**РЕФЕРАТ**

Обсяг роботи \_\_ сторінки, \_\_ ілюстрації, \_\_ таблиць, \_\_ додатки, \_\_ джерело літератури.

Об’єкт дослідження – алгоритми потокового шифрування із самосинхронізацією HBB, SSS, Moustique.

Предмет дослідження – дослідження та аналіз шифрів із самосинхронізацією за їх характеристиками, особливостями будови, швидкодією, огляд та імплементація криптоатак на ці шифри.

ПОТОКОВІ ШИФРИ, САМОСИНХРОНІЗАЦІЯ, HBB, SSS, MOUSTIQUE, АТАКА

Зміст

[ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ 4](#_Toc389755585)

[ВСТУП 5](#_Toc389755586)

[1 ОЗНАЧЕННЯ НЕОБХІДНИХ В РОБОТІ ТЕРМІНІВ ТА ПОНЯТЬ 8](#_Toc389755587)

[1.1 Базові поняття 8](#_Toc389755588)

[1.2 Основні типи криптографічних атак залежно від типу відомої інформації 9](#_Toc389755589)

[1.3 Блокові шифри 11](#_Toc389755590)

[1.4 Режими роботи блокових шифраторів 12](#_Toc389755591)

[1.5 Потокові шифри 15](#_Toc389755592)

[1.6 Синхронні потокові шифри 16](#_Toc389755593)

[1.7 Потокові шифри із самосинхронізацією 17](#_Toc389755594)

[1.8 Лінійні регістри зсуву 20](#_Toc389755595)

[2 ОГЛЯД ТА АНАЛІЗ 23](#_Toc389755596)

[2.1 Шифр Moustique 23](#_Toc389755597)

[2.1.1 Характеристики шифру Moustique 23](#_Toc389755598)

[2.1.2 Опис шифру Moustique 23](#_Toc389755599)

[2.2 Шифр SSS 28](#_Toc389755600)

[2.2.1 Характеристики шифру SSS 28](#_Toc389755601)

[2.2.2 Сімейство шифрів SOBER 28](#_Toc389755602)

[2.2.3 Основні операції, необхідні для імплементації шифру 29](#_Toc389755603)

[2.2.4 Генерація потокової послідовності 29](#_Toc389755604)

[2.2.5 S-Box 31](#_Toc389755605)

[2.3 Шифр HBB 32](#_Toc389755606)

[2.3.1 Характеристики шифру HBB 33](#_Toc389755607)

[2.3.2 Короткий опис клітинних автоматів 33](#_Toc389755608)

[2.3.3 Основні функції шифру HBB 35](#_Toc389755609)

[2.3.4 Алгоритм роботи шифру HBB 37](#_Toc389755610)

[2.3.5 Предметна область та імплементація шифру HBB 39](#_Toc389755611)

[3 АНАЛІЗ КРИПТОАТАК 43](#_Toc389755612)

[3.1 Аналіз атаки на основі вибраного ШТ на шифр SSS 43](#_Toc389755613)

[3.2 Засоби для реалізації атаки на основі вибраного ШТ для шифру SSS 45](#_Toc389755614)

[3.3 Імплементація атаки на основі вибраного ШТ для шифру SSS 46](#_Toc389755615)

[3.4 Модифікація атаки на шифр SSS 47](#_Toc389755616)

[3.5 Аналіз атаки на основі вибраного ШТ на шифр HBB 48](#_Toc389755617)

[3.6 Порівняльна характеристика атак на основі вибраного ШТ для шифрів HBB та SSS 50](#_Toc389755618)

[4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ 53](#_Toc389755619)

[4.2 Опис приміщення 54](#_Toc389755620)

[4.3 Аналіз шкідливих факторів 56](#_Toc389755621)

[4.3.1 Повітря робочої зони 56](#_Toc389755622)

[4.3.2 Освітлення 58](#_Toc389755623)

[4.3.3 Шум 61](#_Toc389755624)

[4.3.4 Випромінювання 62](#_Toc389755625)

[4.3.5 Електробезпека 62](#_Toc389755626)

[4.3.6 Надзвичайні ситуації. Пожежна безпека 63](#_Toc389755627)

[ПЕРЕЛІК ПОСИЛАНЬ 66](#_Toc389755628)

[ДОДАТКИ 67](#_Toc389755629)

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

|  |  |
| --- | --- |
| ***IV*** | Вектор ініціалізації |
| ***ШТ*** | Шифр текст |
| ***ВТ*** | Відкритий текст |
| ***SSS*** | Потоковий шифр із самосинхронізацією із сімейства шифрів SOBER |
| ***XOR*** | Виключне АБО |
| ***СПШ*** | Синхронний потоковий шифр |
| ***АПШ*** | Асинхронний потоковий шифр |
| ***НФФ*** | Нелінійна фільтруюча функція |

# ВСТУП

За останні десятиліття ми стали свідками швидкого розвитку інформаційних технологій, зокрема зростання цифрових сховищ зберігання інформації та обміну даними. Причиною такого динамічного руху технологій уперед можна пояснити популяризацією мережі Інтернет та бездротових мереж. Нові комунікаційні технології вимагають належного рівня технологій безпеки інформації.

Криптологія – це наука, що забезпечує інформаційний захист у сучасному цифрову світі. Зазвичай цю науку розділяють на дві сфери: криптографію та криптоаналіз. Криптографія вивчає дизайн алгоритмів та протоколів для інформаційної безпеки. Ідеальною вважається ситуація, коли можливо розробити алгоритми, які доказово стійкі до відомої множини атак, але зазвичай, таке можливо в обмеженій кількості випадків. Криптоаналіз в свою чергу займається математичними методами для обходу чи злому криптографічних примітивів.

Криптографічні алгоритми зазвичай розбивають на два сімейства: симетричні та асиметричні. Симетричні алгоритми вимагають наявності секретного ключа, що розподіляється між сторонами комунікації. Асиметричні алгоритми засновані на системах із відкритим ключем, який відомий усім сторонам, та із секретним ключем, що зберігається у секреті однією стороною.

Існує два типи симетричних алгоритмів: блочні та потокові шифри. Представники останнього класу і є предметом вивчення даної роботи.

Блочні шифри – це сфера симетричної криптографії, вивченням якої займались найбільше. Поштовхом до розвитку блочних шифрів можна вважати прийняття шифру DES, як національного стандарту шифрування в США в 1977 році. Наслідком цього можна вважати виникнення нових напрямків: диференціального та лінійного криптоаналізу.

Не зважаючи на успіх блочних шифрів, існує потреба в потокових шифрах, які надають нові переваги в багатьох сценаріях.

Потокові шифри на базі [зсувних регістрів](https://uk.wikipedia.org/w/index.php?title=%D0%97%D1%81%D1%83%D0%B2%D0%BD%D0%B8%D0%B9_%D1%80%D0%B5%D0%B3%D1%96%D1%81%D1%82%D1%80&action=edit&redlink=1) активно використовувалися в роки війни, ще задовго до появи електроніки. Вони були прості в проектуванні та реалізації.

1965 Ернст Селмер, головний криптограф норвезького уряду, розробив теорію послідовності зсувних регістрів. Пізніше [Соломон Голомб](https://uk.wikipedia.org/w/index.php?title=%D0%A1%D0%BE%D0%BB%D0%BE%D0%BC%D0%BE%D0%BD_%D0%92%D0%BE%D0%BB%D1%8C%D1%84_%D0%93%D0%BE%D0%BB%D0%BE%D0%BC%D0%B1&action=edit&redlink=1), [математик](https://uk.wikipedia.org/wiki/%D0%9C%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA) [Агентства Національної Безпеки США](https://uk.wikipedia.org/wiki/%D0%90%D0%B3%D0%B5%D0%BD%D1%82%D1%81%D1%82%D0%B2%D0%BE_%D0%BD%D0%B0%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%97_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8), написав книгу під назвою «Shift Register Sequences» («Послідовності зсувних регістрів»), в якій виклав свої основні досягнення в цій галузі, а також досягнення Селмер.

Велику популярність потоковим шифрів принесла робота [Клода Шеннона](https://uk.wikipedia.org/wiki/%D0%9A%D0%BB%D0%BE%D0%B4_%D0%A8%D0%B5%D0%BD%D0%BD%D0%BE%D0%BD), опублікована в 1949 році, в якій Шеннон довів абсолютну стійкість [шифру Вернама](https://uk.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%92%D0%B5%D1%80%D0%BD%D0%B0%D0%BC%D0%B0). У шифрі Вернама [ключ](https://uk.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F)) має довжину, рівну довжині самого переданого повідомлення. Якщо кожен [біт](https://uk.wikipedia.org/wiki/%D0%91%D1%96%D1%82) ключа вибирається випадково, то розкрити шифр неможливо (тому що всі можливі відкриті тексти будуть рівноймовірними). Шифри, в яких довжина ключа менша від довжини тексту, згідно з Шенноном, не можуть бути «ідеально безпечними» [1].

З лютого 2000р. по лютий 2003р. проходив європейський дослідницький проект NESSI (New European Schemes of Signatures, Integrity and Encryption) для визначення безпечних алгоритмів шифрування. На цьому проекті було представлено лише 6 потокових шифрів, причому наприкінці конкурсу жоден з них не був схвалений як такий, котрий міг би задовольнити всім вимогам. Саме цей проект став поштовхом до оголошення нового європейського конкурсу, присвяченого виключно потоковим шифрам – eSTREAM. На конкурс eSTREAM було пред’явлено 34 шифри, що порівняно з конкурсом NESSI було великим кроком уперед.

Головною метою конкурсу eSTREAM було отримання шифру широкого використання, котрий працював би швидше за AES (у режимі лічильника).

**Актуальність роботи**. В процесі створення систем шифрування гостро постає проблема знаходження компромісу між високою швидкістю роботи та низькими вимогами до використання обчислювальних ресурсів. Саме потокові шифри є таким компромісом – питання побудови стійких і водночас ефективних потокових систем шифрування знаходиться в центрі уваги сучасної криптографічної спільноти. Підтвердженням цього є проведення у 2005-2008р.р. у рамках проекту ECRYPT загальноєвропейського конкурсу eSTREAM, присвяченого виключно потоковим шифрам. Цей конкурс став найвизначнішою подією у розвитку теоретичної та прикладної криптографії останнього десятиліття. eSTREAM сприяв пожвавленню науково-практичної роботи в галузі розробки та криптоаналізу потокових шифрів. Вивчення, дослідження, осмислення результатів цього проекту – одна з актуальних задач сучасної криптографії.

**Мета і завдання дослідження**. Метою роботи є дослідження та аналіз деяких сучасних потокових шифрів із самосинхронізацією, огляд та імплементація існуючих криптоатак на них.

*Об’єкт дослідження*: алгоритми потокового шифрування із самосинхронізацією HBB, SSS, Mostique.

*Предмет дослідження*: аналіз шифрів із самосинхронізацією за їх характеристиками, особливостями будови, швидкодією, огляд та імплементація криптоатак на ці шифри; виявлення на цій основі сучасних тенденцій розвитку потокового шифрування.

**Практичне значення одержаних результатів.** Отримані результати можна використовувати, як аналіз по реалізації деяких потокових шифрів із самосинхронізацією та криптоатак для них.

# 1 ОЗНАЧЕННЯ НЕОБХІДНИХ В РОБОТІ ТЕРМІНІВ ТА ПОНЯТЬ

## 1.1 Базові поняття

Текст – це послідовність букв деякого алфавіту. Надалі вважатимемо, що алфавіт є скінченним. Позначимо його як . Відкритий текст (ВТ) - це текст, що підлягає шифруванню. Відповідно, шифр текст (ШТ) – текст, що підлягає розшифруванню.

Криптографічна система – це набір апаратних і програмних засобів, інструкцій і правил, за допомогою яких, використовуючи криптографічні перетворення, можна зашифрувати повідомлення і розшифрувати криптограму різними способами, один із яких вибирається за допомогою секретного ключа, а також здійснювати інші криптографічні протоколи.

Криптографічна стійкість – у широкому розумінні це – здатність криптосистеми або криптоалгоритму протистояти атакам з використанням методів криптоаналізу; у вузькому розумінні – чисельна характеристика складності розкриття криптографічного алгоритму з урахуванням тих науково-технічних методів та засобів, які може використати криптоаналітик.

Поняття стійкості (за Шенноном) розділяється на два типи: теоретична та практична.

Теоретична стійкість – стійкість криптосистеми за наявності у криптоаналітика необмеженого часу, необмежених обчислювальних ресурсів, якнайкращих методів криптоаналізу.

Практична стійкість – стійкість криптосистеми на теперішній час з урахуванням того, що криптоаналітик володіє обмеженим часом, обмеженими обчислювальними ресурсами і сучасними методами криптоаналізу.

## 1.2 Основні типи криптографічних атак залежно від типу відомої інформації

1. Атака на основі (з використанням) тільки ШТ. У криптоаналітика є ШТ декількох повідомлень, зашифрованих одним і тим же алгоритмом шифрування. Задача криптоаналітика полягає в розкритті ВТ як можна більшого числа повідомлень або, що краще, отриманні ключа (ключів), використаного для шифрування повідомлень з метою дешифрування також і інших повідомлень, зашифрованих тими ж ключами.
2. Атака на основі (з використанням) ВТ. У криптоаналітика є доступ не тільки до ШТ декількох повідомлень, але і до відповідних відкритих текстів цих повідомлень. Його задача полягає в отриманні ключа (або ключів), використаного (використаних) для шифрування повідомлень з метою дешифрування інших повідомлень, зашифрованих тим же ключем (ключами).
3. Атака на основі вибраного відкритого тексту. У криптоаналітика не тільки є доступ до ШТ і відповідних відкритих текстів декількох повідомлень, але є і можливість вибирати відкритий текст (тексти) і отримати зашифрований. Це надає більше варіантів, ніж атака з використанням відкритого тексту, оскільки криптоаналітик може вибирати шифровані блоки відкритого тексту із спеціальними властивостями, що може надати більше інформації про ключ. Його задача полягає в отриманні ключа (або ключів), використаного для шифрування повідомлень, або алгоритму, що дозволяє дешифрувати нові повідомлення, зашифровані тим же ключем (або ключами).
4. Адаптивна атака з використанням відкритого тексту. Криптоаналітик не тільки може вибирати тексти для шифрування, але також може будувати свій подальший вибір текстів на базі одержаних результатів шифрування. При розкритті з використанням вибраного відкритого тексту криптоаналітик міг вибрати для шифрування тільки один великий блок відкритого тексту, при адаптивному розкритті з використанням вибраного відкритого тексту він може вибрати менший блок відкритого тексту, потім вибрати наступний блок, використовуючи результати першого вибору і так далі. Атаки 2-4 можливі, наприклад, при шифруванні з відкритим ключем.
5. Атака на основі вибраного ШТ. Криптоаналітик може вибрати різні ШТ для розшифрування і має доступ до розшифрованих відкритих текстів (наприклад, криптоаналітик має доступ до апарату-шифратора).
6. Адаптивна атака на основі вибраного ШТ (аналогічно п.4).
7. Атака на основі вибраного тексту (адаптивна) – об'єднує можливості атак п.3, п.5 (п.4, п.6).

Атаки в цьому списку з більшим номером сильніші і небезпечніші ніж з меншим. Для всіх сучасних шифраторів обов'язкова вимога – стійкість до атаках типу 1 і 2. Якщо у криптоаналітика є деяка інформація про ключі або про зв'язок між різними ключами, то напади на криптосистему стають ще небезпечнішими.

В даній роботі буде розглянути імплементація атаки на основі вибраного ШТ. Розглянемо простий приклад-пояснення цієї атаки для кращого її розуміння.

*Приклад.*

Нехай генерал А надсилає повідомлення генералу Б, використовуючи шифр Віженера. Криптоаналітик якимсь чином втрутився в їхній канал зв’язку і замінив зашифроване повідомлення на вибраний ним набір літер («вибраний ШТ»), нехай це буде повідомлення «NLLCJOVFXXHMLY». Генерал Б розшифровує його і в результаті отримує наступне «AKRUWNBXKWNEYX», що для нього не несе жодного змісту. Вважаючи, що ця інформація не має жодної цінності, він телефонує по незакритому каналу генералу А та запитує: «Що Ви мали на увазі під AKRUWNBXKWNEYX? Ви змінили секретний ключ без мого відому?». В цей час Криптоаналітик підслуховує цю розмову і зміг встановити відповідність, що ШТ «NLLCJOVFXXHMLY» відповідає ВТ «AKRUWNBXKWNEYX». Враховуючи використання шифру Віженера, одного розшифрованого повідомлення достатньо, щоб відновити секретний ключ.

## 1.3 Блокові шифри

У сучасних шифраторах ВТ і ШТ записуються у двійковому алфавіті. При блоковому шифруванні ВТ поділяється на блоки завдовжки *n*, тобто кожен блок можна розглядати як двійковий вектор довжини *n* (якщо число знаків у ВТ не кратне довжині блоку, то останній блок доповнюється зарані обумовленими символами, наприклад, нулями). Таким чином, блоковий шифр являє собою взаємно-однозначне перетворення множини двійкових векторів довжини  у себе, тобто не що інше, як підстановку на алфавіті з символів. Кількість можливих підстановок на такому алфавіті (кількість можливих варіантів зашифрування) дорівнює . У сучасних блокових шифраторах довжина блоку  досить велика (частіше за все 64, 128 або 256 бітів), тому алфавіт виходить величезним, а кількість підстановок на ньому – тим більше. Довжина ключа, який задавав би довільну підстановку з цієї множини (шифр простої заміни), дорівнює  біт і є надто великою, щоб таким шифром можна було користуватися на практиці. Наприклад, вже при  . Тому практично шифри реалізують більш вузькі множини підстановок, що мають, однак, ряд необхідних криптографічних властивостей.

Існує декілька різних режимів роботи блокових шифраторів, які відповідають певним практичним потребам і мають свої переваги й недоліки.

Надалі будемо позначати через  *і*-й блок ШТ, а  – *і*-й блок відповідного йому відкритого тексту .

## 1.4 Режими роботи блокових шифраторів

1.1 Режим ECB (Electronic Code Book) - режим електронної кодової книги

Це найпростіший режим роботи блокових шифраторів. Рівняння шифрування та розшифрування в цьому режимі задаються співвідношеннями:

 (1.1)



де  - операції шифрування та розшифрування блоковим алгоритмом з ключем .

Власне, тільки в режимі *ECB* блокові шифратори реалізують алгоритми блокового шифрування. В решті режимів вони породжують залежність блоку ШТ від його місця, а також, можливо, й від інших блоків, що притаманне потоковим шифрам.

1. Режим CBC (Cipher Block Chaining) – режим зчеплення блоків ШТ

Рівняння шифрування та розшифрування:

, (1.2)

.

 - так звана синхропосилка - є спільною для відправника й одержувача і може бути як секретною, так і відкритою.

2. Режим CFB (Cipher Feed Back) – режим зворотного зв’язку за шифрованим текстом

Рівняння шифрування та розшифрування:

 (1.3)



Блок  називається синхропосилкою і є спільним для відправника та одержувача.

Властивості цього режиму схожі на властивості режиму *CBC*. Блок ВТ впливає на всі наступні блоки ШТ, в той час як спотворення або втрата блоку ШТ призводить до помилок при розшифруванні тільки у двох послідовних блоках ВТ, тобто режим є таким, що самосинхронізується. Розпаралелювання можливе тільки при розшифруванні. Цей режим має ще одну перевагу: для шифрування і для розшифрування використовується одна й та сама функція .

1. Режим OFB (Output Feed Back) – режим зворотного зв’язку за виходом

Рівняння шифрування та розшифрування:

 (1.4)



, де  – синхропосилка (не є секретною).

3. Режим лічильника (Counter)

Деякий пристрій (лічильник) генерує послідовність блоків  за правилом:

, (1.5)

де  – синхропосилка .

Функція  звичайно проста, наприклад:

 (1.6)

(звідси і назва – лічильник). Те, що послідовні блоки, які генерує лічильник, мало відрізняються, не впливає на стійкість. Адже у доброму блоковому шифраторі при зміні одного біта на вході, на виході змінюється в середньому половина бітів.

Рівняння шифрування та розшифрування:

 (1.7)

У режимах *OFB* та лічильника блокові шифратори працюють як потокові шифри адитивного типу: шифруюча послідовність (гама) складається побітово за з ВТ. При цьому гама генерується незалежно від ВТ.

## 1.5 Потокові шифри

Потоковий шифр – це симетричний шифр, в якому кожен символ ВТ перетворюється в символ ШТ в залежності не тільки від вибраного ключа, але від розміщення даного символу в потоці ВТ.

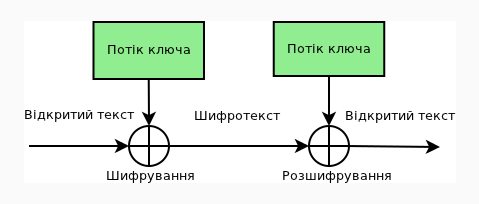


Рисунок 1.1 – Схематичне зображення потокового шифру

Генератор гами видає ключовий потік (гаму): . Позначимо потік бітів ВТ . Тоді потік бітів ШТ отримують з допомогою застосування операції XOR до блоків із ВТ і ключового потоку:

(1.8)

Розшифрування здійснюється операцією XOR між тою ж гамою і зашифрованим текстом:

(1.9)

Якщо послідовність бітів гамми не має періоду і обирається випадково, то «зламати» шифр неможливо. Але ключі з довжиною близькою до довжини ВТ, важко використовувати на практиці. Саме через це застосовують ключі меншої довжини (наприклад, 128 біт). З його допомогою генеруються псевдовипадкова гамуюча послідовність. Саме псевдовипадковість гами може бути використана при атаці на потоковий шифр.

На відміну від блокових систем, у потокових системах шифрування відкритого тексту виконується посимвольно, причому перетворення, за допомогою якого здійснюється шифрування символу, може залежати від часу (тобто від місця даного символу у послідовності ВТ). Крім того, шифруюче перетворення може мати пам’ять, тобто залежати від попередніх символів тексту.

Таким чином, при блоковому шифруванні один і той самий блок символів ВТ шифрується однаково незалежно від його розташування. Це дозволяє зловмиснику непомітно для отримувача спотворювати інформацію, виключати її частину або ж вводити хибну інформацію. Очевидно, що внаслідок залежності шифруючого перетворення від часу потокові системи вільні від цього недоліку. Вказана перевага потокових систем шифрування породжує, однак, проблему синхронізації. Помилка при передачі (втрата або спотворення знаку) може призвести до того, що весь подальший ШТ буде розшифрований неправильно. В залежності від того, як розв’язується ця проблема, потокові шифратори розділяють на синхронні системи та системи з самосинхронізацією.

## 1.6 Синхронні потокові шифри

*Означення:*

Синхронні потокові шифри (СПШ) — шифри, в яких потік ключів генерується незалежно від ВТ і ШТ. При шифруванні генератор потоку ключів видає біти потоку ключів, які ідентичні бітам потоку ключів при дешифруванні. Втрата знаку ШТ приведе до порушення синхронізації між цими двома генераторами і неможливості розшифрування залишкової частини повідомлення. В цій ситуації відправник і адресат повинні повторно синхронізуватися для продовження роботи.

Зазвичай синхронізація здійснюється вставкою в передане повідомлення спеціальних маркерів. Як результат, пропущений при передачі знак призводить до невірного розшифрування лише до тих пір, поки не буде прийнято один із маркерів.

Виконуватись синхронізація повинна так, щоб жодна частина потоку ключів не була повторена. Тому переводити генератор в більш ранній стан не має сенсу.

Позитивні сторони СПШ:

* відсутність ефекту розповсюдження помилок (тільки створений біт буде розшифрований невірно);
* убезпечують від будь-яких вставок і видалення частин ШТ, адже вони спричинять втрату синхронізації і будуть виявлені.

Негативні сторони СПШ:

* Уразливі до змін окремих бітів ШТ. Якщо Криптоаналітику відомий ВТ, то може змінити ці біти так, щоб вони розшифровувались, як йому це потрібно.

## 1.7 Потокові шифри із самосинхронізацією

*Означення:*

Потокові шифри із самосинхронізацією (асинхронні потокові шифри (АПШ)) – шифри, в яких ключовий потік створюється функцією ключа і фіксованим числом знаків ШТ.

Внутрішні стани генератора потоку ключів є функцією попередніх N бітів ШТ. Саме тому розшифровуючий генератор потоку ключів, прийнявши N бітів, автоматично синхронізується із шифруючим генератором.

Реалізація цього режиму проходить наступним чином: кожне повідомлення починається випадковим заголовком довжини N бітів; заголовок шифрується, передається і розшифровується; розшифрування невірне, але після цих N біт обидва генератори будуть синхронізовані.

Позитивні сторони АПШ:

* Змішування статистики ВТ. Оскільки кожен знак ВТ впливає на наступний ШТ, статистичні властивості ВТ розповсюджується на весь ШТ. АПШ може бути стійкішим до атак на основі збитковості ВТ, чим СПШ.

Негативні сторони АПШ:

* Розповсюдження помилки (кожному неправильному біту ШТ відповідають N помилок у ВТ);

чутливі до злому через повторну передачу.

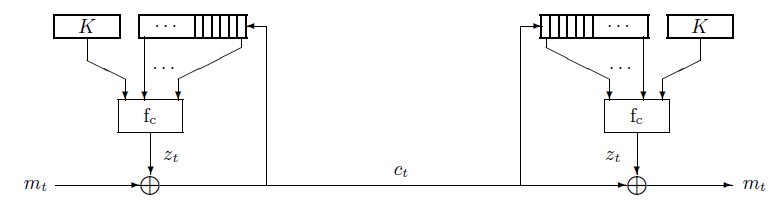


Рисунок 1.2 – Схематичне спрощене зображення потокового шифру із самосинхронізацією

За такого дизайну шифру, наступний знак (біт) ключового потоку повністю визначається останніми знаками (бітами) ШТ та ключем К. Модель: на вхід деякої функції приходить стан регістру зсуву, що містить символів ШТ, та ключ, як результат отримуємо символ потокової послідовності. Для перших символів ВТ ще немає відповідного ШТ, їх задають з допомогою ініціалізуючих символів, що називаються вектором ініціалізації IV.

Потокові ***системи з самосинхронізацією*** дають можливість правильно розшифровувати не тільки у випадку спотворення знаку ШТ, але й у разі його втрати. Прикладом таких систем є режими роботи блокових шифраторів СВС (зчеплення блоків ШТ) та CFB (зворотного зв’язку за ШТ). Для режиму CFB, наприклад, розшифрування відбувається за правилом , де -й блок ВТ, -й блок ШТ,  ‑ алгоритм шифрування з ключем . При розшифруванні ШТ  з втраченим -м блоком маємо:

, (1.10)

, але .

Отже, один блок ВТ спотворюється і один губиться, а далі все розшифровується правильно.

Режими ж ОFB (зворотного зв’язку за виходом) та лічильника є синхронними системами. Їх особливістю є те, що на ВТ посимвольно накладається ключова послідовність , яка генерується незалежно від ВТ. Послідовність  називається **гаммою**, а шифри, в яких ШТ  одержується шляхом додавання знаків ВТ та ключової послідовності

 (1.11)

називаються ***шифрами гамування*** (додавання у(1) виконується у відповідній алгебраїчній структурі). Переважна більшість систем потокового шифрування є шифрами гамування.

Зазвичай замість чисто випадкової ключової послідовності використовується псевдовипадкова, що виробляється генератором псевдовипадкових чисел (ГПВЧ), який керується відносно коротким ключем. (Власне шифратор у цьому випадку і являє собою ГПВЧ). Для того, щоб було можливо застосувати псевдовипадкову послідовність ***z***, в якості ключової, вона повинна мати добрі криптографічні характеристики, тобто бути “схожою” на випадкову. Це необхідно для того, щоб ключова послідовність для супротивника, який не знає ключа, була непередбачуваною. Тому до ГПВЧ, які використовуються у криптографії, ставляться більш жорсткі вимоги, ніж при використанні у інших сферах.

Найбільш розповсюдженими та вивченими вузлами, що складають основу багатьох ГПВЧ, в тому числі і сучасних потокових шифраторів, є регістри зсуву з лінійним зворотним зв’язком (РЗЛЗЗ) або коротше – лінійні регістри зсуву (ЛРЗ).

## 1.8 Лінійні регістри зсуву

ЛРЗ генерують псевдовипадкові послідовності ***s***, що задовольняють лінійним рекурентним співвідношенням:

 (1.12)

для фіксованого . У виразі (2) члени послідовності ***s***, а також коефіцієнти  належать скінченному полю , а операції додавання та множення – це операції у цьому полі. Такі послідовності називають **лінійними рекурентними послідовностями** порядку над скінченним полем .

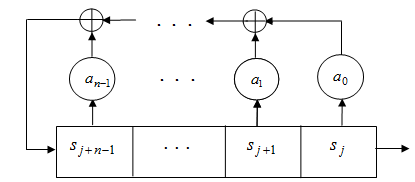


Рисунок 1.3 – Схема регістра із лінійним зсувом

Власне регістр складається з послідовності комірок, у кожній з яких записаний елемент скінченного поля . Кількість комірок регістра n називається довжиною цього регістра, а значення , що містяться в комірках у момент , - **станом регістра** у момент j. Стан ЛРЗ у момент  називається **початковим заповненням** регістра.

Регістр працює у дискретному часі. На кожному такті роботи регістра відбувається наступне: вміст кожної комірки множиться на відповідний коефіцієнт , а результати додаються; далі вміст усіх комірок зсувається праворуч на одну комірку, число з крайньої правої комірки подається на вихід пристрою, а звільнена крайня ліва комірка заповнюється одержаною сумою , де  – номер такту.

Якщо основним скінченним полем є GF(2), то коефіцієнти  є нулями або одиницями і в схемі регістра можна не вказувати зйоми з комірок, яким відповідають нульові коефіцієнти, а ті, яким відповідають , замінити на провідники без множників. Таким чином, схема регістра набуває вигляду:

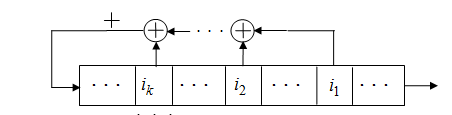


Рисунок 1.4 – Зображення лінійного регістра зсуву над полемGF(2)

де , решта .

Лінійні рекурентні послідовності є періодичними. Оскільки кількість різних станів ЛРЗ скінченна, то рано чи пізно деякий стан ЛРЗ повториться, а вся подальша послідовність залежить тільки від стану регістра у даний момент. Якщо коефіцієнт  (на практиці це завжди саме так, інакше можна розглядати регістри меншої довжини), то послідовності, що генеруються таким ЛРЗ, не мають передперіоду. Надалі вважатимемо, що умова  виконана.

**Приклад 1**. Нехай ЛРЗ заданий своїм характеристичним поліномом , що відповідає лінійному рекурентному співвідношенню між членами послідовності . Схема такого регістра має вигляд:

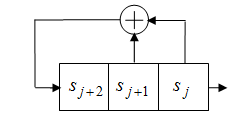


Рисунок 1.5 – Схема ЛРЗ з характеристичним поліномом 

Задамо ненульове початкове заповнення регістра, наприклад, 001. Тоді регістр згенерує послідовність 0010111001…. (знаки лінійної рекурентної послідовності ми записали зліва направо в тому порядку, як вони з’являються на виході регістра; проте цілком можливе дзеркальне зображення ЛРЗ, коли вихід знаходиться зліва).

**Висновки до розділу 1**

В даному розділі було означено загальні поняття, що використовуються у роботі; наведений опис основних видів атак залежно від типу відомої інформації; розглянуто два типи шифрів: потокові та блокові; детально описано два підвиди потокових шифрів: синхронні та асинхронні. Для останніх, як шифрів із самосинхронізацією, було надано особливу увагу в даному розділі, оскільки шифри цього типу виступають предметом дослідження даної роботи. Також, розглянули лінійні регістри зсуву, як основну складову в побудові потокових шифрів.

# 2 ОГЛЯД ТА АНАЛІЗ

## 2.1 Шифр Moustique

### 2.1.1 Характеристики шифру Moustique

**Параметри:** шифр, що самосинхронізується, довжина ключа 96 біт, довжина IV від 0 до 13 байтів.

**Основні операції:** додавання та множення за модулем 2.

**Конструктивні особливості:** зчеплення елементів шифрованого тексту (подібно до режиму СFВ у блоковому шифруванні); використання регістрів з умовним доповненням.

**Переваги:** незвичайна архітектура, можливість використання для аутентифікації повідомлення (МАС), наявність режиму, в якому шифр працює як синхронний.

**Криптоатаки:** знайдено корельовані шифруючі гамми [7].

**Конкурс/Конференція: eStream.**

### 2.1.2 Опис шифру Moustique



Рисинок 2.1 – Схема зашифрування–розшифрування шифру Moustique

Ключ K – 96 бітів подається на вхід спеціального регістру зсуву CCSR, що складається із 96 комірок, розмір кожної з комірок в бітах задано таблицею:

Таблиця 2.1 – Нумерація комірок та бітів для внутрішнього регістру CSSR шифру

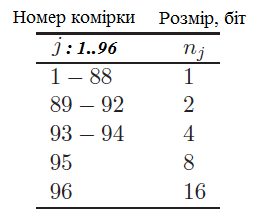




Рисунок 2.2 – Схема вхід-вихід для шифру Moustique



Рисунок 2.3 – Схема ЛРЗ CCSR

Розглянемо як заповнюється регістр: математичні вирази для кожної комірки та кожного її біта.

Для :

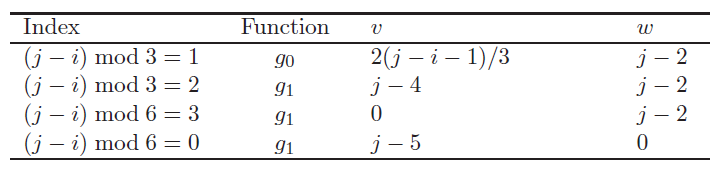
(2.1)

Для є загальна формула:

*,* (2.2)

де , а значення та всіх комбінацій в Таблиці 2.2.

Таблиця 2.2 – Значення залежно від



Розглянемо, як отримують значення деякі біти цих комірок:

… (2.3)

…

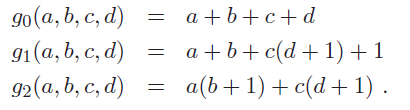
Для є окрема формула:

(2.4)

Обрахуємо випадок, коли :

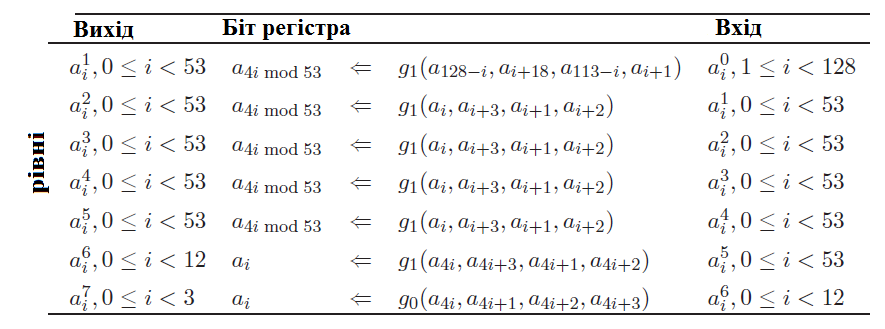
(2.5)

Визначимо функцію :



Заповнення інших рівнів шифру описано в Таблиці 2.3.

Таблиця 2.3 – Правила заповнення різних рівнів шифру



де , де *i* – номер біту регістра *k-го –* рівня.

**Приклад**: 11-й біт, регістру 1-го рівня, знаходимо, коли

, (2.6)

де – це біти CCSR

Аналогічно рахуємо за схемою, зображеній в Таблиці 2.3, для всіх рівнів. Останній 7-й рівень має лише 3 біти. Біт шифр тексту , відповідно (2.7)

## 2.2 Шифр SSS

### 2.2.1 Характеристики шифру SSS

**Параметри:** шифр, що самосинхронізується, довжина ключа до 128 біт, максимальна допустима довжина вихідної послідовності на фіксованому ключі 2128 16-бітових слів; генерує за такт 16 бітів.

**Основні операції:** додавання за модулем 2 (XOR), додавання за модулем 216, циклічний зсув, підстановка (S-блок) 816.

**Конструктивні особливості:** є продовженням родини потокових шифрів SOBER, використана схема нелінійної фільтрації лінійного регістра зсуву над полем GF(216).

**Переваги:** вимагає невеликої пам’яті, можливість використання для аутентифікації повідомлення (МАС).

**Криптоатаки:** існує атака, що дозволяє знайти секретний ключ з вибраним шифротекстом довжиною менше 10 Кбайт.

**Конкурс/Конференція:**eStream.

### 2.2.2 Сімейство шифрів SOBER

SSS створений на основі шифрів із сімейства SOBER, що вперше були запропоновані Грегорі Роузом в 1998 році. Назва сімейства – це акронім-назва для шифрів, що засновані на регістрах зсуву, в яких 17 комірок розміром в 1 байт (Seventeen Octet Byte Enabled Register). Завданням цих шифрів було замінити слабкі до атак шифри, що застосовувались у мобільних телефонах. Початкові версії шифрів із даного сімейства містили в собі 17 байтні регістри зсуву та нелінійні фільтруючі функції виходу. Але вони легко піддавались до атак розпізнавання. Згодом для покращення стійкості шифрів було запропоновано використовувати 2-байтні слова в якості комірок регістру замість 1-байтних.

### 2.2.3 Основні операції, необхідні для імплементації шифру

«⨁» – виключне або (XOR);

«+» – звичайне додавання;

«>>>» – циклічний зсув на 8 бітів вправо;

«^» – побітове «і» для 16-бітного слова;

«~» – бітова інверсія 16-бітного слова;

«aH »– старший байт 16-бітного слова.

### 2.2.4 Генерація потокової послідовності

Потоковий генератор шифру SSS в основі має звичайний регістр зсуву та нелінійну фільтруючу функцію. Базові операції здійснюються з 16-бітними блоками потокової послідовності, кожен 16-бітний блок називатимемо «словом». Вектор «слів» будемо називати «станом» регістру в час *t*, а стан – «початковим станом».

Тепер визначимо, яким чином здійснюється перехід до наступного стану регістру:

1. залишається без змін;
2. , для ;
3. ;
4. ;
5. ;
6. .

Опісля стан регістру знімається і передається на вхід в нелінійну фільтруючу функцію (НФФ), на виході з якої отримуємо потокове слово :

.

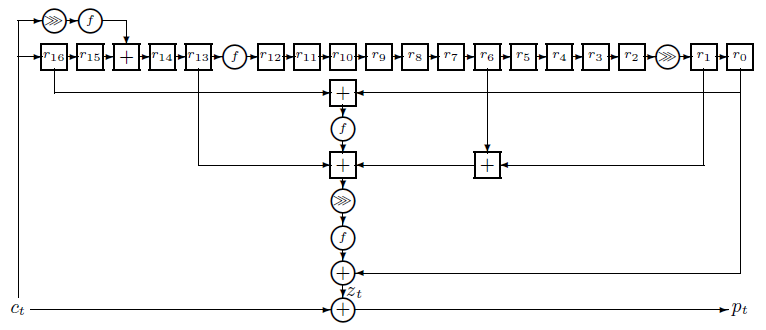


Рисунок 2.4 – Схема формування потокових символів

Основним будівельним блоком є НФФ *f*, що залежить від ключа, а по суті являється перестановкою бітів в 16-бітному слові. Формульно її можна представити так:

, (2.8)

де - старший байт слова (MSB) ***x***, а S-Box – залежна від ключа функція, що визначається на етапі встановлення ключа. Вважатимемо, що це таблиця із 256 16-бітних слів.

### 2.2.5 S-Box

НФФ *f,* визначена у формулі (2.8) вище, – нелінійна функція, що залежить від ключа шифру. По суті, це єдиний елемент шифру, що залежить від секретного ключа. Тому попередньо обраховане значення цієї функції у вигляді таблиці із 16 бітних слів цілком може вважатись ключем всього шифру. Всього можливих комбінацій таких таблиць –, звідки і випливає складність перебору такого ключового простору.

Функція S-Box, що фігурує у формулі (#), – це комбінація Skipjack [#] S-Box (інша назва F-table) та Q-Box [#] Центру Розробки в галузі Інформаційної Безпеки (Information Security Research Centre, ISRC).

Skipjack S-Box – нелінійна перестановка 8-бітних векторів. Q-Box – нелінійна таблиця, на вхід якої приходить 8-бітний вектор, а на виході отримуємо 16-бітний. Розглянемо, яким чином поєднуються ці дві функції в одну в імплементації S-Box шифру SSS.

Нехай довжина ключа в бітах становить , -й біт ключа – . Вхідний байт поєднується із відповідним байтом ключа для обрахунків власне функції S-Box:

, (2.9)

де – це тимчасовий проміжний результат, що йде як вхід для Q-Box. Наглядно це можна продемонструвати на прикладі програмного коду на мові С:

WORD

Sbox(UCHAR \*key, int keylen, WORD w)

{

register int i;

WORD t;

UCHAR b;

t = 0;

b = HIGHBYTE(w);

for (i = 0; i < keylen; ++i) {

b = Ftable[b ^ key[i]];

t ^= ROTL(Q-box[b], i);

}

return ((b << (WORDBITS-8)) | (t & LOWMASK)) ^ (w & LOWMASK);

}

Для оптимізації часу роботи шифру, ця функція може буде обрахована і представлена у вигляді таблиці до виконання операцій зашифрування-розшифрування. Як результат, її використання зводиться до виконання операції XOR між вхідним словом та відповідним словом із попередньо обрахованої таблиці S-Box.

## 2.3 Шифр HBB

В оригінальній статті із специфікацією шифру вказується, що HBB – це новий потоковий шифр, в основі якого лежить поєднання нелінійного та лінійного відображень. Лінійне відображення базується на використанні двох 256-бітних клітинних автоматів. Нелінійна частина шифру реалізована таким чином, щоб уникнути використання арифметики над скінченними полями. Автори шифру наполягають на тому, що максимальна кореляція, яка може виникати між входом та виходом вищезгаданих відображень, становить не більше ніж 2-13. Цей шифр в базовому режимі є власне синхронним, але підтримує режим із самосинхронізацією на ряду із іншим режимом – MAC (Message Authentication Code). Саме режим самосинхронізації для HBB ми розглядатимемо в даній роботі. Як тільки 4 блоки розміром в 128 бітів отримані без наявності помилок, система автоматично синхронізується.

### 2.3.1 Характеристики шифру HBB

**Параметри:** шифр, що самосинхронізується, довжина ключа 128 (256) біт, внутрішній стан описується 640 бітами.

**Основні операції:** додавання за модулем 2 (XOR) та стандартні бітові операції.

**Конструктивні особливості:** складається із лінійної компоненти, що представлена двома клітинними автоматами, як альтернатива регістрам зсуву.

**Переваги:** вимагає невеликої пам’яті, можливість використання для аутентифікації повідомлення (МАС).

**Криптоатаки:** існує атака, що дозволяє знайти секретний ключ з вибраним ШТ довжиною приблизно в 2 Кбайт.

**Конкурс/Конференція:** представлений на конференції eCrypt, автор Palash Sarkar.

### 2.3.2 Короткий опис клітинних автоматів

Лінійну систему можна представити як деяке лінійне перетворення. Нехай деякий вектор – визначає стан *k*-бітної лінійної системи в час . Тоді наступний стан в момент часу визначається як множення вектору із фіксованою матрицею розмірності .

Клітинний автомат (КА) – це лінійна система, що визначається деякою матрицею . У випадку клітинного автомату ця матриця – тридіагональна. Характеристичний поліном такої матриці – це характеристичний поліном для всіх послідовностей, що можуть бути отримані з кожної клітини такого автомату. Якщо такий поліном примітивний, то період лінійної послідовності на виході є максимальним: . Справедливе також наступне твердження, що якщо характеристичний поліном примітивний, то верхня та нижня субдіагоналі матриці складаються із одиниць. Саме в такому випадку КА називається 90/150 КА. Наступні рівняння описують вектори стану такого 90/150 КА.

(2.10)

Вектор називається вектором-правилом 90/150 КА. Значення 0 визначає правило 90, а значення 1 - правило 150.

В шифрі, що розглядається в даній роботі, клітинні автомати визначаються наступними характеристичними поліномами:

*,* (2.11)

*.*

Бінарні рядки та мають довжину в 256 бітів та вагу 128 кожний. В шістнадцятковій системі числення ці рядки мають наступний вигляд:

Правила 90/150 для даних клітинних автоматів знайдено з допомогою алгоритму Тезуки та Фушимі [джерело] та мають наступне шістнадцяткове представлення:

### 2.3.3 Основні функції шифру HBB

Шифр може працювати в трьох різних режимах: базовий (**B**), із аутентифікацію повідомлень (**MAC**), із самосинхронізацією (**SS**). В ході даної роботи буде реалізовано базовий режим та на його основі режим із самосинхронізацією, буде проведено аналіз атаки на останній.

Введемо наступні позначення:

* – повідомлення ВТ, що буде подано на вхід функції шифрування;
* – 128-бітний блок повідомлення ВТ;
* , де кількість 128-блоків, з яких складається повідомлення ВТ;
* секретний ключ системи шифрування;
* – ключова потокова послідовність;
* 128-бітні блоки ШТ;
* лінійна компонента внутрішнього стану шифру, займає 512 бітів;
* нелінійна компонента внутрішнього стану шифру, на яку припадає 128 бітів;

Отже, внутрішній стан шифру описується 640 бітами, які визначаються лінійною та нелінійною компонентами.

Опишемо основні функції, що використовуються під час роботи шифру:

* : – це рядок із бітів, довжина якого додатне число кратне .

1. де та для всіх
2. .

* де розмір ключа становить 128 бітів.
* – функція, що на вхід приймає лінійну та нелінійну компоненту шифру та відповідно, та на виході видає наступні 128 бітів потокової послідовності. Будемо вважати кожен із клітинних автоматів масивом довжини 16, де кожен елемент - це 32-бітне слово. Тому стан першого клітинного автомату позначатимемо як , другого – , – 128-бітні блоки потокової послідовності.

1. , де ;
2. <<<;

8.

* – нелінійне перестановка компоненти шифру . Це перетворення використовує функцію для перестановки бітів у кожному байті . Функція - це функція байт-перестановки із AES [джерело].
* – це функція, в яку на вхід приходить 128 бітів , що трактуються як елементи матриці , де кожний рядок це 32-бітне слово. Дана функція здійснює часткове транспонування вхідної матриці.
* – це функція, що задає відповідність між 512 бітовими рядками, тобто це лінійне відображення із 512-бітового вектору в 512-бітовий вектор.

Змінні та – це правила 90/150 для клітинних автоматів, що використовуються в даному шифрі.

### 2.3.4 Алгоритм роботи шифру HBB

Знаючи усі необхідні складові шифру, сформуємо псевдокод роботи алгоритму шифру на основі попереднього опису та оригінальної статті:

1.

2.

3.

4.

5.

6. ;

7.

8. ;

9. enddo;

10. output .

Даний псевдокод представляє роботу функції зашифрування, щоб отримати відповідний алгоритм дешифрування, достатньо змінити декілька рядків:

6. ;

10. output .

Режим із самосинхронізацією реалізується шляхом введення залежності для символів потокової послідовності від попередніх символів ШТ. Рядки 7-8 вищезгаданого алгоритму роботи шифру HBB описують конкретну реалізацію введення даної залежності.

В кінці ітерації останні 4 блоки ШТ (кожен блок по 128 бітів), визначені як , додаються за із бітами ключа . Результатом даної операції є новий стан нелінійної компоненти (Рядок 8 алгоритму HBB).

Новий стан лінійної компоненти отримується шляхом додаванням за конкатинованих останніх чотирьох блоків ШТ та розширеного ключа. (Рядок 7 алгоритму HBB).

Таким чином, на початку кожної нової ітерації внутрішній стан шифру лінійно залежить лише від секретного ключа та останніх 512 бітів ШТ.

### 2.3.5 Предметна область та імплементація шифру HBB

Оскільки шифр HBB не представлявся на конкурсах типу eStream, то його конкретної реалізації немає у відкритому доступі. Тому, було запропоновано предметну область для шифру та на її основі реалізовано власне шифр HBB на мові C# засобами програмного середовища MS Visual Studio та .Net.

Запропоновано 3 класи для імплементації основних складових шифру:

* Block – для опису блоків, з яких складаються ВТ, ШТ та потокова послідовність символів;
* CA – для опису двох клітинних автоматів, що відіграють роль лінійної компоненти шифру;
* NLC – для опису нелінійної компоненти шифру.

Коротко опишемо ці класи на прикладі коду.

Таблиця 2.3.№ - Опис класу «Block»

|  |  |
| --- | --- |
| Код класу | Пояснення |
| public class Block  {  public UInt32 first;  public UInt32 second;  public UInt32 third;  public UInt32 fourth;  } | Повідомлення ВТ та ШТ розбиваються на блоки по 128 бітів. Кожен блок складається із чотирьох 32-бітних слів, щоб таким чином реалізувати структуру, що описує 128-бітне представлення 1 блоку. |

Таблиця 2.3№ - Опис класу «CA»

|  |  |
| --- | --- |
| Код класу | Пояснення |
| public class CA  {  public UInt32 state0;  public UInt32 state1;  public UInt32 state2;  public UInt32 state3;  public UInt32 state4;  public UInt32 state5;  public UInt32 state6;  public UInt32 state7;  CAorder order;  UInt32 RULE00 = 0x80ffaf46;  UInt32 RULE01 = 0x977969e9;  UInt32 RULE02 = 0x71553bb5;  UInt32 RULE03 = 0x99be6b2b;  UInt32 RULE04 = 0x4b337295;  UInt32 RULE05 = 0x2308c787;  UInt32 RULE06 = 0xb84c7cce;  UInt32 RULE07 = 0x36d501e6;  UInt32 RULE10 = 0xdd18c62b;  UInt32 RULE11 = 0x153df31a;  UInt32 RULE12 = 0xc98e86c1;  UInt32 RULE13 = 0x910fee24;  UInt32 RULE14 = 0x2942d51b;  UInt32 RULE15 = 0x4201eb3d;  UInt32 RULE16 = 0xc1d1a85f;  UInt32 RULE17 = 0x57b8919b;  public void Exp()  public void EvolveCA256()  } | Клас, що реалізовує клітинний автомат, стан якого описують 256 бітів - вісім 32-бітних слів, що відповідають за опис внтріщнього стану автомата, його номер (всього в шифрі застосовується 2 таких автомати), та набір функцій, що застосовуються до відповідного автомату, наприклад, Exp() та Evolve256(). |

|  |  |
| --- | --- |
| Код класу | Пояснення |
| [StructLayoutAttribute(LayoutKind.Explicit)]  public class NLC  {  [FieldOffsetAttribute(0)]  public UInt32 word;    [FieldOffsetAttribute(0)]  public byte byte0;  [FieldOffsetAttribute(1)]  public byte byte1;  [FieldOffsetAttribute(2)]  public byte byte2;  [FieldOffsetAttribute(3)]  public byte byte3;  } | Клас, що описує нелінійну компоненту. Основним атрибутом цього класу, є 32-бітне слово, що розбивається на 4 байти. Особливість реалізації цього класу полягає в тому, що зміна будь-якого із чотирьох байтів провокує зміну основного слова «word». |

Повна імплементація шифру викладена у додатку #.

**Висновки до розділу 2**

В даному розділі описано три шифри із самосинхронізацією: Moustique, HBB та SSS. Для кожного шифру надані короткі відомості та характеристика, проаналізовано основні складові функції та компоненти, описано загальний алгоритм їхньої роботи на прикладі псевдокоду або математичних виразів. Для шифру HBB запропонована предметна область для імплементації шифру на мові C#.

# 3 АНАЛІЗ КРИПТОАТАК

## 3.1 Аналіз атаки на основі вибраного ШТ на шифр SSS

З опису шифру випливає, що секретним ключем для шифрування можна вважати саме таблицю Sbox із 256 16-бітних слів. Тому головною ціллю атаки є відтворити цю таблицю.

Ми будемо розшифровувати один ШТ, що складається із 263 однакових патернів, отримаємо відповідний йому ВТ та ключовий потік як результат. Патерни складатимуться із 18 16-бітних слів та завжди має наступний формат:

(3.1)

де має певне значення для кожного патерну, визначимо це значення згодом. Із схематичного зображення шифру випливає, що

(3.2)

Значення цих регістрів в момент часу *t =* 18:

(3.3)

По суті, вміст регістрів сталий для всіх патернів, окрім регістру r[13]. Зробимо деяку заміну:

(3.4)

,

в результаті отримаємо наступний вираз:

. (3.5)

Важливо зауважити, що доданки в дужках – це 2-байтові слова, в яких ми будемо позначати старші байти (MSB) відповідно та , молодші байти - та . Щоб віднайти старший байт , використаємо 8 патернів із 256 по 263, що мають наступний вигляд:

(3.6)

Виходячи із вигляду патернів вище, перетворимо формулу для потокового символу на 18 часовому кроці:

(3.7)

здійснимо операцію XOR для значень символів потокової послідовності, що відповідають часовим крокам 18 та 0 і отримаємо наступне:

(3.8)

.

Виходячи із результату останньої операції, можна судити про значення :

дорівнює , то відповідний біт буде 0, інакше – 1.

Як тільки відновлено, то можна спробувати відновити цілком усю таблицю, що відповідає Sbox. Надалі це здійснюватиметься простим перебором: вгадуємо значення та - загалом 24 біти, тобто складність такого перебору 224. Зробимо це з допомогою патернів від 0 до 255. Формат у них наступний:

та для Проробимо аналогічні дії як для :

(3.9)

Враховуючи, що атака на основі обраного ШТ, тому ми завжди можемо порівняти вгадані значення із істинними, розшифровуючи за вгаданою таблицею Sbox.

(3.10)

Якщо пройтись по всім 256 патернам, то можемо відновити всю таблицю.

## 3.2 Засоби для реалізації атаки на основі вибраного ШТ для шифру SSS

Атака реалізована у вигляді консольного програмного додатку Win32. Для реалізації атаки на основі ШТ для шифру із самоорганізацією SSS були використанні наступні засоби:

1. Microsoft Visual Studio Express 2012 – інтегроване середовище розробки програмного забезпечення;
2. Microsoft Visual C++ (MSVC) — інтегроване середовище розробки програмного забезпечення на мові C++, розроблена фірмою Microsoft. Visual C++.NET підтримує розробку програмних додатків як на Managed C++, так і на звичайному С++, і тим самим дозволяє генерувати код як для платформи .NET Framework, так і для виконання в середовищі операційної системи Windows;
3. Вихідний код шифру SSS, представлений на конкурсі eStream.

**Обґрунтування**: Відкритий код шифру реалізований на мові програмування C, що є звичним явищем для шифрів. Саме програми реалізовані мовою С дозволяють максимально реалізувати швидкодію роботи шифру за рахунок керування пам’яттю комп’ютера. Код мови С мало відрізняється від мови C++ для додатків, що використовують структурне програмування, тому код шифру легко портується під засоби Microsoft Visual Studio та Visual C++. Виходячи з того, що атака вимагає наявності дешифратора, що реалізований на мові C++, атака теж імплементована засобами інтегрального середовища Visual C++.

## 3.3 Імплементація атаки на основі вибраного ШТ для шифру SSS

Основною ціллю атаки є відтворення значень таблиці S-box, що залежать від бітів ключа. Для швидкодії ця таблиця може обраховуватись на початковому етапі роботи шифру, що передує етапові зашифрування повідомлення. Відповідно, для реалізації атаки нам необхідно лише 2 базові функції із відкритого коду шифру та 4 допоміжні, що необхідні в процесі розшифрування:

1. «sss\_key» – базова функція, що обраховує значення S-box, як результат змішування бітів ключа та двох таблиць: ftable та Qbox;
2. «sss\_deconly» – базова функція розшифрування на основі значень S-box та бітів ШТ;
3. «BYTE2WORD», «WORD2BYTE» – дві допоміжні функції для конвертації «слів» шифру в байти та навпаки;
4. «cycle» – функція циклічного зсуву для регістра;
5. «nltap» – функція, що здійснює нелінійне перетворення від деяких частин регістру.

Допоміжні функції описані в пунктах 3-5 використовуються під час виконання базових функцій 1-2. Код всіх функцій представлений в додатку.

Для реалізації атаки з допомогою програмного додатку, представленого в даній роботі, необхідно отримати розшифроване повідомлення, що відповідає ШТ із патернів описаних в розділі 3.1.

Опишемо короткий алгоритм роботи програмного додатку, що реалізовує атаку на SSS на прикладі програмного коду в додатку:

1. Обрахунок таблиці S-box на основі ключа;
2. Генерація ШТ із 263 патернів;
3. Розшифрування ШТ із патернів та отримання відповідного ВТ;
4. Визначення за результатами попереднього пункту значення старшого байту Аh, описаної в розділі 3.1;
5. Визначення значення всієї таблиці S-box через повний перебір («brute force»;
6. Валідація отриманого ключа-таблиці.

## 3.4 Модифікація атаки на шифр SSS

В оригінальній статті [#], що описує атаку на даний шифр, автор говорить про можливу модифікацію атаки, використовуючи патерни, що перетинаються. Під перетином мається на увазі, що одні і ті самі патерни використовуються як для знаходження старшого біту так і для загального перебору значень таблиці S-box.

Неважко помітити, що не має сенсу генерувати обраний ШТ більшого розміру, якщо деякі патерни однакові. Програмна модифікація дозволяє віднайти такі патерни за лінійний час, що залежить від кількості патернів. Провівши невелике дослідження, можна помітити, що патерни та повністю співпадають. В коді, що викладений в додатку #, кількість надлишкових патернів описана змінною «NumberOfExtraPatterns». Відповідно, обраний ШТ можна скоротити в розмірі до 256 патернів, замість 263.

Автору атаки знадобилось близько 9,5 Кбайт обраного ШТ, щоб зламати ключ шифру – таблицю S-box. Виходячи із опису імплементації та модифікації, для реалізації атаки необхідно 256 патернів, кожен з яких становить 36 байтів, загалом необхідно 9 Кбайт. Тобто зменшення розміру необхідного ШТ становить близько 6%.

## 3.5 Аналіз атаки на основі вибраного ШТ на шифр HBB

У пункті 2.3.3 даної роботи зазначили, що кожна ітерація шифру HBB в режимі із самосинхронізацією складається із фіксованого числа функцій, що застосовуються до ключа та останніх чотирьох блоків ШТ. Дана конструкція шифру не стійка перед атакою на основі обраного ШТ.

Оскільки атака на основі обраного ШТ, тому вважатимемо, що є оракул на вхід якого приходить ШТ і на виході правильно розшифрований ВТ.

Головна мета даної атаки – отримати два виходи нелінійної компоненти для функції , що відрізняються лише в 1 байті із різницею в . Щоб досягти такої різниці, можемо просто згенерувати дві послідовності із блоків ШТ наступним чином:

та .

Нехай – це позиція цієї різниці в 1 байт, – відповідний байт секретного ключа. На перший погляд, криптоаналітик не має доступу до внутрішнього стану, щоб дізнатись різницю між виходами після роботи функції, що оновлює стан нелінійної компоненти. Але як зазначалось в кінці розділу 2.3.3, на початку кожної нової ітерації внутрішній стан шифру лінійно залежить лише від секретного ключа та останніх 4 блоків ШТ. Тому криптоаналітик, що володіє бітами потокової послідовності, може відмінити дію гамування та отримати у відкритому вигляді різницю для двох виходів функції оновлення стану нелінійної компоненти.

Як зазначалось вище в описі самого шифру, функція, що оновлює стан нелінійної компоненти – складається із декількох етапів, першим з яких є деяка функція перестановки бітів для кожного байту нелінійної компоненти. Тому, початкова різниця в 1 байт, після дії цієї перестановки, змінить лише 1 байт за тією ж самою позицією . Ця різниця матиме наступний вигляд:

де – відомий байт, залежно від заданого ШТ. Другим етапом функції оновлення – є лінійне перетворення. Якщо різниця має гамуючий ефект ваги 1, то згідно [#], гамуючий ефект після лінійного перетворення буде ваги 3. Тобто, лише 3 байти будуть відрізнятись після застосування останнього кроку функції оновлення.



Рисунок 3.1 – Ланцюжок гамування для нелінійної компоненти

Узагальнимо результат: якщо гамуючий ефект для буде ваги 1, то різниця між виходами нелінійної компоненти нуль для 13 байтів із 16. Згідно з оригінальною статтею [#], подія, коли виникає гамуючий ефект ваги 1, трапляється з ймовірністю 0,03125. Згідно «парадоксу про дні народження» [#], перебору значень для , має бути достатньо, щоб отримати вище описаний випадок, коли для 13 із 16 байтів гамуючий ефект рівний нулю. Використовуючи формулу [#] та знання про вищезгадану подію, отримаємо умову для :

Як результат, 1 байт секретного ключа можна зламати, опрацювавши блоків потокової послідовності. Щоб зламати весь ключ, треба 16 разів повторити дану процедуру. Складність такої атаки можна оцінити з точки зору розміру необхідного обраного ШТ. Щоб опрацювати блоків потокової послідовності, має бути достатньо повідомлення розміром 3 + , що вимагає приблизно 2 Кбайт обраного ШТ.

3.6 Порівняльна характеристика атак на основі вибраного ШТ для шифрів HBB та SSS

Оскільки розглянуті в роботі шифри одного типу – потокові шифри із самосинхронізацією та розглянуті для них атаки на основі обраного ШТ теж схожі, як узагальнення та підсумок для даного дослідження доцільно привести порівняльну характеристику цих атак.

Таблиця 3.6.1№ – Порівняльна характеристика атак для шифрів HBB та SSS

|  |  |  |
| --- | --- | --- |
|  | HBB | SSS |
| Тип шифру | Потоковий із самосинхронізацією | |
| Тип атаки | На основі обраного ШТ | |
| Необхідний розмір ШТ, байт | 2048 | 9216 |
| Передумови | Наявність оракула – функції розшифрування | |
| Елемент, на який здійснюється атака | Нелінійна компонента шифру | Регістр зсуву |
| Необхідні попередні обчислення | Знаходження колізій, при яких виникає гамуючий ефект ваги 1 згідно формул #. Генерація обраного ШТ до виконання умови # | Генерація патернів для створення обраного ШТ.  Знаходження старшого байту згідно формул 3.4-3.10. |
| Складність частини атаки, де здійснюється перебір | – перебір для знаходження колізій: 16 разів для кожного байту ключа | – перебір можливих входів та виходів для таблиці S-box згідно формули # |
| Відновлення ключа | Повністю відтворюється весь ключ | Відновлення внутрішнього стану S-box, що по суті виступає ключем |
| Можливі модифікації | Аналогічні атаки, що підтримують колізії для гамуючих ефектів ваги 2, 3, 4 | Скорочення необхідного ШТ через знаходження патернів, що перетинаються |

**Висновки до розділу 3**

В даному розділі проаналізована атака на основі вибраного ШТ для шифру SSS, описана її математична частина та алгоритм програмної реалізації атаки на мові Visual С++. Наведено обґрунтування використання засобів необхідних для імплементації даної атаки. Також, описано практичну складність реалізації атаки та можлива її модифікація, що дозволяє скоротити величину обраного ШТ на 6%.

Для іншого шифру HBB проаналізовано атаку на основі обраного ШТ та можливість практичної її реалізації.

# 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Аналіз умов праці

Роботи, що проводяться при проектуванні системи інформації для менеджменту, можна кваліфікувати як творчу роботу з ПК та іншими периферійними пристроями. Вивчення і вирішення проблем, пов'язаних із забезпеченням здорових та безпечних умов, в яких працює людина - одна з найбільш важливих завдань при розробці нових систем. Вивчення та виявлення можливих причин виробничих нещасних випадків, професійних захворювань, аварій, пожеж, і розробка заходів та вимог, спрямованих на усунення цих причин, дозволяють створити безпечні та сприятливі умови для праці людини. Робота співробітників безпосередньо пов'язана комп'ютером, а відповідно з додатковим шкідливим впливом цілої групи факторів, що істотно знижує продуктивність їх праці. До таких факторів можна віднести:

* Порушення мікроклімату;
* Неправильне освітлення;
* Ненормальний рівень шуму;
* Вплив шкідливих випромінювань;
* Наявність електричної напруги;
* Небезпека пожежі;
* Надзвичайні ситуації.

## 4.2 Опис приміщення

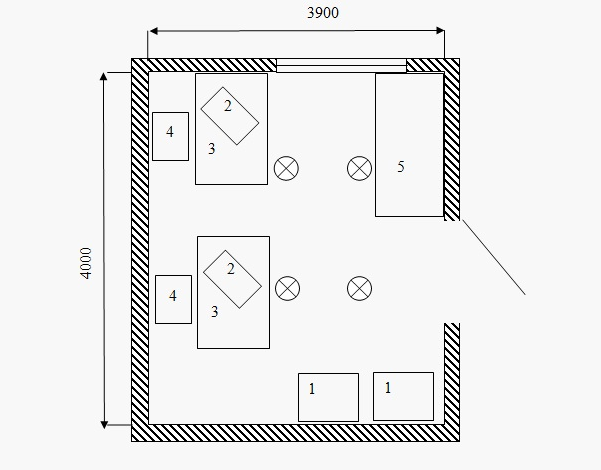


Рисунок 4.1 План приміщення

Таблиця 4.1 Розміри офісного приміщення

|  |  |
| --- | --- |
| Довжина (м) | 4.0 |
| Ширина (м) | 3.9 |
| Висота стелі (м) | 2.8 |
| Загальна площа (м2) | 15.6 |
| Загальний об’єм (м3) | 43.68 |
| Кількість робочих місць | 2 |

Таблиця 4.2 Нормативні та фактичні значення площі та об’єму

|  |  |  |
| --- | --- | --- |
|  | Норматив | Фактичне значення |
| Площа для 1 робочого місця, м2 | >6 | 7.8 |
| Об’єм для 1 робочого місця, м3 | >20 | 21.84 |

На рисунку 4.1 зображено план офісного приміщення, у таблиці 4.2 подано нормативні (за НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації ЕОМ») та розраховані фактичні значення параметрів робочого приміщення. З чого робимо висновок, що габарити приміщення є такими, що відповідають діючим нормам.

## 4.3 Аналіз шкідливих факторів

### 4.3.1 Повітря робочої зони

Основний принцип нормування мікроклімату - створення оптимальних умов для теплообміну тіла людини з довкіллям. У ДСанПІН 3.3.2.007-98 встановлені величини параметрів мікроклімату, що створюють комфортні умови.

Таблиця 4.3 Норми мікроклімату для приміщень з ЕОМ

|  |  |  |  |
| --- | --- | --- | --- |
| Пора року | Температура повітря, град.С | Відносна вологість повітря, % | Швидкість руху повітря, м/с |
| Холодний | 22-24 | 40-60 | 0,1 |
| Теплий | 23-25 | 40-60 | 0,1 |

Таблиця 4.4 Фактичні параметри мікроклімату у приміщенні

|  |  |  |  |
| --- | --- | --- | --- |
| Пора року | Температура повітря, град.С | Відносна вологість повітря, % | Швидкість руху повітря, м/с |
| Холодний | 22-24 | 40-60 | 0,1 |
| Теплий | 23-25 | 40-60 | 0,1 |

Для отримання комфортного мікроклімату в теплу пору року в приміщенні встановлено кондиціонер Mitsubishi Heavy SRK20HG-S.

Таблиця 4.5 Технічні характеристики кондиціонера

|  |  |
| --- | --- |
| Площа дії | 20 м2 |
| Режим роботи | Охолодження/обігрів |
| Потужність охолодження | 2,07 кВт |
| Потужність обігріву | 2,22 кВт |
| Споживча потужність охолодження/обігрів | 0,64/ 0,61 кВт |
| Рівень шуму | 27 дБ |
| Тип холодогента | R-410А |
| Напруга/ частота/ фаза | 220-240 В/ 50 Гц/ 1Ф |
| Габаритні розміри внутрішній блок, ШхВхГ | 790х268х199 мм |
| Габаритні розміри зовнішній блок, ШхВхГ | 780х540х290 мм |
| Вага (внутрішній блок/зовнішній блок) | 8,5 кг / 31 кг |
| Іонізатор | 24 год/добу |
| Антибактеріальна дія (знищує) | Кишкові бактерії (Escherichia coli, IFO 3972) |
|  | Стафілококи (Staphylococcus aureus, IFO 12732) |
|  | Аспергіли (Aspergillus niger, IFO 6341) |

Висновок: повітря робочої зони відповідає нормам, кондиціонер виконує антиалергенну та антибактеріальну дію, очищує повітря від шкідливих речовин, іонізує повітря та забезпечує сприятливі мікрокліматичні умови для роботи. Взимку працює опалення.

### 4.3.2 Освітлення

У робочому приміщенні використовується штучне освітлення, доступ сонячного світла обмежують жалюзі на вікнах.

В якості освітлювальних приборів використовуються 4 люмінесцентні лампи ЛД 65 виробництва ООО «Завод ГРЛ», м. Полтава. Характеристики лампи наведені у Таблиці 4.6

Таблиця 4.6 Характеристики лампи ЛД 65

|  |  |  |  |
| --- | --- | --- | --- |
| Потужність, Вт | Світловий потік, лм | Напруга, В | Струм, А |
| 65 | 3900 | 100-120 | 0.67 |

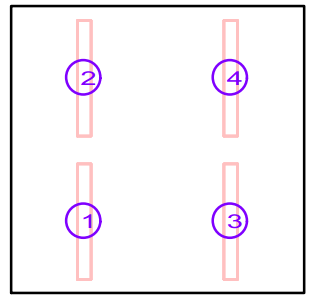


Рисунок 4.2 Схема розташування ламп у приміщенні

На рисунку 4.2 зображено схему розташування ламп у приміщенні. У таблиці 4.6 зазначено точні координати ламп, що були використані для розрахунку освітлення у приміщенні за допомогою програми DIALux 4.10. Результати розрахунку відображені на рисунку 4.3

Таблиця 4.7 Розташування ламп у приміщенні

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | Y | Z |
| 1 | 1.000 | 0.970 | 2.800 |
| 2 | 1.000 | 2.920 | 2.800 |
| 3 | 3.000 | 0.970 | 2.800 |
| 4 | 3.000 | 2.920 | 2.800 |

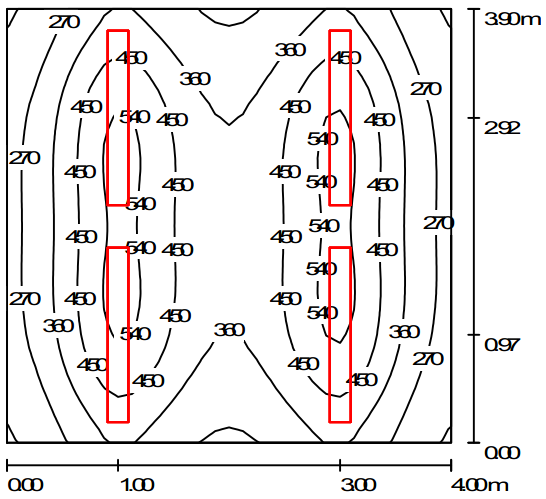


Рисунок 4.3 Розрахунок освітлення приміщення

Таблиця 4.8 Нормативні та фактичні значення освітленності

|  |  |  |
| --- | --- | --- |
|  | Норматив | Фактичне значення |
| Мінімальна освітленність на поверхні робочого столу, лк | 300 | 300 |
| Максимальна освітленність на поверхні робочого столу, лк | 500 | 450 |

У Таблиці 4.8 подано нормативні (за ДСанПіН 3.3.2-007-98. «Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин») та розраховані фактичні значення освітленості в робочих зонах працівників. Як бачимо, фактичні значення освітленості відповідають нормативним.

### 4.3.3 Шум

Таблиця 4.9 Рівні шуму комплектуючих ПК

|  |  |  |
| --- | --- | --- |
| Назва джерела шуму | Рівень шуму, дБА | Звуковий тиск, Вт/м2 |
| Блок живлення | 17 | 5.01 × 10-11 |
| Корпус | 19 | 7.94 × 10-11 |
| Відеокарта | 32 | 1.58 × 10-9 |
| Кулер процесора | 35 | 3.16 × 10-9 |

У Таблиці 549 зібрано список комплектуючих ПК, які є джерелами шуму, зазначено відповідні рівні шуму у дБ. Для розрахунку загального рівня шуму спочатку обрахуємо звуковий тиск кожного джерела шуму за формулою:

*Pi = P0* ×*10Di/10*

Де *P0* – еталонний звуковий тиск (10-12 Вт/м2)

Обрахуємо сумарний рівень шуму за формулою:

*D = 10* × *lg( P / P0 )*

Де P – сумарний звуковий тиск комплектуючих

Таблиця 4.10 Нормативні та фактичні значення рівня шуму

|  |  |  |
| --- | --- | --- |
|  | Норматив, дБА | Фактичне значення, дБА |
| Рівень шуму ПК | <50 | 37 |

Висновок: рівень шуму відповідає нормативному.

4.3.4 Випромінювання

Для роботи використовуються монітори 27" Samsung S27A850D, що сертифіковані за стандартом TCO 5.0 / Energy Star.

### 4.3.5 Електробезпека

Для роботи освітлення, ЕОМ та іншого електроустаткування у робочому приміщенні використовується електроживлення з однофазної мережі змінного струму з частотою 50 Гц і напругою 220 В.

За класифікацією приміщень за рівнем електробезпеки (відповідно до НПАОП 0.00-1.28-10) робоче приміщення належить до категорії без підвищеної небезпеки електротравматизму.

ЕОМ та комплектуючі становлять потенційну небезпеку для працівника. Враження струмом може трапитися в результаті торкання до відкритих частин, які перебувають під напругою, при ушкодженні мережних шнурів, при пробої, короткому замиканні, або в результаті необережних дій людини.

ЕОМ відносяться до установок, які споживають напругу < 1000 В. Корпуси сучасних ЕОМ виготовлені із пластмас (передня панель, з якої працює оператор) і металу (верхня кришка й задня панель). Це може призвести до електротравми, при торканні людини до металевих частин у випадку пробою на корпус. Тому конструкцією передбачена спеціальна мережна вилка із трьома контактами (два контакти служать для підключення живлення, а третій - для підключення до проводу на землю) у системі занулення.

Корпуса дисплеїв виготовляються з матеріалів, що не проводять струм, а живлення здійснюється за допомогою спеціального кабелю, що підключається до системного блоку. Це служить для виключення ймовірності ураження струмом.

Робочі місця розташовані на відстані 2 та 3 метра від батареї, що виключає випадкові торкання до батареї.

Висновок: електрообладнання, що використовується у робочому приміщенні, відповідає вимогам електробезпеки для побутових приладів і не вимагають додаткових методів захисту.

### 4.3.6 Надзвичайні ситуації. Пожежна безпека

Серед ймовірних надзвичайних ситуацій (стихійних лих, аварій, катастроф, впливів зброї масового ураження), найбільш вірогідною в робочому приміщенні є пожежа.

У приміщенні знаходяться наступні речі, які можуть горіти у випадку пожежі:

* папір;
* ПК;
* шкафи;
* столи;
* стільці;
* підлога.

За класифікацією приміщень щодо пожежної небезпеки робоче приміщення відноситься до категорії В (важкозаймисті тверді й волокнисті речовини й матеріали) і до класу П-IIа.

Приміщення обладнане пожежною сигналізацією РУОП-1. У приміщенні знаходяться 2 вуглекислотних вогнегасника ОУ-5 (відповідно до норми: 2 шт. на 20м2).

У разі виникнення пожежі, загрози вибуху або руйнування будинку працівникам необхідно негайно звільнити офісне приміщення згідно плану евакуації. План евакуації зображено на рисунку 5.4 і розташовано на видному місці у приміщенні.

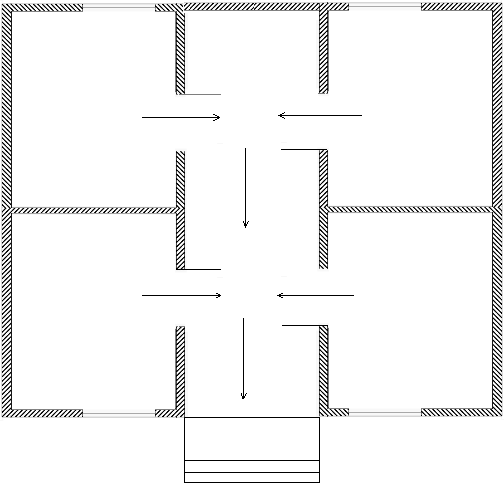


Рисунок 4.4 План евакуації приміщення

**Висновки до розділу 4**

У даному розділі проведено аналіз умов праці та аналіз ймовірних шкідливих факторів, серед яких порушення мікроклімату, неправильне освітлення, ненормальний рівень шуму, вплив шкідливих випромінювань, небезпека пожежі та ураження електричним струмом. Рівень шуму, повітря робочої зони, освітлення, електрообладнання відповідають нормам. У приміщенні встановлено кондиціонер, що виконує антиалергенну та антибактеріальну дію, очищує повітря від шкідливих речовин, іонізує повітря та забезпечує сприятливі мікрокліматичні умови для роботи. Взимку у приміщенні працює опалення. Монітори сертифіковані за стандартом TCO/5.0, що також відповідає нормам. Приміщення обладнане пожежною сигналізацією РУОП-1, встановлено 2 вуглекислотних вогнегасника. На видному місці розташовано план евакуації, якого слід дотримуватися в разі загрози виникнення пожежі, вибуху та інших надзвичайних ситуацій.

# ПЕРЕЛІК ПОСИЛАНЬ

1. Daemen J. Chosen Ciphertext Attack on SSS [Електронний ресурс] / J. Daemen, J. Lano. – 2005. – Режим доступу до ресурсу: http://www.ecrypt.eu.org/stream/papersdir/044.pdf.
2. Hawkes P. Primitive Specification for SSS [Електронний ресурс] / P. Hawkes, G. G. Rose, M. Paddon. – 2005. – Режим доступу до ресурсу: http://www.ecrypt.eu.org/stream/ciphers/sss/sss.pdf.
3. Daemen J. The Self-synchronizing Stream Cipher Moustique / J. Daemen, P. Kitsos // New Stream Cipher Designs / J. Daemen, P. Kitsos., 2008. – (Lecture Notes in Computer Science). – С. 210–223.
4. Joux A. Two attacks against the HBB Stream Cipher / A. Joux, F. Muller. // FSE Proceedings of the 12th international conference on Fast Software Encryption. – 2005. – №5. – С. 330–341.
5. Sarkar P. Hiji-bij-bij: A new Stream Cipher with Self-Synchronizing and MAC Modes of Operation / Palash Sarkar – India: Indocrypt, 2003. – (Progress in Cryptology). – (LNCS 2904).
6. Masoodi F. SOBER Family of Stream Ciphers: A Review / F. Masoodi, S. Alam, M. Bokhari. // International Journal of Computer Applications.
7. Robshaw M. Stream Ciphers [Електронний ресурс] / M.J.B. Robshaw // RSA Laboratories. – 1995. – Режим доступу до ресурсу: ftp://nic.funet.fi/.m/archive1e/idea.sec.dsi.unimi.it/rsa.com/pdfs/tr701.pdf.gz.

# ДОДАТКИ

// SSSproject.cpp.

#include "stdafx.h"

#include <stdlib.h>

#include "sss.h"

#include "ssssbox.h"

#include "sssmultab.h"

#include <iostream>

#define NumberOfExtraPatterns 8

#define B(x,i) ((UCHAR)(((x) >> (8\*i)) & 0xFF))

#define BYTE2WORD(b) ( \

(((WORD)((b)[1]) & 0xFF)<<8) | \

(((WORD)((b)[0]) & 0xFF)) \

)

#define WORD2BYTE(w, b) { \

(b)[1] = B(w,1); \

(b)[0] = B(w,0); \

}

#define XORWORD(w, b) { \

(b)[1] ^= B(w,1); \

(b)[0] ^= B(w,0); \

}

WORD

Sfunc(UCHAR \*Key, int KeyLength, WORD w)

{

register int i;

WORD t;

UCHAR b;

t = 0;

b = HIGHBYTE(w);

for (i = 0; i < KeyLength; ++i) {

b = ftable[b ^ Key[i]];

t ^= ROTL(Qbox[b], i);

}

return ((b << (WORDBITS-8)) | (t & LOWMASK)) ^ (w & LOWMASK);

}

static void

cycle(sss\_ctx \*State, WORD ctxt)

{

register int i;

for (i = 0; i < N-1; ++i)

State->ShiftRegister[i] = State->ShiftRegister[i+1];

State->ShiftRegister[16] = ctxt;

State->ShiftRegister[14] += SBoxFromWord(State, ROTR(ctxt, 8));

State->ShiftRegister[12] = SBoxFromWord(State, State->ShiftRegister[12]);

State->ShiftRegister[1] = ROTR(State->ShiftRegister[1], 8);

}

static WORD

nltap(sss\_ctx \*c)

{

register WORD t;

t = c->ShiftRegister[0] + c->ShiftRegister[16];

//printf("OK? %04x\n",t);

t = SBoxFromWord(c,t) + c->ShiftRegister[1] + c->ShiftRegister[6] + c->ShiftRegister[13];

t = ROTR(t, 8);

//printf("inputlastf %04x\n",t);

return SBoxFromWord(c,t) ^ c->ShiftRegister[0];

}

void

sss\_key(sss\_ctx \*State, UCHAR Key[], int KeyLength)

{

int i;

if (KeyLength > MAXKEY)

abort();

for (i = 0; i < 256; ++i)

State->SBox[i] = Sfunc(Key, KeyLength, (WORD)(i << (WORDBITS-8))) ^ (i << (WORDBITS-8));

void

sss\_key(sss\_ctx \*c, UCHAR key[], int keylen)

{

int i;

if ((c->keylen = keylen) > MAXKEY)

abort();

for (i = 0; i < keylen; ++i)

c->key[i] = key[i];

/\* in case no nonce... \*/

sss\_nonce(c, (UCHAR \*)0, 0);

}

void

sss\_nonce(sss\_ctx \*State, UCHAR nonce[], int nlen)

{

int i;

UCHAR nb[2];

if ((nlen % WORDBYTES) != 0)

abort();

for (i = 0; i < N; ++i)

State->ShiftRegister[i] = State->CRC[i] = 0;

for (i = 0; i < nlen; i += WORDBYTES) {

nb[0] = nonce[i];

nb[1] = nonce[i+1];

sss\_decrypt(State, nb, WORDBYTES);

}

nb[0] = nb[1] = 0;

for (i = 0; i < N; ++i) {

sss\_maconly(State, nb, WORDBYTES);

}

State->NumberOfBitsBuffered = 0;

}

void

sss\_enconly(sss\_ctx \*c, UCHAR \*buf, int nbytes)

{

WORD t = 0;

if (c->NumberOfBitsBuffered != 0) {

while (c->NumberOfBitsBuffered != 0 && nbytes != 0) {

\*buf ^= c->StreamBuf & 0xFF;

c->CipherTextBuf ^= \*buf << (WORDBITS - c->NumberOfBitsBuffered);

c->StreamBuf >>= 8;

++buf;

c->NumberOfBitsBuffered -= 8;

--nbytes;

}

if (c->NumberOfBitsBuffered != 0) /\* still not a whole word yet \*/

return;

cycle(c, c->CipherTextBuf);

}

while (nbytes >= WORDBYTES)

{

t = nltap(c) ^ BYTE2WORD(buf);

WORD2BYTE(t, buf);

cycle(c, t);

buf += WORDBYTES;

nbytes -= WORDBYTES;

}

if (nbytes != 0) {

c->StreamBuf = nltap(c);

c->CipherTextBuf = 0;

c->NumberOfBitsBuffered = WORDBITS;

while (c->NumberOfBitsBuffered != 0 && nbytes != 0) {

\*buf ^= c->StreamBuf & 0xFF;

c->StreamBuf >>= 8;

c->CipherTextBuf ^= \*buf << (WORDBITS - c->NumberOfBitsBuffered);

c->NumberOfBitsBuffered -= 8;

--nbytes;

}

}

}

void

sss\_deconly(sss\_ctx \*State, UCHAR \*CipherTextBuffer, int CipherTextLength)

{

WORD t = 0, t2 = 0;

if (State->NumberOfBitsBuffered != 0) {

while (State->NumberOfBitsBuffered != 0 && CipherTextLength != 0) {

State->CipherTextBuf ^= \*CipherTextBuffer << (WORDBITS - State->NumberOfBitsBuffered);

\*CipherTextBuffer ^= State->StreamBuf & 0xFF;

State->StreamBuf >>= 8;

State->NumberOfBitsBuffered -= 8;

++CipherTextBuffer;

--CipherTextLength;

}

if (State->NumberOfBitsBuffered != 0) /\* still not a whole word yet \*/

return;

cycle(State, State->CipherTextBuf);

}

while (CipherTextLength >= WORDBYTES)

{

t = nltap(State);

t2 = BYTE2WORD(CipherTextBuffer);

cycle(State, t2);

t ^= t2;

WORD2BYTE(t, CipherTextBuffer);

CipherTextBuffer += WORDBYTES;

CipherTextLength -= WORDBYTES;

}

if (CipherTextLength != 0) {

State->StreamBuf = nltap(State);

State->CipherTextBuf = 0;

State->NumberOfBitsBuffered = WORDBITS;

while (State->NumberOfBitsBuffered != 0 && CipherTextLength != 0) {

State->CipherTextBuf ^= \*CipherTextBuffer << (WORDBITS - State->NumberOfBitsBuffered);

\*CipherTextBuffer ^= State->StreamBuf & 0xFF;

State->StreamBuf >>= 8;

State->NumberOfBitsBuffered -= 8;

--CipherTextLength;

}

}

}

int \_tmain(int argc, \_TCHAR\* argv[])

{

sss\_ctx State; // the State we are trying to determine

sss\_ctx StateGuess; // our guess for the State

UCHAR CipherText[36\*256 + 36\*NumberOfExtraPatterns]; // our chosen CipherText, which will be always the same to recover any secret key

UCHAR PlainText[36\*256 + 36\*NumberOfExtraPatterns]; // the decrypted PlainText corresponding to our CipherText

int i,j,CipherTextLength,correct;

int ctr\_aL, ctr\_SaL;

UCHAR aL, aH, aHg1,aHg2;

UCHAR SboxInput;

WORD SboxGuess;

WORD a, Rotated\_a, a\_plus\_i, Rotated\_a\_plus\_i;

int EverythingCorrect;

CipherTextLength = 36\*256 + 36\*NumberOfExtraPatterns;

//We use a zero key and print the actual secret key-dependent SBox - You can put any other key here.

UCHAR ZeroKey[16] = {0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0};

sss\_key(&State, ZeroKey, 16);

// for (i=0;i<256;i++) printf("%02x \t %04x\n",i,State.SBox[i]);

// Now we choose our CipherText

for (i = 0; i < CipherTextLength; i++)

CipherText[i] = 0; // all values init to 0

for (i = 0; i < 256; i++)

CipherText[36\*i + 26] = i; // 255 modifications in LSB of r[13]

for (i = 0; i < NumberOfExtraPatterns; i++)

CipherText[256\*36 + 36\*i + 27] = i; // NumberOfExtraPatterns modifications in MSB of r[13]

// And obtain the corresponding PlainText

for (i = 0; i < CipherTextLength; i++)

PlainText[i] = CipherText[i];

sss\_deconly(&State, PlainText, CipherTextLength);

for (ctr\_aL = 0; ctr\_aL < 256; ctr\_aL++)

{

//for (ctr\_aL=0x11;ctr\_aL<0x12;ctr\_aL++){

aL = ctr\_aL;

// determine a\_H

aH = 0;

//for (i=0;i<256;i++){ // try all possible aH

for (i = 0; i < 256; i++)

{ // try all possible aH

aHg1 = i;

correct = 1;

for (j = 0; j < NumberOfExtraPatterns; j++)

{

aHg2 = aHg1 + j;

if ( (PlainText[34]^PlainText[256\*36 + 36\*j + 34]) != (aHg1^aHg2) )

correct = 0; //{correct=0; printf("probleem\n");} else printf("geen probleem!\n");

}

if (correct)

aH = aHg1; //{aH=aHg1; printf("%02x\n",aH);}

}

a = (aH<<8)^aL;

Rotated\_a = (aL<<8)^aH;

for (ctr\_SaL = 0; ctr\_SaL < 65536; ctr\_SaL++)

{

//for (ctr\_SaL=0x4cd9;ctr\_SaL<0x4cda;ctr\_SaL++){

// Set the guess back on the beginning values

for (i = 0; i < 256; i++)

StateGuess.SBox[i] = 0;

StateGuess.SBox[aL] = ctr\_SaL;

// determine the entire SBox

for (i = 1; i < 256; i++)

{

a\_plus\_i = a+i;

Rotated\_a\_plus\_i = ( (a\_plus\_i & 0xff) << 8) ^ ( (a\_plus\_i & 0xff00) >> 8);

//printf("a\_plus\_i %04x\t rotated %04x\n",a\_plus\_i,Rotated\_a\_plus\_i);

SboxInput = (aL + i); //printf("%d\n",SboxInput);

StateGuess.SBox[SboxInput] = (PlainText[35]<<8)^PlainText[34]^(PlainText[36\*i+35]<<8)^PlainText[36\*i+34]^StateGuess.SBox[aL]^Rotated\_a^Rotated\_a\_plus\_i;

}

//for (i=1;i<256;i++) printf("%02x\t Actual: %04x \t Guess: %04x\n",i,State.SBox[i],StateGuess.SBox[i]);

// Print the solution if it's the correct one:

EverythingCorrect = 1;

for (i=0;i<256;i++)

{

if (State.SBox[i] != StateGuess.SBox[i])

{

EverythingCorrect = 0;

i = 256;

}

}

if (EverythingCorrect)

{

printf("The key has been recovered entirely!\n");

for (i = 0; i < 256; i++)

std::cout<<i<<"\t"<<State.SBox[i]<<"\t"<<StateGuess.SBox[i]<<std::endl;

//printf("%02x\t Actual: %04d \t Guess: %04d\n",i,State.SBox[i],StateGuess.SBox[i]);

ctr\_aL = 256;

ctr\_SaL = 65536;

} } } getchar(); return 1;}