Міністерство освіти і науки України
Вінницький національний технічний університет

Методичні вказівки
до виконання курсового проекту

з дисципліни
"ПРИКЛАДНА КРИПТОЛОГІЯ"

Для студентів денної та заочної форм навчання
напряму підготовки 6.170101 – Безпека інформаційних та комунікаційних систем
та спеціальності125 – Кібербезпека

Вінниця 2018

Методичною радою Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 8 від 19.04.2018 р.) надано гриф "Електронні методичні вказівки" та рекомендовано до використання в навчальному процесі.

Укладачі:
Володимир Андрійович Лужецький
Юрій Володимирович Баришев
Аліна Василівна Остапенко-Боженова

Рецензенти:
к. т. н., доцент Л. В. Крупельницький
к. т. н., доцент Ю. В. Булига

Методичні вказівки до виконання курсового проекту з дисципліни "Прикладна криптологія" / Укладачі: В. А. Лужецький, Ю. В. Баришев, А. В. Остапенко-Боженова. - Вінниця: ВНТУ, 2018. – 40 с.

Містять рекомендації та стислі теоретичні відомості щодо тематики та етапів виконання курсового проекту з дисципліни "Прикладна криптологія" для студентів денної та заочної форм навчання напряму підготовки 6.170101 – Безпека інформаційних та комунікаційних систем та спеціальності 125 – Кібербезпека. Запропонована структура курсового проекту, визначено основні напрями та зміст курсового проектування. Наведено графік виконання курсового проекту відповідно до етапів. Наведено правила оформлення пояснювальної записки та графічної частини курсового проекту.

Навчальне самостійне електронне мережне видання

Методичні вказівки до виконання курсового проекту
з дисципліни "ПРИКЛАДНА КРИПТОЛОГІЯ"

Укладачі:
Лужецький Володимир Андрійович
Баришев Юрій Володимирович
Остапенко-Боженова Аліна Василівна

Електронний ресурс PDF.
Підписано до видання 25.07.2018 р. Зам. № Р2018-010
Видавець та виготовлювач - Вінницький національний технічний університет,
Інформаційний редакційно-видавничий центр.
ВНТУ, ГНК, к.114, Хмельницьке шосе, 95, м. Вінниця, 21021,
тел. (0432) 65-18-06.
press.vntu.edu.ua;
Email: irvc.vntu@gmail.com.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.

ЗМІСТ

1 ОСНОВНІ ВИМОГИ ДО КУРСОВОГО ПРОЕКТУ

1.1 Мета та задачі курсового проектування

Курсовий проект – навчальний проект з дисципліни, який містить елементи ескізного і технічного проектів та робочої документації.

Внаслідок виконання курсового проекту з дисципліни "Прикладна криптологія" студент повинен закріпити знання структури криптографічних засобів захисту та основних підходів до їх проектування, принципів їх функціонування; здобути навички з перевірки коректності виконання криптографічних протоколів, розробки програмних та апаратних засобів для криптографічного захисту інформації, розв’язання задач з галузі кібербезпеки засобами криптографічного захисту інформації.

Під час виконання курсового проекту студенти повинні використати знання, отримані ними під час вивчення дисциплін, "Основи інформаційної безпеки", "Архітектура комп’ютерних систем", "Технології програмування", "Захист операційних систем", "Засоби програмування", "Інформаційно-комунікаційні системи", "Теорія інформації та кодування", "Теорія ймовірностей та математична статистика".

Під час виконання курсового проекту студенти повинні вміти:

- правильно обґрунтовувати вибір способу розв’язання поставленого завдання;
- аналізувати методи криптографічного захисту інформації та робити їх декомпозицію на структурні складові;
- аналізувати коректність виконання криптографічних протоколів;
- розробляти алгоритми реалізації криптографічних протоколів;
- програмувати алгоритми для їх реалізації у вигляді програмних засобів;
- розробляти структуру спеціалізованих апаратних засобів для криптографічного захисту інформації;
- визначати основні технічні характеристики спеціалізованих апаратних

засобів для криптографічного захисту інформації.

1.2 Тематика курсового проектування

Зміст курсового проекту повинен відповідати навчальній програмі та робочому плану дисципліни "Прикладна криптології" і повинен відображати суть обраної студентом теми. Зміст курсового проекту визначається завданням, яке видається на першому тижні семестру викладачем кожному студенту.

Тематика курсового проекту стосується розв’язання за допомогою криптографічних методів та засобів задач у галузі кібербезпеки:

- автентифікації користувачів;
- автентифікації даних;
- автентифікованого розподілу ключової інформації;
- захисту даних, що зберігаються на електронних носіях інформації;
- захисту даних, що передаються каналами зв’язку;

Автентифікація користувачів передбачає реалізацію одного з криптографічних протоколів одно- або багатосторонньої автентифікації. Завдання цього класу потребують аналізу низки протоколів автентифікації, визначення переваг і недоліків заданого протоколу порівняно з відомими аналогами, а також визначення задач, в яких доцільно використовувати засіб, що розробляється. Основна увага в курсових проектах такого типу приділяється реалізації криптографічного протоколу та організації віддаленого обміну даних між користувачами відповідно до цього криптографічного протоколу.

Автентифікація даних передбачає реалізацію криптографічних методів перевірки цілісності та автентичності даних, які базуються на методах формування електронних цифрових підписів та гешування даних. Завдання такого типу потребують аналізу студентом відомих методів формування електронних цифрових підписів або методів гешування, визначення переваг і недоліків цих методів порівняно з відомими аналогами, а також визначення задач, в яких доцільно використовувати пристрій, що розробляється. При цьому основна увага має приділятися генеруванню відкритого та закритого ключів для

електронних цифрових підписів, реалізації алгоритмів формування цифрових підписів або геш-значень даних, організації віддаленого обміну даними між користувачами відповідно до цього криптографічного протоколу.

Автентифікований розподіл ключової інформації передбачає реалізацію криптографічних протоколів, що поєднують автентифікацію користувачів з протоколом генерації і розподілу ключів по каналу зв'язку. Завдання такого типу потребують аналізу відомих протоколів розподілу ключової інформації, визначення переваг і недоліків заданого протоколу порівняно з відомими аналогами, а також визначення задач, в яких доцільно використовувати засіб, що розробляється. Основна увага в таких курсових проектах приділяється реалізації трьох основних етапів протоколів даного типу: генерації, реєстрації та комунікації. На етапі комунікації реалізується власне протокол автентифікованого ключового обміну, який завершується формуванням спільного секретного ключа відповідно до цього криптографічного протоколу.

Захист даних, що зберігаються на електронних носіях інформації передбачає реалізацію одного з методів блокового шифрування. Даний клас завдань потребує аналізу студентом низки методів блокового шифрування, визначення переваг і недоліків заданого методу шифрування порівняно з відомими аналогами, а також визначення задач, в яких доцільно використовувати засіб, що розробляється. Основна увага в таких курсових проектах приділяється реалізації процедури розгортання ключів, раундового криптоперетворення та організації обміну даними між засобом, що розробляється, та пристроєм, що зберігає інформацію.

Захист даних, що передаються каналами зв'язку передбачає реалізацію одного з методів потокового шифрування даних, що передаються в цифровому або аналоговому вигляді відповідно. Також курсові проекти цього напряму можуть передбачати захист цілісності даних за допомогою використання кодів, які забезпечують самосинхронізацію обміну, виявлення та виправлення помилок, ущільнення тощо. Для розв'язання завдань цієї тематики студенту необхідно проаналізувати основні характеристики та протоколи обміну даними

в заданих каналах зв’язку, проаналізувати методи захисту каналів зв’язку та обґрунтувати вибір методу, який буде реалізовуватись в ході курсового проектування. Основна увага курсового проекту даної тематики повинна приділятися розробці засобів, що реалізують методи криптографічного захисту інформації.

Індивідуальне завдання для курсових проектів визначається викладачем із загального переліку завдань на курсовий проект. Типові завдання наведені у додатку А даних методичних вказівок. Пропозиції студентів щодо вибору теми курсового проекту поза межами запропонованого переліку заохочуються і враховуються при оцінюванні результатів курсового проектування. Однак такі теми потребують обов’язкового попереднього узгодження з викладачем та присвоєння темі унікального номера варіанта завдання, який в подальшому буде використовуватись студентом при оформленні графічної частини та пояснювальної записки до курсового проекту.

1.3 Етапи курсового проектування

Процес проектування апаратного та програмного засобу криптографічного захисту інформації розбивається на такі етапи:

а) аналіз відомих розв’язків задачі;

б) аналіз та обґрунтування вибору методів, які будуть використовуватись для досягнення мети проектування;

в) аналіз коректності криптографічних протоколів;

г) розробка структури апаратного засобу;

д) визначення технічних характеристик апаратних засобів для криптографічного захисту інформації;

е) розробка алгоритму роботи програмного засобу;

ж) розробка програмного забезпечення, що реалізує криптографічні протоколи.

Аналіз відомих розв’язків задачі. На даному етапі розглядаються відомі криптографічні засоби (з посиланням на джерела та наведенням їх технічних

характеристик) для розв’язання задачі. Так для засобів, що реалізовуватимуть криптографічні протоколи, мають розглядатися особливості протоколу, який реалізовуватиметься. Завершити аналіз бажано порівнянням характеристик рішень та навести огляд криптографічних засобів, що ці рішення реалізують.

Наприклад, при виконанні теми курсового проекту "Спеціалізовані засоби для реалізації протоколу двосторонньої автентифікації з використанням випадкових чисел та ключової геш-функції SHA" на цьому етапі передбачається аналіз протоколів автентифікації користувачів, звертаючи особливу увагу на інші протоколи двосторонньої автентифікації.

Аналіз та обґрунтування вибору методів, які будуть використовуватись для досягнення мети проектування. Даний етап присвячений визначенню конкретних криптографічних методів які обираються для проектування апаратного та програмного засобу криптографічного захисту інформації. Для цього виконується огляд відомих методів та обґрунтовується вибір одного з них. Зокрема, при виконанні курсового проекту "Спеціалізовані засоби для реалізації протоколу двосторонньої автентифікації з використанням випадкових чисел та ключової геш-функції SHA" на цьому етапі доцільно розглянути алгоритм роботи геш-функції SHA та розробити детальний опис алгоритму реалізації криптопротоколу з використанням випадкових чисел для суб’єктів автентифікації.

Аналіз коректності криптографічних протоколів. Під час виконання даного етапу необхідно проаналізувати коректність виконання криптографічного протоколу. Пропонується виконувати цей аналіз на основі логічної моделі Берроуза - Абаді - Нідхема (BAN-логіки) [13], що використовується для аналізу властивостей «знання і довіра» роботи криптопротоколу в цілому або його окремих етапів. Так у курсовому проекті "Спеціалізовані засоби для реалізації протоколу двосторонньої автентифікації з використанням випадкових чисел та ключової геш-функції SHA" розглядається ідеалізована форма криптопротоколу та на основі постулатів BAN-логіки виконується аналіз протоколу. За результатами аналізу можна зробити висновок, що протокол є стійким та дозволяє виявити несанкціоноване

втручання сторонньої особи.

Розробка структури апаратного засобу. Розробляється загальна структура спеціалізованого апаратного засобу, розглядаються зв'язки між структурними компонентами, визначається низка задач, які розв'язуватимуться кожним структурним компонентом. Після розробки загальної схеми, деталізується реалізація кожного структурного компоненту, алгоритму його роботи, задач, які він розв'язуватиме. За результатами даного етапу розробляється схема електрична структурна.

Так для реалізації протоколу двосторонньої автентифікації з використанням випадкових чисел та ключової геш-функції SHA до складу узагальненої структури будуть входити:

- блок пам'яті, для запису необхідних для обчислення констант ;

- блок геш-функції, який забезпечує реалізацію специфічних для протоколу обчислень;

- блок керування, що забезпечує подання вхідних даних на блок геш-функції;

- блок генерування випадкових чисел для сторони А та В;

- блок порівняння відповідей на стороні А та В.

Визначення технічних характеристик апаратних засобів для криптографічного захисту інформації. Для розробленого спеціалізованого апаратного засобу визначаються такі технічні характеристики:час реалізації криптопротоколу; складність апаратури для обчислень. Час реалізації криптопротоколу визначається в умовних одиницях як сума часу необхідних для виконання всіх обчислень.

Так для спеціалізованого апаратного засобу, що реалізує двосторонню автентифікацію з використанням випадкових чисел та ключової геш-функції SHA, час реалізації криптопротоколу будемо визначати в таких умовних одиницях:час додавання за модулем 2^{32}; час зсуву на один двійковий розряд; час виконання однієї логічної операції;час множення за модулем; час піднесення до степеня за модулем; час знаходження оберненого. Час реалізації криптопротоколу (t) – це час, який потрібен для автентифікації: знаходження

хеш-значення, генерація випадкових чисел. Обраховується як сума часових характеристик усіх блоків апаратного засобу. Розрахунок складності апаратури для апаратного засобу потрібно шість 32-розрядних регістри, два 64-розрядних регістри, та два мультиплексора, оперативна пам'ять для зберігання 320 розрядів. Тому складність апаратури $6 \times 32 + 2 \times 64 + 2 = 322$ розрядів регістра.

Розробка алгоритму роботи програмних засобів. На даному етапі розглядаються основні етапи реалізації криптопротоколу які в подальшому деталізуються до рівня виконання операцій в межах структурного блоку. В результаті отримується загальна блок-схема функціонування програмного засобу. На основі даного етапу реалізується програмне забезпечення.

Блок схема загального функціонування програмного засобу для моделювання протоколу двосторонньої автентифікації за допомогою випадкових чисел та хеш-функції SHA складається з таких основних блоків: введення ідентифікаторів сторін A та B; генерування випадкових чисел; обмін геш-значеннями від створених повідомлень між сторонами; порівняння значень геш-функції; вивід повідомлення про проходження або не проходження автентифікації.

Розробка програмного забезпечення, що реалізує криптографічні протоколи. Даний етап передбачає розробку та відлагодження програмних засобів для реалізації криптопротоколів. Також, відбувається обґрунтування вибору мов та середовищ програмування для реалізації програмного засобу. Розроблений програмний засіб підлягає тестуванню.

Зокрема, при виконанні курсового проекту "Спеціалізовані засоби для реалізації протоколу двосторонньої автентифікації з використанням випадкових чисел та ключової геш-функції SHA" на цьому етапі моделюється програмний засіб на мові програмування Delphi та наводиться реалізація основних функцій програми: генератор випадкових чисел для сторін A та B; функція для реалізації алгоритму гешування SHA; процедура отримання геш-значення повідомлення. Також, відбувається розробка рекомендацій по роботі із програмним засобом.

2 ВИМОГИ ДО СТРУКТУРИ ТА ОФОРМЛЕННЯ КУРСОВОГО ПРОЕКТУ

2.1 Загальна структура пояснювальної записки

Кожен етап курсового проектування обов'язково має знайти своє відображення у пояснювальній записці. Пояснювальна записка повинна відповідати індивідуальному завданню, а її оформлення – ГОСТ 2.105-95, які слід враховувати на момент виконання розробки з врахуванням всіх офіційних змін, введених в дію.

Пояснювальна записка до курсового проекту повинна мати таку структуру:

1 ***Інформаційно-змістовна частина,*** яка містить:

- титульний аркуш;
- індивідуальне завдання;
- анотацію;
- зміст.

2 ***Основна частина***, яка складається з:

- вступу;
- аналіз предметної області;
- розробка та аналіз криптопротоколу;
- розробки структури апаратного засобу;
- розробки програмного забезпечення та тестування коректності роботи;
- висновків;
- переліку використаних джерел.

3 ***Додатки***, які складаються з технічного завдання, лістингу програмного забезпечення, а також, за необхідності, рисунків, таблиць, розрахунків, результатів тестування тощо, які з певних причин не увійшли до складу основної частини пояснювальної записки, однак нерозривно з нею пов'язані і дозволяють детальніше висвітлювати певні етапи проектування.

Крім пояснювальної записки курсовий проект включає ***графічну***

частину, яка містить результати курсового проектування, оформлені у вигляді схем. Наприкінці подається відомість курсового проекту, яка описує перелік документів, розроблених під час курсового проектування.

2.2 Інформаційно-змістовна частина пояснювальної записки

Титульний аркуш є першою сторінкою курсового проекту, на якій не проставляється номер. На титульному аркуші позначаються повні назви вищого навчального закладу, факультету, кафедри, назва виду документа, тема, розробник, керівник, члени комісії, рік написання. Крім того титульний аркуш містить рамку спеціального типу.

Приклад оформлення титульного аркушу наводиться у додатку Б.

В ***індивідуальному завданні*** подається конкретний зміст кожного курсового проекту, етапи його виконання, вихідні дані розробки, які визначаються керівником. Воно розглядається і затверджується на засіданні кафедри, про що свідчить відповідний підпис завідувача кафедри. Індивідуальне завдання в перелік змісту не вноситься і має бути другою сторінкою після титульного аркуша.

Приклад індивідуального завдання до курсового проекту наведено в додатку Д.

Керівник проекту пропонує зміст пояснювальної записки, як правило, в розроблених методичних вказівках, або в навчальних цілях зміст може висвітлюватись в індивідуальному завданні.

На підставі індивідуального завдання розробляється технічне завдання, яке подається першим з додатків. Приклад оформлення технічного завдання наведено у додатку Ж.

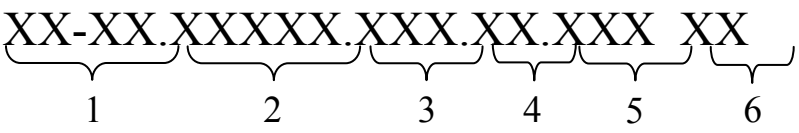
Анотація призначена для ознайомлення з текстовим документом курсового проекту. Вона повинна коротко характеризувати мету проекту, засоби, використані для досягнення поставленої задачі, коротку інформацію про досягнуті результати. Розмір анотації повинен становити приблизно третину сторінки.

Анотацію розміщують безпосередньо за аркушем з індивідуальним завданням, починаючи з нової сторінки (третьої), нумерація якої не позначається. Заголовок (слово АНОТАЦІЯ) розміщується по центру сторінки, після нього пропускається один рядок. Анотація подається двома мовами – українською та однією з міжнародних мов (зазвичай англійською).

Зміст розташовують безпосередньо після анотації, починаючи з нової сторінки. До змісту включають: вступ; послідовно перелічені назви всіх розділів, підрозділів, пунктів і підпунктів (якщо вони мають заголовки) пояснювальної записки; висновки; перелік використаних джерел; назви додатків і номери сторінок, з яких починається викладення відповідного матеріалу. До змісту не вносяться титульний аркуш, індивідуальне завдання на курсовий проект та анотація.

Перша сторінка змісту оформляється на аркуші з рамкою, яка має великий штамп, в якому зазначається назва документу, умовне позначення (див далі), розробник, нормоконтролер тощо, решта сторінок – на аркуші з рамкою іншої форми, яка містить лише умовне позначення (додаток В). Номер сторінки на першій сторінці змісту проставляється у відповідній графі рамки. Сам зміст за нумерацією пояснювальної записки є, як правило, четвертою сторінкою.

Для курсових проектів доцільною є предметна система умовних позначень, яка має таку структуру:



де 1 (ХХ-ХХ) – числовий шифр кафедри, прийнятий у ВНТУ (для кафедри захисту інформації – 08-20);

2 (ХХХХХ) – умовне скорочення для дисципліни (ПК);

3 (ХХХ) – перша цифра 0 позначає, що це проект (1 – якщо робота), друга і третя цифри означають рік, наприклад, 16 – 2016 рік);

4 (ХХ) – варіант завдання (наприклад, 01, 02, ..., 99);

5 (ХХХ) – перша цифра – номер групи (1, 2 тощо), наступні дві цифри

позначають таке:

- номер студента за списком у журналі академічної групи – для пояснювальної записки, технічного завдання, відомості курсового проекту;
- порядковий номер – для схем та переліків елементів (наприклад, 001, 002 тощо).

6 (ХХ) – код документа (наприклад ПЗ – для пояснювальної записки, ТЗ – для технічного завдання, Е1 – для схеми електричної структурної, А8 – для схеми роботи системи та схеми ресурсів системи).

Таким чином, пояснювальна записка до курсового проекту, виконаного у 2016 році студентом першої групи, якому в переліку академічної групи відповідає порядковий номер 25, на тему, що має порядковий номер 3 в загальному переліку тем курсових проектів, повинен використовувати умовне позначення 08-20.ПК.016.03.125 ПЗ. При цьому для даного випадку структура спеціалізованого засобу виконана як схема електрична структурна повинна позначатися 08-20.ПК.016.03.001 Е1, а схема роботи системи відповідно – 08-20.ПК.016.03.002 А8.

Нумерація у змісті починається зі вступу (відповідно до нумерації у пояснювальній записці). Нумерація сторінок по всій пояснювальній записці, включаючи додатки, повинна бути наскрізною.

Назви заголовків змісту повинні однозначно відповідати назвам заголовків пояснювальної записки за текстом. Формування змісту у текстовому документі бажано здійснювати автоматично, використовуючи засоби обраного текстового редактора. Назви усіх розділів, підрозділів, пунктів, підпунктів повинні використовувати вирівнювання до лівого краю аркуша.

2.3 Зміст та оформлення основної частини

У ***вступі*** заголовок "ВСТУП" розташовують посередині з нової пронумерованої сторінки на аркуші з рамкою.

Вступ повинен стисло висвітлювати такі питання:

- стан розвитку проблеми в даній галузі;
- галузь використання та призначення даної розробки;
- актуальність;
- мету та задачі проектування.

У вступі і далі за текстом не дозволяється використовувати скорочені слова, терміни, крім загальноприйнятих. Якщо ж в тексті є необхідність використовувати певні загальноприйняті скорочення (абревіатури), то при введенні їх вперше в дужках слід вказати скорочення. І лише після цього дане скорочення можна використовувати по тексту. Наприклад, блоковий шифр (БШ). У назвах розділів, підрозділів, пунктів і підпунктів використовувати скорочення не рекомендується.

При викладенні актуальності основну увагу необхідно приділити конкретній розробці, уникаючи узагальненої характеристики переваг криптографічних методів.

Мета курсового проектування формулюється таким чином, щоб вказувати на конкретну характеристику, яка покращується під час проектування. Приклад оформлення та подання вступу наведено у додатку Г.

Обсяг вступу не повинен перевищувати 2 сторінки.

Розділ ***аналізу предметної області*** передбачає огляд алгоритмів криптографічних засобів, що використовуються у курсовому проекті, а також відомих аналогів. На основі даного огляду відзначаються недоліки аналогів та обґрунтовується вибір засобів, необхідних для досягнення мети курсового проектування. Посилання на джерела інформації, використаної в тексті пояснювальної записки загалом і в даному підрозділі зокрема є обов’язковими.

Рекомендований обсяг розділу – 2-3 сторінок.

Розділ, присвячений ***розробці та аналізу криптопротоколу***, має містити детальний опис конкретних криптографічних методів які використовуються для проектування; узагальнений опис криптопротоколу та аналіз коректності виконання криптографічного протоколу.

Рекомендований обсяг розділу – 5-7 сторінок.

Розділ, присвячений ***розробці структури апаратного засобу***, повинен містити опис основних блоків, їх взаємозв'язків та подальший детальний опис їх структури, що детальніше описано у підрозділі 1.3 цих методичних вказівок. Він повинен відображати суть прийнятих рішень щодо структури апаратного засобу та його основних структурних блоків. При цьому рекомендується використовувати рівень деталізації на рівні схем електричних структурних.

Рекомендований обсяг розділу – 7-9 сторінок.

Розділ, присвячений ***програмного забезпечення та тестування коректності роботи***, передбачає представлення узагальненого алгоритму роботи програмного засобу та його основних структурних блоків. Крім того, даний розділ повинен містити опис обраних студентом засобів для комп'ютерного моделювання, результати проведеного тестування.

Рекомендований обсяг розділу – 8-10 сторінок.

Висновки оформлюють з нової пронумерованої сторінки, починаючи зі слова "ВИСНОВКИ" посередині рядку великими літерами, після чого пропускається один рядок.

У висновках наводяться основні результати роботи над курсовим проектом. Коротко по основних розділах описуються етапи реалізації задачі курсового проекту. Визначається тип установ та підприємств для яких доцільне впровадження розробки.

На основі отриманих в ході курсового проектування результатів надаються обґрунтовані висновки щодо переваг та недоліків розроблених апаратних та програмних засобів для криптографічного захисту інформації. Обов'язково слід зазначити перспективи удосконалення розроблених криптографічних засобів.

Перелік використаних джерел оформлюють з нової пронумерованої сторінки, починаючи із заголовку "ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ" посередині рядка великими літерами, після чого пропускається один рядок.

Перелік повинен містити використані джерела інформації, які було використано в процесі виконання проекту, і на які повинні бути обов'язкові посилання в тексті пояснювальної записки. Джерела інформації (книги, статті,

патенти, журнали, інтернет-сторінки) в загальний список записується в порядку посилання на них в тексті пояснювальної записки. Посилання на літературу наводять в квадратних дужках в місця використання інформації з даного джерела, вказуючи порядковий номер за списком. Наприклад, посилання на певну статтю, яка подається четвертою в переліку використаних джерел, оформлюється таким чином: "Серед симетричних алгоритмів виділяють найбільш відомі [4] : …".

Якщо виникає необхідність послатися на декілька джерел їх записують в порядку зростання номерів. При цьому, якщо в послідовності номерів джерел поспіль зустрічається більше двох номерів, то з даної частини переліку вказується лише перше та останнє джерело, а між ними ставлять дефіс. В інших випадках між номерами джерел ставиться кома. Наприклад, посилання на джерела, які мають в переліку номера 1, 4, 5, 6, 8 повинно оформлюватись таким чином: [1, 4-6, 8].

Кожне джерело повинно бути вказано разом з видавництвом, роком видання, кількістю сторінок. Джерела інформації в перелік записують мовою оригіналу. У переліку кожне джерело записують з абзацу, нумерують арабськими цифрами, починаючи з одиниці. Правильне оформлення певного джерела інформації можна переглянути у переліку літературних джерел у будь-якому навчальному посібнику. Якщо у списку використаних джерел є посилання на електронні ресурси, слід наводити режим доступу до даного ресурсу. Наприклад, для електронних журналів вказується уніфікований локатор ресурсів (URL).

Приклад оформлення переліку використаних джерел різного характеру:

Посилання на книги:

1. Грайворонський М. В. Безпека інформаційно-комунікаційних систем. / М. В. Грайворонський, О. М. Новіков. – К. : Видавнича група BHV, 2009. – 608 с.

2. Мікропроцесорна техніка: Підручник / [Ю. І. Якименко та ін.]; за ред. Т. О. Терещенко. – 2-ге вид., перероб. і доповн. – К.: ІВЦ "Політехніка"; "Кондор", 2004. – 440 с.

Посилання на статті в журналах:

3. Рудницький В. М. Модель уніфікованого пристрою криптографічного перетворення інформації / В. М. Рудницький, В. Г. Бабенко // Системи обробки інформації. – №3. – 2009. – С. 91-95.

4. Лужецький В. А. Апаратні засоби для реалізації багатоканального керованого хешування. / В. А. Лужецький, Ю. В. Баришев. // Системи обробки інформації. – №3. – 2011. – С. 130-133.

Посилання на матеріали та тези конференцій:

5. V.A. Luzhetskyi Methods of Generic Attacks Infeasibility Increasing for Hash Functions / Volodymyr Luzhetskyi, Yurii Baryshev // The 7th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2013), September 12-14, 2013 Berlin, Germany. – P. 661-664

6. Баришев Ю. В. Структури спеціалізованих процесорів для гешування, стійкого до загальних атак / Баришев Ю. В., Зозуля А. О. // Тези доповідей Четвертої Міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерна інженерія» м. Вінниця, 28-30 травня 2014 року. – Вінниця: ВНТУ, 2014. – С 216-219.

7. Баришев Ю. В. Структури спеціалізованих мікропроцесорів для передавання даних в лініях з великим рівнем завад. / Баришев Ю. В., Репетій В. М. // Тези доповідей Четвертої Міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерна інженерія» м. Вінниця, 28-30 травня 2014 року. – Вінниця: ВНТУ, 2014. – С 222-223.

Посилання на стандарти:

8. Захист інформації. Технічний захист інформації. Основні положення : ДСТУ 3396.0-96. – К.: Держспоживстандарт України, 1996. – 5 с.

Посилання на патенти:

9. Патент України на корисну модель № 94039 МПК G 09 C 1/00. Спосіб паралельного ключового гешування даних теоретично доведеної стійкості /

Лужецький В. А., Баришев Ю. В.; .заявник та патентовласник Вінницький національний технічний університет. – № u201405191; заявл. 16.05.2014; опубл. 27.10.2014, Бюл. № 20.

10. Патент України на корисну модель № 53615 МПК H 04 L 9/06. Спосіб шифрування даних на основі трьох несумісних груп операцій / Лужецький В. А., Дмитришин О. В., Баришев Ю. В.; .заявник та патентовласник Вінницький національний технічний університет. – № u201004697; заявл. 20.04.2010; опубл. 11.10.2010, Бюл. № 19.

11. Патент України на корисну модель № 55211 МПК H 04 L 9/06. Конвеєрний криптографічний обчислювач. / Корченко О. Г., Паціра Є. В., Панасюк А. Л., Гнатюк С. О., Кінзерявий В. М.; заявник та патентовласник Національний авіаційний університет. – № u201006041; заявл. 19.05.10; опубл. 10.12.10, Бюл. №23.

Посилання на web-сторінки:

12. Van der Spiegel J. VHDL Tutorial / Jan Van der Spiegel [Електроний ресурс]. – Режим доступу: http://www.seas.upenn.edu/~ese171/vhdl/ vhdl_primer.html (дата звернення 22.03.2016) – Назва з екрану.

13. Лабораторія імені професора Канєвського. [Електроний ресурс]. Режим доступу: http://kanyevsky.kpi.ua/VHDLlabukraine/VHDLlabukraine.html/ (дата звернення 22.03.2016) – Назва з екрану

2.4 Оформлення додатків

Першим аркушем додатків для курсових проектів має бути технічне завдання, в якому вказуються: найменування та галузь застосування розробки; основа для розробки; мета і призначення; джерела розробки; технічні вимоги (показники призначення, показники надійності, вимоги безпеки тощо); стадії та етапи розробки; порядок контролю та приймання. Технічне завдання повинно бути додатком А до пояснювальної записки. Приклад оформлення технічного завдання наведений у додатку Ж.

Крім технічного завдання, додатки містять матеріал, який:

- є необхідним для повноти викладення результатів і розуміння пояснювальної записки, але їх включення до основної частини може змінити впорядковане й логічне уявлення про курсовий проект;
- не може бути послідовно розміщений в основній частині звіту через великий обсяг (додаткові ілюстрації, схеми або таблиці, лістинг програми, інструкції, методики, опис комп'ютерних програм, розроблених або використаних у процесі курсового проектування тощо).

Додатки необхідно починати з нової сторінки, вказуючи зверху посередині рядка слово "Додаток" і через пропуск – його позначення. Додатки позначають послідовно великими українськими літерами, за винятком літер Ґ, Є, З, І, Ї, Й, О, Ч, Ь. Якщо додатків більше ніж літер, то продовжують позначати арабськими цифрами. Дозволяється позначати додатки латинськими літерами, за винятком літер *I* і *O*.

Кожен додаток повинен мати тематичний (змістовний) заголовок, який записують посередині рядка, наприклад, "Додаток Б. Лістинг програми".

У тексті пояснювальної записки необхідно обов'язково посилатись на додатки у відповідних місцях з метою звернення уваги читача на те, що результати виконання певного етапу курсового проектування не обмежуються лише наведеними в пояснювальній записці. Крім того, допускається посилання на певні частини додатків. Наприклад посилання на певні таблиці та рисунки оформлюються таким чином: "(у табл. В.3)", "... характеристики проаналізованих блокових шифрів наведено у табл. В.3", "... на рис. Г.1 наведено вигляд вхідних вихідних сигналів блоку піднесення до степеня за модулем простого числа після обробки першого блоку даних".

Сторінки додатків нумеруються, продовжуючи загальну нумерацію у пояснювальній записці. Всі додатки включають до змісту, вказуючи номер, заголовок і сторінки, з яких вони починаються.

2.5 Оформлення графічної частини

Графічна частина розміщується після додатків. Для відділення графічної частини від пояснювальної записки використовується аркуш формату А4 на якому по центру великими літерами пишуть "ГРАФІЧНА ЧАСТИНА", після якого подають розроблені схеми.

У графічній частині курсового проекту повинні подаватись схеми, які призначені для використання під час реалізації засобів криптографічного захисту інформації. Схеми, наведені в графічній частині мають шифр, який визначається відповідно до загальних правил для курсового проекту (див. підрозділ 2.2), де як код документа використовується позначення виду та типу схем відповідно ГОСТ 2.701-84.

Для відображення основних результатів, пов’язаних зі структурою спеціалізованих засобів криптографічного захисту інформації , спеціалізованих процесорів необхідно використовувати схеми електричні, які оформлюються відповідно до ДСТУ ГОСТ 2.702:2013, ГОСТ 2.708-81, ГОСТ 2.721-74 (з урахуванням внесених змін, зокрема редакції 2000 року). З урахуванням мети курсового проектування рекомендується оформляти результати у вигляді схем структурних, також допускається оформлення у вигляді схем функціональних та схем об’єднаних (лише за умови, що вони об’єднують елементи схем структурних або функціональних з елементами схем іншого типу, наприклад з елементами схеми з’єднань або схеми загальної).

Для відображення основних результатів, пов’язаних з алгоритмами роботи та програмами для засобів криптографічного захисту інформації необхідно використовувати схеми алгоритмів, програм, систем. Дані схеми оформлюються відповідно до ГОСТ 19.701-90 (з урахуванням внесених змін, зокрема редакції 2008 року). Згідно з метою курсового проектування рекомендується оформлювати результати у вигляді схеми програми. У випадку використання декількох спецпроцесорів в системі допускається використання схем взаємодії програм для відображення особливостей організації спільної обробки даних цими мікропроцесорами та особливостей передавання керування

між різними мікропроцесорами (у випадку наявності).

Відповідно до тематики курсового проектування рекомендується розробляти не менше двох схем: електрична та схеми алгоритмів, програм. Наприклад, для курсового проекту, що реалізує Спеціалізовані засоби для реалізації протоколу двосторонньої автентифікації з використанням випадкових чисел та ключової геш-функції SHA графічна частина може складатися з таких схем:

- Узагальнена структура спеціалізованого засобу для реалізації криптопротоколу. Схема електрична структурна – для відображення основних структурних блоків мікропроцесорної системи.

- Блок геш-функції SHA. Схема електрична структурна – для відображення елементів та їх зв'язків, необхідних для реалізації арифметичних операцій передбачених геш-функцією SHA;

- Схема функціонування програмного засобу. Схеми програми – для відображення основних етапів роботи програмного засобу криптографічного захисту інформації.

2.6 Загальні правила оформлення

Пояснювальна записка відноситься до текстових документів, які містять інформацію, подану в основному технічною мовою та графічну інформацію у вигляді ілюстрацій. Пояснювальна записка виконується згідно вимог міждержавного стандарту ГОСТ 2.105-95. Текст пояснювальної записки повинен бути набраний на комп'ютері та роздрукований на стандартних аркушах паперу формату А4 (210×297 мм) з однієї сторони.

Рамки. Кожен аркуш пояснювальної записки до курсового проекту (крім анотації та індивідуального завдання) повинен мати стандартну рамку робочого поля і основний напис. Титульний аркуш повинен мати рамку, наведену у додатку Б, перша сторінка розділу ЗМІСТ повинна бути оформлена на аркуші з рамкою, наведеною у додатку В, наступна та всі інші сторінки повинні бути оформлені на аркушах з рамкою, наведеною у додатку Г. У кожну рамку (окрім

рамки титульного аркуша) обов'язково повинні бути вписані номер сторінки та шифровий код проекту. Для формування рамок при виконанні пояснювальної записки у текстовому редакторі Microsoft Office Word рекомендується користуватись можливостями оформлення колонтитулів.

Шрифт і відступи. Текст пояснювальної записки повинен бути набраний у будь-якому текстовому редакторі (наприклад, Microsoft Office Word) шрифтом гарнітури Times New Roman кеглем 14. Текст записки слід друкувати через півтора інтервали. Текст розміщують таким чином, щоб відстань від рамки до робочого поля становила: зліва і справа – не менше 5 мм; зверху і знизу – не менше 10 мм. Наявність рамок у додатках не є обов'язковою.

Нумерація сторінок. Сторінки повинні бути пронумеровані, починаючи з четвертої (перша сторінка розділу ЗМІСТ). Сторінки 1-3 (які містять титульний аркуш, індивідуальне завдання, анотація) не нумеруються. Сторінки пояснювальної записки слід нумерувати арабськими цифрами, додержуючись наскрізної нумерації впродовж усього тексту. Номер сторінки проставляють у відповідному місці рамки. Нумерація додатків продовжує основну нумерацію.

Оформлення розділів і підрозділів. Структурними елементами основної частини ПЗ є розділи, підрозділи, пункти, підпункти, переліки.

Розділ – головна ступінь поділу тексту, позначена номером і має заголовок. *Підрозділ* – частина розділу, позначена номером і має заголовок. *Пункт* – частина розділу чи підрозділу, позначена номером і може мати заголовок. *Підпункт* – частина пункту, позначена номером і може мати заголовок. Заголовки структурних елементів необхідно нумерувати тільки арабськими числами.

Кожен розділ рекомендується починати з нової сторінки. Заголовки усіх основних розділів (заголовки першого рівня) записуються з абзацу великими літерами з вирівнюванням по ширині. Заголовки розділів, що містять анотацію, зміст, список використаних джерел виконують також великими літерами, однак вирівнювання відбувається посередині рядка. Після заголовків розділів пропускають один рядок.

Заголовки усіх підрозділів, пунктів та підпунктів записують з абзацу.

Перед заголовками підрозділів і після них пропускають один рядок. Назви розділів і підрозділів не повинні мати крапки в кінці.

В кінці назви пунктів та підпунктів ставиться крапка і потім з нового речення починається викладення їх змісту, тобто виділяти їх заголовки відступами не потрібно. Заголовки розділів і підрозділів, пунктів і підпунктів не повинні містити знаків переносу на новий рядок.

Основні розділи нумерують порядковими номерами в межах всього документа (1, 2, і т.д.). Підрозділи нумерують в межах кожного розділу, пункти – в межах підрозділу і т.д. за формою: 1.1, 1.2 – для розділів; 1.2.1, 1.2.2 – для пунктів; 1.2.2.1, 1.2.2.2 – для підпунктів. Цифри, які вказують номер, не повинні виступати за абзац. Після номера крапку не ставлять, а пропускають один знак. Допускається розміщувати текст між заголовками розділу і підрозділу.

Переліки. В тексті документа може наводитись перелік, який рекомендується нумерувати малими літерами української абетки з дужкою або дефіс перед текстом. Для подальшої деталізації використовують арабські цифри з дужкою. Наприклад:

а) тут пишеться текст першого пункту з переліку та його продовження;

б) тут пишеться текст другого пункту з переліку і подальша його деталізація:

1) текст переліку подальшої деталізації переліку вищого рівня та його продовження;

2) . . . ;

в) останній пункт переліку.

Оформлення таблиць. Таблицю розміщують симетрично до тексту після першого посилання на даній сторінці або на наступній, якщо на даній вона не уміщується і таким чином, щоб зручно було її розглядати без повороту або з поворотом на кут 90°. Таблиці у тексті пояснювальної записки набираються основним шрифтом, в деяких випадках розмір шрифту може бути зменшений до 10-12. Підписи таблиць розташовуються над таблицею із зазначенням її номеру і назви, вирівнявши за лівою межею. Наприклад,

Таблиця 3.1 – Характеристики блокових шифрів

Блоковий шифр	Кількість раундів *r*	Довжина ключа *K* (біт)	Розмір блоку *W* (біт)
Blowfish	16	32-448	64
Camellia	18	128	128
CAST-128	16	128	64
DEAL	6	128/192	128
DFC	8	128/192/256 (або 0-256)	128

На всі таблиці мають бути посилання за формою “ ... в табл. 3.1 або в дужках за текстом (табл. 3.1). Посилання на раніше наведену таблицю дають зі скороченим словом "дивись" (див. табл. 3.1) за ходом чи в кінці речення.

При перенесенні частин таблиці на інші сторінки, повторюють або продовжують найменування граф. Допускається виконувати нумерацію граф на початку таблиці і при перенесенні частин таблиці на наступні сторінки повторювати тільки нумерацію граф. У всіх випадках найменування (при його наявності) таблиці розміщують тільки над першою частиною, а над іншими частинами зліва пишуть "Продовження таблиці 3.1" без крапки в кінці, наприклад,

Продовження таблиці 3.1

Блоковий шифр	Кількість раундів *r*	Довжина ключа *K* (біт)	Розмір блоку *W* (біт)
RC5	1-255	0-2040	32/64/128
TEA	64	128	64
XTEA	64	128	64

Оформлення рисунків. Рисунки розміщують в тексті або в додатках. В тексті рисунок розміщують симетрично до тексту після першого посилання на нього або на наступній сторінці, якщо на даній для нього не вистачає місця, без повороту. На всі рисунки мають бути посилання за формою: " ... на рис. 2.1", або в дужках по тексту (рис. 2.1). Посилання на раніше наведений рисунок

дають зі скороченим словом "дивись" (див. рис. 2.1) за ходом чи в кінці речення.

Кожен рисунок повинен мати номер і підпис, розташовані під рисунком по центру. Нумерують рисунки в межах розділів, вказуючи номер розділу і порядковий номер рисунку в розділі, розділяючи їх крапкою. Дозволяється нумерувати рисунки в межах всього документа. Між номером та назвою рисунку ставлять тире. Крапку в кінці підпису не ставлять, знак переносу не використовують. Якщо найменування рисунка довге, то його продовжують у наступному рядку.

Між рисунком і текстом пропускають один рядок. Наприклад,

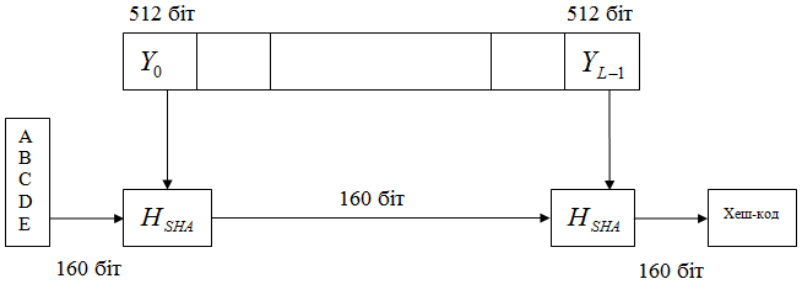


Рисунок 2.1 – Схема обчислення значення геш-функції SHA

Оформлення формул. Кожну формулу записують з нового рядка, симетрично до тексту, курсивом. Між формулою і текстом пропускають один рядок.

Умовні літерні позначення (символи) в формулі повинні відповідати установленим ДСТУ IEC 60027-1; ДСТУ IEC 60027-2. Їх пояснення наводять в тексті або зразу ж під формулою. Для цього після формули ставлять кому і записують пояснення до кожного символу з нового рядка в тій послідовності, в якій вони наведені у формулі, розділяючи крапкою з комою. Перший рядок повинен починатися з абзацу зі слова "де" і без будь-якого знака після нього.

Всі формули нумерують в межах розділу арабськими числами. Номер вказують в круглих дужках з правої сторони, в кінці рядка, на рівні закінчення формули. Номер формули складається з номера розділу і порядкового номера формули в розділі, розділених крапкою. Дозволяється виконувати нумерацію в межах всього документа.

2.7 Графік виконання курсового проекту і порядок його захисту

Рекомендується такий графік виконання курсового проекту, який враховує самостійну роботу студентів під час 8-го триместру бакалаврату (16 тижнів).

Зміст розділу	Термін виконання
Отримання завдання на курсовий проект, розробка і оформлення індивідуального завдання	1 тиждень
Аналіз підходів до проектування та обґрунтування вибору одного з них.	2 тиждень
Оформлення технічного завдання	3 тиждень
Реалізація узагальненого опису та аналізу криптографічного алгоритму.	4-7 тижні
Розробка загальної структури апаратного засобу криптографічного захисту інформації. Розробка схеми роботи засобу.	8-10 тижні
Реалізація пристрою. Розробка схеми електричної.	11-12 тижні
Написання програмного засобу. Його тестування.	12-14 тижні
Здача курсового проекту на попередню перевірку: демонстрація чернетки пояснювальної записки	14 тиждень
Корегування і доповнення згідно зауважень керівника курсового проекту, врахування і виправлення пояснювальної записки	15 тиждень
Захист курсового проекту	16 тиждень

Готовність до захисту курсового проекту визначає керівник за результатами попередньої перевірки якості пояснювальної. Записка повинна бути здана керівнику на перевірку не менш, як за тиждень до визначеного терміну захисту проекту. Якщо курсовий проект виконаний в повному обсязі та у ньому відсутні принципові помилки, керівник допускає студента до захисту. В іншому випадку проект повертається студенту на доопрацювання. Після позитивного висновку про готовність курсового проекту студент повинен захистити його перед комісією у складі двох викладачів, які призначені кафедрою.

ПЕРЕЛІК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Лужецький В. А. Основи інформаційної безпеки / В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович. – Вінниця: ВНТУ, 2013. – 267 с.

2. Грайворонський М. В. Безпека інформаційно-комунікаційних систем. / М. В. Грайворонський, О. М. Новіков. – К. : Видавнича група BHV, 2009. – 608 с.

3. Бабич М. П. Комп’ютерна схемотехніка: Навчальний посібник / М. П. Бабич, І. А. Жуков. – К.: "МК-Прес", 2004. – 412 с.

4. Поточные шифры. / [А. В. Асосков и др.] – М. : КУДИЦ-ОБРАЗ, 2003. – 336 с.

5. Фергюсон Н. Практическая криптография : пер. с англ. / Н. Фергюсон, Б. Шнайер. - М. : Издательский дом "Вильямс", 2005. – 424 с.

6. Введение в криптографию. / Под ред. В. В. Ященко. – М. : МЦНМО, 2000. – 288 с.

7. Рябко Б. Я. Криптографические методы защиты информации. Учебное пособие для вузов. / Б. Я. Рябко, А. Н. Фионов. – М.: Горячая линия-Телеком, 2005. – 229 с.

8. Смарт Н. Криптография / Н. Смарт. – М.: Техносфера, 2005. – 528 с.

9. Щербаков Л. Ю. Прикладная криптография. Использование и синтез криптографических интерфейсов. / Л. Ю. Щербаков, А. В. Домашев. – М.: Издательско-торговый дом "Русская Редакция", 2003. – 416 с.

10. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. – М. : МЦНМО, 2003. – 328 с.

11. Бабаш А. В., Шанкин Г. П. Криптография. Под ред. В. П. Шерстюка, Э. А. Применко / А. В. Бабаш, Г. П. Шанкин. - М.: СОЛОН-Р, 2002. - 512 с.

12. Алферов А. П. Основы криптографии. Учебное пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. - М.: Гелиос АРВ, 2001. - 480 с.

13. Петров А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. - М.: ДМК, 2000. - 448 с.

14. Брассар Ж. Современная криптология / Ж. Брассар. - М.: Полимед, 1999. - 354 с.

15. Нечаев В. И. Элементы криптографии. Основы теории защиты информации. - М.: Высшая школа, 1999. - 278 с.

16. Столингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. - 672 с.

17. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. - М.: КУДИЦ-ОБРАЗ, 2001. - 346 с.

18. Грушо А .А., Тимонина Е. Е. Анализ и синтез криптоалгоритмов / А .А. Грушо, Е. Е. Тимонина, Э.А. Применко. - М.: СОЛОН-Р, 2000. - 108 с.

19. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. 2-е изд. - СПб., 2000. - 789 с.

20. Чмора А. Л. Современная прикладная криптографія / А. Л. Чмора. - М.: Гелиус АРВ, 2001. - 244 с.

21. Молдовян Н. А., Молдовян А. А. Введение в криптосистемы с открытым ключом / Н. А. Молдовян, А. А. Молдовян. - СПБ.: Петербург, 2005. – 288 с.

22. Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. – М.: КомКнига, 2006. – 328 с.

23. Лужецький В. А. Апаратні засоби для реалізації багатоканального керованого хешування. / В. А. Лужецький, Ю. В. Баришев // Системи обробки інформації. – №3. – 2011. – С. 130-133.

24. Лужецький В. А. Криптографічні примітиви для реалізації керованого хешування / В. А. Лужецький, Ю. В. Баришев // Вісник ВПІ. – №1. – 2011. – С. 108-111.

25. Лужецький В. А. Підходи до побудови швидких алгоритмів хешування / В. А. Лужецький, Ю. В. Баришев // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – №. 2 (19), 2009 р. – С. 57-65.

26. Баришев Ю. В. Структура спеціалізованого криптографічного процесора для керованого хешування / Баришев Ю. В. // Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2011): матеріали V Міжнародної науково-технічної конференції, м. Вінниця, 19-21 травня 2011 р. – Вінниця: ВНТУ, 2011. – С. 169-170.

27. Лужецький В. А. Блочний шифр на основі псевдонедетермінованих послідовностей криптопримітивів / В .А. Лужецький, А. В. Остапенко, // Наукові праці ВНТУ. – № 4 (2010). – Режим доступу до статті: http://www.nbuv.gov.ua

28. Лужецький В. А. Аналіз алгоритмів симетричного блокового шифрування / В .А. Лужецький, А. В. Остапенко // Інформаційні технології та комп'ютерна інженерія. – 2012. – № 3. – С. 55-64.

29. Патент України на корисну модель № 94039 МПК G 09 C 1/00. Спосіб паралельного ключового гешування даних теоретично доведеної стійкості / Лужецький В. А., Баришев Ю. В.; .заявник та патентовласник Вінницький національний технічний університет. – № u201405191; заявл. 16.05.2014; опубл. 27.10.2014, Бюл. № 20.

30. Патент України на корисну модель № 53615 МПК H 04 L 9/06. Спосіб шифрування даних на основі трьох несумісних груп операцій / Лужецький В. А., Дмитришин О. В., Баришев Ю. В.; .заявник та патентовласник Вінницький національний технічний університет. – № u201004697; заявл. 20.04.2010; опубл. 11.10.2010, Бюл. № 19.

Додаток А. Варіанти завдань на курсовий проект

1. Засоби автентифікації користувачів за допомогою алгоритму DES.
2. Засоби автентифікації користувачів за допомогою алгоритму ГОСТ.
3. Засоби автентифікації користувачів за допомогою алгоритму AES.
4. Засоби автентифікації користувачів за допомогою алгоритму Threefish.
5. Засоби автентифікації користувачів за допомогою алгоритму ElGamal.
6. Засоби автентифікації користувачів за допомогою алгоритму SEAL.
7. Засоби автентифікації користувачів за допомогою алгоритму Panama.
8. Засоби автентифікації користувачів за допомогою алгоритму ORIX.
9. Засоби автентифікації користувачів за допомогою алгоритму 3DES.
10. Засоби автентифікації користувачів за допомогою алгоритму SOBER.
11. Засоби автентифікації користувачів за допомогою алгоритму PIKE.
12. Засоби автентифікації користувачів за допомогою алгоритму Wide-mouthed Frog.
13. Засоби автентифікації користувачів за допомогою алгоритму Blowfish.
14. Засоби автентифікації користувачів за допомогою алгоритму асиметричного шифрування McEliece.
15. Засоби автентифікації користувачів за допомогою алгоритму асиметричного шифрування Pohlig-Hellman.
16. Засоби автентифікації користувачів за допомогою алгоритму Serpent.
17. Засоби автентифікації користувачів за допомогою алгоритму MARS.
18. Засоби автентифікації користувачів за допомогою алгоритму RC6.
19. Засоби для шифрування даних за допомогою алгоритму Seal.
20. Засоби для шифрування даних за допомогою регістрів зсуву з нелінійним зворотнім зв’язком.
21. Засоби для шифрування даних за допомогою алгоритму RC5.
22. Засоби для шифрування даних за допомогою алгоритму AES.
23. Засоби для шифрування даних за допомогою алгоритму ГОСТ.
24. Засоби для шифрування даних за допомогою алгоритму Threefish.
25. Засоби для шифрування даних за допомогою алгоритму RSA.

26. Засоби для шифрування даних за допомогою алгоритму ElGamal.

27. Засоби для створення електронного цифрового підпису DSA.

28. Засоби для створення електронного цифрового підпису ECDSA.

29. Засоби для створення електронного цифрового підпису ГОСТ.

30. Засоби для автентифікації даних за допомогою алгоритму SHA-3.

31. Засоби для автентифікації даних за допомогою алгоритму Skein.

32. Засоби для автентифікації даних за допомогою алгоритму BMW.

33. Засоби для автентифікації даних за допомогою алгоритму Blake.

34. Засіб захищеного зберігання паролів.

35. Засоби автентифікації користувачів за протоколом Фейга-Шаміра.

36. Засоби автентифікації користувачів за протоколом Шнорра.

37. Засоби автентифікації користувачів за допомогою ключової хеш-функції MD2.

38. Засоби генерування та обміну сеансовими ключами за протоколом Діффі-Хеллмана.

39. Засоби генерування та обміну сеансовими ключами за протоколом ECDH

40. Засоби генерування та обміну сеансовими ключами за протоколом "точка-точка".

41. Засоби генерування та обміну сеансовими ключами за протоколом Shamir.

42. Засоби генерування та обміну сеансовими ключами за протоколом Needham-Schroeder.

43. Засоби генерування та обміну сеансовими ключами за протоколом Otway-Rees.

44. Розробка протоколу спільного підписання контракту у разі наявності арбітра.

45. Розробка протоколу групового підписання документу.

46. Розробка протоколу довіреного підписання документу.

47. Розробка протоколу сліпого підписання документу.

48. Розробка протоколу розподілення знання секрету.

Додаток Б. Приклад оформлення титульного аркуша

Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

КУРСОВИЙ ПРОЕКТ
з дисципліни "Прикладна криптологія"
на тему: "Засоби для реалізації протоколу двосторонньої автентифікації з використанням випадкових чисел та ключової геш-функції SHA"
08-20.ПК.016.01.101 ПЗ

Студента (ки) 4 курсу 1БС-16б групи
напряму підготовки 125 – Кібербезпека
спеціальності _____
Іваненка Бориса Степановича
(прізвище та ініціали)
Керівник доц. каф. ЗІ, к. т. н.
Баришев Ю. В.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Національна шкала _____
Кількість балів: _____ Оцінка: ECTS _

Члени комісії:

_____ _____
(підпис) (прізвище та ініціали)

_____ _____
(підпис) (прізвище та ініціали)

_____ _____
(підпис) (прізвище та ініціали)

м. Вінниця – 2016 року

Інв. № | Підпис та | На зам. | Інв. № | Підпис та

Додаток В. Приклад оформлення змісту

ЗМІСТ

					08-20.ПК.016.01.101 ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Іваненко Б. С.			Засоби для реалізації протоколу двосторонньої автентифікації з використанням випадкових чисел та ключової геш-функції SHA	Літ.	Арк. 4 / Аркушів 42
Перевір.		Баришев Ю. В.					
Реценз.						ВНТУ, гр. 1 БС-16б	
Н. Контр.		Баришев Ю. В.					
Затверд.		Лужецький В. А.					

ВСТУП

Віддалена обробка інформації сприяє збільшенню швидкості її обробки та передавання, а як наслідок покращенню прийнятих управлінських рішень. Така можливість забезпечується низкою технологій, зокрема криптографічними протоколами автентифікації користувачів, які дозволяють захистити конфіденційність та автентичність інформації, що обробляється віддалено. Водночас впровадження протоколів автентифікації ускладнюється низкою обставин. Основними з яких є недостатня швидкість реалізації алгоритмів автентифікації та низка атак на підсистеми автентифікації, зокрема перехоплення повторне надсилання автентифікаційних даних користувача. Використання спеціалізованих процесорів як основи для реалізації криптографічних перетворень дозволить усунути недоліки. Саме тому розробка спеціалізованих засобів, що реалізує протокол двосторонньої автентифікації з використанням ключової геш-функції SHA [1, 3-5], є актуальною для галузі кібербезпеки зокрема та інформаційних технологій загалом.

Об’єктом курсового проектування є протоколи автентифікації користувачів. Предметом – програмні та апаратні засоби двосторонньої автентифікації з використанням ключової геш-функції SHA.

Метою курсового проекту є збільшення швидкодії інформаційних систем під час автентифікації користувачів.

Для досягнення мети необхідно розв’язати такі задачі:

- огляд відомих протоколів автентифікації;
- аналіз методів двосторонньої автентифікації;
- кориптоаналіз протоклу двосторонньої автентифікації;
- розробка структури спеціалізованого апаратного засобу для автентифікації користувачів;
- розробка алгоритму роботи програмного засобу;
- реалізація та тестування коректності роботи програмного засобу.

Додаток Д. Приклад оформлення індивідуального завдання

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії

ЗАТВЕРДЖУЮ

Зав. кафедри ЗІ, д. т. н., професор

_____В. А. Лужецький

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

на курсовий проект з дисципліни " Прикладна криптологія "
студенту групи 1БС-16б Іваненку Борису Степановичу
Тема: " Засоби двосторонньої автентифікації користувачів "

1. Проаналізувати криптографічний алгоритм, визначити аналогічні та виконати порівняльний аналіз з ними.
2. Виконати аналіз криптографічного протоколу з використанням BAN-логіки.
3. Розробити структуру спеціалізованого процесора, що реалізує криптографічний протокол. Результати виконання даного етапу формалізувати у вигляді схем електричних структурних.
4. Для спеціалізованого процесора визначити:
   - час реалізації криптографічного протоколу (в умовних одиницях);
   - складність апаратури (в умовних одиницях);
   - обсяг пам'яті.
5. Розробити алгоритм, що реалізує протокол та реалізувати його у вигляді програмного засобу. Результати виконання даного етапу формалізувати у вигляді схем програми.

Вихідні дані:
криптографічний алгоритм – геш-функція SHA;
метод рандомізації – випадкові числа;
довжина ключа – 128 біт.

Дата видачі 01 лютого 2016 р.

Керівник _____ Ю. В. Баришев

Завдання отримав _____ Б. С. Іваненко

Додаток Ж. Приклад оформлення технічного завдання

Вінницький національний технічний університет
Факультет інформаційних технологій та комп’ютерної інженерії

ЗАТВЕРДЖУЮ
Керівник, к. т. н., доцент кафедри ЗІ
_____ Ю. В. Баришев
_____ 20__ р.

ТЕХНІЧНЕ ЗАВДАННЯ
на курсовий проект
з дисципліни "Прикладна криптологія"
на тему: " Засоби для реалізації протоколу двосторонньої автентифікації з використанням випадкових чисел та ключової геш-функції SHA "
08-20.ПК.016.01.101 ТЗ

Вінниця 2016

1 Назва та галузь використання

Спеціалізовані засоби для реалізації протоколу двосторонньої автентифікації з використанням випадкових чисел та ключової геш-функції SHA призначена для захисту автентичності джерела даних, що зберігаються та передаються інформаційно-комунікаційними мережами.

2 Основа для розробки

Робоча навчальна програма та робочий план дисципліни "Прикладна криптологія".

3 Мета та призначення розробки

Покращення швидкості автентифікації користувачів комп'ютерної системи шляхом розробки спеціалізованих засобів, що реалізує протоколу двосторонньої автентифікації з використанням випадкових чисел та ключової геш-функції SHA.

Спеціалізовані програмні та апаратні засоби призначені для перевірки автентичності користувача комп'ютерної системи.

4 Джерела розробки

1. Фергюсон Н. Практическая криптография : пер. с англ. / Н. Фергюсон, Б. Шнайер. - М. : Издательский дом "Вильямс", 2005. – 424 с.

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — 816 с.

5 Вимоги до системи

5.1 Параметри розроблюваної системи:

- протокол автентифікації – геш-функції SHA;
- метод рандомізації – випадкові числа;
- довжина ключа – 128 бітів;
- метод криптоаналізу – BAN-логіка.

5.2. Результати розробки:

- детальний опис протоколу;
- аналіз протоколу за допомогою BAN-логіки;
- структурна схема спеціалізованого процесора, що реалізує розроблений протокол;
- програмний засіб, що реалізує розроблений протокол.

6 Вимоги до супровідної документації

6.1 Графічна і текстова документація повинна відповідати діючим

стандартам України.

6.2 Засоби повинні супроводжуватись:

- лістингом програми;
- результатами тестування роботи програмного засобу;
- схемою електричною структурною спеціалізованого процесора двосторонньої автентифікації з використанням випадкових чисел та ключової геш-функції SHA;
- схемою роботи програмного засобу двосторонньої автентифікації з використанням випадкових чисел та ключової геш-функції SHA;

7 Стадії та етапи розробки

Робота з теми виконується у 7 етапів.

Етап	Зміст	Початок	Закінчення	Результат
1	Аналіз протоколів автентифікації.	01.02.16	15.02.16	Чорновий варіант розділу 1
2	Узагальнений опис протоколу двосторонньої автенитфікації. Його криптоаналіз з використанням BAN-логіки.	16.02.16	01.03.16	Чорновий варіант розділу 2
3	Розробка структури спеціалізованого апаратного засобу.	2.03.16	16.03.16	Схема електрична структурна, чорновий варіант розділу 3
4	Розробка алгоритмів роботи програмного засобу.	17.03.16	1.04.16	Схема роботи прогами, чорновий варіант розділу 4
5	Розробка програми.	02.04.16	23.04.16	Лістинг програми, чорновий варіант розділу 4
6	Тестування роботи програмного засобу.	25.04.16	01.05.16	Результати тестування, чорновий варіант розділу 4
7	Оформлення пояснювальної записки.	02.12.16	06.05.16	Пояснювальна записка

8 Порядок контролю та прийому.

До прийому і захисту курсового проекту подається:

- заключний звіт;

- лістинг програми;
- спеціалазований апаратний засіб для двосторонньої автентифікації користувачів з використанням ключової геш-функції SHA. Схема електрична структурна;
- програмний засіб для двосторонньої автентифікації користувачів з використанням ключової геш-функції SHA. Схема роботи програми.

Початок розробки 01. 02.2016.
Крайній термін виконання курсового проекту 06.05.2016.

Розробив студент групи 1БС-16б _____ Б. С. Іваненко