МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Сумський державний університет

Факультет електроніки та інформаційних технологій

(повна назва інституту/факультету)

Кафедра електроніки та комп'ютерної техніки

(повна назва кафедри)

«До захисту допущено»

Завідувач кафедри

_____ Анатолій ОПАНАСЮК

(підпис) (Ім'я та ПРІЗВИЩЕ)

____ _____ 20__ р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня бакалавр

(бакалавр / магістр)

зі спеціальності 171 Електроніка,

(код та назва)

освітньо-професійної програми Електронні системи та компоненти

(освітньо-професійної / освітньо-наукової) (назва програми)

на тему: «Пристрій шифрування інформації на базі алгоритму Цезаря з ключовим словом»

Здобувача групи ЕС-91 Мельника Романа Валерійовича

(шифр групи) (прізвище, ім'я, по батькові)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Мельник Роман

(підпис) (Ім'я та ПРІЗВИЩЕ здобувача)

Керівник доцент, доцент, к.т.н., Бережна О.В.

(посада, науковий ступінь, вчене звання, Ім'я та ПРІЗВИЩЕ) (підпис)

Суми – 2023

Сумський державний університет

Факультет ЕлІТ__Кафедра електроніки і комп'ютерної техніки

Спеціальність: 171– Електронні системи та компоненти

ЗАТВЕРДЖУЮ
Завідувач кафедри
електроніки і
комп’ютерної техніки
_____ А. С. Опанасюк
“___”_____2023 р.

ЗАВДАННЯ
до виконання кваліфікаційної роботи бакалавра

Мельник Роман Валерійович

1.Тема роботи :« Пристрій шифрування інформації на базі алгоритму Цезаря з ключовим словом »

затверджена наказом по університету № 0310-VI від “ 30 ” березня 2023 р.

2.Термін здачі студентом закінченої роботи 10.06.2023.

3.Вихідні дані до роботи:: Розробити пристрій шифрування інформації на базі алгоритму Цезаря з ключовим словом. Синтез пристрою виконати на базі мікроконтролера.

4.Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно вирішити)

Вступ.Огляд літератури та постановка задачі проектування. Розробка, обґрунтування алгоритму функціонування схеми пристрою, що проектується. Розробка та розрахунок принципових електричних схем, вузлів та блоків. Висновки. Список використаної літератури

5. Перелік обов’язкового графічного матеріалу (з точним зазначенням обов’язкових креслень або плакатів)

1. Блок-схема алгоритма функціонування.
2. Схема електрична структурна.
3. Схема електрична принципова.

Календарний план

№ п/п	Найменування етапів дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Огляд літератури	10.04.2023	
2	Розробка алгоритму роботи	24.04.2023	
3	Розрахунок і синтез основних блоків	15.05.2023	
4	Розроблення схем електричних	29.05.2023	
5	Представлення роботи керівнику	5.06.2023	

Студент-дипломник Мельник Роман Валерійович _____
(підпис)

Керівник проекту Бережна Ольга Володимірівна _____
(підпис)

«_____»_____20___р.

Анотація

Пояснювальна записка містить: 37 аркушів, 11 рисунків, , 13 джерел літератури.

Графічна частина роботи містить: схему алгоритму роботи пристрою, структурну, та принципову електричні схеми.

Пояснювальна записка містить три розділи: огляд літератури і постановку завдання проектування, розробку структурної схеми пристрою та алгоритму його функціонування, розробку принципової схем пристрою.

Перший розділ містить загальну інформацію про прилади шифрування, їх призначення, основні функції та види, а також постановку завдання на проектування.

Другий розділ присвячений розробці алгоритму функціонування та структурної схеми проектованого пристрою.

Третій розділ присвячений розробці принципової схеми пристрою.

Зміст

1.Вступ

У сучасному цифровому світі, коли інформація є одним з найцінніших активів, захист конфіденційності, цілісності та доступності інформаційних ресурсів стає основною проблемою. Зростання кількості зберіганої і передаваної інформації, швидкий розвиток технологій зв'язку та зберігання даних створюють нові виклики і загрози безпеці інформації.

Пристрій захисту інформації є ключовим компонентом в реалізації ефективної системи безпеки. Він використовує різноманітні технології, методи та механізми для забезпечення безпеки інформаційних ресурсів від несанкціонованого доступу, зламу, крадіжки чи викриття.

Основна мета пристрою захисту інформації - забезпечити конфіденційність, цілісність та доступність даних. Конфіденційність забезпечує захист інформації від несанкціонованого доступу, забезпечуючи, що лише уповноважені особи мають доступ до неї. Цілісність гарантує, що дані не були змінені або порушені під час передачі або зберігання. Доступність забезпечує постійний доступ до інформації для уповноважених користувачів.

Пристрій захисту інформації може включати різні компоненти, такі як криптографічні алгоритми, системи контролю доступу, вогневі стіни, антивірусні програми та інші технології. Він також враховує фізичну безпеку, процедури управління, аудит безпеки та свідомість користувачів.

Ефективний пристрій захисту інформації є критичним для забезпечення довіри, конфіденційності та цілісності інформаційних ресурсів. Він допомагає запобігати несанкціонованому доступу, зламам та крадіжкам, а також забезпечує впевненість у тому, що дані залишаються захищеними та доступними лише авторизованим особам.

Дослідження, розробка та впровадження пристроїв захисту інформації є критичними завданнями в сучасному цифровому світі, які допомагають забезпечити безпеку інформації та захистити цінні активи від загроз інформаційної безпеки.

1.1 Обґрунтування актуальності проблеми шифрування даних у сучасному світі

У сучасному світі шифрування даних є надзвичайно важливим процесом, який використовується для захисту конфіденційної інформації в різних галузях. Завдяки шифруванню даних, конфіденційна інформація може бути захищена від несанкціонованого доступу, зламу або крадіжки. Шифрування даних використовується в електронній комерції, фінансових послугах, військових операціях, а також в приватному житті, де люди часто обмінюються конфіденційною інформацією через Інтернет.

Однак, кібератаки та порушення безпеки даних показали, що шифрування даних не є повністю надійним. Наприклад, у 2020 році стало відомо про злам електронної пошти Microsoft Exchange, який зумовив порушення безпеки великої кількості даних. Це підкреслює потребу в розвитку та вдосконаленні методів шифрування даних, щоб забезпечити безпеку даних.

Ще однією проблемою, пов'язаною з шифруванням даних, є підвищення потужності обчислювальної техніки. Розвиток квантових комп'ютерів може значно скоротити час, необхідний для злому шифрування даних, які базуються на нинішніх методах. Це може спричинити серйозні наслідки для безпеки даних, що вимагає вдосконалення методів шифрування та пошук нових, більш надійних алгоритмів.

Крім того, у світі технологій та інтернету шифрування даних стає все більш складним завданням, оскільки з'являється все більше нових технологій та інструментів для злому шифрів. Це може привести до того, що нинішні методи шифрування даних будуть вважатися застарілими та ненадійними.

Таким чином, актуальність проблеми шифрування даних в сучасному світі зумовлена постійним розвитком технологій, збільшенням кількості кібератак та необхідністю захисту конфіденційної інформації в різних сферах діяльності. Нові методи шифрування даних, які будуть більш надійними та здатні протистояти сучасним викликам безпеки, є необхідними для забезпечення безпеки даних в майбутньому.

У теоретичній частині дипломної роботи буде розглянуто алгоритм Цезаря з ключовим словом як метод шифрування даних. Будуть детально

проаналізовані принципи роботи даного алгоритму та основні принципи шифрування даних взагалі. В рамках роботи буде вивчено існуючі методи шифрування даних та їх переваги та недоліки. Також буде розглянуто сучасні виклики безпеки та існуючі проблеми у сфері шифрування даних.

Дослідження проблеми шифрування даних у сучасному світі є дуже важливим та актуальним завданням, оскільки інформація є однією з найцінніших ресурсів у сучасному світі. У більшості сфер діяльності використовується різноманітна інформація, яка потребує надійного захисту від несанкціонованого доступу.

Зважаючи на те, що в сучасному світі стає все більше кіберзлочинів, де зловмисники можуть отримати доступ до конфіденційної інформації, захист даних стає дедалі важливішим. У бізнесі це може призвести до серйозних фінансових втрат та порушення довіри клієнтів, в державних структурах - до ризику національної безпеки та втрати державної таємниці, а в особистому житті - до порушення приватності та крадіжки особистих даних.

Таким чином, розробка та вдосконалення методів шифрування даних є одним з найважливіших завдань сучасної інформаційної безпеки. У дипломній роботі буде проведено детальний аналіз алгоритму Цезаря з ключовим словом, що дозволить визначити його ефективність та внести певні покращення у метод шифрування даних [4].

1.2. Криптографія з відкритим ключем та цифрові конверти,типи алгоритмів, порівняння алгоритмів.

Найбільший клас - це асиметричні криптосистеми або системи з відкритим ключем. Основна ідея цього класу криптографії полягає в генерації двох ключів: один відкритий ключ поширюється по відкритому каналу зв'язку і використовується для шифрування повідомлення. На приймальній стороні приватний ключ використовується для розшифровки повідомлення. Основою для створення таких шифрів є, як зазначалося вище, складні задачі. Наразі для вирішення таких проблем використовуються методи теорії факторизації, дискретного логарифмічного розкладання та завадостійкого кодування.

Асиметричні алгоритми шифрування - це алгоритми шифрування, які використовують різні ключі для шифрування та розшифрування даних.

Основне досягнення асиметричного шифрування полягає в тому, що воно дозволяє людям без існуючих угод про безпеку обмінюватися секретними повідомленнями. Відправнику та одержувачу не потрібно узгоджувати секретний ключ через спеціальний захищений канал. Процедура шифрування обрана таким чином, що вона є незворотною за наявності відомого ключа шифрування. Це означає, що якщо ключ шифрування і зашифрований текст відомі, неможливо відновити початкове повідомлення, яке можна прочитати лише за допомогою другого ключа - ключа розшифрування. Якщо це так, то ключ шифрування для відправлення комусь листа може бути взагалі не прихований - навіть якщо ви його знаєте, прочитати зашифроване повідомлення все одно неможливо. Тому в асиметричних системах ключ шифрування називається "відкритим ключем", тоді як ключ розшифрування повинен зберігатися в таємниці одержувачем повідомлення і називається "секретним ключем". Алгоритми шифрування і дешифрування розроблені таким чином, що секретний ключ неможливо обчислити, якщо відомий відкритий ключ.

Симетричні алгоритми шифрування - це схеми шифрування, які використовують один і той же ключ шифрування для шифрування і розшифрування. До винаходу асиметричних схем шифрування, єдиними існуючими схемами були симетричні схеми шифрування. Ключ алгоритму повинен зберігатися в таємниці обома сторонами. Алгоритми шифрування і дешифрування даних широко використовуються в комп'ютерних технологіях в системах, призначених для приховування конфіденційної або комерційної інформації від зловживань з боку сторонніх осіб. Основний принцип полягає в тому, що сторона, яка отримує повідомлення, заздалегідь знає алгоритм шифрування і ключ до нього, без якого інформація є лише набором символів, що не мають ніякого сенсу. Симетричні алгоритми шифрування перетворюють невеликі (1-бітові або 32-128-бітові) блоки даних відповідно до ключа, так що оригінальне повідомлення можна прочитати, тільки якщо відомий секретний ключ.

Симетричні криптоалгоритми діляться на:

– Скремблери.

– Блокові шифри.

Скремблер - це програмна або апаратна реалізація алгоритму, який може зашифрувати безперервний потік інформації біт за бітом. Сам скремблер - це набір бітів, які змінюються на кожному кроці певного алгоритму. По завершенні кожного кроку на виході скремблера з'являється біт шифрування (0 або 1), який накладається на поточний біт інформаційного потоку за допомогою операції XOR ("побітове виключне АБО"). Основним недоліком алгоритму скремблювання є те, що він не захищений від несанкціонованого доступу.

Блокові шифри перетворюють блок вхідної інформації певної довжини і отримують блок результату такого ж розміру, до якого не може отримати доступ неавторизований користувач без ключа. Тому схеми блочних шифрів можна описати функціями Z=EnCrypt(X,Key) і X=DeCrypt(Z,Key). Ключ Key є параметром блочного алгоритму і являє собою блок двійкової інформації певного розміру. Вихідний блок даних (X) і зашифрований блок даних (Z) також мають фіксовану бітову глибину, яка дорівнює один одному, але не обов'язково дорівнює довжині ключа.

Порівняння асиметричних і симетричних криптоалгоритмів:

Асиметричні криптографічні алгоритми:

Криптографічний алгоритм з відкритим ключем;

Відкритий ключ використовується для шифрування повідомлення, а закритий ключ використовується для розшифрування повідомлення. Це означає, що якщо ключ шифрування і зашифрований текст відомі, відновити оригінальне повідомлення неможливо;

Якщо конфіденційність k-ї робочої станції порушено, зловмисник знає лише "секретний" ключ k. Це дозволяє йому читати всі повідомлення, отримані абонентом k, але не може видавати себе за нього при надсиланні повідомлень;

В асиметричних системах кількість існуючих ключів лінійно залежить від кількості абонентів (в системі з N користувачами використовується 2*N ключів).

Симетричні криптографічні алгоритми

Криптографічна схема з секретним ключем;

Секретний ключ використовується як для шифрування, так і для розшифрування. Це означає, що якщо ключ шифрування і зашифрований текст відомі, повідомлення можна розшифрувати;

Якщо конфіденційність робочої станції порушена, зловмисник отримає доступ до всіх ключів цього користувача і може надсилати повідомлення всім абонентам, з якими переписується "жертва", нібито від його імені;

У симетричних системах кількість ключів збільшується в квадратичній залежності від кількості користувачів.

1.3. Опис проблеми безпеки інформації в електронному віці

У сучасному світі проблема безпеки інформації є вкрай актуальною. З розвитком інформаційних технологій та зростанням використання електронних пристроїв, таких як комп'ютери, смартфони, планшети та інші, проблема безпеки інформації стає дедалі важливішою.

Одна з найбільших проблем безпеки інформації в електронному віці полягає у тому, що інформація може бути викрадена або використана несанкціонованою особою. Кіберзлочини стали частим явищем в останні роки, а злочинці використовують все більш складні методи для доступу до конфіденційної інформації. Наприклад, злочинці можуть використовувати соціальні мережі для отримання доступу до особистих даних користувачів, або використовувати фішингові атаки для отримання доступу до паролів та інших конфіденційних даних.

Інша проблема безпеки інформації в електронному віці полягає в тому, що інформація може бути пошкоджена або втрачена через технічні проблеми. Наприклад, комп'ютер може зламатися, або на нього може напасти вірус, що призведе до втрати даних. Також можуть відбуватися випадкові видалення файлів або форматування диска, що також може призвести до втрати інформації.

Одним із рішень проблеми безпеки інформації є шифрування даних. Шифрування даних - це процес перетворення звичайного тексту у зашифрований текст, який може бути прочитаний лише за допомогою спеціального ключа або пароля. Шифрування даних дозволяє зберігати конфіденційну інформацію в безпеці, оскільки навіть у випадку зламу

системи, злочинець не зможе прочитати зашифровані дані без ключа або пароля.

Проте, існують різні алгоритми шифрування, і не всі з них є достатньо надійними. Деякі алгоритми можуть бути легко зламані, що може призвести до викрадення інформації. Крім того, ключі та паролі можуть бути викрадені, або ж користувачі можуть просто забути їх, що також може призвести до втрати інформації.

З огляду на зростаючу кількість кіберзлочинів та загроз безпеці інформації в електронному віці, розробка та використання надійних алгоритмів шифрування є важливим завданням. Одним з найбільш поширених алгоритмів є алгоритм Цезаря з ключовим словом, який дозволяє зашифрувати дані з використанням ключа, що робить його надійним інструментом для зберігання конфіденційної інформації.

Отже, розробка нових технологій та методів шифрування, а також поліпшення вже існуючих, може допомогти забезпечити безпеку інформації в електронному віці та захистити її від несанкціонованого доступу.

1.4. Історична довідка про історію шифрування та розвиток алгоритмів шифрування на основі перестановки та заміни

Історія шифрування сягає віддалених часів і починається з розвитку дипломатії та воєнного мистецтва. В давні часи люди використовували різноманітні способи шифрування для збереження конфіденційної інформації та передачі її в безпеці. З часом шифрування стало значно складнішим, оскільки з'явилися більш складні системи та методи атак.

Перші методи шифрування базувалися на перестановці символів, де символи повторювалися з певною частотою. Ці перестановки забезпечували достатньо низький рівень безпеки, оскільки злочинці могли легко зламати ці системи, якщо вони знали їх структуру та методи шифрування.

З часом були розроблені більш складні методи шифрування, зокрема метод заміни, де символи замінювалися на інші символи за певними правилами. Ці методи забезпечували значно вищий рівень безпеки, оскільки злочинці повинні були знати правила заміни символів для того, щоб розшифрувати повідомлення.

У 20 столітті шифрування стало значно більш складним та ефективним завдяки розвитку комп'ютерної технології та криптографії. Було розроблено багато нових методів шифрування на основі різних алгоритмів, зокрема на основі перестановки та заміни.

Один з найбільш поширених методів шифрування на основі перестановки є алгоритм Цезаря, який був розроблений у Давньому Римі. Цей метод полягає в тому, що кожен символ замінюється на символ з певним кроком в алфавіті. Іншим поширеним методом є шифр Плейфера

У 20-му столітті з'явилися нові методи шифрування, які використовують математичні функції, такі як шифр RSA, що базується на складності факторизації великих простих чисел, і шифр Діффі-Хеллмана, який використовує проблему обернення в кільці вищого порядку. Ці методи шифрування залишаються досить складними для зламування, проте вони потребують значно більшої обчислювальної потужності для їх застосування, що може бути проблемою в деяких випадках.

Загалом, розвиток шифрування продовжується і на сьогоднішній день. Хоча нові методи шифрування можуть стати більш складними для зламування, вони також можуть бути дорожчими в розробці та використанні. З цієї причини алгоритм Цезаря з ключовим словом залишається популярним інструментом шифрування, особливо для невеликих обсягів даних.

Отже, історія шифрування відображає розвиток цієї науки від простих методів заміни та перестановки до складних математичних функцій, які захищають конфіденційні дані від несанкціонованого доступу. Розуміння цієї історії дозволяє нам краще оцінити сучасні методи шифрування та їх потенційні переваги та недоліки [11].

1.5 Огляд існуючих методів шифрування

Шифрування є важливим інструментом для захисту конфіденційної інформації, тому існує багато методів шифрування. Огляд існуючих методів шифрування включає в себе опис різних методів шифрування та їх відмінності.

Одним з найпростіших методів шифрування є заміна символів. Заміна символів полягає в тому, що кожен символ у повідомленні замінюється на інший символ. Наприклад, символ "А" може бути замінений на символ "В", а символ "Б" - на символ "Г". Цей метод дуже легко зламати, оскільки просто можна замінити кожен символ повідомлення на його еквівалент з шифртексту, щоб розшифрувати повідомлення.

Ще один простий метод шифрування - це метод перестановки. Метод перестановки полягає в тому, що символи повідомлення замінюються в певному порядку. Наприклад, перший символ повідомлення може бути переміщений на третє місце, другий - на перше місце, а третій - на друге місце. Цей метод також досить легко зламати, оскільки можна відновити оригінальний порядок символів шляхом перебору всіх можливих комбінацій.

Більш складні методи шифрування, які використовуються в сучасній криптографії, використовують математичні алгоритми. Ці методи шифрування можуть бути класифіковані на дві категорії: симетричне шифрування та асиметричне шифрування.

Симетричне шифрування полягає в тому, що один ключ використовується для шифрування та розшифрування повідомлення. Ключ має бути досить випадковим та довгим, щоб захистити повідомлення від зламування

Ще одним популярним методом шифрування є RSA, який використовується для шифрування та розшифрування даних з використанням публічного ключа. У цьому методі відкритий ключ відомий усім, хто бажає надіслати повідомлення, а закритий ключ відомий лише отримувачу. RSA є безпечним методом шифрування, оскільки його складність базується на факторизації великих простих чисел.

Крім того, існують методи шифрування, які використовуються в окремих сферах діяльності. Наприклад, методи шифрування для банківських

транзакцій, використовуються в криптографії на базі еліптичних кривих, а методи шифрування для захисту інформації у мережі Інтернет - TLS та SSL.

Хоча існують різні методи шифрування, жоден з них не є повністю недоліків, і кожен з них має свої переваги та недоліки. Іноді потрібно використовувати комбінацію різних методів шифрування для досягнення максимального рівня захисту даних. У цілому, розуміння різних методів шифрування та їх застосування дозволяє зберігати дані в безпеці та уникнути ризиків відкриття конфіденційної інформації.

1.6 Переваги та недоліки різних методів шифрування

Переваги та недоліки різних методів шифрування є важливими аспектами розгляду при розробці пристроїв шифрування інформації. Різні методи шифрування мають свої переваги та недоліки, які слід враховувати при виборі оптимального методу залежно від конкретної ситуації.

Один з переваг методу шифрування на базі алгоритму Цезаря з ключовим словом є його простота та ефективність. Даний метод шифрування використовує один з найстаріших методів шифрування - зсув символів, що дозволяє швидко та ефективно зашифрувати дані. Ключове слово в методі Цезаря додає додатковий рівень безпеки до шифрування, оскільки він дозволяє змінювати зсув символів в залежності від вибраного ключового слова. Таким чином, метод Цезаря з ключовим словом може бути корисним для шифрування невеликої кількості даних, де швидкість шифрування є ключовим фактором.

Однак, недоліком методу Цезаря з ключовим словом є його низький рівень безпеки відносно сучасних методів криптоаналізу. Адверсар може використовувати різноманітні методи атак на дані зашифровані методом Цезаря з ключовим словом, що дозволяє розшифрувати дані з високою ймовірністю. Крім того, метод Цезаря з ключовим словом є вразливим до атак, заснованих на статистичному аналізі тексту, оскільки він не змінює частоту символів у тексті.

1.7 Пристрій шифрування інформації

Пристрій шифрування інформації - це електронний пристрій, призначений для захисту інформації від несанкціонованого доступу. Його основною функцією є перетворення відкритого тексту в зашифрований текст з метою збереження конфіденційності інформації. Для шифрування інформації пристрій використовує спеціальні алгоритми, що дозволяють змінювати оригінальний текст в нерозпізнаваний для незаконного користувача.

Основні компоненти пристрою шифрування інформації включають блок шифрування, блок керування, блок перетворення і блок управління. Блок шифрування - це ключовий компонент, який використовується для захисту інформації від несанкціонованого доступу. Його функція полягає в перетворенні відкритого тексту в зашифрований текст з використанням алгоритму шифрування. Блок керування відповідає за управління процесом шифрування, забезпечуючи координацію роботи інших компонентів пристрою.

Блок перетворення забезпечує передачу інформації між компонентами пристрою. Це здійснюється з використанням різноманітних методів, таких як модуляція або демодуляція сигналів, відображення сигналів на дисплеї або інші методи передачі даних.

Блок управління - це компонент, який забезпечує керування роботою пристрою шифрування, зокрема включенням та вимиканням, зміною налаштувань, відображенням інформації про стан пристрою та іншими функціями.

Щоб забезпечити ефективне функціонування пристрою шифрування інформації, необхідно розробити відповідний алгоритм шифрування, який гарантує безпеку і конфіденційність інформації. При цьому важливо врахувати, що алгоритм повинен бути стійким до криптоаналізу і несанкціонованого розшифрування.

Застосування пристроїв шифрування інформації може бути широким і включати такі сфери, як комунікації, банківські та фінансові установи, військові організації, медичні установи, державні органи та багато інших.

Вони використовуються для захисту конфіденційної інформації, обміну даними, забезпечення безпеки мереж та інших комунікаційних систем.

Узагальнюючи, пристрій шифрування інформації є важливим інструментом для забезпечення безпеки і конфіденційності інформації. Він включає різні компоненти та алгоритми, що дозволяють перетворити відкритий текст у зашифрований формат. Застосування таких пристроїв має велике значення в різних сферах діяльності, де збереження інформації є критично важливим аспектом [2].

1.8 Опис алгоритму Цезаря та його особливості (Опис алгоритму Цезаря та його застосування)

Алгоритм Цезаря - це один з найпростіших методів шифрування, який базується на зсуві кожної літери вхідного тексту на певне число позицій в алфавіті. Алгоритм був названий на честь Юлія Цезаря, який використовував його для зашифрування своїх таємних повідомлень.

Основна ідея алгоритму полягає в заміні кожної літери вхідного тексту на літеру, яка знаходиться на відстані k від неї в алфавіті. Якщо, наприклад, відстань k = 3, то літера "А" буде замінена на літеру "Д", "Б" на "Е" і так далі.

Однією з особливостей алгоритму Цезаря є те, що він є дуже простим і легко реалізовується на практиці. Іншою важливою особливістю є те, що його можна застосувати до будь-якої мови, оскільки він працює з символами алфавіту, а не з конкретними мовними знаками.

Однак, алгоритм Цезаря має деякі недоліки, які обмежують його застосування в практичних ситуаціях. Перш за все, легкість розшифрування є його слабким місцем. Зловмисники можуть легко зламати зашифроване повідомлення, застосувавши метод статистичного аналізу. Крім того, його можна легко піддасти атакам перебору, коли зловмисники перебирають всі можливі ключі шифрування, доки не знайдуть правильний.

Математичний аналіз алгоритму Цезаря зазвичай включає в себе аналіз його складності та опірності до атак. Складність алгоритму визначається кількістю можливих ключів (тобто кількість позицій, на яку можна зсунути символи в алфавіті), що відповідає розміру алфавіту. Наприклад, якщо ми використовуємо алфавіт з 26 символів, то кількість ключів дорівнює 26 [1].

Однак, опірність алгоритму Цезаря до атак залежить від того, яким чином здійснюється зміщення символів в алфавіті. Якщо ключ залишається сталим для всіх символів, то атака методом перебору буде ефективною, оскільки можна перебрати всі можливі ключі, щоб знайти правильний. У цьому випадку кількість можливих ключів - це кількість символів в алфавіті. Наприклад, у випадку алфавіту з 26 символів, це буде 26 ключів.

Проте, якщо ключ змінюється для кожного символу окремо, то атака методом перебору не буде ефективною, оскільки кількість можливих ключів у цьому випадку дуже велика. Наприклад, якщо ключі змінюються на випадкові числа, то кількість можливих ключів буде величезною, що робить атаку методом перебору непрактичною [7].

1.9 Опис пристрою шифрування на базі алгоритму Цезаря з ключовим словом

Пристрій шифрування на базі алгоритму Цезаря з ключовим словом - це пристрій, який використовується для захисту інформації за допомогою алгоритму Цезаря. Його особливість полягає у використанні ключового слова, яке дозволяє збільшити складність розшифрування повідомлення.

Опис пристрою може бути розділений на кілька складових частин. Першою складовою є вхідний блок, в який вводиться повідомлення, яке потрібно зашифрувати. Далі вхідний блок передає дані в блок ключового слова. В цьому блоку вводиться ключове слово, яке буде використовуватися для шифрування повідомлення.

Далі використовується блок шифрування. В цьому блоку застосовується алгоритм Цезаря, збільшуючи значення кожної літери повідомлення на значення відповідної літери ключового слова. Після цього зашифроване повідомлення передається в вихідний блок.

Остання складова частина - вихідний блок, в який виводиться зашифроване повідомлення. Цей блок може містити також функцію дешифрування, яка застосовується для розшифрування повідомлення за допомогою введеного ключового слова.

Для підвищення безпеки повідомлення може бути зашифровано декілька разів з різними ключовими словами. Такий метод шифрування

називається множинним шифруванням і дозволяє підвищити складність розшифрування повідомлення.

Таким чином, пристрій шифрування на базі алгоритму Цезаря з ключовим словом може бути ефективним інструментом для захисту важливої інформації. Використання ключового слова дозволяє збільшити складність аналізу шифротексту та зменшити ймовірність успішного злому шифру.

Пристрій складається з компонентів, таких як клавіатура, екран, процесор, пам'ять та інтерфейс зв'язку з користувачем. Користувач вводить повідомлення на клавіатурі, яке потім оброблюється процесором. Алгоритм Цезаря з ключовим словом застосовується до повідомлення, і шифрований текст зберігається в пам'яті пристрою. Зашифроване повідомлення можна переслати за допомогою інтерфейсу зв'язку або вивести на екран.

1.10 Опис методів криптоаналізу шифрування на основі алгоритму Цезаря з ключовим словом

Один з основних методів криптоаналізу Цезаря з ключовим словом - це метод перебору. Цей метод полягає в тому, що атакуючий спробує всі можливі комбінації ключа або ключового слова, поки не знайде правильну комбінацію, яка розкриє зашифровану інформацію. Звичайно, чим більша довжина ключового слова, тим більше можливих комбінацій, тому цей метод може бути дуже часо- та ресурсоємним.

Інший метод криптоаналізу Цезаря з ключовим словом - це метод аналізу частоти. Цей метод ґрунтується на тому, що деякі символи в мові використовуються частіше, ніж інші. Наприклад, українською мовою найбільш часто вживається буква "о". Тому, якщо атакуючий знає, що текст, що був зашифрований за допомогою алгоритму Цезаря з ключовим словом, був написаний українською мовою, він може спробувати розшифрувати текст, аналізуючи частоту використання символів та порівнюючи їх з частотою використання символів української мови. Цей метод може бути особливо ефективним, якщо текст достатньо довгий.

Існує також метод криптоаналізу Цезаря з ключовим словом, який базується на аналізі контексту. Цей метод полягає у використанні статистичних методів для аналізу зшифрованого тексту з метою визначення ключа. Зазвичай для цього використовуються методи частотного аналізу, коли зібрані статистичні дані про частоту вживання символів в зшифрованому тексті порівнюють з даними про частоту вживання символів у мові, на якій написаний вихідний текст.

1.11 Оцінка безпеки пристрою шифрування

Щоб оцінити безпеку пристрою шифрування на базі алгоритму Цезаря з ключовим словом, можна використовувати різні методи аналізу. Один з таких методів - це аналіз ймовірності. Цей метод полягає в тому, щоб визначити, які символи у відкритому тексті з'являються частіше, і відповідно, які символи найбільш ймовірно будуть відповідати певним символам у зашифрованому тексті. З цими даними можна складати таблицю, що вказує

ймовірність, з якою кожен символ у відкритому тексті буде зашифровано певним символом у зашифрованому тексті. Чим менша ймовірність, тим більш стійкий є пристрій шифрування.

Інший метод аналізу полягає у визначенні частотного спектра зашифрованого тексту. Частотний спектр - це графічне представлення частоти використання кожного символу у зашифрованому тексті. Цей метод дозволяє виявити будь-які неспівпадіння у розподілі частот між відкритим і зашифрованим текстами, що може свідчити про наявність певних закономірностей у зашифрованому тексті, які можна використовувати для розшифрування.

Крім того, існують інші методи криптоаналізу, які можуть використовуватися для розшифрування тексту, такі як метод "грубої сили". Цей метод полягає в тестуванні всіх можливих ключів, поки не буде знайдено правильний ключ, що може зайняти дуже багато часу, але він гарантує розшифрування зашифрованого тексту.

Отже, оцінка безпеки пристрою шифрування на базі алгоритму Цезаря з ключовим словом залежить від багатьох факторів, таких як довжина ключа, складність ключового слова, складність самого алгоритму та можливості зловмисників. Якщо дотримуватися високих стандартів безпеки та правильно використовувати алгоритм, то його можна вважати достатньо надійним для захисту важливої інформації. Однак, в сучасному електронному світі, де існує багато потенційних загроз для безпеки даних, можуть бути більш сучасні та складні методи шифрування, які забезпечують вищий рівень безпеки.

1.12 Постановка завдання

Метою роботи є розробка пристрою шифрування інформації на базі алгоритму Цезаря з ключовим словом.

Для досягнення цієї мети необхідно виконати наступне:

1. Визначити основні функції та завдання, які повинен виконувати пристрій шифрування інформації.

2. Розробити алгоритм функціонування пристрою.

3. Розробити схему електричну структурну пристрою шифрування.

4. Розробити схему електричну принципову пристрою шифрування інформації на базі алгоритму Цезаря з ключовим словом.

2 Проектування пристрою

2.1 Розробка алгоритму роботи пристрою

1 блок: Вводимо повідомлення яке потрібно зашифрувати

2 блок: Перевіряємо повідомлення з можливістю повернутися на редагування

3 блок: Визначаємо алфавіт за яким буде проводитися шифрування

4 блок: Вибір українського алфавіту для шифрування

5 блок: Вибір англійського алфавіту для шифрування

6 блок: Вибір алфавіту якого немає в списку

7 блок: Вводимо ключ – К. Це число визначає, на скільки позицій вправо будуть зсуватися символи алфавіту при шифруванні повідомлення (Число має мати межі від 0 до до 33 якщо ми беремо український алфавіт)

8 блок: Зсув ключового слова на К символів. Змінює позицію кожного символу алфавіту для створення зашифрованого повідомлення (Наприклад 3 – ключове слово буде починатися з В)

9 блок: Введення ключового слова яке придумав користувач залежно від алфавіту який він обрав. Ключове слово перетворюється на числовий ключ шифрування, де кожна літера ключового слова представляється числом від 0 до 25 (наприклад, А=0, Б=1, ..., Я=33). Це числове значення використовується для визначення зсуву символів алфавіту при шифруванні або розшифруванні повідомлення.

10 блок: Запис ключового слова яке будет починатися з місця 8 блоку. Наприклад, якщо ключове слово - "ДІМ", то кожна літера перетворюється на числове значення, наприклад, Д=5, І=11, М=16. Ці числа використовуються для обчислення зсуву символів алфавіту при шифруванні або розшифруванні повідомлення.

11 блок: Формування алфавіту залежно від обраної мови

12 блок: Формування таблиці Цезаря для візуалізації

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я

Рисунок 2.1- Візуалізація українського алфавіту в таблиці Цезаря

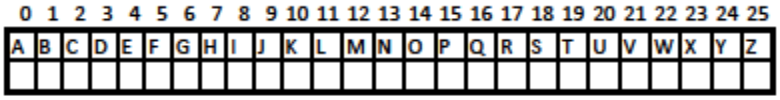

Рисунок 2.2-Візуалізація англійського алфавіту в таблиці Цезаря

13 блок: Вводимо повідомлення яке буде шифруватися згідно з вибраної мови алфавіту

14 блок: Заміна символів повідомлення яке ми шифруємо на все зашифроване повідомлення. Для кожного символу повідомлення виконується зсув. Зсув визначається шляхом додавання числового значення символу повідомлення до відповідного числового значення символу ключового слова. Зсунуті символи перетворюються назад на літери алфавіту, утворюючи зашифроване повідомлення

Символ шифрується за допомогою формули:

$c = (p + k) \bmod n$

де c - символ шифротексту, p - символ відкритого тексту, k - число, що відповідає символу ключового слова, а n - кількість символів в алфавіті.

15 блок: Запис шифрограми

16 блок: Передача шифрограми користувачу для обробки

17 блок: Можливість повернутися до початку шифрування задля повторного шифрування повідомлення

Блок схема

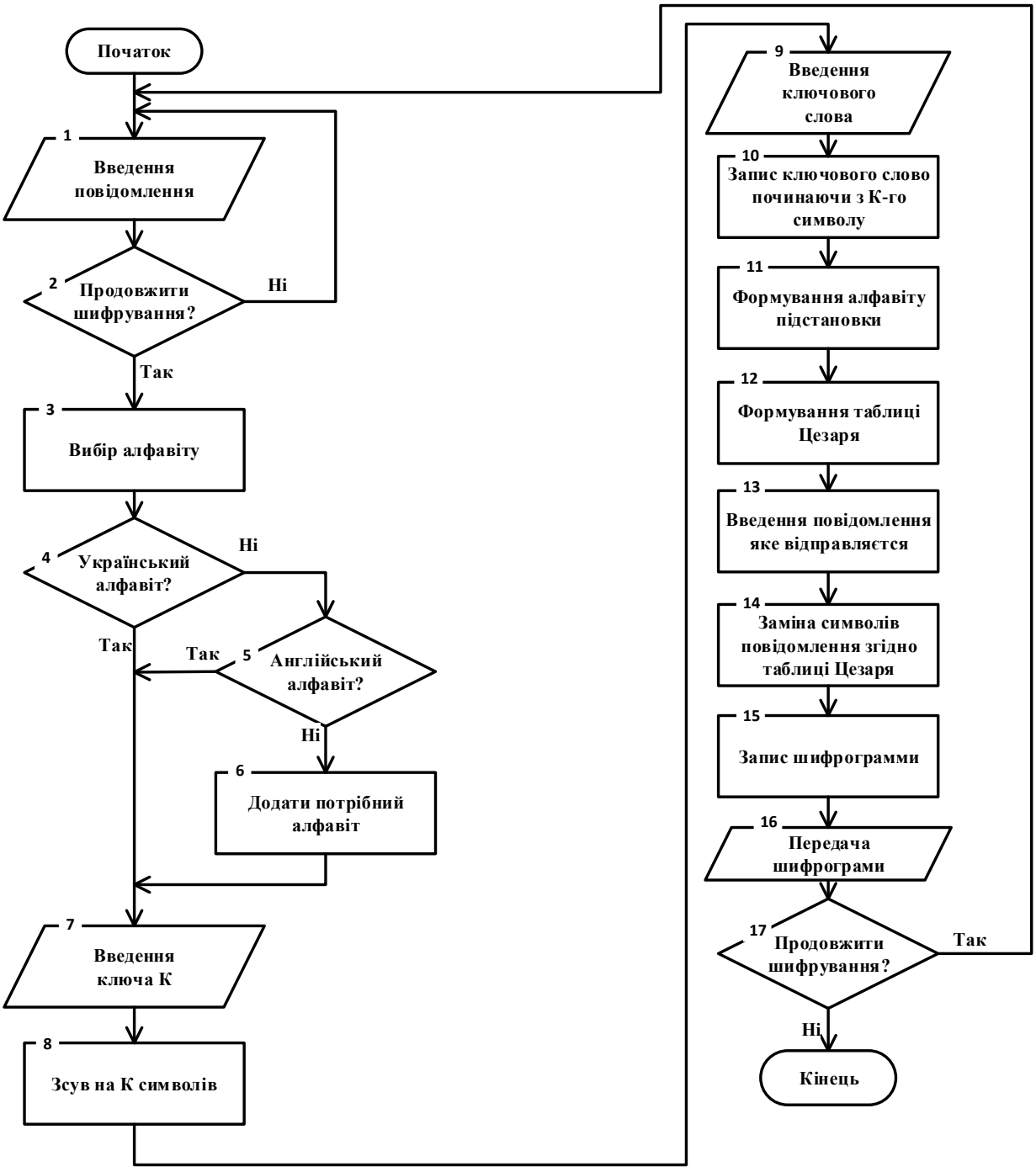

Рисунок 2.1 – Схема алгоритму роботи

Розроблення структурної схеми пристрою захисту конфіденційної інформації

Блоки в структурній схемі виконують певні функції:

Блок введеня повідомлення – блок в якому вводиться повідомлення яке ми хочемо зашифрувати.

Блок визначення алфавіту – блок призначений для вибору мови з якою ми будемо працювати.

Сховище алфавітів – блок в якому можна вибрати алфавіт який вам потрібно.

Формувач первинного алфавіту – це блок в якому формується алфавіт залежно від вибраної мови

Блок введення ключа К - цей блок призначений для введення ключа (К) за допомогою якого буде відбуватися зміщення символів. 1<К<Р (Р-максимальна кількість букв в алфавіті)

Регістр зсуву на К символів – блок призначений для зсуву на К символів.

Блок введення ключового слова - даний блок призначений для вводу слова за яким в свою чергу буде проводитись шифрувальний зсув букв в таблиці.

Блок запису ключового слова – блок призначений для запису ключового слова в пам'ять

Формувач алфавіту підстановки – блок який призначений для формування алфавіту підстановки.

Блок формування таблиці Цезаря – даний блок формує таблицю Цезаря. Формується алфавітний рядок, рядок з ключовим словом який був зміщений за допомогою ключа К.

Блок по символьного введення повідомлення – блок в якому вводиться по символьно повідомлення.

Блок заміни символів повідомлення згідно таблиці Цезаря – призначений для заміни символів повідомлення на зашифрований символ.

Блок запису шифрограми – блок в який записується шифрограма.

Блок передачі шифрограми – блок який передає шифрограму.

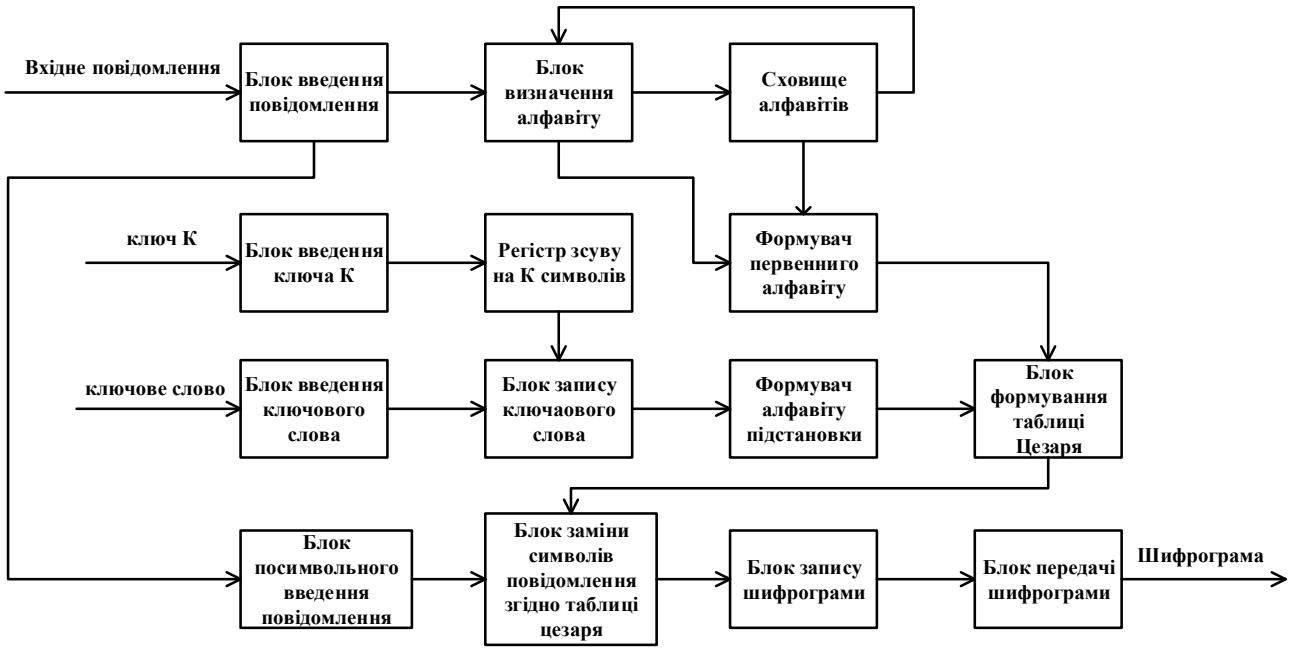

Рисунок 2.3 – Структурна схема

3. Розроблення принципової електричної схеми пристрою

3.1 Вибір елементної бази

Для побудови пристрою шифрування необхідно вибрати мікросхему, яка дозволятиме реалізувати всі блоки пристрою.

Хорошим вибором буде мікроконтролер ATMEGA8535, переваги цього мікроконтролера:

-має доступну ціну в порівнянні з іншими мікроконтролерами з подібними можливостями і функціональністю.

-висока продуктивність, він працює на тактовій частоті до 16 МГц.

-низька споживана потужність мікроконтролера. Має різні режими енергозбереження, що дозволяє знизити споживання енергії.

-легка програмованість. Підтримує мову програмування С і має широкий набір периферійних бібліотек, що спрощує розробку програмного забезпечення

3.2 Мікропроцесорний блок

Центральний модуль є основним блоком контролера, що забезпечує управління та синхронізацію роботи пристрою, забезпечує видачу інформації, зберігання даних та обробку даних

Мікроконтролер ATMEGA8535 має 40 виводів, які зображені на рисунку 3.1

VCC - джерело напруги.

GND- заземлення

Port A - служить 8-бітним двонаправленим портом вводу-виводу, якщо аналого-цифровий перетворювач не використовується. Виводи порту можуть забезпечувати внутрішні підтягуючі резистори

Port B - це 8-розрядний двонаправлений порт вводу/виводу з внутрішніми підтягуючими резисторами

Port C - це 8-розрядний двонаправлений порт вводу/виводу з внутрішніми підтягуючими резисторами

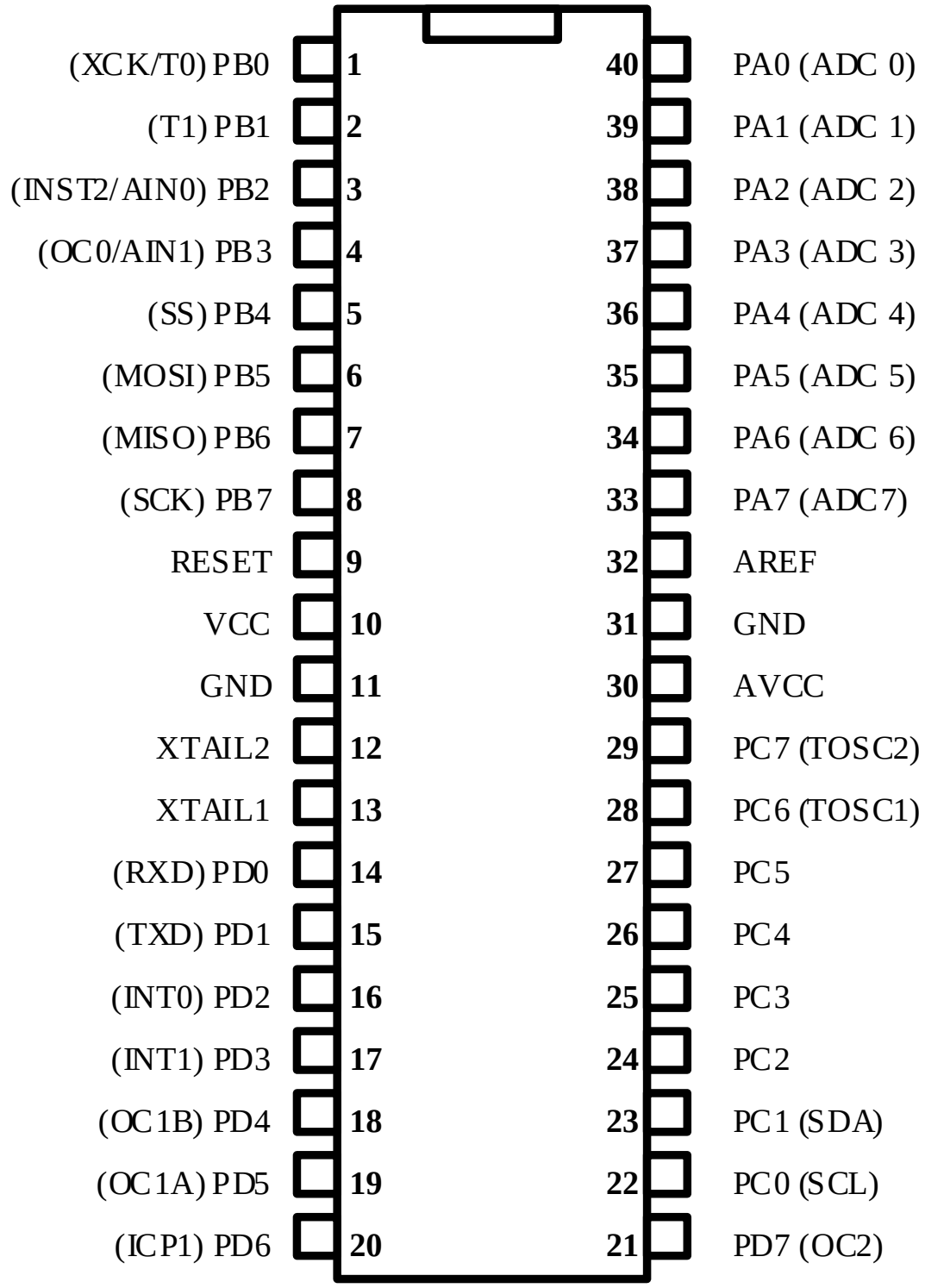

Рисунок 3.1 – Призначення виводів мікроконтролера ATMEGA8535

TQFP/MLF

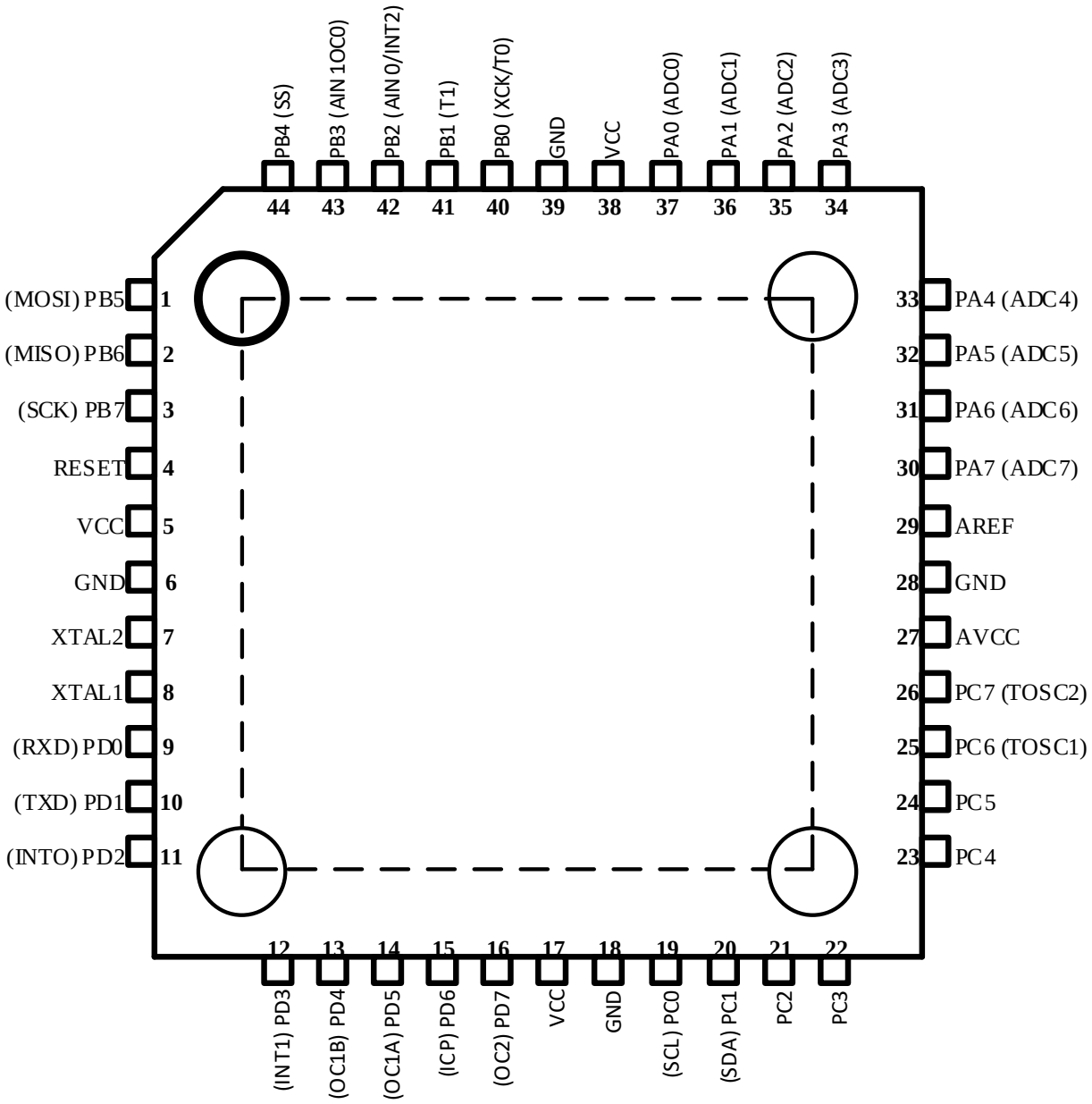

Рисунок 3.2 – Призначення виводів мікроконтролера ATMEGA8535 в корпусі TQFP

Port D - це 8-розрядний двонаправлений порт вводу/виводу з внутрішніми підтягуючими резисторами

RESET - Вхід для скидання.

XTAL1- Вхід до підсилювача інвертувального генератора та вхід до робочої схеми внутрішнього годинника.

XTAL2 - Вихід з інвертувального підсилювача генератора.

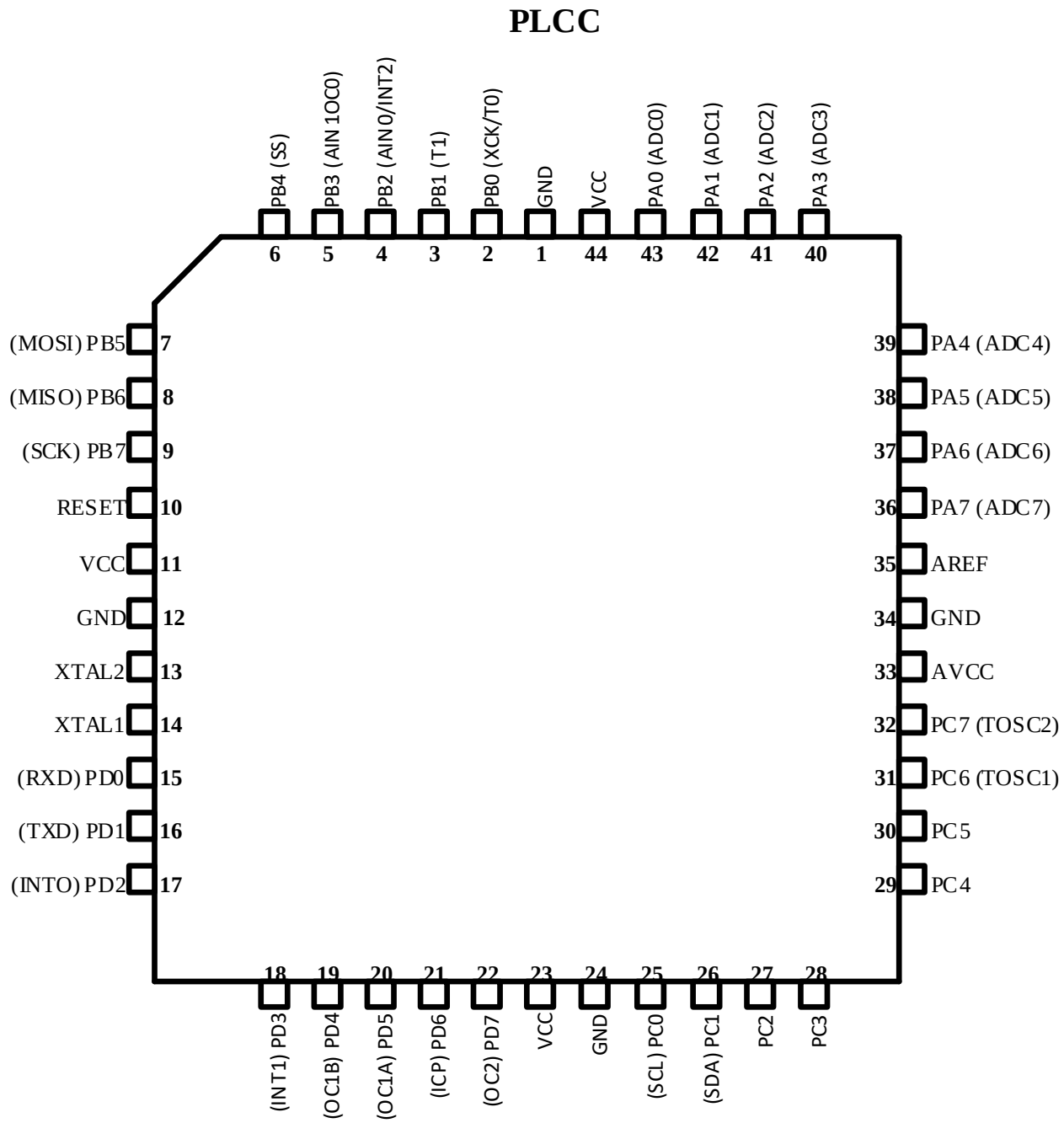

Рисунок 3.3 – Призначення виводів мікроконтролера ATMEGA8535 в корпусі PLCC

AVCC - це контакт напруги живлення для порту A та аналого-цифрового перетворювача.

AREF - аналоговий еталонний контакт для аналого-цифрового перетворювача [7].

Мікросхема 74HKT573 має 20 виводів, які зображені на рисунку 3.4

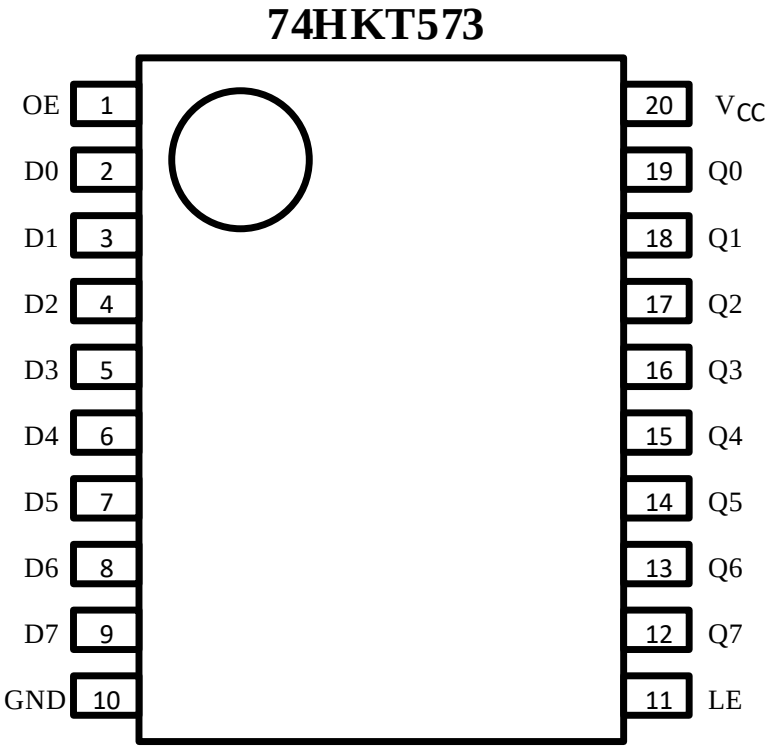

Рисунок 3.4 – Блок 74HKT573

OE - 3-становий вхід дозволу виходу (активний низький рівень)

D[0:7] - введення даних

GND – земля

LE - вхід дозволу фіксації

Q[0:7] - 3-становий вихід із засувкою

VCC - напруга живлення [5].

Мікросхема K6T4008C1B-GB 55 має 32 виводів, які зображені на рисунку 3.5

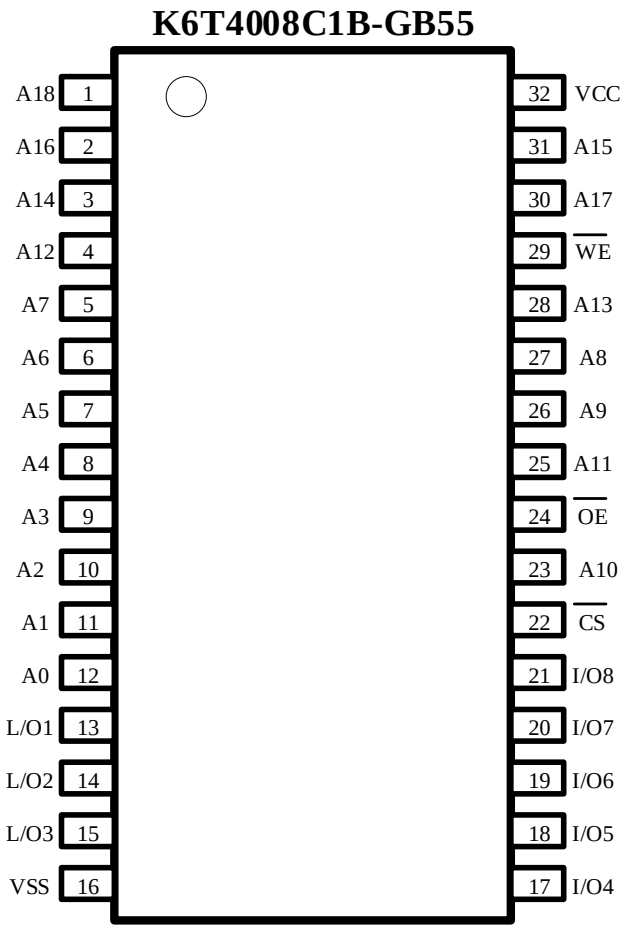

Рисунок 3.5 - Блок K6T4008C1B-GB55

WE – Вхід запису

CS – Вхід вибору мікросхеми

OE – вихід дозволити вхід

A – введення адреси

I/O – введення/виведення даних

VCC – Джерело напруги

VSS - заземлення [6].

Мікросхема MAX232E має 16 виводів, які зображені на рисунку 3.4

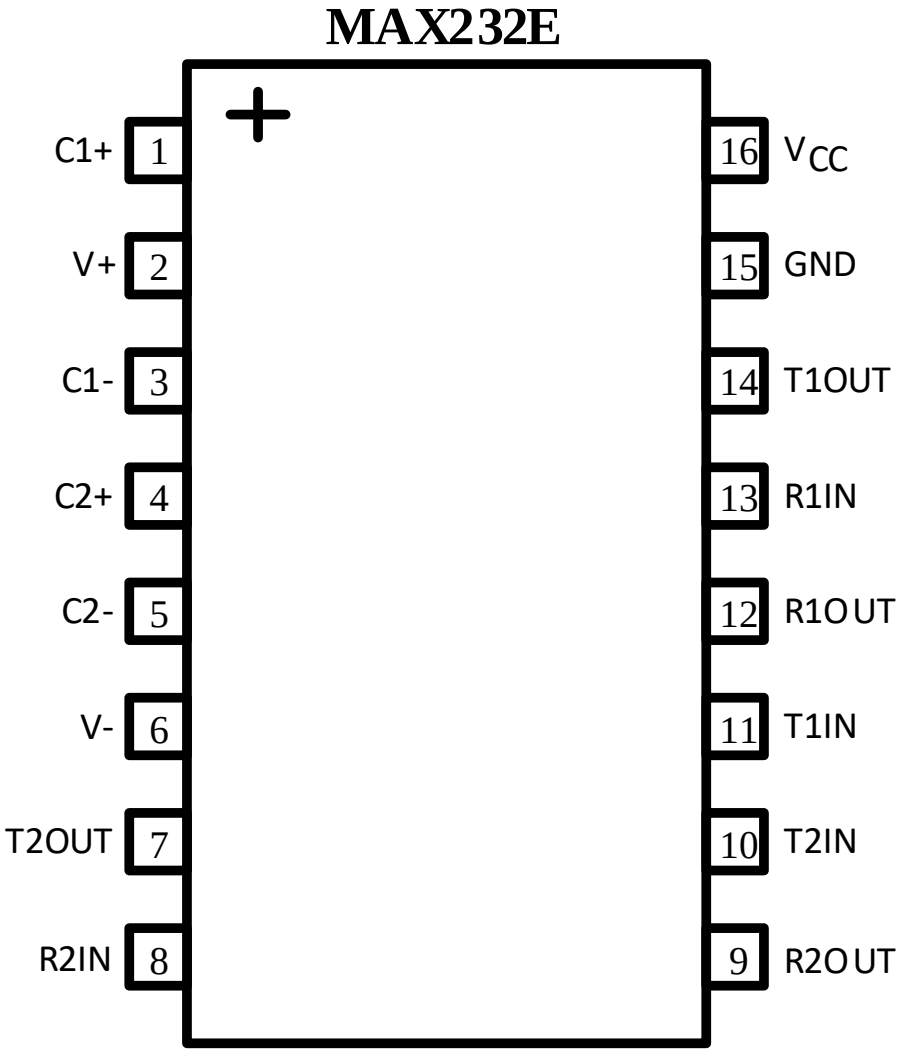

Рисунок 3.6 – блок MAX232E

C1+, C1- - Виводи для конденсатора накачування позитивного заряду.

V+ - Напруга $+2V_{CC}$, створена насосом заряду.

C2+, C2- - Виводи для конденсатора накачки негативного заряду.

V - $-2V_{CC}$ Напруга, що генерується зарядним насосом.

T_OUT - Виходи драйвера RS-232

R_IN - Входи приймача RS-232

R_OUT - Виходи приймача RS-232.

T_IN - Входи драйвера RS-232.

GND – Заземлення.

V_{CC} - Вхідна напруга живлення від +4,5 В до +5,5 В [12].

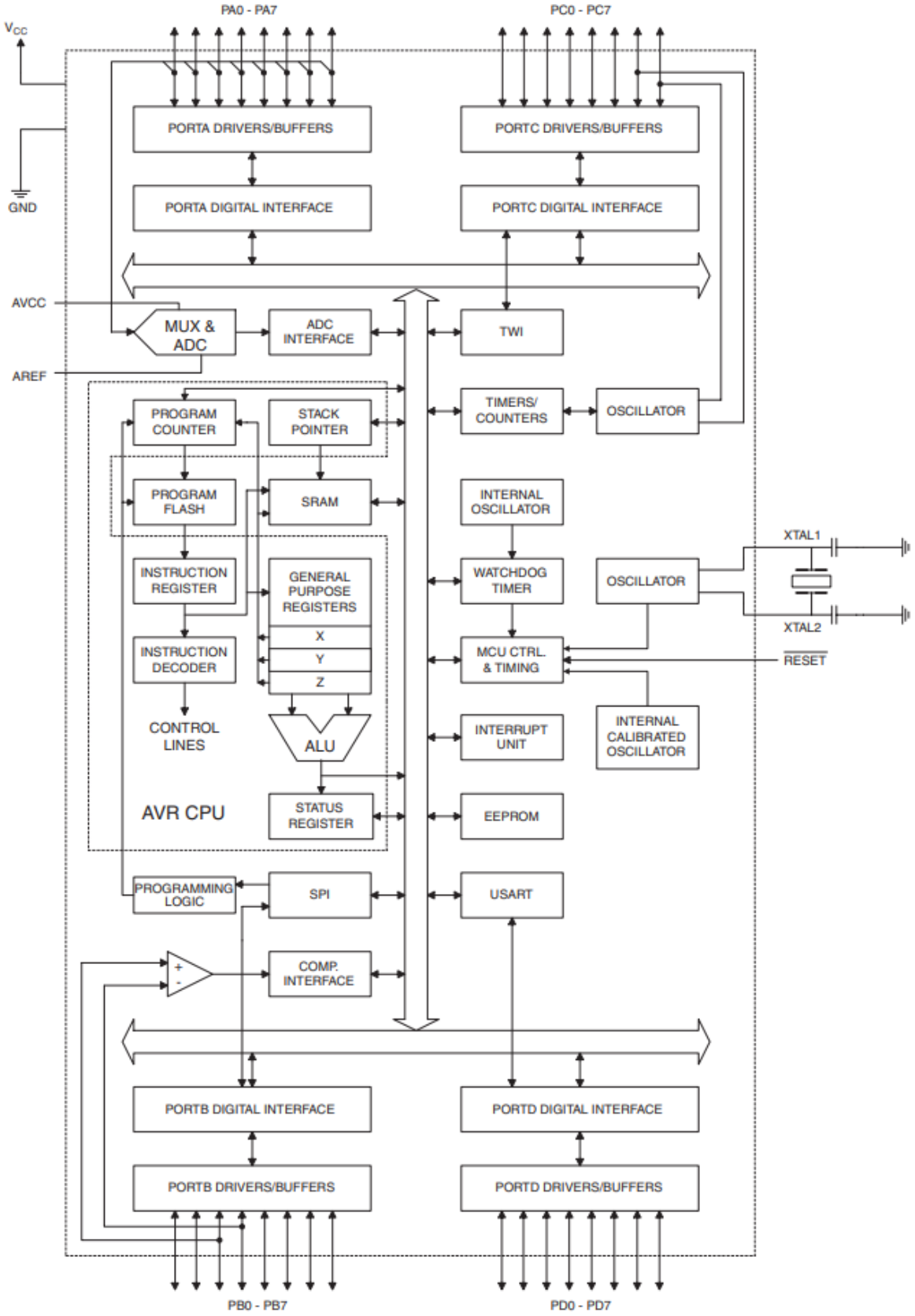

Рисунок 4.5 - Функціональна схема мікроконтролера ATMEGA8535

4 Розробка програмного забезпечення пристрою

Нижче приведена програма для шифрування
AVR GCC –компілятор мов С и С++ для AVR;
avr-libc–стандартна С бібліотека для використання з GCC;
avr-as - ассемблер для мікроконтролерів AVR

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

#define MAX_LENGTH 1000

void encryptMessage(char *message, int shift, char *keyword) {
    int messageLength = strlen(message);
    int keywordLength = strlen(keyword);
    int i, j;

    for (i = 0, j = 0; i < messageLength; i++) {
        char currentChar = message[i];

        int charShift = shift;

        if (j < keywordLength) {
            charShift += keyword[j];
            j++;
        }

        if (currentChar >= 'a' && currentChar <= 'z') {
            currentChar = 'a' + (currentChar - 'a' + charShift) % 26;
        } else if (currentChar >= 'A' && currentChar <= 'Z') {
            currentChar = 'A' + (currentChar - 'A' + charShift) % 26;
        }

        message[i] = currentChar;
    }
}
```

```
int main() {
    char message[MAX_LENGTH];
    int shift;
    char keyword[MAX_LENGTH];
    char confirm;

    printf("Введіть текст для шифрування: ");
    fgets(message, sizeof(message), stdin);
    message[strcspn(message, "\n")] = '\0';

    printf("Підтвердження для продовження (Y/N): ");
    scanf(" %c", &confirm);

    if (confirm != 'Y' && confirm != 'y') {
        printf("Програма завершила роботу.\n");
        return 0;
    }

    printf("Виберіть мову (1 - українська, 2 - англійська): ");
    int language;
    scanf("%d", &language);

    printf("Введіть ключ K: ");
    scanf("%d", &shift);

    printf("Введіть ключове слово: ");
    scanf("%s", keyword);

    encryptMessage(message, shift, keyword);

    printf("Зашифроване повідомлення: %s\n", message);

    return 0;
}
```

Висновки

У даному проекті було розроблено пристрій шифрування інформації за методом Цезаря з ключовим словом. Сьогодні захист конфеденційної інформації є актуальним і вимагає надійних методів захисту.

Було розроблено алгоритм функціонування пристрою.

На основі функціонального алгоритму розроблено структурну схему пристрою. Це набір блоків, що показує відповідні зв’язки між ними.

Було створено принципову схему пристрою .

Література

1. https://studfile.net/preview/3270386/page:3/

2. Тарнавський Ю.А., Технології захисту інформації - КПІ ім. Ігоря Сікорського, 2018р.

3. Журнал «Захист інформації». Том 21, №1 (2019)

4. Кобозева А. А., Мачалін І. О., Хорошко В. О. Аналіз захищеності інформаційних систем. К., 2010.

5. https://datasheetspdf.com/pdf-file/1392454/nexperia/74HCT573/1

6. https://octopart.com/datasheet/k6t4008c1b-gb55-samsung-2270581

7. https://pdf1.alldatasheet.com/datasheet-pdf/view/164169/ATMEL/ATMEGA8535.html

8. Усатенко, Т.М. Криптологія: навч. посіб. / Т.М. Усатенко. - Суми : СумДУ, 2008. - 164 с.

8. Stallings W. Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley, 2019. 800 p.

9. Sagare A.A., Khondoker R. Security Analysis of SDN Routing Applications. In: Khondoker, R. (eds) SDN and NFV Security. Lecture Notes in Networks and Systems, vol. 30. Cham: Springer, 2018. pp. 1-17

10. Нільс Фергюсон, Брюс Шнайер. Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. — М. : 2004. — 432 с.

11. Гребенніков В.В. Історія криптології & секретного зв'язку. Ужгород. – 803 с

12. https://eu.mouser.com/datasheet/2/609/MAX202E_MAX241E-3112135.pdf

13. Юрченко В.І., Бортова система вагового контролю автомобіля / Бережна О.В., Горячев О.Є., Юрченко В.І., Мельник Р.В., Мороз М.В. // Фізика, електроніка, електротехніка (ФЕЕ-2023). Матеріали та програма науково-технічної конференції. – Суми: СумДу, 2023. – С.72.

Бортова система вагового контролю автомобіля

Бережна О.В., *доцент*; Горячев О.Є., *ст. викладач*;
Юрченко В.І., *студент гр. ЕС.м-21*;
Мельник Р.В., *студент гр. ЕС-91*; Мороз М.В., *студент гр. ЕС.м-21*
Сумський державний університет, м. Суми, Україна

Для підвищення ефективності здійснення вантажоперевезень, для підвищення рівня безпеки на дорогах та для мінімізації надмірного зносу дорожнього полотна під впливом вантажівок, що порушують встановлені для них вагогабаритні норми, необхідно впровадження пристроїв та систем контролю навантаження на вісь автомобілів та оцінки ваги вантажу, що перевозиться.

Серед сучасних систем вагового контролю автомобілів виділяється три типи бортових систем зважування, таких як гідравлічна, пневматична та механічна. Системи, які базуються на вимірюванні тиску мастила в гідравлічній системі або повітря в пневматичній, мають загальні недоліки – складність налаштування системи та низька ремонтопридатність. Перспективним для створення бортових систем зважування бачиться універсальне рішення для багатьох типів автомобілів з використання тензодатчиків та їх встановлення на кожну вісь вантажівки.

Аналіз показав, що таке рішення забезпечує незалежність від типу підвіски автомобіля, високу надійність, великий період експлуатації, високу точність, відсутність похибки від зовнішніх умов та стану підвіски. Для зменшення вартості такого рішення пропонується використовувати оптимальну кількість тензодатчиків, одного мікроконтролеру з необхідним програмним забезпеченням замість блоку аналізу і розподільної коробки та під'єднання тензодатчиків до мікроконтролеру за допомогою модуля підсилення сигналу, що спрощує експлуатацію, збільшує модифікаційні можливості системи та полегшує ремонт.

Системи вагового контролю, що базуються на тензодатчиках, можуть здійснювати контроль навантаження, що припадає на кожну з осей автомобіля, визначати вагу вантажу, що перевозиться автомобілем, сигналізувати про перевищення осьового навантаження. Параметри, що визначаються, можна відображати на дисплеї водія і передавати до відповідних систем контролю та моніторингу.