УДК 004.6

Ренат ДАВЛЕТОВ, Василь КУЗИК
Галицький фаховимй коледж імені В'ячеслава Чорновола

ПРОГРАМНИЙ ЗАСІБ ДЛЯ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ З КОРЕКЦІЄЮ ПОМИЛОК

Вступ. Швидкий розвиток технологій та зростання кількості кіберзагроз ставлять під загрозу безпеку інформаційних систем. Дані стають основним ресурсом, забезпечення їх конфіденційності, цілісності та доступності є важливою задачею. В процесі передачі даних можуть виникати помилки різного роду, що можуть бути як результатом технічних збоїв, так і навмисних атак на комунікаційні канали. Зважаючи на це, необхідно використовувати надійні методи шифрування для захисту від несанкціонованого доступу та методи корекції помилок для забезпечення цілісності переданої інформації.

Використання традиційних методів шифрування дозволяє забезпечити ефективний захист від перехоплення, проте не гарантує відсутність помилок під час передачі даних. Для забезпечення безпеки і надійності інформаційних систем необхідно інтегрувати ці методи з алгоритмами корекції помилок, які дозволяють виявляти та виправляти помилки в процесі декодування без втрати даних. У зв'язку з цим, створення програмного засобу для захищеного обміну даними з виявленням і корекцією помилок є важливим кроком для підвищення ефективності інформаційних систем, знижуючи ризики від помилок та атак на канали зв'язку.

Мета: дослідження властивостей кодів для корекції помилок та розробка інструменту безпечного обміну даними є важливим етапом у підвищенні рівня інформаційної безпеки.

1. Класифікація методів корекції помилок

Коди для корекції помилок (ККП) - це математичні конструкції, які використовуються для виявлення та виправлення помилок, що можуть виникнути під час передачі або збереження даних. Вони є ключовим елементом у забезпеченні надійності інформаційних систем, особливо в умовах, де можливі збої в каналах зв'язку або збереженні даних. Ці коди дозволяють зберегти цілісність інформації, навіть якщо частина даних була пошкоджена чи втрата під час передачі. Коригуючі коди можна класифікувати за кількома основними ознаками (рисунок 1) [1].

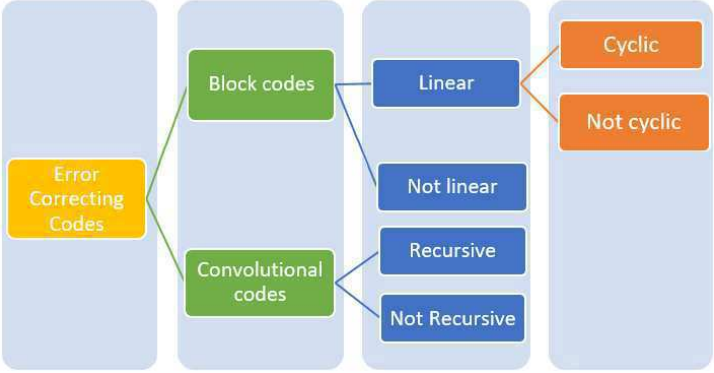

Рисунок 1 - Класифікація ККП

Блокові коди працюють з фіксованими блоками даних, де кожне повідомлення кодується окремо, зазвичай з додаванням контрольних бітів. Згорткові - використовують потік даних, обробляючи його поетапно, зберігаючи попередні значення для кодування кожного наступного елемента.

Лінійні ККП задовольняють принцип лінійності, тобто сума двох кодових слів завжди дає нове кодове слово. Структура нелінійних є більш складною, що може підвищити безпеку кодування. Рекурсивні коди характеризуються тим, що для кодування і декодування використовуються рекурсивні алгоритми, що зазвичай дозволяє скоротити обчислювальні витрати. Нерекурсивні - не використовують рекурсії і, як правило, застосовуються там, де важлива простота реалізації. Властивістю циклічних кодів є те, що будь-який циклічний зсув кодового слова також є допустимим кодовим словом. Нециклічні коди працюють з фіксованими структурами без можливості зсуву.

Наведені класифікаційні ознаки ККП дозволяють визначити, які коригуючі коди є оптимальними для використання у конкретних умовах і відповідають вимогам до надійності та ефективності передачі даних.

2. Аналіз властивостей та ефективності кодів для корекції помилок

Корегуючі коди, такі як коди Хеммінга, Ріда-Соломона, LDPC [2], є важливими інструментами для виявлення та виправлення помилок, які виникають під час передачі та зберігання інформації. Кожен з них має свої специфічні властивості, такі як здатність до виправлення кратних посилок, помилок певного рівня, вимоги до обчислювальних ресурсів та ефективність у різних умовах використання.

Коди Хеммінга класифікуються як лінійні, блокові, нерекурсивні та нециклічні коди. Вони мають просту структуру та ефективні у реалізації, що робить їх оптимальними для використання в реальному часі та в умовах обмежених ресурсів. Вони здатні коригувати одну помилку та виявляти дві, що робить їх ефективними для невеликих обсягів даних. Вони вимагають менше місця для зберігання і мають невеликий обсяг додаткової інформації (паритетних бітів), що знижує витрати на пам'ять і передачу.

Недоліками застосуваня кодів Хеммінга є те, що вони дозволяють виправити лише одну помилку на блок. Якщо кількість помилок у пакеті перевищує одну, система не зможе виправити помилку, що знижує надійність у більш складних умовах. Їх застосування обмежене для ситуацій, де ймовірність помилок висока або де потрібно виправляти кілька помилок одночасно.

Коди Ріда-Соломона належать до блокових та лінійних кодів, а також є нециклічними за своєю структурою, хоча існують і циклічні варіанти цих кодів. На відміну від кодів Хеммінга коди Ріда-Соломона можуть виправляти до t помилок у блоках розміром $2t$. Це дозволяє ефективно їх використовувати в умовах високої ймовірності помилок. Ці ККП широко використовуються в різних технологіях, таких як CD/DVD, QR-коди. Параметри коду можна варіювати залежно від вимог до корекції помилок і пропускної здатності каналу. Оскільки коди Ріда-Соломона потребують більш складних операцій, таких як обчислення в полях Галуа, їх реалізація зазвичай потребує більших обчислювальних ресурсів. Чим більше помилок потрібно коригувати, тим більше бітів необхідно додавати

для кодування, що збільшує витрати на пам'ять та обчислювальні ресурси.

Коди Гоппа - це тип лінійних і циклічних блокових кодів, що мають значні можливості для корекції помилок і використовуються у криптографії завдяки їх високій стійкості до атак. Вони є основою для деяких сучасних криптографічних алгоритмів. Ці ККП забезпечують високу корекцію помилок навіть для випадкових та систематичних помилок проте потребують значних обчислювальних ресурсів, особливо на етапах кодування та декодування, що може уповільнювати роботу системи, особливо при великих обсягах даних.

Коди з низькою щільністю перевірок парності (LDPC) є лінійними блоковими кодами, що забезпечують високий рівень корекції помилок при невеликому збільшенні витрат для кодування. Вони, завдяки здатності до корекції багатьох помилок, використовуються в складних системах, таких як супутникові системи зв'язку або в сучасних безпровідних мережах (Wi-Fi, 5G). LDPC коди потребують значних обчислювальних ресурсів для декодування та значних обсягів пам'яті що може бути менш ефективними в реальних системах з обмеженими ресурсами.

Основні характеристики ККП полягають у наступному:

- виявлення та виправлення помилок;
- забезпечення безпеки даних;
- підвищення надійності систем;
- оптимізація використання ресурсів;
- зменшення витрат на повторну передачу.

ККП дозволяють виявляти помилки, які виникають при передачі або зберіганні даних, і автоматично виправляти їх без потреби в повторній передачі. Це особливо важливо для систем, де необхідно забезпечити високий рівень доступності та швидкості обміну інформацією, наприклад, у телекомунікаціях або бездротових мережах.

Під час передачі даних можуть виниками різні перешкоди, наприклад шум, завади або технічні збої. Тому використання ККП дозволяє підвищити надійність системи та дає можливість компенсувати негативний вплив цих факторів, забезпечуючи коректність отриманих даних. ККП дозволяють уникнути необхідності повторної передачі інформації, що забезпечує раціональне використання ресурсів і часу, що має особливу актуальність для систем з обмеженими ресурсами, таких як пристрої інтернету речей (IoT) або комунікації, де повторні передачі можуть бути дуже дорогими або неможливими. Використання ККП дозволяє ефективно використовувати доступну пропускну здатність каналу зв'язку, наприклад в системах де передача даних обмежена, зокрема мобільних мережах або IoT, де зазвичай є потреба у передачі великих обсягів інформації через обмежені канали.

ККП використовуються у поєднанні з методами шифрування для забезпечення додаткового рівня безпеки даних. Вони допомагають гарантувати, що навіть у разі атаки на канал зв'язку інформація буде захищена від несанкціонованого доступу і не втратить свою цілісність.

Коригуючі коди є важливим інструментом для забезпечення надійності і безпеки в інформаційних системах та можуть застосовуватися у широкому колі застосувань, від телекомунікацій до сучасних криптографічних технологій [3].

3. Розробка програмного засобу безпечного обміну даними

Хоча коди Ріда-Соломона, LDPC є потужними та ефективними для складних сценаріїв, таких як високошвидкісні канали зв'язку або постквантова криптографія, їх застосування може бути обмежене в умовах обмежених ресурсів. Наприклад, коди Гоппа забезпечують високий рівень стійкості до помилок та квантових атак, але потребують значних обчислювальних ресурсів і мають великий розмір ключів, що ускладнює їх використання в компактних системах. У простіших системах зв'язку або пристроях з обмеженими ресурсами коди Хеммінга часто є оптимальним вибором завдяки меншій обчислювальній складності та можливості корекції одиничних помилок. Для розробки програмного засобу обрано саме їх, оскільки ці коди забезпечують базовий рівень надійності та ефективності, якого достатньо для багатьох простих застосувань, і дозволяють уникнути надмірних витрат на обробку, характерних для більш складних кодів.

Запропонований програмний засіб для захищеного обміну даними з корекцією помилок, реалізований на мові програмування Python (рисунок 2). Він забезпечує надійну передачу інформації між користувачами, поєднуючи методи шифрування та виправлення помилок.

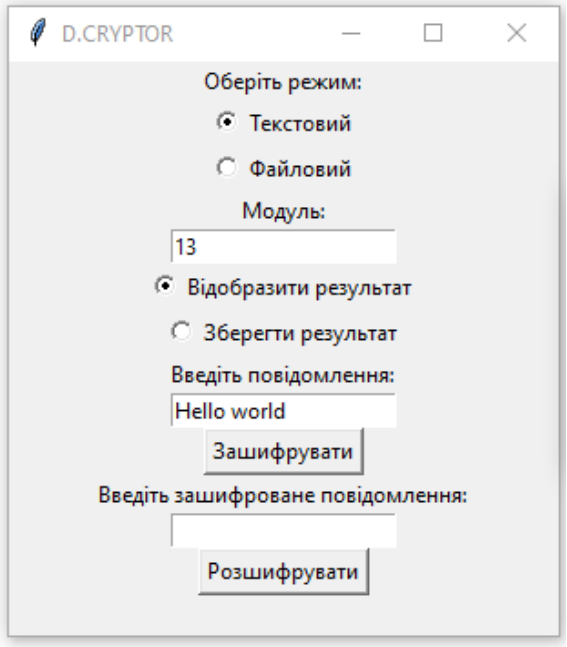

Рисунок 2 - Головне вікно та результат кодування

На рисунку 3 наведено результат кодування вихідного повідомлення. Кодування відбувається шляхом переведення коженого символу в його ASCII-код та побудови коду Хеммінга в скінченому полі Галуа [3], в даному випадку GF(13).

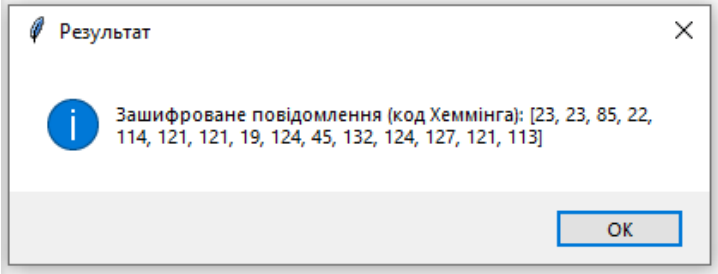

Рисунок 3 - Результат кодування

Основні функції програмного засобу:

- конфіденційність даних за допомогою кодування перед відправкою, що запобігає несанкціонованому доступу до інформації;
- захистит даних від спотворень під час передачі за допомогою ККП здатних вилявити та виправляти одиничні помилки (рисунок 3);
- декодування даних (рисунок 4), що дозволяє отримувачу отримати цілісну інформацію, навіть якщо під час передачі виникли незначні помилки.

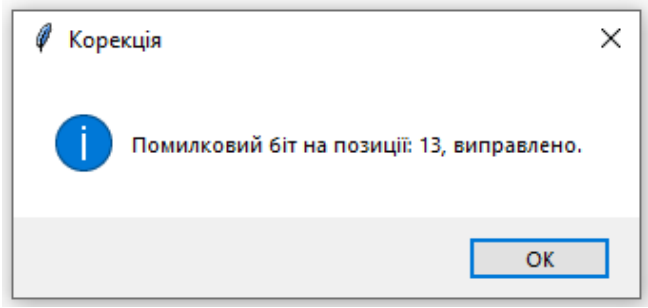

Рисунок 3 - Приклад корекції помилки

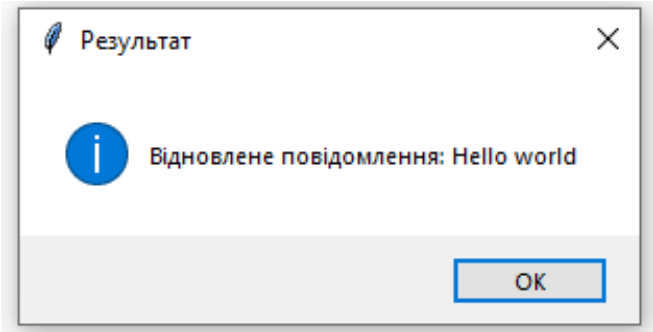

Рисунок 4 –Результат декодування

Запропонований програмний засіб забезпечує захист даних від несанкціонованого доступу та автоматичне виявлення та корекцію помилок, що можуть виникати під час передачі. Це досягається завдяки використанню корегуючих властивостей кодів Хеммінга.

Висновок. Запропонований програмний засіб дозволяє ефективно обмінюватися інформацією в умовах ненадійних каналів зв'язку, забезпечуючи конфіденційність, цілісність та стійкість до помилок в переданих даних.

Перелік використаних джерел.

1. Imrane C., Nouh S., Bellfkih El M., el Kasmi A., M. Seddiq, Abdelaziz M. Machine learning for decoding linear block codes: case of multi-class logistic regression model. Indonesian Journal of Electrical Engineering and Computer Science. 2021. 24. 538. 10.11591/ijeecs.v24.i1.pp538-547.

2. Денбновецький С.В. Кодування сигналів в електронних системах. Частина 3. Способи кодування сигналів: Том 1. Натуральні, ефективні та лінійні коди / С.В. Денбновецький, І.В. Мельник, Л.Д. Писаренко; КПІ ім. Ігоря Сікорського. - Київ: КПІ ім. Ігоря Сікорського.- 2021.- 470с.

3. Davletova A. Construction of Hamming Codes in Finite Galois Fields. Herald of Khmelnytskyi National University. Technical sciences. 2024. 333. 28-34. 10.31891/2307-5732-2024-333-2-4.