УДК 004.056.26

Тимченко Д. І.

Салієва О. В.

ЗАСТОСУВАННЯ СТОХАСТИЧНИХ ПРОЦЕСІВ ДЛЯ ШИФРУВАННЯ ТЕКСТОВИХ ПОВІДОМЛЕНЬ

Вінницький національний технічний університет

Анотація

У роботі розглянуто підходи до використання стохастичних процесів у задачах шифрування текстової інформації. Наведено основні моделі стохастичних процесів, що застосовуються для генерації ключів, маскування даних і побудови випадкових перестановок. Проаналізовано переваги та обмеження такого підходу порівняно з класичними методами криптографії.

Ключові слова: стохастичні процеси, шифрування, криптографія, ланцюги Маркова, випадкові ключі.

Abstract

This paper explores the use of stochastic processes in encrypting textual information. The main stochastic models for key generation, data masking, and random permutation construction are described. Advantages and limitations of this approach compared to classical cryptographic methods are analyzed.

Key words: stochastic processes, encryption, cryptography, Markov chains, random keys.

Вступ

Сучасні криптографічні системи дедалі частіше поєднують детерміновані алгоритми з елементами стохастичного моделювання для підвищення рівня захищеності інформації. Стохастичні процеси дозволяють створювати динамічні, непередбачувані ключі шифрування, що ускладнює криптоаналіз і робить злам системи практично неможливим без знання стохастичної моделі. Мета цієї роботи – дослідити принципи застосування стохастичних процесів у шифруванні текстових повідомлень і визначити їх потенціал для побудови адаптивних систем безпеки.

Результати дослідження

У процесі дослідження розглянуто підходи до застосування стохастичних процесів у системах шифрування текстових повідомлень, що дозволяють створювати криптографічні механізми з високим рівнем ентропії та непередбачуваності [1]. В основі такого підходу лежить ідея про те, що випадковість, керована математичними моделями, може забезпечити більш гнучкий і захищений процес шифрування даних у порівнянні з детермінованими алгоритмами.

Одним із найбільш поширених інструментів у цьому контексті є ланцюги Маркова, які використовуються для генерації ключових послідовностей або псевдовипадкових перестановок символів [2]. Марковський підхід надає змогу моделювати залежність між символами тексту або елементами ключа, формуючи стохастичний процес, у якому майбутній стан залежить від попереднього, але не від усього ланцюга. Це дозволяє створювати ключі, що водночас є випадковими та керованими, забезпечуючи баланс між хаотичністю та контрольованістю. Завдяки цьому метод може бути адаптований до шифрування природномовних текстів, де певна статистична структура (наприклад, частоти букв або слів) може бути навмисно порушена чи замаскована для підвищення стійкості системи до частотного аналізу [2].

Важливе місце в дослідженні займає застосування процесів Пуассона для керування часовими характеристиками передавання зашифрованих даних. У таких моделях часові інтервали між передачею блоків або символів генеруються випадковим чином, що унеможливлює виявлення закономірностей у потоці повідомлення [3]. Наприклад, у системах, де текст передається мережею у вигляді послідовності зашифрованих пакетів, пуассонівський розподіл може використовуватися для визначення часу надсилання кожного пакета, тим самим приховуючи реальну структуру та довжину повідомлення. Такий

підхід ефективно протидіє атакам, що базуються на аналізі трафіку, і може бути корисним у стеганографічних системах.

Іншим перспективним напрямом є введення стохастичного шуму на етапі шифрування або формування ключа [4]. Зокрема, моделі броунівського руху, білого шуму чи стохастичних диференціальних рівнянь можуть використовуватися для генерації шумових сигналів, що додаються до тексту перед або після шифрування. Такі шумові компоненти виконують роль додаткового маскування структури повідомлення, що унеможливлює відновлення вихідного тексту навіть у випадку часткової компрометації системи. Випадковість при цьому контролюється детермінованими параметрами – наприклад, ініціалізаційним вектором або початковим станом генератора, який може змінюватися за певним законом.

Окремий інтерес становлять гібридні стохастично-детерміновані методи шифрування, у яких традиційні криптографічні алгоритми (наприклад, AES, RSA чи ChaCha20) доповнюються випадковими стохастичними модифікаторами. Стохастичний процес у таких системах може впливати на порядок перестановок, довжину блоку, зміщення ключа або параметри хеш-функції. Це створює багаторівневий захист, при якому навіть відомий алгоритм без конкретного стохастичного параметра стає практично нерозв’язним.

Крім того, стохастичні процеси можуть застосовуватися для динамічного оновлення ключів під час тривалих сесій зв’язку [5]. На відміну від класичних схем, де ключ є статичним протягом певного часу, стохастичний підхід дозволяє змінювати ключ у непередбачувані моменти згідно з випадковою функцією часу. Це ускладнює будь-які спроби перехоплення або реконструкції ключа за допомогою методів криптоаналізу.

Використання стохастичних процесів має низку очевидних переваг. По-перше, це підвищена стійкість до статистичних атак, оскільки випадковий характер формування ключів і параметрів робить неможливим відновлення закономірностей. По-друге, стохастичні системи можуть бути адаптивними, змінюючи свої параметри у відповідь на зовнішні умови або спроби злому. По-третє, випадковість забезпечує високий рівень ентропії, що є ключовою характеристикою надійності криптографічної системи. Такий підхід також добре поєднується з технологіями штучного інтелекту, які можуть прогнозувати оптимальні параметри стохастичної моделі для кожного конкретного сценарію використання.

Водночас, застосування стохастичних процесів супроводжується певними недоліками та технічними викликами. Найбільш критичною проблемою є забезпечення синхронізації генераторів випадкових послідовностей на стороні відправника та одержувача. Будь-яке відхилення у генерації навіть на один крок може призвести до неможливості дешифрування. Другою проблемою є підвищене навантаження на обчислювальні ресурси, адже реалізація складних стохастичних моделей потребує великої кількості операцій із плаваючою точкою або генерації великих обсягів випадкових даних.

Додатковим викликом є необхідність забезпечення відтворюваності стохастичного процесу [5]. У криптографії це особливо важливо, оскільки для розшифрування потрібна точна реконструкція випадкової послідовності, яка використовувалася під час шифрування. Для цього застосовують різні механізми ініціалізації стохастичних процесів за допомогою спільного секретного насіння (seed) або функцій, що генерують відтворювані випадкові траєкторії.

Таким чином, стохастичні процеси утворюють потужний математичний інструментарій для побудови сучасних криптографічних систем. Вони забезпечують високу гнучкість, здатність до самоадаптації та непередбачуваність, що є ключовими чинниками інформаційної безпеки в умовах постійного розвитку засобів криптоаналізу.

Висновок

Стохастичні процеси відкривають нові можливості для побудови гнучких і надійних систем шифрування текстових повідомлень. Використання випадкових імовірнісних моделей дозволяє створювати криптосистеми, які динамічно адаптуються до умов роботи, ускладнюючи їх злам. Подальші дослідження можуть бути спрямовані на розробку ефективних методів синхронізації та оптимізації стохастичних генераторів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Shannon C. Communication Theory of Secrecy Systems. Bell System Technical Journal, 1949.
2. Приймак М. В., Млинко Б. Б. Періодичні ланцюги маркова та їх використання в задачах електроенергетики. Математичні методи та моделі технічних і економічних систем. Тернопільський національний технічний університет ім. Івана Пулюя, Україна. URL: https://elartu.tntu.edu.ua/bitstream/lib/39315/2/MMMTES_2022_Pryimak_M_V-Periodic_markov_chains_48-50.pdf (дата звернення: 23.10.2025).
3. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. CRC Press, 1996.
4. Brown R. Stochastic Methods in Cryptography and Data Security. IEEE Transactions on Information Theory, 2021.
5. Основні поняття теорії сигналів. КНУБА. Основи теор. кіл, сигнали та проц. в електроніці. URL: https://org2.knuba.edu.ua/mod/book/view.php?id=23040&chapterid=131 (дата звернення: 24.10.2025).

Тимченко Денис Ігорович – студент групи 2КІТС-24м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: denesonik03@gmail.com

Науковий керівник: ***Салієва Ольга Володимирівна*** − доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@vntu.edu.ua

Tymchenko Denys I. – student of 2KITS-24m, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: denesonik03@gmail.com

Supervisor: ***Saliieva Olha V.*** − Doctor of Philosophy (PhD) in 125 "Cybersecurity", Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: salieva8257@vntu.edu.ua