УДК 004.056.55
©Д. Маковецький[1] , П. Гаранюк[2], 2014

АНАЛІЗ МЕТОДІВ ТА ЗАГАЛЬНИХ ВЛАСТИВОСТЕЙ ГЕНЕРУВАННЯ КЛЮЧІВ ДЛЯ КРИПТОГРАФІЧНИХ ДОДАТКІВ

У статті розглянуто сучасні методи генерації ключів та ключової інформації для криптографічних додатків, проведено класифікацію та порівняльний аналіз оцінки якості існуючих методів генерації випадкових та псевдовипадкових послідовностей.

The modern methods of key generation and key information for cryptographic applications, the classification and comparative analysis of existing methods for evaluating the quality of random and pseudorandom sequences had been considered in the article.

1. ВСТУП

На теперішній час першорядним фактором, що впливає на політичну і економічну складові національної безпеки, є ступінь захищеності інформації та інформаційного середовища. Ось чому важливе, значення набувають питання забезпечення безпеки (інформації та інформаційного середовища.) Інформаційних і телекомунікаційних технологій і гарантованого захисту даних в комп'ютерних мережах економічно значущих структур.

Криптографічні методи знайшли широке застосування в практичній інформатиці для вирішення численних проблем інформаційної безпеки. У проблематиці сучасної криптографії можна виділити наступні три типи основних завдань:

- забезпечення конфіденційності (секретності);
- забезпечення анонімності (невідслідковності);
- забезпечення аутентифікації інформації джерела повідомлень.

На даний момент в Україні прийняті та виконуються Закони «Про електронні документи і електронний документообіг» [1], «Про електронний цифровий підпис» [2], «Про захист інформації в інформаційно-телекомунікаційних системах» [3], національні стандарти України [4-6], нормативні документи системи технічного захисту інформації [7,8], постанови Кабінету Міністрів України [9-11].

[1]Харьківський національний університет радіоелектроніки
[2]Національний університет «Львівська політехніка»

Однією з найважливіших складових в існуючих криптографічних системах, яка впливає на криптографічну стійкість і в цілому на безпеку криптографічного захисту інформації, є ключові данні та ключова інформація. На сьогоднішній час загальним підходом до генерування ключів, ключової інформації та параметрів є стандартизація методів, механізмів і практичних (конкретних) алгоритмів їх генерування. Були розроблені та прийняті спочатку регіональні, а потім і міжнародні стандарти, у яких були визначені вимоги, методи, механізми та алгоритми реалізації генераторів ключів та ключової інформації. (ISO/IEC 18031 [12], ANSI X9.82-3 [13], NIST SP 800-90 [14], NIST SP 800-22 [15])), згідно яких до цих генераторів висуваються жорсткі вимоги по критеріям нерозрізнюваності, необоротності, швидкодії тощо.

Основною складовою, яка визначає якість ключів, є генератори випадкових чисел (послідовностей). Випадкові числа використовуються для побудови гами в поточних криптосистемах, ключів сеансів та інших ключів у блочних криптосистемах, початкових значень, для генерації параметрів в асиметричних криптосистемах, випадкових значень параметрів для багатьох систем електронного цифрового підпису, "випадкових наборів" даних у протоколах аутентифікації тощо.

Визнаним є факт, що криптографічна стійкість криптографічних перетворень і безпечність реалізації різноманітних криптографічних протоколів суттєвою мірою залежать від того, яким чином генеруються та застосовуються різні види ключових даних (ключів).

2. ОСНОВНІ ДОДАТКИ ЗАСТОСУВАННЯ КЛЮЧІВ ТА КЛЮЧОВОЇ ІНФОРМАЦІЇ

На сьогоднішній час усі відомі криптографічні перетворення можна розділити на дві великі групи – симетричні та асиметричні. Класифікація та призначення криптографічних перетворень наведені на рис. 1

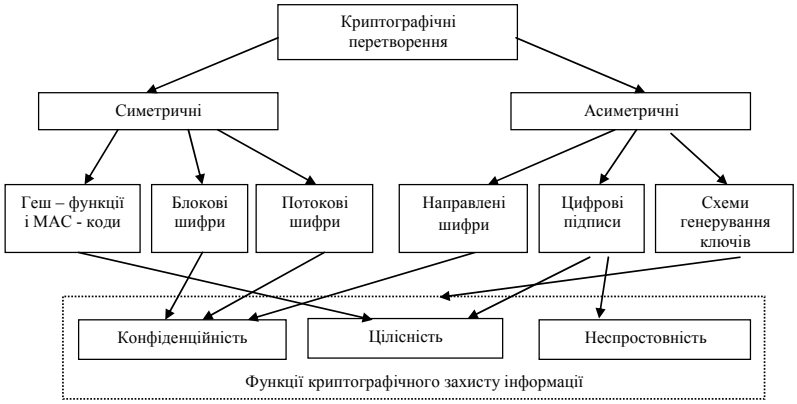

Рис. 1. Класифікація та призначення криптографічних перетворень

До симетричних крипто перетворень відносять криптографічні перетворення, для яких ключі прямого $К_{пр.пер.}$ та зворотного перетворень $К_{зв.пер}$ або співпадають, тобто

$$К_{пр.пер.} = К_{зв.пер.} \quad (1)$$

або можуть бути обчислені один знанні іншого не вище ніж з поліноміальною складністю. Симетричні крипто перетворення, у свою чергу, можна розділити на два великі класи – блокові шифри та потокові симетричні шифри.

До асиметричних відносяться крипто перетворення, у яких

$$К_{пр.пер.} \neq К_{зв.пер.} \quad (2)$$

один з ключів є особистим, або секретним, а інший відкритим. Причому обчислити особистий ключ при відомому відкритому можна не нижче ніж із субекспоненційною складністю.

Симетричні крипто перетворення, у свою чергу, можна розділити на два великих класи – блокові симетричні шифри (далі – БСШ) та потокові симетричні шифри. Функції хешування також необхідно відносити до симетричних криптографічних перетворень, оскільки в ключових функціях хешування використовуються симетричні криптографічні перетворення та ключі, що задовольняють вимозі (1).

Асиметричні криптографічні перетворення використовуються при здійсненні направленого шифрування, за де яких умов – при виконанні цифрового підпису, а також реалізації механізмів генерування ключів.

Усі наведенні на рис. 1 криптографічні перетворення застосовуються для надання таких послуг, як конфіденційність,

цілісність, автентичність (справжність), неспростовність і захист від несанкціонованого доступу.

Якщо $F_{пр}$ та $F_{зв}$ – функції прямого та зворотного крипто перетворень, то пряме перетворення, тобто зашифрування можна подати як перетворення вигляду

$$C_j = F_{пр} \ (M_j, Kз_j, P_r) \ , \qquad (3)$$

де M_j – блок довжини lб, що підлягає зашифруванню;

$Kз_j$ – ключ зашифрування блоку бітів M_j;

P_r – параметр криптографічного перетворення.

При зворотному перетворенні здійснюється розшифрування згідно з правилом:

$$Mj = Fзв \ (Cj, Kpj, Pr), \qquad (4)$$

де Kp_j – ключ розшифрування. Причому якщо $Kз_j = Kp_j$ то такі ключі симетричного криптоперетворення називаються симетричними ключами інволютивного шифру.

У цей час симетричні БСШ є основним криптографічним засобом забезпечення конфіденційності при обробці інформації в сучасних інформаційно – телекомунікаційних системах. Крім того блочні шифри використовуються для забезпечення цілісності, а також як базовий елемент при побудові інших криптографічних примітивів, таких як генератори псевдовипадкових послідовностей (далі – ГПВП), потокові шифри та функції гешування.

На цей час необхідно виділити три методологічних підходи до побудування перспективних БСШ . Перший пов'язаний з використанням SPN структур. Загальна структура – SPN, square – type, байт – байт орієнтований шифр. На основі таких структур були розроблені та здобули визнання БСШ Rijndael та його звужена версія AES (FIPS – 197), що побудовані на основі попередньої розробки авторів – шифру Square. У цьому напрямі було достатньо досліджень, за результатами яких було запропоновано використання в проекті стандарту БСШ "Калина" [16].

У процесі досліджень звернули увагу на БСШ, що мають IDEA – подібну структуру. Відомо, що де-факто Європейський стандарт IDEA пройшов великі випробування часом і до цих пір забезпечує задекларований рівень стійкості. На початку XXI століття було запропоновано проект вдосконаленого БСШ, що отримав назву FOX. Алгоритм IDEA NXT (раніше відомий як FOX), являє собою блоковий симетричний шифр та є нападником алгоритму IDEA і використовує розширену схему Лея – Массея, відомому своєю стійкістю до

криптоаналізу. Проект IDEA NXT є власністю швейцарської компанії MediaCrypt, якій належать права на поширення IDEA і яка є власником патентів на IDEA NXT. Шифр IDEA NXT являє собою сімейство різних модифікацій шифрів з різними розмірами блоків і розмірами ключів: Standard NXT64 (64 – бітовий блок, 128 – бітовий ключ, 12 раундів). Можуть бути також побудовані версії Standard з розміром ключа від 0 до 256 бітів, числом раундів від 2 до 255, а також можуть завантажуватися індивідуальні таблиці (sbox, матриця перестановок – permutation matrix), що заміняють стандартну таблицю.

В основу реалізації третього методологічного підходу покладено вже добре випробовувану Фейстель – подібну схему. Вона реалізована у випробуваних часом стандартах БСШ DES, DEA, IDEA, ГОСТ 28147 – 89, а також в MISTY1, Cammelia. На цей час стандарти БСШ, що мають Фейстель – подібну структуру, ще значною мірою застосовуються на практиці і не втратили перспективу застосування, можливо при деякому вдосконаленні.

Як наслідок БСШ знайшли широке застосування на практиці для розв'язання задач забезпечення конфіденційності, цілісності, доступності, захисту від несанкціонованого доступу тощо. Разом з тим, БСШ мають ряд недоліків, серед яких необхідно відмітити:

достатньо велика складність перетворень при шифруванні, треба виконувати багато перетворень і більше ідентичних циклів;

недостатньо швидкодія прямих і зворотних крипто перетворень, можна говорити, що забезпечується середня швидкодія. Так, при прикладенні суттєвих зусиль досягати швидкодії порядку Гбітів/с практично не можливо;

складність, а в ряді випадків і неможливість розпараллелювання процесів крипто перетворень;

всі блоки зашифровуються з використанням одного й того самого ключа тощо.

У той же час у ряді застосувань необхідно забезпечувати швидкодії в десятки та й сотні Гбітів/с.

Вирішення цього протиріччя покладається на потокові симетричні перетворення – потокові симетричні шифри (ПСШ). Необхідно відмітити, що зважаючи на вказані переваги ПСШ, на міжнародному рівні проведено та виконано ряд наукових – практичних результативних проектів - Nessie, eSTREAM. Так, за результатами виконання міжнародного проекту eSTREAM створено:

програмні шифри – HC 128, Rabbit, Salsa 20/12, Sosemanuk;

апаратні шифри – F – FCSR – H v2, Grain v1, MISKEY v2, Trivium.

На рис 2 наведено структурна схема каналу захищеного інформаційного обміну користувачів А та В, яки застосовують ПСШ. Нехай M_j – мова деякого алфавіту m джерела інформації А. Символи повідомлення m алфавіту M_j послідовно подаються на вхід шифратора. З ключового засобу попередньо або за необхідністю у шифратор зчитується початковий ключ K_n. Якщо шифрування здійснюється з безумовною стійкістю, то довжина такого ключа повинна бути не менше довжини повідомлення, що належить зашифруванню. Якщо потрібно забезпечити гарантовану (обчислювальну стійкість), у шифраторі на основі початкового ключа генерується гама зашифрування згідно за правилом:

$$\Gamma_i = \varphi(K_n, P_r), \qquad (5)$$

де Pr – параметри потокового шифру, у тому числі послідовність C_n або вектор ініціалізації.

При організації зв'язку на першому етапі кожного разу здійснюється передача вектора ініціалізації, яка разом із ключем визначає правило формування гам зашифрування та розшифрування. На другому етапі передачі здійснюється потокове зашифрування згідно з правилом:

$$C_i = (M_i + \Gamma_i) \bmod m\ . \qquad (6)$$

Джерело ключів забезпечує управління ключами та їх конфіденційність, цілісність, доступність, і справжність. Джерело ключів також забезпечує генерування ключової інформації, до складу якої може входити синхропослідовність (вектор ініціалізації). Таке зашифрування називається потоковим.

Далі символи передаються по відкритому каналу зв'язку.

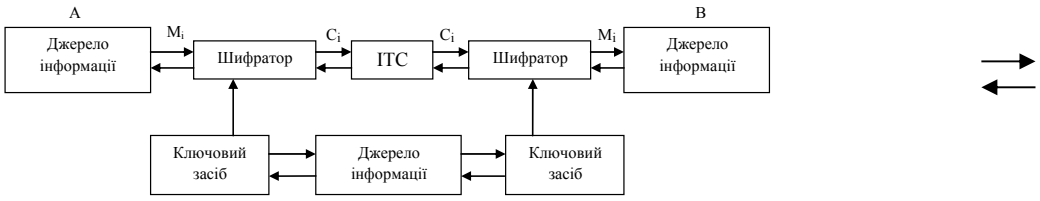

Рис. 2. Схема застосування ПСШ

Спочатку розшифрування на прийомі виділяється вектор ініціалізації, символи якого використовуються разом з ключем для генерування гами розшифрування. Але для правильного розшифрування C_n має бути прийнята правильно. За наявності хоча б однієї не виявленої помилки гама розшифрування буде генерована з помилками і здійснити розшифрування буде не можливо.

Одержавши криптограму та правильний вектор ініціалізації послідовності, користувач В здійснює потокове, тобто послідовне розшифрування криптограми Сі згідно з правилом:

$$C_i = (M_i - \Gamma_i) \bmod m . \qquad (7)$$

На при кінці символи розшифрованого повідомлення надходять одержувачу В.

Історично першими у 80-ті роки XX століття широкого розповсюдження набули асиметричні криптоперетворення (криптосистема) з відкритими ключами, що нині відома як RSA.

Основною особливістю RSA криптосистеми є її асиметричність, коли ключ зашифрування Кз не співпадає з ключем розшифрування $К_р$, тобто

$$К_{jз} \neq К_{jр}. \qquad (8)$$

А знайти один ключ при відомому другому для відповідних значень загальносистемних параметрів можна не нижче з субекспоненційною складністю. Хоча сьогодні RSA криптосистема подається нападам в щодо неї робляться різні прогнози, але вона проіснувала майже 35 років і дозволяє реалізовувати направлене шифрування (далі – НШ). Крім того RSA система дозволяє якісно реалізовувати криптографічними методами таку основну функцію, як спостережливість, у сенсі причетності відправника та одержувача. Так, причетність відправника може бути забезпечена за рахунок здійснення цифрового підпису з використанням особистого (таємного) ключа, а перевірка цілісності і справжності підписаної інформації здійснюється з використанням особистого (публічного)ключа. Направлене шифрування може бути здійснено з використанням другою ключової пари, відкритий ключ одержувача який застосовують для направленого шифрування, а особистий ключ застосовується для розшифрування повідомлення. Необхідно відзначити, що згідно з вимогами нормативних документів та міжнародних стандартів, в інформаційних технологіях повинні надаватися послуги причетності джерела та одержувача інформації (спостережливість) причетність джерела. Тобто авторство може бути забезпечено за рахунок

застосування електронного цифрового підпису (далі – ЕЦП). Складніше забезпечити причетність одержувача. Ця задача може бути розв’язана за рахунок використання направлених шифрів.

Особливістю крипто перетворень типу НШ є такі:

пряме криптографічне перетворення виконується з використанням відкритого ключа Кв;

зворотне криптографічне перетворення виконується з використанням особистого ключа Ко;

ключова пара (Кв , Ко) має бути випадковою та вибиратися із повної множини дозволених для використання ключових пар, причому

$$Кв \neq Ко. \qquad (9)$$

В асиметричних криптографічних системах ключі, як правило, є різним і один з них може бути визначений, якщо інший відомий не нижче ніж із субекспоненційною складністю. Відповідно в названих криптографічних системах використовуються симетричні або асиметричні криптографічні перетворення. В останні роки були визнані, набули розвитку і впроваджуються комбіновані протоколи криптографічного захисту інформації, включаючи встановлення й узгодження ключів. Практичне одночасне застосування симетричних і асиметричних криптографічних перетворень дозволило визначити їх основні недоліки та переваги щодо узгодження та встановлення ключів.

При застосування асиметричних криптографічних перетворень з'являються такі переваги та можливості:

немає необхідності розповсюдження групового таємного ключа або таємних ключів напрямків серед користувачів;

практичне надання користувачам з необхідною якістю послуг неспростовності власником інформації, відправником, тим, хто отримує і зберігає тощо;

особисте генерування асиметричної пари ключів і, як правило, можливість забезпечення необхідного рівня захищеності особистого ключа.

При використанні традиційних асиметричних криптоперетворень з відкритими ключами постає задача розв’язання таких проблемних питань:

створення і використання інфраструктури обслуговування відкритих ключів із забезпеченням їх цілісності, справжності, доступності, неспростовності та надійності;

забезпечення справжності відкритих ключів конкретного кожного користувача, наприклад, за рахунок зав'язування відкритого ключа з інформацією ідентифікації (як правило, це досягається виготовленням сертифікатів);

організаційно – технічна складність виведення з дії чи блокування відкритих ключів при їх компрометації тощо.

3. КЛАСИФІКАЦІЯ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ГЕНЕРУВАННЯ ПСЕВДО ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Основною складовою, що визначає якість ключів, є генератори випадкових чисел (далі – ГВЧ) або генератори випадкових послідовностей (далі – ГВП). Випадкові числа використовуються для побудови гами в поточних криптосистемах, ключів для сеансів (сеансових) та інших ключів у блочних криптосистемах, початкових значень, для генерації параметрів в асиметричних криптосистемах, випадкових значень параметрів для багатьох систем електронного цифрового підпису, "випадкових наборів" даних у протоколах автентифікації тощо.

Теорія генерації випадкових послідовностей вперше була розроблена Блюмом, Мікалі [17] і Яо [18] на початку 1980-х років. Блюм і Мікалі [17] висунули вимоги, розробили загальну модель криптографічно-стійких ГВП і запропонували першу конкретну реалізацію криптографічно-стійкого ГВП під назвою генератор Блюма – Мікалі. Потім Яо [18] показав як побудувати криптографічно - стійкий ГВП з використанням будь-якої односторонньої перестановки [19]. Хастад і інші [20] узагальнили цей результат і представили схему криптографічно-стійкого ГВП, який ґрунтується на використанні будь-якої односторонньої функції. Згідно вказаних робіт побудувати ГВП з односторонньою функцією не складно, тим більше що в [20] висунуті необхідні і достатні умови існування ГВП. Одностороння функція – це функція, яка дозволяє не вище ніж з поліноміальною складністю обчислити образ, а прообраз тільки з експоненційно складністю. Проте про існування теоретично досконалих односторонніх функцій не відомо. Кращими видами односторонньої функції в реальності вважаються функції блокового шифрування і криптографічні геш – функції. Якщо послабити вимогу ефективного обчислення ГВП, то можна знайти криптографічно-стійкі ГВП, які проходять всі

тестування поліноміального часу [19]. Келсі і інші [21] розглянули можливі криптографічні атаки на запропоновану модель ГВП. Вони досліджували ГВП з точки зору зловмисника і представили сильні і слабкі сторони чотирьох реальних ГВП: ANSI X9.17, DSA, RSAREF і CryptoLib. Проте аналіз Келсі і інших був здебільшого спеціалізований і заснований на евристичних аргументах. Дісай, Хеві і Інь [22] надали загальну структуру захисту для ГВП, об'єднавши атаки, про які зазвичай піклуються користувачі, і проаналізували генератори ANSI X9.17 і FIPS 186. В їх структурі захисту ГВП розглядалися з точки зору доказового захисту подібно тлумаченню захисту Беларе та інших [23]. В роботі Десая – Хеві – Іня надається конкретний аналіз захисту для ГВП, заснованих на ефективних криптографічних примітивах, таких як блокові шифри і геш - функції [19].

Генератори випадкових послідовностей, що засновані на геш – функціях, базуються на тому що геш - функції є важко оборотними, практично мають експоненційну складність. Вказані ГВП можуть використовувати будь-яку ISO/IEC криптографічну геш – функцію, що відповідає ISO/IEC 10118-3 [24], і можуть використовуватися застосуваннями, що вимагають різні рівні захисту, за умови використання відповідної геш – функції і забезпечення достатньої ентропії для початкового значення. Нині на міжнародному рівні проводиться заключний етап проекту створення перспективної геш – функції, значну перспективу мають кандидати на стандарт Skein і Blake [25]. Тому реалізація висунутих вимог не викликає сумнівів.

До ГВП, що засновується на геш – функції, висуваються такі припущення:

- вихідні дані геш – фу нкції є випадковими для різних вхідних даних;

- початкове значення має відповідну ентропію, що заснована на необхідних бітах захисту, аж до максимуму бітової довжини вихідних даних геш - функції.

- ГВП, що заснований на геш - функції, проектується відповідно різним рівням захисту в залежності від геш - функції, що використовується [25].

- довжина початкового значення дорівнює найбільшому розміру блоку гешованих вихідних даних ;

- повинна існувати можливість використання геш – функції декілька разів, включаючи процеси ініціалізації і пере ініціалізації.

- повинна завжди використовуватися однакова геш – функція, яка відповідає або перевищує бажану стійкість, що висувається криптографічним додатком.

У табл. 1 надано приклад затвердженої геш – функції, з ілюстрацією стійкості захисту, необхідної мінімальної ентропії і довжини початкового значення.

Таблиця 1

Значення стійкості, необхідної мінімальної ентропії і довжини початкового значення геш - функції

Геш-функція	Стійкість захисту	Мінімальна необхідна ентропія	Довжина початкового значення
Secure Hash-256 (SHA-256)	80	120	256
	112	120	256
	128	128	256
	192	192	256
	256	256	256

Загальна характеристика оцінка ГВП, що засновані на блоковому шифрі, ґрунтуються на використанні стандартизованих алгоритмів блокового шифрування. ГВП, що засновані на блоковому шифрі, описані в стандарті ISO/IEC 18031[12]. При цьому для обчислення геш – значення може використовуватись будь-який стандарт блокового шифрування, який відповідає вимогам, наприклад ISO/IEC 18033-3 [26]. Причому при застосуванні блокових шифрів різного рівня стійкості може забезпечуватись і різний рівень стійкості ГВП.

В таблиці 2 надано вимоги до стійкості захисту, ентропії і початкового значення, якщо використовується AES із ISO/IEC 18033-3.

Таблиця 2

Значення стійкості захисту, ентропії і початкового значення для ISO затвердженого блокового шифру

Алгоритм блокового шифрування	Стійкості захисту	Необхідна мінімальна ентропія	Довжина початкового числа (у бітах)
AES-128	80, 112, 128	128	256
AES-192	80, 112, 128, 192	192	320
AES-256	80, 112, 128, 192, 256	256	384

ГВП, заснований на блоковому шифрі, повинен ґрунтуватись на алгоритмі блокового шифрування в режимі лічильника, згідно вимог ISO/IEC 10116 [27]. Зрозуміло, що для всіх операцій повинні використовуватися одні і ті ж алгоритми блокового шифрування і довжина ключа.

Певні особливості та переваги, як і недоліки має ГВП, що ґрунтуються на складності вирішення теоретико числових задач (наприклад, задача дискретного логарифма, в тому числі в групі точок еліптичних кривих). Якщо генератор розроблений з урахуванням властивостей асиметричного крипто перетворення, то характеристики випадковості і/або непередбачуваності такого генератора будуть гарантуватися складністю пошуку рішення такої задачі. До такого типу генераторів можна віднести подвійний ГВП на еліптичній кривій і ГВП Майклі – Шнорра [28].

Подвійний ГВП на еліптичній кривій засновано на наступній важкій задачі [28], іноді відомій як «задача дискретного логарифму еліптичної кривої»: для заданих точок P і Q на еліптичній кривій порядку n необхідно знайти таке a, що $Q = aP$. Для ініціювання генерації *blocksize*-бітових псевдовипадкових послідовностей в подвійному ГВП на еліптичній кривій використовується початкове значення m-бітової довжини, а безпосередньо генерування ПВП виконується з використанням операції скалярного множень двох точок в групі точок еліптичних кривих. Такий алгоритм є необоротним навіть у випадку компрометації його внутрішнього стану. Пряма секретність також забезпечується, але тільки при аналізі з використанні даних, що доступні за межами ГВП.

4. ВИМОГИ ДО МЕТОДІВ ТА ЗАСОБІВ ГЕНЕРУВАННЯ КЛЮЧІВ ТА КЛЮЧОВОЇ ІНФОРМАЦІЇ

Нині загальним підходом до генерування ключів, ключової інформації та параметрів є стандартизація методів, механізмів і практичних (конкретних) алгоритмів їх генерування. Причому, як можна судити із ряду джерел, ці метод, механізми й алгоритми намагаються захистити від розповсюдження особливо в частині генерування випадкових послідовностей. Також, у зв’язку із суттєвим розвитком інфраструктури відкритих ключів, виникла потреба у

створенні апаратних, апаратно – програмних і програмних засобів генерування асиметричних пар ключів. Були розроблені та прийняті спочатку регіональні, а потім і міжнародні стандарти, у яких були визначені вимоги, методи, механізми та алгоритми реалізації генераторів. Причому у зв’язку з необхідністю відновлення ключів та ключової інформації у просторі й часі, у них в повному обсязі розглядаються тільки детерміновані генератори випадкових бітів, що визначає їх особливу актуальність.

Основними вимогами, що висуваються до генераторів ключової інформації є непередбачуваність, просторова і часова складність, відновлення у просторі й часі, необоротність, а також період повторення. Він має бути не менше заданого, подібно блочним симетричним шифрам, причому як заданий може використовуватись:

2^{128} – нормальний рівень стійкості;

2^{256} – високій рівень стійкості;

2^{512} – надвисокий рівень стійкості;

Запропоновано декілька підходів до визначення гарантій. Перший із них пов'язаний із тестуванням псевдовипадкових бітів (тобто випадкових бітів, сформованих детермінованим генератором випадкових бітів) на випадковість, для чого наприклад застосовується стандарт FIPS – 140 – 1 [31] або AIS 20 [32]. Більш детальним є вимоги та механізми реалізації визначені в AIS 20, що дозволяє реалізувати різні рівні гарантій – К1, К2, К3, К4. При цьому найвищій рівень гарантій є рівень К4. В AIS 31 [33] визначено два рівні гарантій Р1 і Р2, у яких по суті, Р1 дещо еквівалентний К1, К2, а в Р2 еквівалентний К3, К4. У випадку рівня гарантій К4 вимагається, щоб псевдовипадкові біти мали статистичні властивості, подібно до статистичних властивостей псевдовипадкових бітів, що генеровані ідеальним ДГВБ, була задана ентропія джерела ключів (тобто наявність ключа генератора є обов’язковою), а також має бути практично виключена можливість обчислення попередніх і наступних бітів генератора при відомому поточному стані.

Так, для реалізації потокового симетричного шифру до криптографічно стійкого генератора псевдовипадкової послідовності чисел (гами шифру) висуваються три основних вимоги:

період гами має бути досить великим для шифрування повідомлень різної довжини;

гама має бути практично непередбачуваною, що означає важливість передбачити наступний біт гами, навіть якщо відомі тип генератора і попередній відрізок гами;

генерування гами не повинно викликати великих технічних складностей.

Із наведеного вище можна зробити висновок, що від якості випадковості формування ключів, ключової інформації та системних параметрів суттєво залежить криптографічна стійкість. При цьому алгоритм генерації і тестування послідовностей випадкових чисел є базовими алгоритмами, що забезпечують дійсну криптографічну стійкість алгоритмів і механізмів криптографічного захисту інформації. Базовими міжнародними стандартами, що стандартизують алгоритм генерації послідовностей випадкових чисел, є [29, 30]:

міжнародний стандарт ISO/IEC 18031 “Information technology – Random number generation”, який визначає алгоритм генерації псевдовипадкових і випадкових чисел, а також визначає статистичні тести перевірки генераторів;

міжнародний стандарт ISO/IEC 18032 “Information technology – Prime number generation”, який визначає методи генерації простих чисел і методи тестування чисел на простоту;

національний стандарт ДСТУ ISO/IEC 19790 “Інформаційна технологія – Методи захисту – Вимоги щодо захисту криптографічних модулів”.

Додаткові вимоги до алгоритмів та реалізації методів та засобів генерації й тестування послідовностей випадкових чисел визначаються національними та промисловими стандартами США – FIPS 140-3, ANSI X9.17, ANSI X9.31, ANSI X9.44 та інші, а також рекомендаціями NIST – NIST SP 800-22 [15] і рекомендаціями органу із стандартизації Неметчіни – AIS 20 [32], AIS 31[33] та інші.

5. ВИСНОВКИ

Удосконалення та подальший розвиток систем, комплексів та засобів криптографічного захисту інформації в суттєвій мірі залежить від вирішення ряду проблемних питань, що пов’язані з генеруванням ключів, ключової інформації та загальносистемних параметрів. Із наведеного вище можна зробити висновок, що від якості випадковості формування ключів, ключової інформації та системних параметрів суттєво залежить криптографічна стійкість. ГВП та ГПВП є

важливішими складовими елементами криптографічних систем ключових даних і ключової інформації, від якості якої залежить стійкість криптографічних перетворень. На нинішній час достатньо добре розроблені основні складові, що стосуються стандартизації методів, механізмів та засобів генерування випадкових та псевдовипадкових бітів, а також методик та інструментарію тестування таких послідовностей бітів на випадковість. До них необхідно віднести ISO/IEC 19790, ISO/IEC 18031, AIS 20, AIS 31, FIPS 140-1, FIPS 140-2, FIPS 140-3. Разом з тим в процесі досліджень встановлено, що представлені в них методи та алгоритми мають ряд недоліків в частині суворого доведення періоду повторення, непередбачуваності, необоротності, нерозрізнюваності та складності (швидкодії) при формуванні псевдовипадкових бітів.

Результати проведеного аналізу існуючих методик генерації ключів та ключової інформації показали, що на цей час більшість ГВП хоча й мають прийнятну швидкодію, але мають багато серйозних недоліків, основними з яких є :

– недопустимо короткий або недоведений період повторення;

– послідовні значення бітів не є незалежними, що робить його передбачуваним;

– оборотність відносно визначення закону формування (ключа), що також робить його передбачуваним;

– властивості випадковості, рівноймовірності, незалежності та однорідності не відповідають вимогам тощо.

Існуючі ГВП та ГПВП будуються на основі використання блокових симетричних шифрів, перетворень в групі точок еліптичних кривих та функцій гешування.

ГВП на блокових шифрах є захищеними лише тоді, коли генеровані ними випадкові послідовності бітів є якомога короткими у порівнянні з розміром вихідного блоку шифру, що використовується.

ГВП на еліптичних кривих є обчислювально-складними. Застосування колізійно-стійких функцій гешування [34] дозволяє забезпечити структурну скритність псевдовипадкових бітів, але попередньо необхідно генерувати послідовність елементів (слів), що мають гарантований період повторення та інші властивості.

Не достатньо дослідженими є методи генерування псевдовипадкових бітів, що ґрунтуються на обчисленні у відповідності з ключовими даними елементів простих полів та підгруп полів Галуа, а

також подальшого гешування елементів полів та підгруп з використанням колізійно-стійких функцій гешування [34].

1. *Закон України № 851-IV «Про електронні документи та електронний документообіг» від 22.05.03.* ***2.*** *Закон України № 852-IV «Про електронний цифровий підпис» від 22.05.03.* ***3.*** *Закон України N 2594-IV «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005.****4.*** *Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка ДСТУ 4145-2002 – [Чинний від 2003-07-01]. – К.: Держстандарт України, 2003. – 31 с.- (Національний стандарт України).* ***5.*** *Алгоритм криптографического преобразования. Системы обработки информации. Защита криптографическая: ГОСТ 28147 89. – [введ. 1990-07-01]. М.: Госстандарт СССР, 1989. – 29с.* ***6.*** *Информационная технология. Криптографическая защита информации. Функция хеширования: ГОСТ Р 34.11-94 – Москва.: Госстандарт России, 1994.* ***7.*** *Нормативний документ системи технічного захисту інформації №53 «Типове положення про службу захисту інформації в автоматизованій системі» від 4 грудня 2000 р.* ***8.*** *Нормативний документ системи технічного захисту інформації № 22 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу від 28 квітня 1999 р.* ***9.*** *Постанова Кабінету Міністрів України № 680 «Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу» від 26.05.2004 р.* ***10.*** *Постанова Кабінету Міністрів України № 1452 «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності» від 28.10.2004 р.* ***11.*** *Постанова Кабінету Міністрів України № 1453 «Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади» від 28.10.2004 р.* ***12.*** *ISO/IEC 18031:2005(E). Information technology – Security techniques – Random bit generation.* ***13.*** *ISO/IEC 10118-3:2004. Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions.* ***14.*** *NIST SP 800-90. Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2006.* ***15.*** *NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. August 2008.****16.*** *A. K. Lenstra. Unbelievable security. Matching AES security using public key systems./ A. K. Lenstra.// In Advances in Cryptology – Asiacrypt 2001, volume 2248 of Lecture Notes in Computer Science. Springer-Verlag. – 2001. – P.67–86.* ***17.*** *M. Blum. How to generate cryptographycally strong sequences of pseudorandom bits / M. Blum, S. Micali // SIAM Journal on Computing. – Vol. 1. – 1986. P.850-864.* ***18.*** *A. C. Yao. Theory and applications of trapdoor functions / A. C. Yao //23rd IEEE FOCS. – 1982. – P.80-91.* ***19.*** *Ju-Sung Kang. Security frameworks for pseudorandom number generators / Ju-Sung Kang // Information Center for Mathematical Sciences. – Vol.8, Number 1. – 2005. – P.1-11.* ***20.*** *J. Hastad. Pseudorandom number generators from any one-way function / J. Hastad, R. Impagliazzo, L. A. Levin, M. Luby // SIAM Journal on Computing. – Vol. 28. – 1999. – P.1364-1396.* ***21.*** *J.*

Kelsey. Cryptanalytic attacks on pseudorandom number generators / J. Kelsey, B. Schneier, D. Wagner, C. Hall // FSE. – 1998. ***22.*** *A. Desai. A practice-oriented treatment of pseudorandom number generators / A. Desai, A. Hevia, Y. L. Yin // EUROCRYPT. – 2002. – P.368-383.* ***23.*** *M. Bellare. A concrete security treatment of symmetric encryption / M. Bellare, A. Desai, E. Jokipi, P. Rogaway // FOCS. – 1997.* ***24.*** *ISO/IEC 10118-3:2004. Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions.* ***25.*** *Шапочка Н.В. Перспективний генератор випадкових бітів на геш-функціях та його властивості / Шапочка Н.В. // Молодіжний форум «Радіоелектроніка і молодь у XXI ст.». – Харків – 2009.* ***26.*** *ISO/IEC 18033-3:2005. Information Technology – Security Techniques – Encryption Algorithms – Part 3: Block Ciphers.* ***27.*** *ISO/IEC 10116:2006. Information technology – Security techniques – Modes of operation for an n-bit block cipher.* ***28.*** *Daniel R. L. Brown. A Security Analysis of the NIST SP 800-90 Elliptic Curve Random Number Generator [Електронний ресурс] / Daniel R. L. Brown, Kristian Gjosteen // – 2007. – Режим доступу: http://eprint.iacr.org/.* ***29.*** *ISO/IEC 18031:2005(E). Information technology – Security techniques – Random bit generation.* ***30.*** *ISO/IEC 19790:2006 Information technology – security techniques – security requirements for cryptographic modules.* ***31.*** *Menezes A. Reducing elliptic curve logarithms to logarithms in a finite field. / Menezes A., Vanstone S., Okamoto T. // STOC '91: Proceedings of the twenty-third annual ACM symposium on Theory of computing. – New York, NY, USA: ACM. – 1991.* ***31.*** *Federal Information Processing Standards Publication (FIPS PUB) 140-1. Security requirements for cryptographic modules. NIST, 1994.* ***32.*** *Application Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 1999.* ***33.*** *Application Notes and Interpretation of the Scheme (AIS) 31. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 2001.* ***34.*** *Горбенко І.Д. Порівняльний аналіз генераторів детермінованих випадкових послідовностей на основі гешування елементів підгрупи / Горбенко І.Д., Шапочка. Н.В., Стадченко Е.В. // XIII Міжнародна науково-технічна конференція, Державна служба спеціального звязку та захисту інформації України. – 2010.*