Київський національний торговельно-економічний університет
Кафедра інженерії програмного забезпечення та кібербезпеки

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Розробка криптографічного алгоритму прихованого листування»

Студента 4 курсу, 6 групи,
спеціальності 121 «Інженерія
програмного забезпечення» _____ Лучка Максима
підпис студента Мар'яновича

Науковий керівник
доктор технічних наук,
професор _____ Криворучко Олена
підпис керівника Володимирівна

Гарант освітньої програми
кандидат технічних наук,
доцент _____ Цензура Микола
підпис керівника Олександрович

КИЇВ – 2020

Київський національний торговельно-економічний університет

Факультет інформаційних технологій
Кафедра інженерії програмного забезпечення та кібезбезпеки
Освітній ступінь бакалавр
Спеціальність 121 «Інженерія програмного забезпечення»

Затверджую
Зав. кафедри інженерії програмного забезпечення та кібербезпеки
Криворучко О.В.
"7" листопада 2019 р.

Завдання
на випускна кваліфікаційна робота студентові
Лучка Максима Мар'яновича
(прізвище, ім'я, по батькові)

1. Тема випускної кваліфікаційної «Розробка криптографічного алгоритму прихованого листування»
   Затверджена наказом ректора від "___" _____20__ р. № ___

2. Строк здачі студентом закінченої роботи _____
_____

3. Цільова установка та вихідні дані до роботи
Мета роботи розробка сайту для шифрування тексту.
_____
_____

Об'єкт дослідження криптографічні методи
_____
_____

Предмет дослідження методи та способи створення сайту для шифрування тексту._____

4. Консультанти роботи із зазначенням розділів, які консультують:

Розділ	Консультант (прізвище, ініціали)	Підпис, дата	
		Завдання видав	Завдання прийняв

5. Зміст випускної кваліфікаційної роботи (перелік питань за кожним розділом)

Вступ

Розділ 1. «Історія електронної криптографії»

1.1 Висновки до розділу 1

Розділ 2. «Криптографічні методи захисту інформації»

2.1 Симетричні криптосхеми

2.2 Системи з відкритим ключем

2.3 Як вибрати криптографічний алгоритм

2.4 Висновки до розділу 2

Розділ 3. «Розробка сайту шифрування»

3.1 Формування алгоритму роботи сайту

3.2 Побудова інтерфейсу

3.3 Функціональна частина сайту

3.4 Висновки до розділу 3

Висновки та пропозиції

Список використаних джерел

Додатки

6. Календарний план виконання роботи

№ пор.	Назва етапів випускної кваліфікаційної роботи	Строк виконання етапів роботи	
		за планом	фактично
1	2	3	4
1.	*Вибір теми випускної кваліфікаційної роботи*		
2.	*Вступ та перелік літературних джерел*		
3.	*Розділ 1. «Історія електронної криптографії»*		
4.	*Розділ 2. «Криптографічні методи захисту інформації»*		
5.	*Розділ 3. «Розробка сайту шифрування»*		
6.	*Висновки*		
7.	*Здача випускної кваліфікаційної роботи на кафедру (перша перевірка)*		
8.	*Підготовка автореферату та презентації доповіді*		
9.	*Попередній захист випускної кваліфікаційної роботи*		
10.	*Зовнішнє рецензування випускної кваліфікаційної роботи*		
11.	*Здача прошитої випускної кваліфікаційної роботи на кафедру*		
12.	*Публічний захист випускної кваліфікаційної роботи*		

7. Дата видачі завдання «___»_____20__ р.

8. Науковий керівник випускної кваліфікаційної роботи
_____Криворучко О.В._____
(прізвище, ініціали, підпис)

9. Гарант освітньої програми ____Цензура М.О._____
(прізвище, ініціали, підпис)

10. Завдання прийняв до виконання студент_Лучко М.М._____
(прізвище, ініціали, підпис)

11. Відгук керівника випускної кваліфікаційної роботи

____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____

Науковий керівник випускної кваліфікаційної роботи _Криворучко О.В.____
(підпис, дата)

Відмітка про попередній захист ____
(ПІБ, підпис, дата)

12. Висновок про випускну кваліфікаційну робота

Випускна кваліфікаційна робота студента _____Лучка М.М.______________
(прізвище, ініціали)

може бути допущена до захисту екзаменаційній комісії.

Гарант освітньої програми _Цензура М.О.______________________________
(прізвище, ініціали, підпис)

Завідувач кафедри _____Криворучко О.В._____________________________
(підпис, прізвище, ініціали)

«_____»_________________20 ___ р.

Анотація

Випускна кваліфікаційна робота «Розробка криптографічного алгоритму прихованого листування» складається з: основної частини 28 сторінок, 3 рисунка.

В даній випускній кваліфікаційній роботі представлені: вступна частина, історичний опис криптографії, види та порівняння криптографічних алгоритмів, рекомендації вибору алгоритмів, процес створення інтерфейсу сайту та процес написання функціональної частини.

Annotation

The final qualifying work "Development of cryptographic algorithm of hidden correspondence" consists of: the main part of 28 pages, 3 drawings.

The final qualifying work presents: introductory part, historical description of cryptography, types and comparisons of cryptographic algorithms, recommendations for choosing algorithms, the process of creating a site interface and the process of writing a functional part.

Зміст

ВСТУП

Останнім часом зростає інтерес до питань захисту інформації. Це пов’язано з тим, що комп'ютерні мережі набули більшого поширення, що призводить до того, що є великі можливості для несанкціонованого доступу до переданої інформації. У літературі є різні способи захисту інформації серед них:

1. Фізична (перешкода);
2. Законодавчі;
3. Управління доступом;
4. Криптографічне закриття.

Питанню запобігання витоку інформації криптографічним шляхом приділяється велика увага. Основними факторами, що сприяють підвищенню уразливості є:

1. Різке збільшення обсягів інформації, що накопичується, зберігається та обробляється за допомогою ЕВМ і інших засобів автоматизації;

2. Зосередження в єдиних базах даних інформації різного призначення і різної приналежності;

3. Різке розширення кола користувачів, що мають безпосередній доступ до ресурсів обчислювальної системи і знаходяться в ній масивів даних;

4. Ускладнення режимів функціонування технічних засобів обчислювальних систем: широке впровадження мультипрограмному режиму, а також режиму поділу часу;

5. Автоматизація обміну інформацією, в тому числі і на великих відстанях.

					КНТЕУ 121 06-13.БР			
Зм.	Аркуш	№ докум	Підпис	Дата				
Зав. кафедри		Криворучко О.В.			Розробка криптографічного алгоритму прихованого листування	Стадія	Аркуш	Аркушів
Керівник		Криворучко О.В.				В	3	26
Гарант		Цензура М.О.				Факультет інформаційних технологій, 4 курс, 6 група		
Розроб.		Лучко М.М.			Вступ			

В цих умовах виникає можливість несанкціонованого використання або модифікації інформації (небезпека витоку інформації обмеженого користування). Це викликає особливу заклопотаність користувачів, в зв'язку з чим захист інформації від несанкціонованого доступу (читання) приділяється підвищена увага.

Абсолютно очевидна вразливість незахищених систем зв'язку, в тому числі обчислювальних мереж. Інформація, що циркулює в них, може бути незаконно змінена, викрадена, знищена.

В даний час криптографічні методи застосовуються не тільки для захисту інформації від несанкціонованого доступу, а й лежать в основі багатьох нових електронних інформаційних технологій електронного документообігу, електронних грошей, таємного електронного голосування та ін.

Актуальність теми очевидна, тому що інформація в сучасному суспільстві – одна з найцінніших речей у житті, що вимагає захисту від несанкціонованого проникнення осіб, які не мають до неї доступу.

Об'єктом дослідження є криптографічні методи.

Предметом дослідження є методи та способи створення сайту для шифрування тексту.

Метою є розробка сайту для шифрування тексту.

РОЗДІЛ 1.
ІСТОРІЯ ЕЛЕКТРОННОЇ КРИПТОГРАФІЇ

Історія криптографії налічує приблизно чотири тисячі років. В якості основного критерію періодизації криптографії можливо використовувати технологічні характеристики використовуваних методів шифрування.

Перший період (приблизно з 3-го тисячоліття до н. Е.) Характеризується пануванням моноалфавітних шифрів (основний принцип – заміна алфавіту вихідного тексту іншим алфавітом через заміну букв іншими буквами або символами).

Другий період (хронологічні рамки – з IX століття на Близькому Сході (Ал-Кінді) і з XV століття в Європі (Леон Баттіста Альберті) – до початку XX століття) ознаменувався введенням в обіг поліалфавітних шифрів.

Третій період (з початку і до середини XX століття) характеризується впровадженням електромеханічних пристроїв в роботу шифрувальників. При цьому тривало використання поліалфавітних шифрів.

Четвертий період – з середини до 70-х років XX століття – період переходу до математичної криптографії. В роботі Шеннона з'являються суворі математичні визначення кількості інформації, передачі даних, ентропії, функцій шифрування. Обов'язковим етапом створення шифру вважається вивчення його вразливості для різних відомих атак – лінійного і диференціального криптоаналізу. Однак до 1975 року криптографія залишалася «класичною» або ж, більш коректно, криптографією з секретним ключем.

					КНТЕУ 121 06-13.БР			
Зм.	Аркуш	№ докум	Підпис	Дата				
Зав. кафедри		Криворучко О.В.			Розробка криптографічного алгоритму прихованого листування	Стадія	Аркуш	Аркушів
Керівник		Криворучко О.В.				Р1	5	26
Гарант		Цензура М.О.				Факультет інформаційних технологій, 4 курс, 6 група		
Розроб.		Лучко М.М.			Історія електронної криптографії			

Сучасний період розвитку криптографії (з кінця 1970-х років по теперішній час) відрізняється зародженням та розвитком нового напрямку – криптографія з відкритим ключем. Її поява знаменується не тільки новими технічними можливостями, а й порівняно широким поширенням криптографії для використання приватними особами. Правове регулювання використання криптографії приватними особами в різних країнах сильно розрізняється – від дозволу до повної заборони.

Сучасна криптографія утворює окремий науковий напрям на стику математики та інформатики – роботи в цій галузі публікуються в наукових журналах, організовуються регулярні конференції. Практичне застосування криптографії стало невід'ємною частиною життя сучасного суспільства – її використовують в таких галузях, як електронна комерція, електронний документообіг (включаючи цифрові підписи), телекомунікації та інших.

Поява в середині двадцятого століття перших електронно-обчислювальних машин кардинально змінило ситуацію в області шифрування (криптографії). З проникненням комп'ютерів в різні сфери життя виникла принципово нова галузь – інформаційна індустрія.

У 60-х і частково в 70-х роках проблема захисту інформації вирішувалася досить ефективно застосуванням в основному організаційних заходів. До них ставилися, перш за все, режимні заходи, охорона, сигналізація і найпростіші програмні засоби захисту інформації. Ефективність використання зазначених коштів досягалася за рахунок концентрації інформації на обчислювальних центрах, як правило, автономних, що сприяло забезпеченню захисту відносно малими засобами.

"Розосередження" інформації по місцях її зберігання і обробки, чому в чималому ступені сприяла поява у величезних кількостях дешевих персональних комп'ютерів і побудованих на їх основі локальних і глобальних національних і транснаціональних мереж ЕОМ, що використовують

супутникові канали зв'язку, створення високоефективних систем розвідки і видобутку інформації, загострило ситуацію із захистом інформації. Проблема забезпечення необхідного рівня захисту інформації виявилася (і це предметно підтверджено як теоретичними дослідженнями, так і досвідом вирішення) досить складною, що вимагає для свого рішення не просто здійснення деякою сукупністю наукових, науково-технічних і організаційних заходів і застосування специфічних засобів і методів, а створення цілісної системи організаційних заходів і застосування специфічних засобів і методів щодо захисту інформації.

Обсяг циркулюючої в суспільстві інформації стабільно зростає. Популярність всесвітньої мережі Інтернет в останні роки сприяє подвоєння інформації щороку. Фактично, на порозі нового тисячоліття людство створило інформаційну цивілізацію, в якій від успішної роботи засобів обробки інформації залежить благополуччя і навіть виживання людства в його нинішній якості. Зміни, що відбулися за цей період зміни можна охарактеризувати наступним чином:

1. об'єми оброблюваної інформації зросли за півстоліття на кілька порядків; -доступ до певних даних дозволяє контролювати значні матеріальні і фінансові цінності;

2. інформація придбала вартість, яку навіть можна підрахувати; -характер оброблюваних даних став надзвичайно різноманітним і більше не зводиться до виключно текстовим даними;

3. інформація повністю "знеособлені", тобто особливості її матеріального уявлення втратили своє значення – порівняйте лист минулого століття і сучасне послання по електронній пошті;

4. характер інформаційних взаємодій надзвичайно ускладнився, і поряд з класичною задачею захисту переданих текстових повідомлень від несанкціонованого прочитання і спотворення виникли нові завдання сфери

захисту інформації, що раніше стояли і які вирішувались у рамках використовуваних "паперових" технологій – наприклад, підпис під електронним документом і вручення електронного документа "під розписку" – мова про подібні "нових" задачах криптографії ще попереду;

5. суб'єкта інформаційних процесів тепер є не тільки люди, а й створені ними автоматичні системи, що діють по закладеної в них програмі;

6. обчислювальні "здібності" сучасних комп'ютерів підняли на абсолютно новий рівень як можливості по реалізації шифрів, раніше немислимих через свою високої складності, так і можливості аналітиків по їх злому.

Перераховані вище зміни призвели до того, що дуже швидко після поширення комп'ютерів в діловій сфері практична криптографія зробила в своєму розвитку величезний стрибок, причому відразу по декількох напрямках:

По-перше, були Розроблено стійкі блокові із секретним ключем, призначений для вирішення класичної завдання – забезпечення секретності і цілісності, переданих або збережених даних, вони до сих пір залишаються "робочою конячкою" криптографії, найбільш часто використовуваними засобами криптографічного захисту;

По-друге, були створені методи вирішення нових, нетрадиційних завдань сфери захисту інформації, найбільш відомими з яких є завдання підпису цифрового документа і відкритого розподілу ключів. У сучасному світі інформаційний ресурс став одним з Найбільш потужні важелів економічного розвитку.

Володіння інформацією необхідної якості в потрібний час і в потрібному місці є запорукою успіху в будь-якому вигляді господарської діяльності. Монопольне володіння певною інформацією виявляється найчастіше вирішальною перевагою в конкурентній боротьбі і зумовлює, тим самим, високу ціну "інформаційного фактору"[2].

1.1 Висновки до розділу 1

Широке впровадження персональних ЕОМ вивели рівень "інформатизації" ділового життя на якісно новий рівень. Нині важко уявити фірму або підприємство (включаючи найдрібніші), які НЕ були б озброєні сучасними засобами обробки і передачі інформації. У ЕОМ на носіях даних накопичуються значні обсяги інформації, часто носить конфіденційний характер або становить велику цінність для її власника.

Завдання криптографії, тобто таємна передача, виникає тільки для інформації, яка потребує захисту. У таких випадках кажуть, що інформація містить таємницю або є що захищається, приватної, конфіденційної, таємної.

РОЗДІЛ 2.
КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Сучасна криптографія включає в себе чотири великих розділа

Рис 2.1 Розділи криптографії

Криптографічними засобами захисту називаються спеціальні засоби і методи перетворення інформації, в результаті яких маскується її зміст.

Основні напряму використання криптографічних методів - передачі конфіденційної інформації по каналах зв'язку (на приклад, електрона пошта), встановлення автентичності передачі повідомлень, зберігання після інформації (документів, баз даних) на носіях в зашифрованому вигляді.

Криптографічні методи можна розбити на два класи:

1. обробка інформації шляхом заміни і переміщення букв, при якому обсяг даних не змінюється (шифрування);

2. стиснення інформації за допомогою заміни окремих поєднань літер, слів або фраз (кодування).

За способом реалізації криптографічні методи можливі в апаратному та програмному виконанні.

Для захисту текстової інформації при передачах на віддалені станції телекомунікаційної мережі використовуються апаратні способи шифрування і кодування. Для обміну інформацією між ЕОМ по телекомунікаційної мережі, а також для роботи з локальними абонентами можливі як апаратні, так і програмні способи. Для зберігання інформації на магнітних носіях застосовуються програмні способи шифрування і кодування.

Апаратні способи шифрування інформації застосовуються для передачі захищених даних по телекомунікаційної мережі.

Для реалізації шифрування з допомогою змішаного алфавіту використовується перестановка окремих розрядів в межах одного або декількох символів.

Програмні способи застосовуються для шифрування інформації, що зберігається на магнітних носіях (дисках, стрічках). Це можуть бути дані різних інформаційно-довідкових систем. Програмні способи шифрування зводяться до операцій перестановки, перекодування і складання по модулю 2 з ключовими словами.

Особливе місце в програмах обробки інформації займають операції кодування. Перетворення інформації, в результаті якого забезпечується зміна обсягу пам'яті, займаної даними, називається кодуванням. На практиці кодування завжди використовується для зменшення обсягу пам'яті, так як економія пам'яті ЕОМ має велике значення в інформаційних системах. Крім того, кодування можна розглядати як криптографічний метод обробки інформації.

2.1 Симетричні криптосхеми

У цій методології і для шифрування, і для розшифровки відправником і отримувачем застосовується один і той же ключ, про використання якого вони домовилися до початку взаємодії. Якщо ключ не був скомпрометований, то при розшифровці автоматично виконується аутентифікація відправника, так як тільки відправник має ключ, за допомогою якого можна зашифрувати інформацію, і тільки одержувач має ключ, за допомогою якого можна розшифрувати інформацію. Так як відправник і одержувач – єдині люди, які знають цей симетричний ключ, при компрометації ключа буде скомпрометовано тільки взаємодія цих двох користувачів. Проблемою, яка буде актуальна і для інших криптосистем, є питання про те, як безпечно поширювати симетричні (секретні) ключі.

Алгоритми симетричного шифрування використовують ключі не дуже великий довжини і можуть швидко шифрувати великі обсяги даних.

Порядок використання систем з симетричними ключами:

1. Чи безпечно створюється, поширюється і зберігається симетричний секретний ключ.

2. Відправник створює електронний підпис за допомогою розрахунку хеш-функції для тексту і приєднання отриманого рядка до тексту

3. Відправник використовує швидкий симетричний алгоритм шифрування – розшифровки разом з секретним симетричним ключем до отриманого пакету (тексту разом з приєднаною електронним підписом) для отримання зашифрованого тексту. Неявно таким чином виробляється аутентифікація, так як тільки відправник знає симетричний секретний ключ і може зашифрувати цей пакет. Тільки одержувач знає симетричний секретний ключ і може розшифрувати цей пакет.

4. Відправник передає зашифрований текст. Симетричний секретний ключ ніколи не передається по незахищених каналах зв'язку.

5. Одержувач використовує той же самий симетричний алгоритм шифрування – розшифровки разом з тим же самим симетричним ключем (який вже є у одержувача) до зашифрованого тексту для відновлення вихідного тексту і електронного підпису. Його успішне відновлення аутентифікує когось, хто знає секретний ключ.

6. Одержувач відокремлює електронний підпис від тексту.

7. Одержувач створює іншу електронний підпис за допомогою розрахунку хеш функції для отриманого тексту.

8. Одержувач порівнює дві цих електронних підписи для перевірки цілісності повідомлення (відсутності його спотворення).

2.2 Системи з відкритим ключем

У цій методології ключі для шифрування і розшифровки різні, хоча і створюються разом. Один ключ робиться відомим всім, а інший тримається в таємниці. Дані, зашифровані одним ключем, можуть бути розшифровані тільки іншим ключем.

Всі асиметричні криптосистеми є об'єктом атак шляхом прямого перебору ключів, і тому в них повинні використовуватися набагато довші ключі, ніж ті, які використовуються в симетричних криптосистемах, для забезпечення еквівалентного рівня захисту. Це відразу ж позначається на обчислювальних ресурсах, необхідних для шифрування, хоча алгоритми шифрування на еліптичних кривих можуть пом'якшити цю проблему.

Для того щоб уникнути низької швидкості алгоритмів асиметричного шифрування, генерується тимчасовий симетричний ключ для кожного повідомлення і тільки він шифрується асиметричними алгоритмами. Саме повідомлення шифрується з використанням цього тимчасового сеансового ключа і алгоритму шифрування / розшифрування, раніше описаного. Потім цей сеансовий ключ шифрується за допомогою відкритого асиметричного

ключа одержувача і асиметричного алгоритму шифрування. Після цього цей зашифрований сеансовий ключ разом із зашифрованим повідомленням передається одержувачу.

Одержувач використовує той же самий асиметричний алгоритм шифрування і свій секретний ключ для розшифровки сеансового ключа, а отриманий сеансовий ключ використовується для розшифровки самого повідомлення.

В асиметричних криптосистемах важливо, щоб сеансу і асиметричні ключі можна було порівняти щодо рівня безпеки, який вони забезпечують.

Якщо використовується короткий сеансовий ключ (наприклад, 40-бітовий DES), то не має значення, наскільки великі асиметричні ключі. Асиметричні відкриті ключі уразливі до атак прямим перебором почасти через те, що їх важко замінити. Якщо атакуючий дізнається секретний асиметричний ключ, то буде скомпрометований не тільки поточне, але і всі наступні взаємодії між відправником і отримувачем.

Порядок використання систем з асиметричними ключами:

1. Чи безпечно створюються і поширюються асиметричні відкриті і секретні ключі. Секретний асиметричний ключ передається його власнику. Відкритий асиметричний ключ зберігається в базі даних і адмініструється центром видачі сертифікатів. Мається на увазі, що користувачі повинні вірити, що в такій системі проводиться безпечне створення, розподіл і адміністрування ключами. Більш того, якщо творець ключів і особа або система, адмініструють їх, не одне і те ж, то кінцевий користувач повинен вірити, що творець ключів насправді знищив їх копію.

2. Створюється електронний підпис тексту за допомогою обчислення його хеш-функції. Отримане значення шифрується з використанням асиметричного секретного ключа відправника, а потім отримана рядок

символів додається до передається тексту (тільки відправник може створити електронний підпис).

3. Створюється секретний симетричний ключ, який буде використовуватися для шифрування тільки цього повідомлення або сеансу взаємодії(Сеансовий ключ), потім за допомогою симетричного алгоритму шифрування / розшифрування і цього ключа шифрується вихідний текст разом з доданою до нього електронним підписом – виходить зашифрований текст (шифр-текст).

4. Тепер потрібно вирішити проблему з передачею сеансового ключа одержувачу повідомлення.

5. Відправник повинен мати асиметричний відкритий ключ центру видачі сертифікатів. Перехоплення незашифрованих запитів на отримання цього відкритого ключа є поширеною формою атаки. Може існувати ціла система сертифікатів, що підтверджують справжність відкритого ключа.

6. Відправник запитує у центру сертифікатів асиметричний відкритий ключ одержувача повідомлення. Цей процес вразливий до атаки, в ході якої атакуючий втручається у взаємодію між відправником і отримувачем і може модифікувати трафік, що передається між ними. Тому відкритий асиметричний ключ одержувача "підписується" у центру сертифікатів. Це означає, що центр сертифікатів використовував свій асиметричний секретний ключ для шифрування асиметричного відкритого ключа одержувача. Тільки центр сертифікатів знає асиметричний секретний ключ, тому є гарантії того, що відкритий асиметричний ключ одержувача отриманий саме від нього.

7. Після отримання асиметричний відкритий ключ одержувача розшифровується за допомогою асиметричного відкритого ключа і алгоритму асиметричного шифрування / розшифрування. Природно, передбачається, що центр сертифікатів повинен був скомпрометований. Якщо ж він виявляється скомпрометованим, то це виводить з ладу всю

мережу його користувачів. Тому можна і самому зашифрувати відкриті ключі інших користувачів, але де впевненість в тому, що вони не скомпрометовані?

8. Тепер шифрується сеансовий ключ з використанням асиметричного алгоритму шифрування-розшифровки і асиметричного ключа одержувача (отриманого від центр сертифікатів і розшифрованого).

9. Зашифрований сеансовий ключ приєднується до зашифрованого тексту (який включає в себе також додану раніше електронний підпис).

10. Весь отриманий пакет даних (зашифрований текст, в який входить крім вихідного тексту його електронний підпис, і зашифрований сеансовий ключ) передається одержувачу. Так як зашифрований сеансовий ключ передається по незахищеній мережі, він є очевидним об'єктом різних атак.

11. Одержувач виділяє зашифрований сеансовий ключ з отриманого пакету.

12. Тепер одержувачу потрібно вирішити проблему з розшифровкою сеансового ключа.

13. Одержувач повинен мати асиметричний відкритий ключ центру видачі сертифікатів.

14. Використовуючи свій секретний асиметричний ключ і той же самий асиметричний алгоритм шифрування одержувач розшифровує сеансовий ключ.

15. Одержувач застосовує той же самий симетричний алгоритм шифрування- розшифровки і розшифрований симетричний (сеансовий) ключ до зашифрованого тексту і отримує початковий текст разом з електронним підписом.

16. Одержувач відокремлює електронний підпис від вихідного тексту.

17. Одержувач запитує в центр сертифікатів асиметричний відкритий ключ відправника.

18. Як тільки цей ключ отриманий, одержувач розшифровує його за допомогою відкритого ключа центр сертифікатів і відповідного асиметричного алгоритму шифрування-розшифровки.

19. Потім розшифровується хеш-функція тексту з використанням відкритого ключа відправника і асиметричного алгоритму шифрування-розшифровки.

20. Повторно обчислюється хеш-функція отриманого вихідного тексту.

21. Дві ці хеш-функції порівнюються для перевірки того, що текст не був змінений.[3]

2.3 Як вибрати криптографічний алгоритм

Коли заходить мова про вибір хорошого криптографічного алгоритму, у що вибирає, як правило, є кілька можливостей:

Можна скористатися відомим алгоритмом, порівняно давно опублікованим в спеціальному виданні з проблем криптографії. Якщо ніхто поки не повідомив про те, що зумів розкрити цей алгоритм, значить, він вартий того, щоб звернути на нього увагу.

Можна довіритися відомій фірмі, що спеціалізується на продажу засобів шифрування. Навряд чи ця фірма буде ризикувати своїм добрим ім'ям, торгуючи нестійкими криптографічними алгоритмами.

Можна звернеться до незалежного експерта. Швидше за все, він зможе об'єктивно оцінити достоїнства і недоліки різних криптографічних алгоритмів.

Можна звернеться за підтримкою до відповідного урядове відомство. Навряд чи уряд буде вводити своїх громадян в оману, даючи їм помилкові поради щодо стійкості того чи іншого криптографічного алгоритму.

Можна спробувати створити власний криптографічний алгоритм. Мало хто зацікавлений сам себе обманювати. Чим чорт не жартує: а раптом ви володієте видатними здібностями в області криптографії?

У всіх перерахованих можливості є свої суттєві вади. Покладатися тільки на одну фірму, на одного експерта або на одне відомство не зовсім розумно. Багато людей, які називають себе незалежними експертами, мало розуміють в криптографії. Більшість фірм, що виробляють засоби шифрування, нітрохи не краще. І навіть якщо ви геній в криптографії, нерозумно використовувати криптографічний алгоритм власного винаходу без того, щоб його всебічно проаналізували і протестували досвідчені криптологи.

Тому найкращою представляється перша з перерахованих можливостей. Даний підхід до оцінки стійкості криптографічних алгоритмів можна було б визнати ідеальним, якби не один його недолік. На жаль, нічого невідомо про результати криптоаналітичних досліджень цих алгоритмів, які, без сумніву, активно велися в минулому і продовжують також активно проводиться у всьому світі численними співробітниками різних урядових відомств, до компетенції яких входять криптологічні вишукування. Ці відомства, швидше за все, набагато краще фінансуються, ніж академічні інститути, провідні аналогічні дослідження. Та й почали вони займається криптологією значно раніше, ніж вчені, які не мають військових звань, і фахівці з приватних фірм. Тому можна припустити, що військові знайшли набагато більш прості способи розтину відомих шифрів, ніж ті, які винайдені за межами суворо охоронюваних будівель надсекретних урядових відомств.

Ну і нехай. Навіть якщо вас заарештують і як доказ конфіскують у вас жорсткий диск з файлами, зашифрованими по DES-алгоритму, то навряд чи криптоаналітики, які перебувають на державній службі, прийдуть на судове засідання, щоб клятвено підтвердити, що дані для вашого обвинувального

висновку отримані шляхом дешифрування конфіскованих файлів. Той факт, що можна розкривати якийсь конкретний криптографічний алгоритм, часто є значно більшим секретом, ніж інформація, отримана шляхом розтину цього алгоритму.

Найкраще виходити з припущення, що полягає в тому, що АНБ, ФАПСИ і вже з ними можуть прочитати будь-яке повідомлення, яке вони побажають прочитати. Однак ці відомства не в змозі читати всі повідомлення, з вмістом яких хочуть ознайомитися. Головною причиною є обмеженість в коштах, що виділяються урядом на криптоаналіз. Інша розумне припущення полягає в тому, що компетентним органам набагато легше отримати доступ до зашифрованої інформації за допомогою грубої фізичної сили, ніж шляхом витончених, але дуже трудомістких математичних викладок, що призводять до розкриття шифру.

У будь-якому випадку набагато надійніше користуватися відомим криптографічним алгоритмом, який придуманий вже досить давно і який зумів вистояти проти численних спроб розкрити його, зроблених авторитетними криптології. [2]

2.4 Висновки до розділу 2

Історично першим завданням криптографії було захист переданих текстових повідомлень від несанкціонованого читання їх змісту, що відображено в назві цієї дисципліни. Цей захист ґрунтується на використанні "таємної мови", відомої лише відправнику та одержувачу, всі методи шифрування – лише подальший розвиток цієї філософської ідеї;

Із ускладненням інформаційних взаємодій у людському суспільстві виникають і продовжують виникати нові завдання щодо їх захисту. Деякі з них були вирішені в контексті криптографії, що вимагало розробки принципово нових підходів та методів.

РОЗДІЛ 3
РОЗРОБКА САЙТУ ШИФРУВАННЯ

3.1 Формування алгоритму роботи сайту

Основою кожного проекту (верстка сайту, написання програмного забезпечення) є схема його алгоритму роботи (Рис. 3.1).

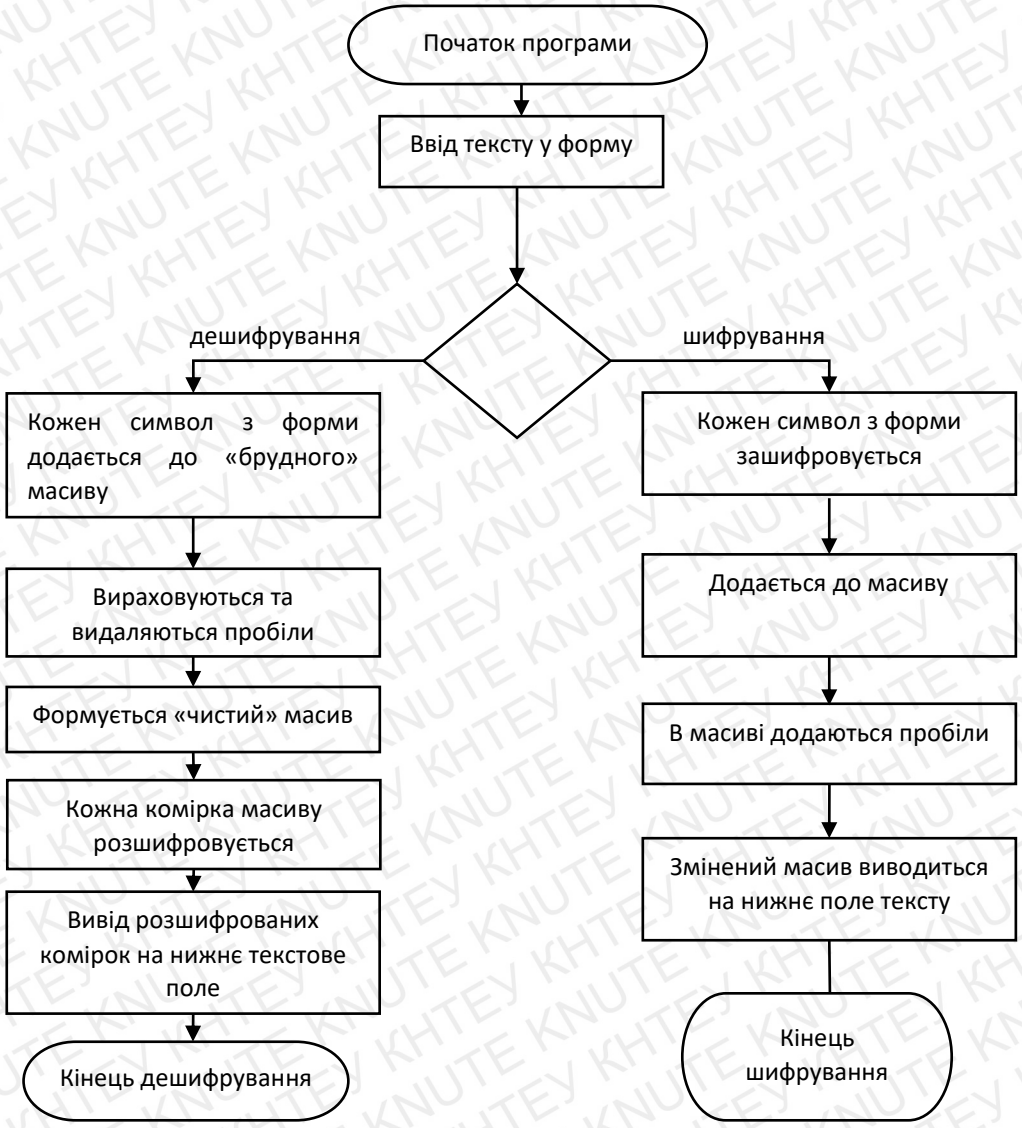

Рис. 3.1 Алгоритм роботи сайту

					КНТЕУ 121 06-13.БР			
Зм.	Аркуш	№ докум	Підпис	Дата				
Зав. кафедри		Криворучко О.В.			Розробка криптографічного алгоритму прихованого листування	Стадія	Аркуш	Аркушів
Керівник		Криворучко О.В.				РЗ	20	26
Гарант		Цензура М.О.				Факультет інформаційних технологій, 4 курс, 6 група		
Розроб.		Лучко М.М.			Розробка сайту шифрування			

3.2 Побудова інтерфейсу

Для більшої доступності було вирішено розробити проект у Веб-просторі, за допомогою HTML, CSS та JavaScript. HTML – це мова для розмітки веб-сторінок, яка використовується на всіх сайтах глобальної мережі. CSS – таблиці стилів, формальна мова зовнішнього вигляду документа який написаний з використанням мови розмітки, в даному випадку HTML.

На сайті розміщено два текстових поля за допомогою тегу «textarea»(верхній для запису тексту, нижній для виведення результату). Кнопки для шифрування, дешифрування тексту та для очистки текстових полів. Кнопки реалізовані за допомогою тегу «button». Також присутня маленька підказка, яка розміщена знизу тегом «span». Всі елементи включені в тег «div» для простішого управляння розміщенням на сторінці сайту.

```
<div id="topForm">
        <textarea class="txta" id="content" placeholder="Type text here"></textarea>
</div>
<div id="centralForm">
        <div align="center">
                <button id="shifr" onclick="scriptFunction()">Script</button>
                <button id="unShifr" onclick="deScriptFunction()">DeScript</button>
                <button id="clear" onclick="clearFunction()">Clear</button>
        </div>
</div>
<div id="botForm">
        <textarea id="content1" disabled="true" class="txta" placeholder="Take the
result"></textarea>
</div>
<div id="anim">
        <span class="tooltip" data-tooltip="Write the text in the box at the top, from the bottom
get the cipher text.">?</span>
</div>
<div id="madeBy">
        Made by student KNUTE FIT 4-6 Luchko Maxim
</div>
```

Далі слід зробити сайт більш привабливим, для цього використано CSS. Текстові поля, зроблені в стилі схожому з сайтом «Перекладач» від Google.

Кнопкам було призначено зелений колір, змінений шрифт та розмір, в такому ж стилі зроблена підказка. У фінальному вигляді маємо результат зображений на Рис. 3.2.

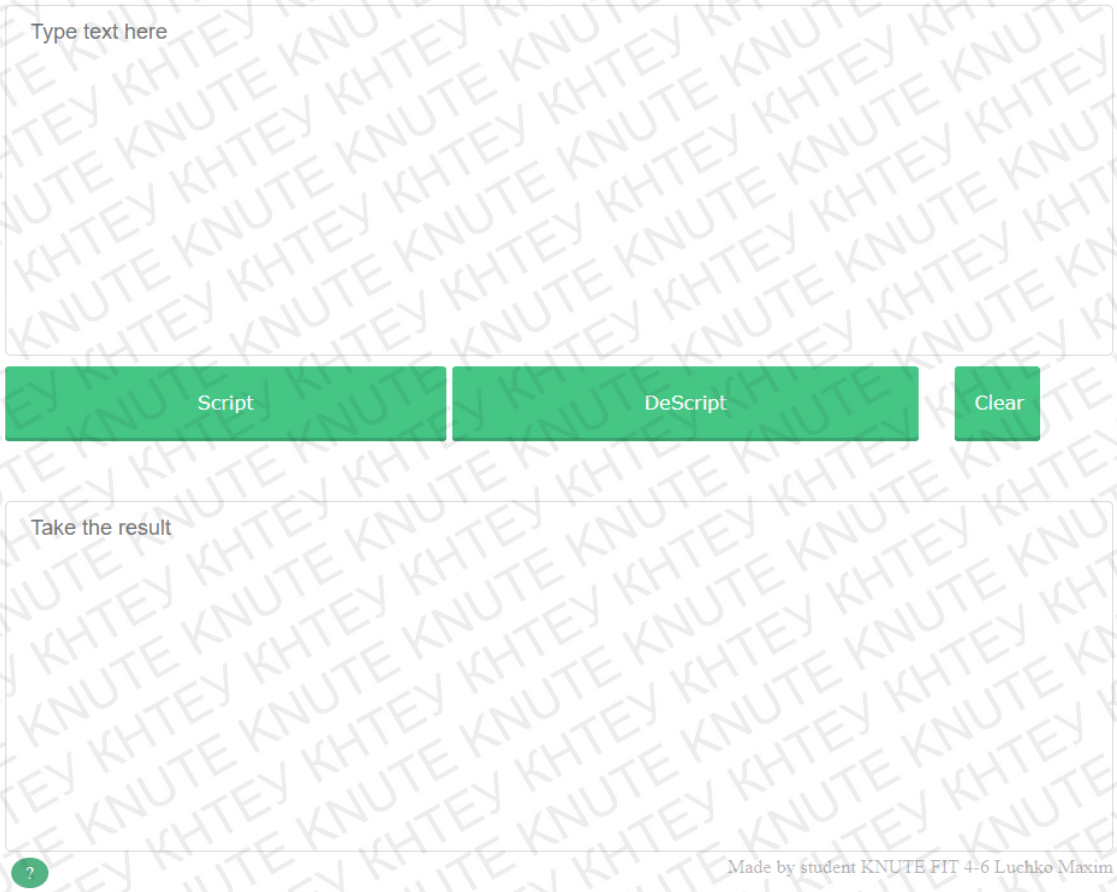

Рис. 3.2 Інтерфейс сайту

3.3 Функціональна частина сайту

Сучасний JavaScript - це «безпечна» мова програмування. Він не надає низькорівневий доступ до пам'яті або процесору, тому що спочатку був створений для браузерів, які не потребують цього.

Функція шифрування працює наступним чином:

1. Змінна this.txt приймає значення ввід текстового поля в який записується текст для шифрування
2. Далі кожен символ конвертується у числове значення, шифрується та присвоюється змінній change

3. Змінна change додається до масиву this.arr

4. В масиві this.arr додаються пробіли для розуміння де починається новий зашифрований символ

5. Функція шифрування закінчується тим, що готовий масив з зашифрованими символами та пробілами записується до текстового поля знизу.

```
script(){
      document.getElementById('content1').value = ""; //clear bottTextArea
    for (let i = 0; i < this.txt.length; i++) {
      let change = this.txt.charCodeAt(i)*2;//script value of textArea
      this.arr.push(change); //push changed value to main array
    }
    for (let i = 1; i in this.arr; i+=2) {
      let spac = ' ';
      this.arr.splice(i, 0, spac); //add spaces to each second index
    }
    for (let i = 0; i in this.arr; i++) {
      document.getElementById('content1').value += this.arr[i]; //print array of changed values to bottom textArea
    }
}
```

Функція дешифрування значно складніше:

1. Формуються декілька змінних, які в подальшому будуть роз’яснені

2. З текстового поля де вводяться дані, зашифрований текст додається до «брудного масиву», який подальшому буде змінюватися

3. Далі іде формування «чистого масиву». Його побудова заключається в видаленні пробілів, та злиття символів в одну комірку.

4. Для цього створюємо switch функцію, в якій залежно від значення змінної count (змінна яка вказує на індекс пробілу) формується комірка «чистого масиву».

5. Формування комірки проходить наступним чином

   a. кожному елементу з індексом меншим ніж у змінної count присвоюється змінна «num»

b. значення змінної конвертується у рядок(тип змінної) та додаються з іншими

c. Значення яке будо отримано в процесі злиття змінних «num» додається до «чистого масиву»

6. Далі іде процес видалення використаних елементів «брудного масиву», та початок нової ітерації циклу формування «чистого масиву»

7. Після створення «чистого масиву» кожна його комірка дешифрується, додається до масиву «this.arr» та виводиться на екран.

Очищення текстових полів, це найпростіша функція в даній роботі, виконується за допомогою присвоєння порожнього значення обидвом текстовим полям.

Програмний код описаний вище, зазначений у Додатку А.

3.4 Висновки до розділу 3

За допомогою новітніх HTML для верстки сайтів, CSS для зовнішнього вигляду сайту та JavaScript для функціоналу. Даний сайт побудований таким чином, щоб надати користувачу уніфікований інтерфейс для шифрування тексту.

За допомогою декількох функціональних елементів:

1. текстових полів для введення та виведення тексту;
2. кнопок для взаємодії

Та за допомогою функцій, для шифрування та дешифрування в результаті маємо сайт який може шифрувати текст.

Криптографія дозволяє передавати інформацію в захищеній формі, забезпечуючи безпеку, конфіденційність і цілісність даних. При захисті конфіденційної інформації криптографія сприяє високому рівню безпеки персональних даних окремих людей і груп.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

З кожним роком комп'ютерна інформація відіграє все більш важливу роль в нашому житті, і все більшої актуальності набувають проблеми її захисту. Спочатку криптографія використовувалася тільки для безпечного зберігання документів. Користувач зашифровував їх, роблячи недоступними для зловмисників. Сьогодні область застосування криптографії істотно розширилася.

Криптографія – це сукупність методів захисту інформаційних взаємодій від відхилень від їх нормального, регулярного потоку, спричинених шкідливими діями різних суб'єктів. Ці методи засновані на алгоритмах перетворення секретної інформації, включаючи алгоритми, які насправді не є секретними, але використовують секретні параметри.

Практичне застосування криптографії стало невід'ємною частиною життя сучасного суспільства – її використовують в таких галузях, як електронна комерція, електронний документообіг (включаючи цифрові підписи), телекомунікації та інших.

За допомогою новітніх HTML для верстки сайтів, CSS для зовнішнього вигляду сайту та JavaScript для функціоналу. Даний сайт побудований таким чином, щоб надати користувачу уніфікований інтерфейс для шифрування тексту. А саме на виході маємо сайт, за допомогою якого користувач має можливість зашифрувати будь-який текст.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Wang and Ming Hu «Timing evaluation of the known cryptographic algorithms» 2009 International Conference on Computational intelligence and security.

2. A.Nath, S.Ghosh, M.A.Mallik «Key cryptography using random key generator»: Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239-244.

3. Neal Koblitz, «A Course in Number Theory and Cryptography»: Second Edition Published by Springer, Vol-4,P-87-94.

4. David Kahn. The Codebreakers – The Story of Secret Writing. – New York: Charles Scribner's Sons, 1967. – 473 с. – ISBN 0-684-83130-9.

5. Richard A. Mollin. Codes: The Guide to Secrecy From Ancient to Modern Times. – 1 edition. – Chapman & Hall/CRC, 2005. – 679 p. – ISBN 1-58488-470-3.

6. Вербіцький О. В. Вступ до криптології. – Л. : ВНТЛ, 1998. – 248 с.

7. І. Н. Войцехівська. Криптографія // Енциклопедія історії України : у 10 т. / редкол.: В. А. Смолій (голова) та ін. ; Інститут історії України НАН України. – К. : Наук. думка, 2009. – Т. 5 : Кон – Кю. – С. 390. – 560 с. : іл. – ISBN 978-966-00-0855-4.

8. Simon Singh, «The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography» - Fourth Estate – 1999 - 416 p – ISBN 978-1-85702-879.

					КНТЕУ 121 06-1 3.БР		
Зм.	Аркуш	№ докум	Підпис	Дата			
Зав. кафедри		Криворучко О.В.			Розробка криптографічного алгоритму прихованого листування	Стадія	Аркуш	Аркушів
Керівник		Криворучко О.В.				СД	26	26
Гарант		Цензура М.О.				Факультет інформаційних технологій, 4 курс, 6 група		
Розроб.		Лучко М.М..			Список використаних джерел			

ДОДАТКИ

Додаток А

```
deScript(){
      document.getElementById('content1').value = "";
      let arrayToDescript = [];
      let triger = ' ';
      let num1 = '';
      let num2 = '';
      let num3 = '';
      let num4 = '';
      for (let i = 0; i < this.txt.length; i++) {
        arrayToDescript.push(this.txt[i]);  //push values from textArea to main array
      }
let clearArr = [];
      let sum;
      let count;
      for(let i = 0; i < arrayToDescript.length+4; i++){
        count = arrayToDescript.indexOf(triger);
        if(count == -1){
          count = arrayToDescript.length; //WORKS!!!!!!
        }
        console.log('count =' + count);
        switch (count) {
          case 2:
          num1 = arrayToDescript[0].toString(); //convet value of mainArray to string
          num2 = arrayToDescript[1].toString();
          sum = num1+num2;
          clearArr.push(sum);
          break;
          case 3:
          num1 = arrayToDescript[0].toString(); //convet value of mainArray to string
          num2 = arrayToDescript[1].toString();
          num3 = arrayToDescript[2].toString();
          sum = num1+num2+num3;
          clearArr.push(sum);
          break;
          case 4:
          num1 = arrayToDescript[0].toString(); //convet value of mainArray to string
          num2 = arrayToDescript[1].toString();
          num3 = arrayToDescript[2].toString();
          num4 = arrayToDescript[3].toString();
          sum = num1+num2+num3+num4;
          clearArr.push(sum);
          break;
          case -1:
          if (arrayToDescript.length == 2) {
            num1 = arrayToDescript[0].toString(); //convet value of mainArray to string
            num2 = arrayToDescript[1].toString();
            sum = num1+num2;
            clearArr.push(sum);
```

```
            }
            if (arrayToDescript.length == 3) {
                num1 = arrayToDescript[0].toString(); //convet value of mainArray to string
                num2 = arrayToDescript[1].toString();
                num3 = arrayToDescript[2].toString();
            }
            if (arrayToDescript.length == 4) {
                num1 = arrayToDescript[0].toString(); //convet value of mainArray to string
                num2 = arrayToDescript[1].toString();
                num3 = arrayToDescript[2].toString();
                num4 = arrayToDescript[3].toString();
                sum = num1+num2+num3+num4;
                clearArr.push(sum);
            }
            break;
        }
        arrayToDescript.splice(0,count+1);
        if (arrayToDescript[i] == ' ') {
            i = 0;
        }
    }

    for (let j = 0; j < clearArr.length; j++) {
        let change = String.fromCharCode(clearArr[j]/2); //decsript value of clearArray
        this.arr.push(change);
        console.log(change);
        document.getElementById('content1').value += this.arr[j];
    }
  }
}
```