УДК 004.056.55:004.934:517.9
DOI: 10.31673/2409-7292.2024.040001

Грищук О. М.

АЛГОРИТМ ГЕНЕРУВАННЯ КЛЮЧІВ ШИФРУВАННЯ В СИМЕТРИЧНІЙ КРИПТОГРАФІЧНІЙ СИСТЕМІ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ НА ОСНОВІ ДИФЕРЕНЦІАЛЬНИХ ПЕРЕТВОРЕНЬ

Стрімкий еволюційний розвиток інформаційних технологій та створення квантових комп'ютерів стали провісниками настання постквантового криптоперіоду під час якого класичні симетричні та асиметричні криптографічні системи стають особливо вразливими. У першому випадку для компрометації симетричних криптографічних систем в постквантовий період достатньо результативно використовуються алгоритми Гровера, у другому – алгоритми Шора відповідно. Таким чином, потенційні вразливості відомих криптографічних систем можуть призвести до значного зниження рівня захищеності об'єктів захисту, особливо тих з них, які віднесені до категорії об'єктів критичної інфраструктури або включені до контуру управління національною безпекою та обороною держави. Тому з метою розроблення гарантовано захищених криптографічних систем захисту інформації на основі диференціальних перетворень в основу криптографічних алгоритмів яких покладено інтегральні рівняння Фредгольма першого роду в статті розроблено відповідний алгоритм генерування ключів шифрування. В якості вихідних даних для генерування ключів шифрування запропоновано використовувати елементарні функції. Для типових алгебричних функцій, які відповідають вимогам, що висуваються до ключів шифрування на основі диференціальних перетворень побудовано їх диференціальні спектри, приведено модельні приклади. Відсутність у науковій літературі подібних рішень щодо побудови алгоритму генерування ключів шифрування в симетричній криптографічній системі захисту мовної інформації на основі диференціальних перетворень визначає пріоритетність одержаних в статті наукових результатів.

Ключові слова: алгоритм генерування, ключ шифрування, симетрична криптографічна система, диференціальні перетворення, диференціальний спектр, дискрета.

Вступ та постановка проблеми в загальному вигляді

Практика висуває жорсткі вимоги до систем захисту інформації інформаційно-комунікаційних систем критичного призначення [1]. Якість надання послуг такими системами значною мірою залежить від рівня гарантій із забезпечення системами захисту конфіденційності, цілісності, доступності та інших властивостей інформації, що захищається. У більшості випадків для гарантування захищеності інформації в системах захисту на сьогодні застосовуються симетричні та асиметричні криптографічні алгоритми [2]. Разом з тим в постквантовий період відомі криптографічні алгоритми належать до групи ризику, тобто потенційно можуть бути скомпрометованими [3]. Тому в умовах, що складуються розвиток нових криптографічних систем, відмінних від відомих, набуває особливої актуальності. У рамках зазначеної проблеми розроблення алгоритмів генерування ключів шифрування для таких систем є важливим науковим та практичним завданням.

Аналіз останніх досліджень і публікацій

Злам найскладнішого в світі ключа шифрування RSA-240 групою французьких та американських дослідників [4] черговий раз актуалізує проблему кібербезпеки [5]. Не виключається, що з розвитком квантових комп'ютерів [6] під загрозою буде злам ключів і інших криптоалгоритмів, наприклад AES-256 [7]. З аналізу відомих публікацій [8], [9] та ін. встановлено, що для захисту мовної інформації в комунікаційних системах критичного призначення пропонується застосовувати симетричну криптографічну систему на основі диференціальних перетворень [10]. Разом з тим, відомі підходи до вибору ключів шифрування для таких систем [11], [12] та ін. не розкривають алгоритм його генерування.

Серед можливих варіантів розроблення відповідного алгоритму генерування ключа шифрування в симетричній криптографічній системі слід відмітити працю [13]. Зокрема в [13] запропоновано модифікувати існуючий алгоритм генерування ключа за рахунок додаткового присвоєння випадкового індексу функціям шифрування. Але введення додаткових варіативних елементів в алгоритм генерування ключа шифрування не суттєво підвищує їх захищеність та стійкість, що пов'язано з розширенням шифротексту не більш ніж на 4,5% [13].

У ін. відомій публікації [14] в ході розроблення нових симетричних алгоритмів потокового шифрування на основі теорії хаосу в якості алгоритму генерування ключа запропоновано використовувати генератор ключа, що формує випадковий бітовий потік. Побудова генератора ключа для таких систем ґрунтується на принципах функціонування хаотичних динамічних систем, а саме динамічної системи Лоренца та одномірного логістичного відображення [14]. Такий підхід дозволяє генерувати лише вісім секретних ключів [14], що в умовах розвитку квантового криптоаналізу [6] можуть бути підібрані методом комбінаторного перебору. Зазначеного недоліку позбавлений алгоритм генерування ключів шифрування на основі шифру "прямокутні ґратки" [15], що дозволяє генерувати послідовності випадкових чисел у заданому діапазоні без повторення. Не зважаючи на достатню стійкість криптографічного алгоритму у разі використання згаданого алгоритму генерування ключа він не є стійким до частотного аналізу, що суттєво обмежує його застосування на практиці. Таким чином, виходячи з аналізу останніх досліджень і публікацій розроблюваний алгоритм генерування ключа шифрування симетричної криптографічної системи захисту мовної інформації на основі диференціальних перетворень повинен бути позбавлений недоліків відомих алгоритмів.

Мета статті полягає у розробленні криптографічного алгоритму генерування ключів шифрування в симетричній криптографічній системі захисту мовної інформації, який має складатися з чисел – дискрет диференціального спектру, що забезпечують гарантовану теоретичну та практичну криптостійкість.

Основні матеріали дослідження

Розробляючи алгоритм генерації ключів шифрування в симетричній криптографічній системі захисту мовної інформації на основі диференціальних перетворень, розглянемо в загальному вигляді, власне, саму криптографічну систему. Принцип шифрування та розшифрування мовної інформації [17] в такій системі описано в [10]. У формалізованому вигляді:

для шифрування мовної інформації він описується як

$$\begin{cases} \int\limits_a^b K(f,t)\, z(t)\, dt = u(f); \\ z(t) = A_m \cos\left(2\pi f_m t + \varphi_m(t) + \varphi_m\right); \\ X(k) = \dfrac{H^k}{k!}\left[\dfrac{d^k x(t)}{dt^k}\right]_{t=0}, \end{cases} \tag{1}$$

де $x(t) \equiv u(f)$;

для розшифрування мовної інформації відповідно –

$$\begin{cases} u(f) = \lim\limits_{\alpha \to 0} u_\alpha(f); \\ x(t) = \sum\limits_{k=0}^{k=\infty} \left(\dfrac{t}{H}\right)^k X(k), \end{cases} \tag{2}$$

де $u_\alpha(f) \equiv X(k)$.

У виразах (1) та (2) прийнято такі позначення: $z(t)$ – математична модель мовної інформації, що підлягає шифруванню, де: A_m – амплітуда сигналу, *В*; f_m – лінійна частота, *Гц*; t – час передачі голосового повідомлення, *с*; $\varphi_m(t)$ – фазова функція, *рад/с*; φ_m – початкова

© Грищук, О. М. (2024). Алгоритм генерування ключів шифрування в симетричній криптографічній системі захисту мовної інформації на основі диференціальних перетворень. Сучасний захист інформації, 4(60), 6–15. https://doi.org/10.31673/2409-7292.2024.040001.

фаза, *рад*; $K(f,t)$ – секретний ключ шифрування (ядро інтегрального рівняння Фредгольма першого роду), що підлягає генеруванню; $u(f)$ – зашифровані дані (шифрограма), які по відкритому каналу від відправника *Alice* передаються до одержувача *Bob*; $X(k)$ – пряме диференціальне перетворення оригіналу $x(t)$, який є безперервною, що диференціюється нескінченну кількість разів і обмежену разом з усіма своїми похідними функцією дійсного аргументу t; k – цілочисловий аргумент $k =: 0, 1, 2, \ldots$; H – масштабна стала, яка має розмірність аргументу t і часто обирається рівною відрізку $0 \le t \le H$, на якому розглядається функція $x(t)$; $\overline{\cdot}$ – символ відповідності між оригіналом $x(t)$ і його диференціальним зображенням $X(k)$. Пряме перетворення (третій вираз у (1)) дозволяє за оригіналом $x(t)$ знайти зображення $X(k)$, а зворотне перетворення (другий вираз у (2)) дозволяє за зображенням $X(k)$ отримати оригінал $x(t)$. Диференціальні зображення $X(k)$ називаються диференціальними *Т-спектрами*, а значення *Т-функції* $X(k)$, за конкретних значень аргументу k – дискретами; $u_\alpha(f)$ – розшифрована мовна інформація з точністю до параметра регуляризації α, де: $u_\alpha(f) = \frac{1}{\alpha} u(f) - \int_a^b K(f,t)\, z_\alpha(t)\, dt$; $z_\alpha(t)$ – мовна інформація, що підлягала шифруванню з точністю до параметра регуляризації α, $z_\alpha(t) \equiv z(t)$.

Зважаючи на описану вище процедуру шифрування (1) розкриємо сутність та зміст алгоритму генерування ключів шифрування в симетричній криптографічній системі захисту мовної інформації на основі диференціальних перетворень. Функціональну схему генерування ключів шифрування подано на рис. 1. Алгоритм складається з чотирьох функціональних блоків. Кожен з блоків алгоритму послідовно реалізує взаємообумовлені процедури генерування ключів шифрування.

У першому функціональному блоці в алгоритмі передбачено реалізацію процедури вибору ключа шифрування $K(f,t)$ з банку даних ключів шифрування, який наповнюється множиною елементарних (цілих та дробових раціональних алгебричних й трансцендентних) функцій.

У другому функціональному блоці алгоритму реалізується *процедура перевірки виконання вимог, які висуваються до обраного ключа шифрування* (див. рис. 1). Обґрунтуємо такі вимоги.

Враховуючи те, що криптографічні перетворення в симетричній криптографічній системі захисту мовної інформації на основі диференціальних перетворень реалізовані на основі інтегрального рівняння Фредгольма першого роду [10], то для забезпечення гарантованої теоретичної та практичної криптостійкості, яка випливає з некоректності по Ж. Адамару [18] до ключів шифрування слід висунути такі вимоги [12].

Вимога 1. При генерації ключа шифрування $K(f,t)$ в симетричній криптографічній системі захисту мовної інформації на основі диференціальних перетворень повинна виконуватися *вимога до неперервності* ядра інтегрального рівняння Фредгольма першого роду, тобто ядро повинно бути неперервним в квадраті $a \le f \le b$, $a \le t \le b$:

$$K(f,t) \in C[a,b]. \tag{3}$$

Вимога 2. Ключ шифрування $K(f,t)$ в симетричній криптографічній системі захисту мовної інформації на основі диференціальних перетворень, який описується ядром інтегрального рівняння Фредгольма першого роду, *повинен бути виродженим*. Виродженість ядра інтегрального рівняння в загальному вигляді описується виразом

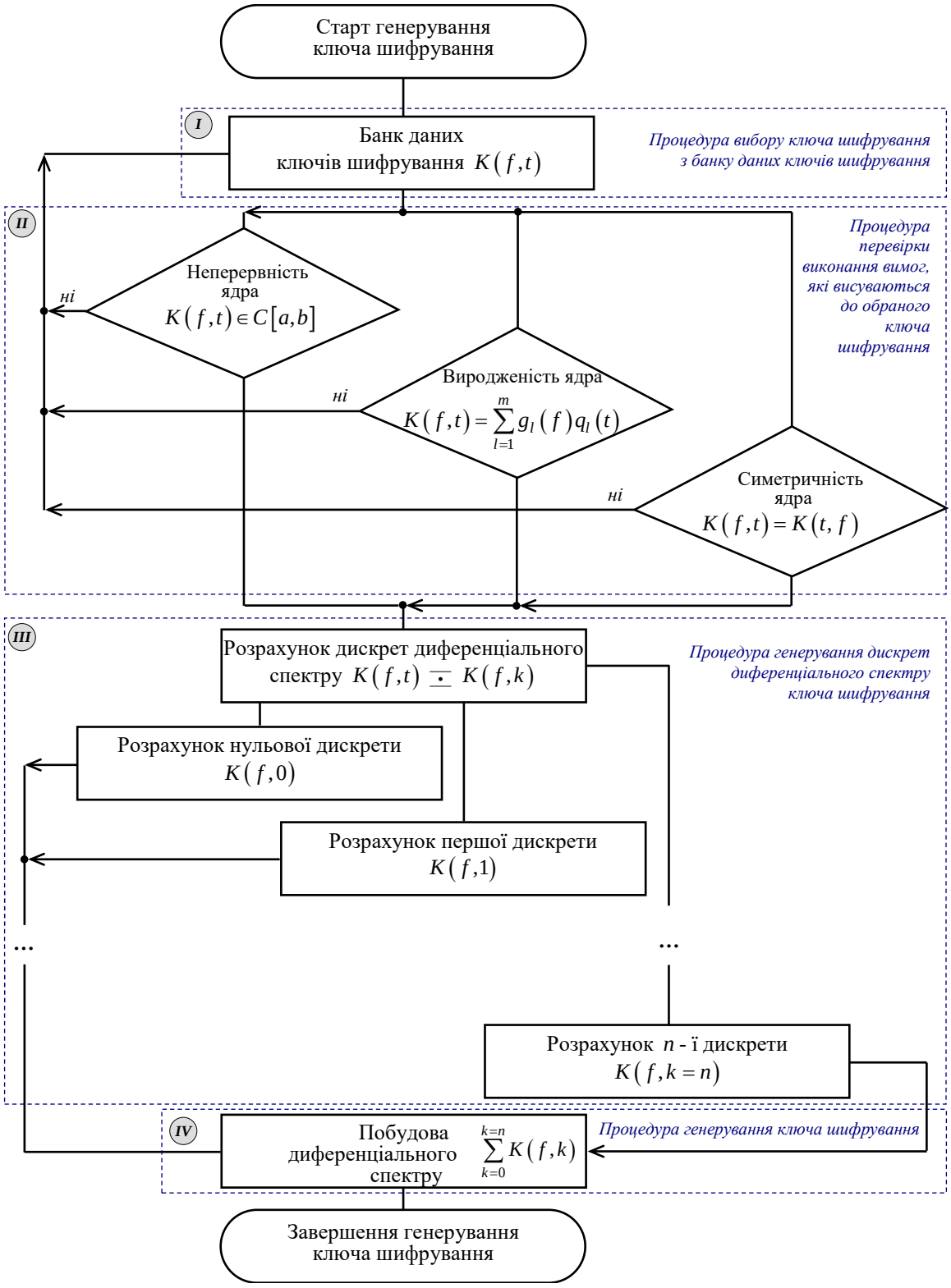


Рис. 1. Функціональна схема генерування ключів шифрування в симетричній криптографічній системі захисту мовної інформації на основі диференціальних перетворень: I–IV – функціональні блоки, які описують послідовність процедур генерування ключів шифрування

© Грищук, О. М. (2024). Алгоритм генерування ключів шифрування в симетричній криптографічній системі захисту мовної інформації на основі диференціальних перетворень. Сучасний захист інформації, 4(60), 6–15. https://doi.org/10.31673/2409-7292.2024.040001.

$$K(f,t)=\sum_{l=1}^{m} g_l(f)q_l(t). \quad (4)$$

Вимога 3. Ключ шифрування $K(f,t)$ в симетричній криптографічній системі захисту мовної інформації на основі диференціальних перетворень, який описується ядром інтегрального рівняння Фредгольма першого роду, *повинен бути симетричним*, тобто для довільних f та t з множини C при $f,t\in C$ повинна виконуватися рівність вигляду

$$K(f,t)=K(t,f). \quad (5)$$

Таким чином, вимоги (3)–(5) можна вважати справедливими для всіх ключів шифрування в симетричній криптографічній системі захисту мовної інформації на основі диференціальних перетворень, адже вони є загальними умовами розв'язності зворотної некоректної задачі – задачі розшифрування мовної інформації, яка описується інтегральним рівнянням Фредгольма першого роду. Отже, виконання згаданих умов закладає математичне підґрунтя для розшифрування (2) всіх криптограм, що отримуються на основі криптографічного алгоритму (1), а також забезпечення гарантованої теоретичної та практичної криптостійкості криптоалгоритму. У разі невиконання хоча б однієї з висунутих вимог (3)–(5) алгоритм (див. рис. 1) передбачає заміну ключа шифрування. У протилежному випадку алгоритм переходить до другої процедури.

У третьому функціональному блоці алгоритму на основі диференціальних перетворень (третій вираз в (1)) реалізується процедура генерування дискрет диференціального спектру $K(f,0)$, $K(f,1)$, …, $K(f,k=n)$ при різних значеннях цілочислового аргументу $k=:0,1,\ldots,n$.

Четвертий функціональний блок в алгоритмі є заключним. Він призначений для реалізації процедури генерування ключа шифрування $\sum_{k=0}^{k=n} K(f,k)$ у вигляді диференціального спектру, що є сумою всіх дискрет знайдених на попередньому кроці, тобто $\sum_{k=0}^{k=n} K(f,k)=K(f,0)+K(f,1)+\ldots+K(f,n)$.

Таким чином, послідовна реалізація зазначених процедур дозволяє генерувати різні ключі шифрування для симетричної криптографічної системи захисту мовної інформації на основі диференціальних перетворень.

Розглянемо модельні приклади генерування ключів шифрування за розробленим алгоритмом.

Модельний приклад загального вигляду.

Відповідно до першого функціонального блоку з банку даних ключів шифрування обирається ключ шифрування $K(f,t)$ у вигляді цілої алгебричної раціональної функції, наприклад вигляду (4).

У другому функціональному блоці перевіряється ключ шифрування (4) на предмет відповідності вимогам (3)–(5). У результаті маємо:

перевірка вимоги 1 щодо неперервності ядра інтегрального рівняння Фредгольма першого роду виконується, тобто ядро неперервне в квадраті

$$C=\{(f,t):\ a\le f\le b,\ a\le t\le b\}; \quad (6)$$

перевірка вимоги 2 щодо виродженості (4) ядра інтегрального рівняння Фредгольма першого роду $K(f,t)$ виконується;

перевірка вимоги 3 щодо симетричності (4) ядра інтегрального рівняння Фредгольма першого роду виконується, тобто

$$K(f,t)=\sum_{l=1}^{m} g_l(f)q_l(t) \Leftrightarrow K(t,f)=\sum_{l=1}^{m} g_l(t)q_l(f). \tag{7}$$

Генерування дискрет диференціального спектру для обраного ключа шифрування (4) *у третьому функціональному блоці* зводиться до прямого диференціального перетворення академіка Г. Пухова, тобто

$$X(k)=\frac{H^k}{k!}\left[\frac{d^k x(t)}{dt^k}\right]_{t=0} \Rightarrow \; \dot{-} \; K(f,k)=\sum_{l=1}^{m} g_l(f)Q_l(k), \tag{8}$$

де $g_l(f)$ – стала, $Q_l(k)$ – зображення оригіналу $x(t)\equiv q_l(t)$, $q_l(k) \; \dot{-} \; Q_l(k)=\frac{H_l{}^k}{k!}\left[\frac{d^k q_l(t)}{dt^k}\right]_{t=0}$.

Підставляючи послідовно значення цілочислового аргументу отримаємо:

для $k=:0$ $$K(f,0)=\sum_{l=1}^{m} g_l(f); \tag{9}$$

для $k=:1$ $$K(f,1)=\sum_{l=1}^{m} g_l(f)H_l\left[\frac{dq_l(t)}{dt}\right]_{t=0}; \tag{10}$$

для $k=:2$ $$K(f,2)=\sum_{l=1}^{m} g_l(f)\frac{H_l{}^2}{2}\left[\frac{d^2 q_l(t)}{dt^2}\right]_{t=0}; \tag{11}$$

для $k=:n$ $$K(f,n)=\sum_{l=1}^{m} g_l(f)\frac{H_l{}^n}{n!}\left[\frac{d^n q_l(t)}{dt^n}\right]_{t=0}. \tag{12}$$

Згенерований у четвертому функціональному блоці ключ шифрування (4) набуває вигляду диференціального спектру

$$K(f,k)=\sum_{l=1}^{m} g_l(f)\left(1+H_l\left[\frac{dq_l(t)}{dt}\right]_{t=0}+\frac{H_l{}^2}{2}\left[\frac{d^2 q_l(t)}{dt^2}\right]_{t=0}+\ldots+\sum_{l=1}^{m} g_l(f)\frac{H_l{}^n}{n!}\left[\frac{d^n q_l(t)}{dt^n}\right]_{t=0}\right). \tag{13}$$

Модельні приклади, що визначають частинні випадки, генерування ключів шифрування в симетричній криптографічній системі захисту мовної інформації на основі диференціальних перетворень на основі (6)–(13) подано в табл. 1. Диференціальні спектри для згенрованих ключів шифрування (див. рис. 1) подамо у вигляді суми дискрет (13) (рис. 2). На рис. 2 приведено графіки функцій ключів шифрування в області оригіналів та їх Т-спектри для згенерованих ключів шифрування на основі (13).

Таблиця 1

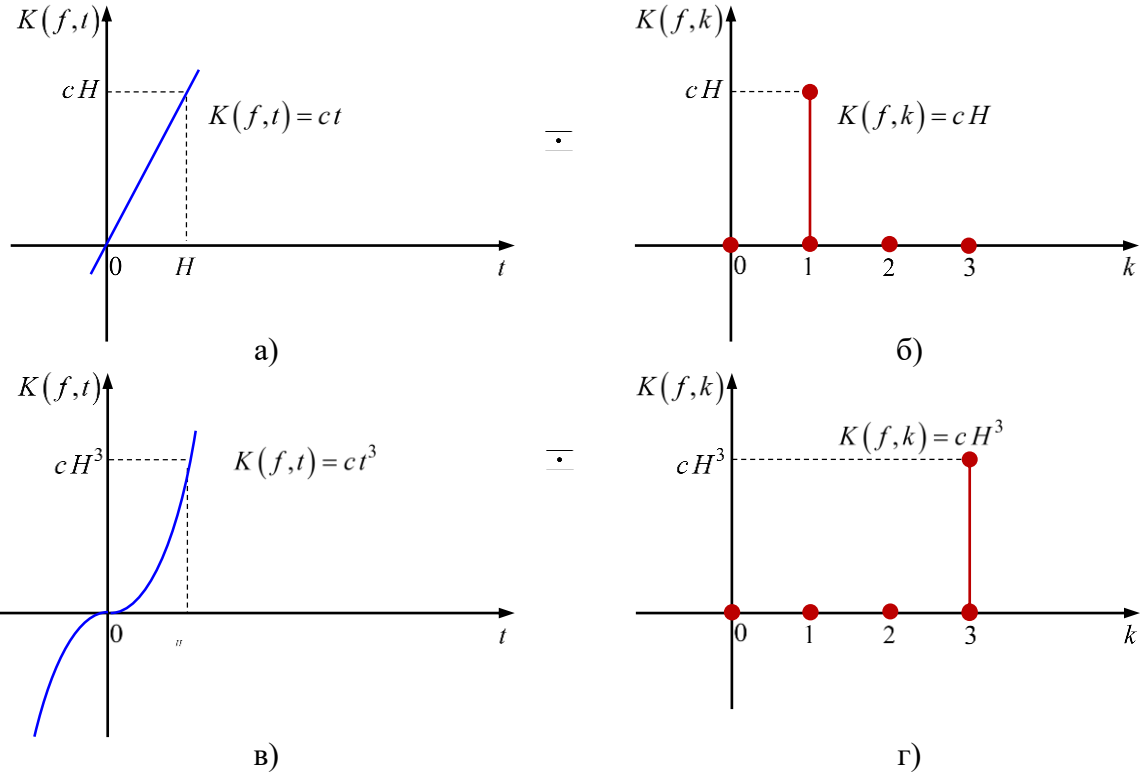
Результати генерування ключів шифрування на основі диференціальних перетворень за розробленим алгоритмом для різних класів елементарних функцій

Функція	**Функціональний блок алгоритму**			
	I	**II**	**III**	**IV**
лінійна	$q_l(t)=t$; $g_l(f)=c$, *де* $c=const$, $c>0$.	*вимоги 1–3 виконуються*	$Q(k)=H^k ъ(k-1)=\begin{cases}H^k, k=1;\\0, \quad k\neq 1,\end{cases}$ *де* $ъ(k-1)$ *– зміщена тета,* $ъ(k-1)=\begin{cases}1, k=1,\\0, k\neq 1.\end{cases}$ *Тоді* $K(x,k)=cH^k ъ(k-1)$, *для* $k=:0$ $K(x,0)=cH^0 ъ(0-1)=0;$ *для* $k=:1$ $K(x,1)=cH^1 ъ(1-1)=cH;$ *для* $k=:2$ $K(x,k\geq 2)=cH^2 ъ(2-1)=0.$	$K(x,k)=cH$
степенева	$q_l(t)=t^n$, *де* $n=3$; $g_l(f)=c$, *де* $c=const$, $c>0$.	*вимоги 1–3 виконуються*	$Q(k)=H^k ъ(k-n)=\begin{cases}H^k, k=n;\\0, \quad k\neq n,\end{cases}$ *де* $ъ(k-n)$ *– зміщена тета,* $ъ(k-n)=\begin{cases}1, k=n,\\0, k\neq n.\end{cases}$ *Тоді* $K(x,k)=cH^3 ъ(k-3)$, *для* $k=:0$ $K(x,0)=cH^0 ъ(0-3)=0;$ *для* $k=:1$ $K(x,1)=cH^1 ъ(1-3)=0;$ *для* $k=:2$ $K(x,2)=cH^2 ъ(2-3)=0;$ *для* $k=:3$ $K(x,3)=cH^3 ъ(3-3)=cH^3.$	$K(x,k)=cH^3$
показникова	$q_l(t)=a^t$, *де* a *- деяка стала,* $a>1$; $g_l(f)=c$, *де* $c=const$, $c>0$.	*вимоги 1–3 виконуються*	$Q(k)=\frac{(H\ln a)^k}{k!}$. *Тоді* $K(x,k)=c\frac{(H\ln a)^k}{k!}$, *для* $k=:0$ $K(x,0)=c\frac{(H\ln a)^0}{0!}=c;$ *для* $k=:1$ $K(x,1)=c\frac{(H\ln a)^1}{1!}=c\,H\ln a;$ *для* $k=:2$ $K(x,2)=c\frac{(H\ln a)^2}{2!}=\frac{c}{2}H^2\ln^2 a;$ *для* $k=:3$ $K(x,3)=c\frac{(H\ln a)^3}{3!}=\frac{c}{6}H^3\ln^3 a.$	$K(x,k)=c\left(1+H\ln a+\right.$ $\left.+\frac{1}{2}H^2\ln^2 a+\frac{1}{6}H^3\ln^3 a+...\right)$
показникова (експоненційна)	$q_l(t)=e^t$; $g_l(f)=c$, *де* $c=const$, $c>0$.	*вимоги 1–3 виконуються*	$Q(k)=\underline{\exp}T(k)=\frac{H^k}{k!}$, *де* $\underline{\exp}T(k)$ *– Т-експонента.* *Тоді* $K(x,k)=c\frac{H^k}{k!}$, *для* $k=:0$ $K(x,0)=c\frac{H^0}{0!}=c;$ *для* $k=:1$ $K(x,1)=c\frac{H^1}{1!}=cH;$ *для* $k=:2$ $K(x,2)=c\frac{H^2}{2!}=\frac{c}{2}H^2;$ *для* $k=:3$ $K(x,3)=c\frac{H^3}{3!}=\frac{c}{6}H^3.$	$K(x,k)=c\left(1+H+\right.$ $\left.+\frac{1}{2}H^2+\frac{1}{6}H^3+...\right)$

© Грищук, О. М. (2024). Алгоритм генерування ключів шифрування в симетричній криптографічній системі захисту мовної інформації на основі диференціальних перетворень. Сучасний захист інформації, 4(60), 6–15. https://doi.org/10.31673/2409-7292.2024.040001.

Продовження таблиці 1

Функція	I	II	III	IV
гармонічна	$q_l(t)=$ $=\sin 2\pi f t,$ $g_l(f)=c,$ *де* $c=const$, $c>0$.	*вимоги 1–3 виконуються*	$Q(k)=\underline{\sin}\,2\pi f T(k)=\frac{(2\pi f H)^k}{k!}\sin\frac{\pi k}{2},$ *де* $\underline{\sin}\,2\pi f T(k)$ – *T-синус.* *Тоді* $K(x,k)=c\frac{(2\pi f H)^k}{k!}\sin\frac{\pi k}{2},$ *для* $k=:0$ $K(x,0)=c\frac{(2\pi f H)^0}{0!}\sin\frac{\pi\cdot 0}{2}=0;$ *для* $k=:1$ $K(x,1)=c\frac{(2\pi f H)^1}{1!}\sin\frac{\pi}{2}=2c\pi f H;$ *для* $k=:2$ $K(x,1)=c\frac{(2\pi f H)^2}{2!}\sin\frac{\pi\cdot 2}{2}=0;$ *для* $k=:3$ $K(x,3)=c\frac{(2\pi f H)^3}{3!}\sin\frac{\pi\cdot 3}{2}=-\frac{4}{3}c\pi^3 f^3 H^3.$	$K(x,k)=2c\pi f H\times$ $\times\left(1-\frac{2}{3}\pi^2 f^2 H^2+\ldots-\ldots\right).$
	$q_l(t)=$ $=\cos 2\pi f t,$ $g_l(f)=c,$ *де* $c=const$, $c>0$.	*вимоги 1–3 виконуються*	$Q(k)=\underline{\cos}\,2\pi f T(k)=\frac{(2\pi f H)^k}{k!}\cos\frac{\pi k}{2},$ *де* $\underline{\cos}\,2\pi f\ T(k)$ – *T-косинус.* *Тоді* $K(x,k)=c\frac{(2\pi f H)^k}{k!}\cos\frac{\pi k}{2},$ *для* $k=:0$ $K(x,0)=c\frac{(2\pi f H)^0}{0!}\cos\frac{\pi\cdot 0}{2}=c;$ *для* $k=:1$ $K(x,1)=c\frac{(2\pi f H)^1}{1!}\cos\frac{\pi}{2}=0;$ *для* $k=:2$ $K(x,2)=c\frac{(2\pi f H)^2}{2!}\cos\frac{\pi\cdot 2}{2}=-2c\pi^2 f^2 H^2;$ *для* $k=:3$ $K(x,3)=c\frac{(2\pi f H)^3}{3!}\cos\frac{\pi\cdot 3}{2}=0.$	$K(x,k)=c(1-$ $-2\pi^2 f^2 H^2+\ldots-\ldots).$



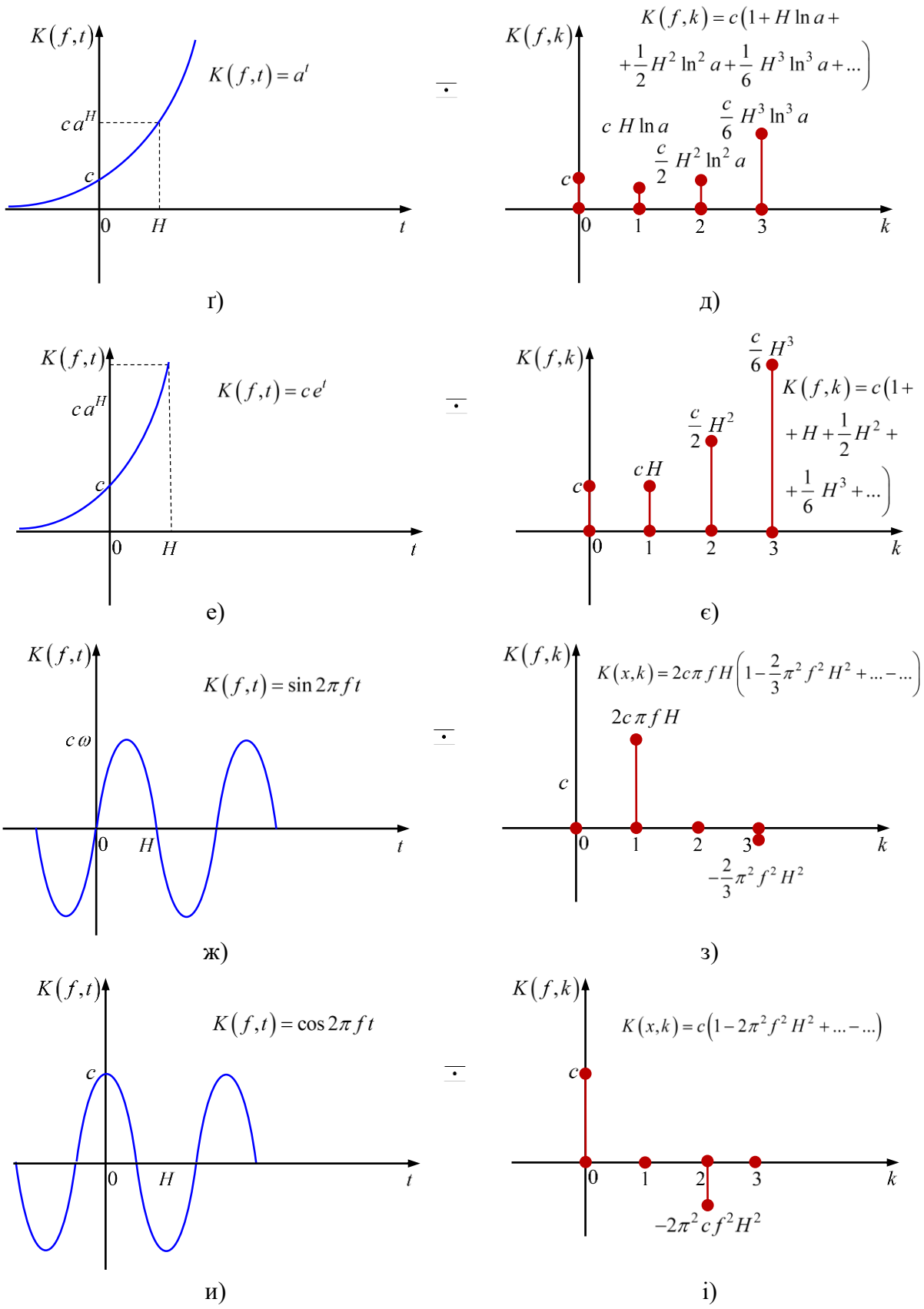


Рис. 2. Функції ключів шифрування: а, в, ґазда, е, ж, и – оригінали;
б, г, д, є, з, і – зображення

Висновки та перспективи подальших досліджень

Запропонований алгоритм генерування ключів шифрування в симетричній криптографічній системі захисту мовної інформації на основі диференціальних перетворень дозволяє генерувати необхідну кількість ключів шифрування для гарантованого захисту мовної інформації в інформаційно-комунікаційних системах. Кількість ключів шифрування обмежується: 1) множиною елементарних функцій, які відповідають вимогам, що висуваються до ключа; 2) кількістю дискрет диференціального спектра; 3) значенням констант для обраних ключів шифрування. Основною перевагою розробленого алгоритму є можливість генерування ключів в масштабі часу, близькому до реального, що забезпечується методом диференціальних перетворень академіка Г. Пухова, чим гарантується висока якість та одночасно надійність передачі захищеної мовної інформації в інформаційно-комунікаційних системах потокового шифрування. У подальшому планується розробити метод шифрування та розшифрування мовної інформації на основі запропонованого алгоритму.

Перелік посилань

1. Методологія синтезу моделей інтелектуальних систем управління та безпеки об’єктів критичної інфраструктури / С.П. Євсеєв, О.Ю. Заковоротний, О.В. Мілов, та ін. // – Харків: Вид. “Новий Світ-2000”, 2024. – 300 с. http://surl.li/lngnur.
2. Горбенко І. Д. Прикладна криптологія. Теорія, практика, застосування: монографія / І. Д. Горбенко, Ю. І. Горбенко. – Харків: Видавництво “Форт”, 2012. – 870 с. http://surl.li/dmdguh.
3. Samoriski J. H. Encryption and Hacking, Cyphers, Hacks and Attacks on the Digital Frontier / J. H. Samoriski // Reimagining Communication. – 2020. – Action (Vol. 3).– P. 89–106. https://doi.org/10.4324/9781351015233-5.
4. Boudot F. Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment / F. Boudot, P. Gaudry, A. Guillevic and et all // Advances in Cryptology – CRYPTO 2020. – Cham: Springer, 2020. – P. 62–91. https://eprint.iacr.org/2020/697.pdf.
5. Грищук Р. В. Основи кібернетичної безпеки : монографія / Р. В. Грищук, Ю. Г. Даник ; за заг. ред. проф. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с. http://surl.li/gvoxvw.
6. Jang K. Differential Cryptanalysis on Quantum Computers / K. Jang, Y. Oh, H. Seo // Cryptology ePrint Archive. – 2024. https://eprint.iacr.org/2024/783.pdf.
7. Baksi A. Quantum Analysis of AES / A. Baksi, K. Jang // Computer Architecture and Design Methodologies. – 2024. https://link.springer.com/chapter/10.1007/978-981-97-0025-7_6.
8. Криптографія нового покоління: інтегральні рівняння як альтернатива алгебраїчної методології / Г .К. Броншпак, А. Н. Ващенко, И. А. Громико та ін. // Прикладна радіоелектроніка. – 2014. – Т. 13, № 3. – С. 337–349. http://surl.li/iljehj.
9. Cryptography of a new generation: integral equations as an alternative of algebraic methodology (mini-presentation paper, with addition) / E. Perchik, G. Bronshpak, I. Gromyko and etc. // ResearchGate. – 2016. http://surl.li/urhwa.
10. Грищук Р. В. Узагальнена модель криптосистеми Фредгольма / Р. В. Грищук, О. М. Грищук // Кібербезпека: освіта, наука, техніка. – 2019. – № 4. – С. 14–23. DOI: 10.28925/2663-4023.2019.4.1423.
11. Грищук О. М. Диференціальний спектр мовної інформації/ О. М. Грищук // Захист інформації. – 2022. – Т. 24, № 3. – Р. 120–128. DOI: 10.18372/2410-7840.24.17189.
12. Грищук О. М. Особливості вибору ключа шифрування для криптосистеми Фредгольма / О. М. Грищук // Матеріали ІІ Всеукр. наук.-практ. конф. здобувачів вищої освіти й молодих учених [“Комп’ютерна інженерія і кібербезпека: досягнення та інновації”], (м. Кропивницький, 25–27 лист. 2020 р.) – Кропивницький : ЦНТУ, 2020. – С. 109–110. https://t.ly/BFNdH.
13. Hryshchuk O. Spectral Model of the Encryption Key for a Symmetric Cryptosystem Based on Differential Transformations / O. Hryshchuk // III International Scientific And Practical Conference [“Information Security And Information Technologies”], (Odesa, 13–19 Sept. 2021 y.). – CEUR Workshop Proceedings, 2021. – P. 1–5. https://t.ly/pKeKU.
14. Джулій В. М. Симетрична криптографічна система з нелінійним шифруванням та можливістю контролю шифротексту з метою маскування / В. М. Джулій, І. В. Муляр, В. С. Орленко та ін. // Вісник Хмельницького національного університету. – 2020. – № 6. – С. 33–38. https://t.ly/L0TIe.
15. Косован Г. В. Моделювання алгоритму генерування ключа шифрування інформації на основі динамічних систем / Г. В. Косован, М. Я. Кушнір, Л. Ф. Політанський // Східно-Європейський журнал передових технологій. – 2013. – Вип. 4/9 (64). – С. 39–43. DOI: 10.15587/1729-4061.2013.16391.
16. Грицюк Ю. І. Математичні основи процесу генерування ключів переставляння з використанням шифру Кардано / Ю. І. Грицюк, П. Ю. Грицюк. – Науковий вісник НЛТУ України. – 2015. – Вип. 25.10. – С. 311 – 323. DOI: https://doi.org/10.15421/40251048.
17. Корченко О. Порівняльний аналіз математичних моделей мовної інформації / О. Корченко, О. Грищук // Безпека інформації. – Т. 28, Вип. 2. – С. 48–56. DOI: 10.18372/2225-5036.28.16949.
18. Perchik E. Methodology of Syntheses of Knowledge: Overcoming Incorrectness of the Problems of Mathematical Modeling [Електронний ресурс] / E. Perchik // Kharkov, Ukraine. – 2018. https://arxiv.org/pdf/math-ph/0302045.
19. Пухов Г.Є. Диференційні спектри та моделі / Г. Є. Пухов. – К. : Наукова думка, 1990. – 184 с. http://surl.li/sucbgs.

Надійшла 07.10.2024