.В. *Схемотехніка телекомунікаційних пристроїв, радіоприймальні пристрої систем мобільного та стаціонарного радіозв'язку, теорія електричних кіл*. М.: СОЛОН–ПРЕСС, 2011. 656 с.

APPLICATION OF CHAOS IN KEY GENERATION ALGORITHMS

O.V. Ahadzhanian, A.R. Ahadzhanian, O.A. Syropiatov

National Odesa Polytechnic University
1, Shevchenko Ave., Odesa, 65044, Ukraine
Emails: o.v.ahadzhanian@op.edu.ua, 7985798@op.edu.ua, o.a.syropiatov@op.edu.ua

Modern requirements for the security of information systems focus on the latest methods of generating cryptographic keys, one of which is the use of the properties of chaotic systems, which makes them promising sources of entropy for cryptography. Research objective: To analyze the possibilities of using chaotic dynamic systems, in particular autogenerators, for generating cryptographic keys in information protection systems. The scientific and practical significance of the work lies in substantiating the effectiveness of chaotic generators for forming high-entropy pseudorandom sequences and their application in creating secure key generation systems in accordance with modern security requirements. The research methodology includes a theoretical analysis of chaotic dynamic systems, a study of the modes of autogenerators using the example of the Lorentz attractor, as well as statistical and probabilistic analysis of signals with an assessment of their distributions and correlations.Main results and conclusions: It was determined that bifurcations are critical points of the system's transition to a chaotic mode that generates signals with high entropy. It is shown that chaotic generators are able to work as noise generators and autogenerators, changing the characteristics of the distribution of output signals. It is confirmed that the output sequences are aperiodic and can have a continuous spectrum, which is a key property for cryptographic stability. The feasibility of using chaos in algorithms for generating noise sequences for information protection is justified.Value of the study: The work has made a significant contribution to understanding the role of chaotic systems in cryptography, in particular in creating new algorithms for generating keys with a high degree of entropy, which expands the range of information security tools. Practical significance: The results obtained can be used in the development of hardware and software cryptographic key generators based on chaotic systems, which will increase the security of information systems from unauthorized access and attacks.

Keywords: chaos, key generation, cryptography, autogenerator, entropy, Lorentz attractor, pseudorandom sequences