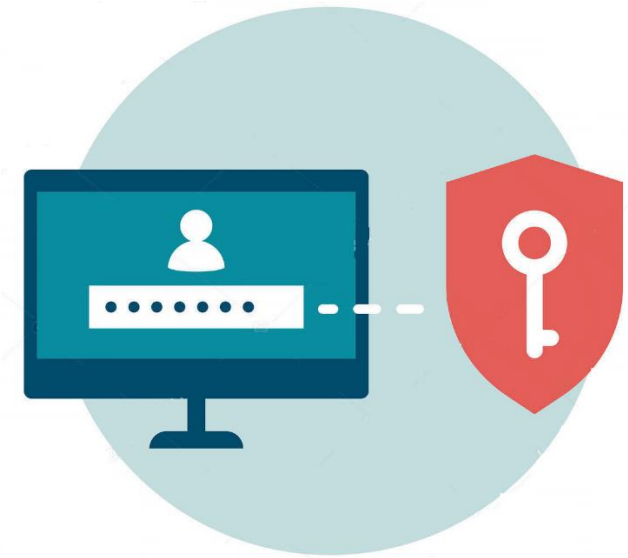
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ ДЕРЖАВНИЙ ПОЛІТЕХНІЧНИЙ КОЛЕДЖ

Для спеціальностей:
123 Комп'ютерна інженерія

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт
з дисципліни:

“ Надійність, діагностика та експлуатація комп'ютерних систем та мереж ”



Харків 2019

Методичні вказівки до виконання лабораторних робіт з дисциплін: “ Надійність, діагностика та експлуатація комп'ютерних систем та мереж” для студентів освітньо-професійної програми «Обслуговування комп′ютерних систем і мереж» спеціальності 123 «Комп’ютерна інженерія»

Укладачі: Величко М.В А.А. Дігтяр - Харків:ХДПК, 2019, 31 с.

Затверджено на засіданні циклової комісії інформаційних технологій
Протокол від _____2019 р. №_____

Голова циклової комісії _____М.М. Бочарніков
“_____” _____ _____ року

Схвалено методичною радою коледжу
Протокол від _____2019 р. №_____

Голова методичної ради _____
“_____” _____ 2019
року

Лабораторна робота №1
Розрахунок показників надійності пристрою ЕОТ.

Цілі та задачі

дослідити методи розрахунків показників надійності пристрою ЕОТ

Теоретична частина

В основу розрахунку на надійність покладено принцип визначення показника надійності системи по характеристикам надійності комплектуючих елементів.

При розрахунку робиться два припущення. Перше це те що відмови елементів є статистично незалежними, що дає відносно реально існуючу систему оцінки і друге це те що систему розглядаємо як послідовну тобто відмова одного елементу схеми веде до відмови всієї системи.

Вихідними даними для розрахунку є значення інтенсивності відмови всіх ЕРЕ і елементів конструкції.

Середній час напрацювання на відмову визначимо за формулою:

$$T_{ср.с} = \frac{1}{\sum_{j=1}^{m} \lambda_j \cdot N_j}$$

де:

m – кількість найменування радіоелементів і елементів конструкції приладу;

λ_j – величина інтенсивності відмови j-го радіоелементу, елементу конструкції з урахуванням заданих для нього умов експлуатації: коефіцієнт електричного навантаження, температури, вологості, технічних навантажень і т. ін.

N_j – кількість радіоелементів, елементів конструкції j-го найменування.

$\lambda_\Sigma = \sum_{j=1}^{m} \lambda_j \cdot N_j$ - сумарне значення інтенсивності відмов.

Таблиця 1

№	Тип елементу	$\lambda_0, 10^{-6}, 1/год$	α_j	$\kappa_{\lambda 1}$	$\kappa_{\lambda 2}$	$\kappa_{\lambda 3}$	$\kappa_н$
1	Інтегральна мікросхема	0.01-2.5	0.35	1.04	1.0	1.2	0.5
2	Напівпровідникові імпульсні діоди	0.2-1.0	1.04	1.04	1.0	1.2	0.7
3	Напівпровідникові випрямляючи діоди	0.35-0.9	1.04	1.04	1.0	1.2	0.7
4	Транзистори середньої потужності високочастотні	1.3-2.5	0.4	1.04	1.0	1.2	0.5
5	Транзистори низької потужності низькочастотні	0.5-1.2	0.4	1.04	1.0	1.2	0.5
6	Резистори постоялого опору – метало плівкові	0.004-0.4	0.6	1.04	1.0	1.2	0.5
7	Конденсатори постійної ємності - керамічні	0.04-0.7	1.10	1.04	1.0	1.2	0.7
8	Конденсатори постійної ємності – метало паперові	0.003-0.37	1.10	1.04	1.0	1.2	0.7
9	Конденсатори постійної ємності – метало плівкові	0.003-1.7	1.10	1.04	1.0	1.2	0.7
10	Трансформатори живлення	0.5-7	1.20	1.04	1.0	1.2	0.7
11	Дроселі	0.05-1.0	1.20	1.04	1.0	1.2	0.8
12	Друкована плата	0.1	-	1.04	1.0	1.2	-
13	Монтажні елементи	0.02-0.4	-	1.04	1.0	1.2	-
14	Пайка з'єднуюча	0.0002-0.04	-	1.04	1.0	1.2	-
15	Дроти з'єднуючи	0.01-0.12		1.04	1.0	1.2	-
16	Плавкий запобіжник	0.3-0.8	-	1.04	1.0	1.2	-
17	Корпус	0.03-2.0	-	1.04	1.0	1.2	-
18	Двигун постійного струму	8-10	-	1.07	1.0	1.2	-

$$\lambda_\Sigma = (0.001 \cdot 0.35 + 0.2 \cdot 1.04 + 0.35 \cdot 1.04 + 1.3 \cdot 0.4 + 0.5 \cdot 0.4 + 0.004 \cdot 0.6 + 0.04 \cdot 1.1 + 0.003 \cdot 1.1 +$$
$$+ 0.003 \cdot 1.1 + 0.5 \cdot 1.2 + 0.05 \cdot 1.2 + +0.1 + 0.0002 + 0.01 + 0.3 + 0.03 + 8) \cdot 10^{-6} = 10.46 \cdot 10^{-6}\, 1/год.$$

з урахуванням поправочних коефіцієнтів визначимо середній час напрацювання на відмову

$$T_{ср.с} = \frac{1}{1.4 \cdot 10.46 \cdot 10^{-6}} = 68290\, год.$$

Визначимо вірогідність безвідмовної роботи за формулою:

$$p_c(t) = \exp(-t\lambda_\Sigma) = 0.81.$$

Отримане значення напрацювання на відмову більше часу яке було задане, 27000 годин, що гарантує надійну роботу розроблювального пристрою.

Хід роботи:

1. Вивчити теоретичний матеріал.

2. Одержати індивідуальну принципову схему пристрою ЕОТ та дані про умови експлуатації пристрою.

3. Обчислити сумарну інтенсивність відказів пристрою.

4. Обчислити напрацювання на відмову пристрою.

5. Обчислити ймовірність безвідмовної роботи пристрою на заданому проміжку часу.

Вимоги до написання звіту:

1 Вкажіть тему та мету лабораторної роботи.

2. Складіть звіт по лабораторній роботі за планом вказаним у ході роботи.

3 Дайте відповіді на контрольні запитання.

Контрольні запитання:

1. Яке основне завдання теорії надійності?
2. Характеризуйте поняття «надійність».
3. Назвіть кількісну характеристику надійності ЕОТ.

Лабораторна робота №2.
Порівняння даних за допомогою хешу

Цілі та задачі

Використати програму хешування для перевірки цілісності даних.

Довідкова інформація/Сценарій

Важливо виявляти, пошкодження або підмінену дані. Програма хешування може бути використана для перевірки, чи змінилися дані, чи вони залишилися незмінними. Програма хешування виконує хеш-функцію на даних або файлі, та повертає значення (як правило, набагато коротше) . Є багато різних хеш-функцій, деякі дуже прості, а деякі дуже складні. Коли однакова хеш-функція виконується з однаковими даними, то значення, що повертається, завжди однакове. Якщо з даними відбуваються будь-які зміни, то повернене значення хешу буде іншим.

Примітка: Для встановлення Windows програм вам знадобляться відповідні привілеї та деякі знання.

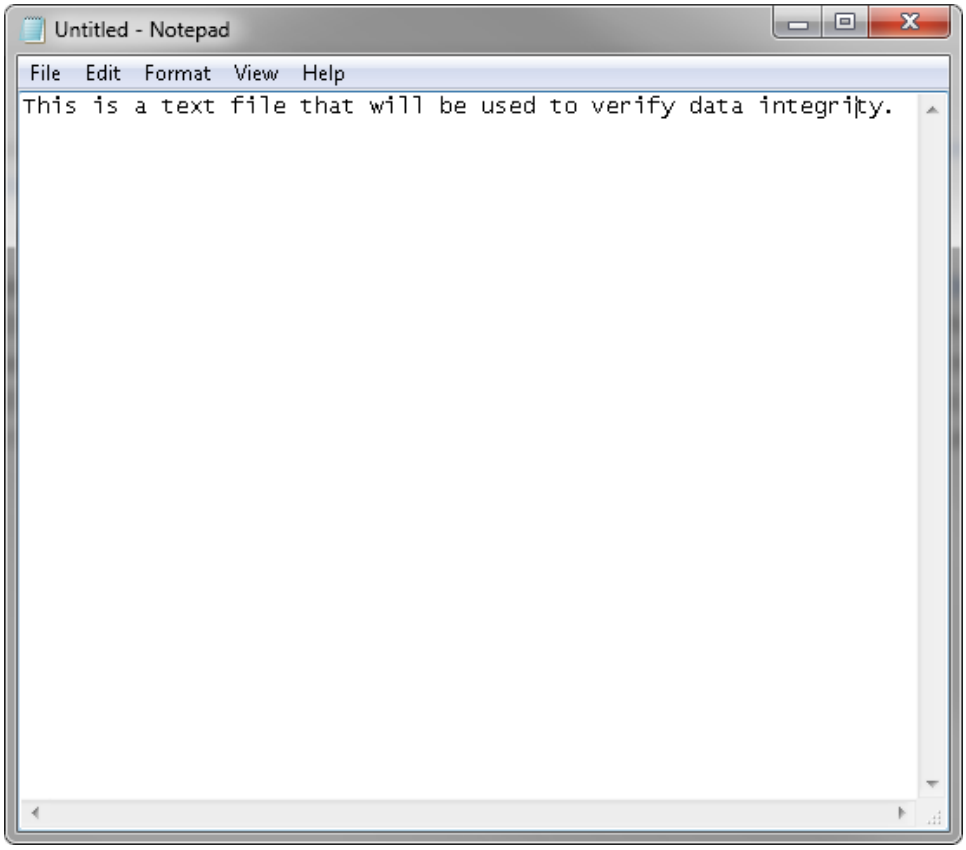
Необхідні ресурси

- ПК з доступом до Інтернету

Крок 1: Створіть текстовий файл

1) Знайдіть на своєму комп'ютері програму Блокнот (Notepad) і відкрийте її.

2) Введіть текст у програмі.



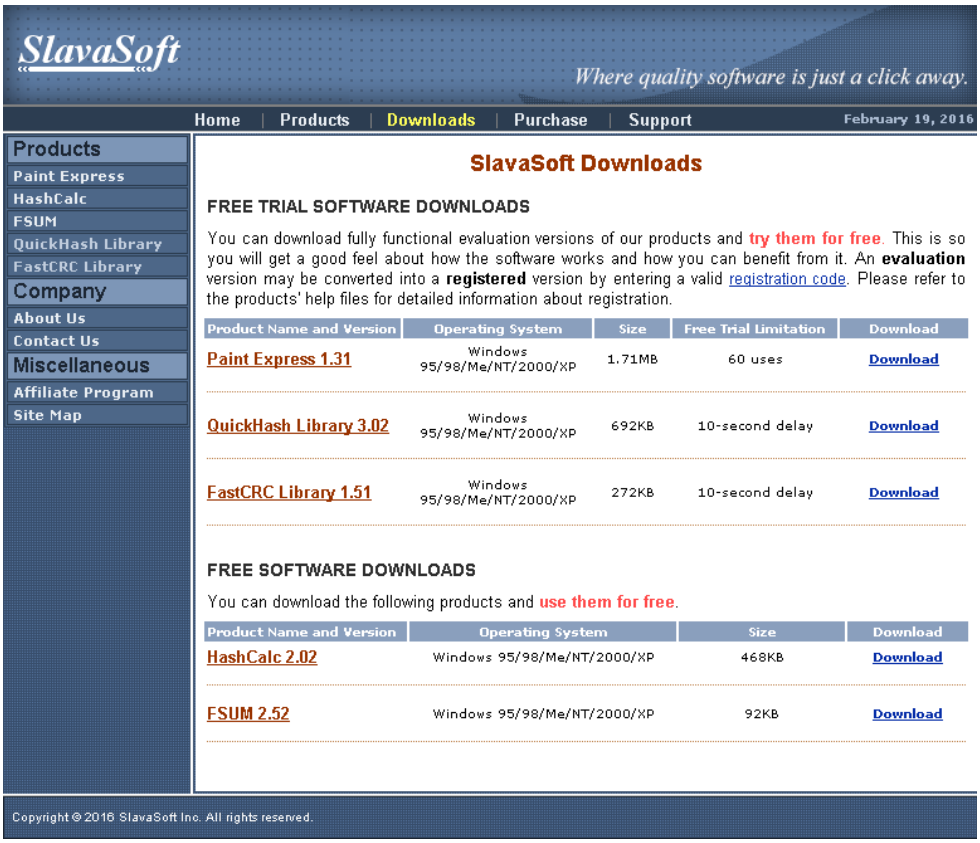
3) Виберіть Файл> Зберегти (File > Save).

4) Перейдіть до Робочого столу

5) ВведітьHash у поле Ім'я файлу: (File name:)і натисніть Зберегти (Save).

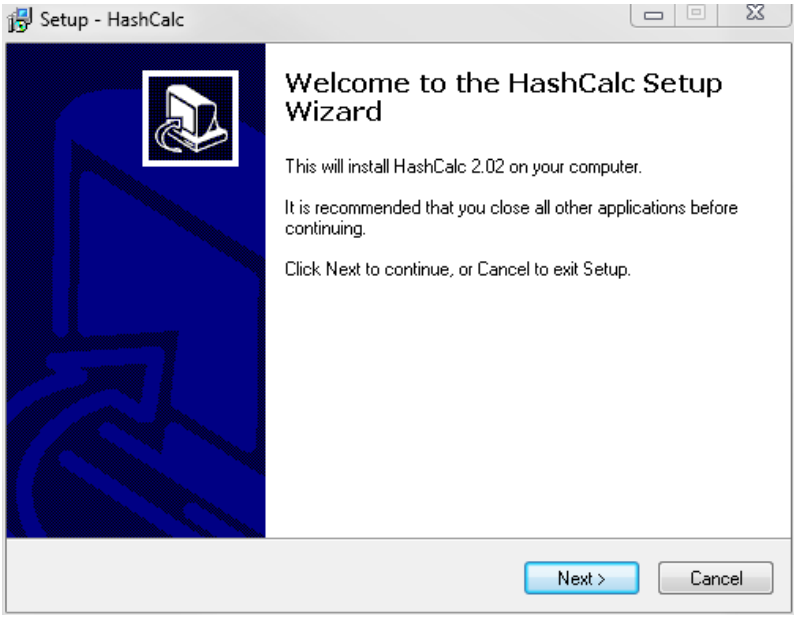
Крок 2: Встановіть HashCalc

1) Відкрийте веб-браузер і перейдіть за посиланням http://www.slavasoft.com/download.htm.



2) Натисніть Завантажити (Download) у рядку HashCalc.

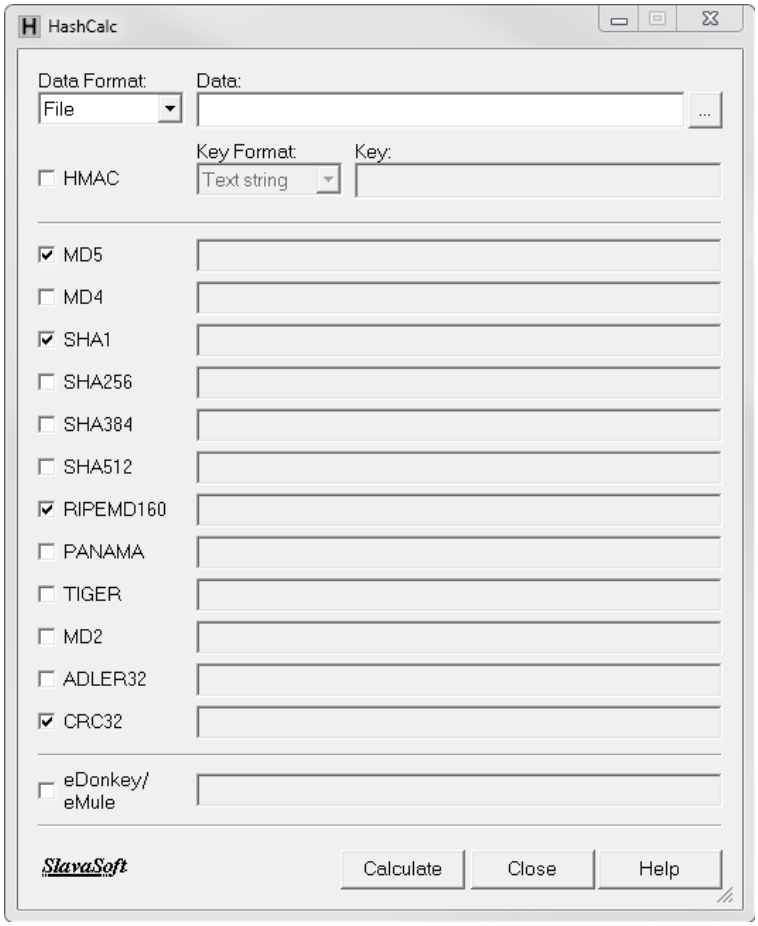
3) Відкрийте hashcalc.zip файл та запустіть файл setup.exe всередині.



4) Дотримуйтесь вказівок Майстра установки (Installation wizard), щоб встановити HashCalc.

5) Натисніть кнопку **Готово (Finish)** на останньому екрані та закрийте файл **README**, якщо він відкритий. Ви можете прочитати файл, якщо захочете.

g HashCalc тепер встановлено та запущено.



Крок 3: Обчисліть хеш файлу Hash.txt

a. Вкажіть наступні елементи у HashCalc:

1. Формат даних (Data Format): **Файл (File)**.

2. Дані: натисніть **...**Поруч із полем Дані (Data), перейдіть на **Робочий стіл (Desktop)**і виберіть файл**Hash.txt**.

3. Зніміть прапорець **HMAC**

4. Зніміть усі типи хешів, крім **MD5**

ii. Натисніть кнопку **Обчислити (Calculate)**.

Яке значення поряд із **MD5**?.

_____

_____

Крок 4: Внесіть зміни у файлі Hash.txt

a. Перейдіть на **Робочий стіл** і відкрийте файл **Hash.txt**.

ii. Зробіть невелику зміну тексту, наприклад, видалення літери або додавання пробілу.

iii. Натисніть **Файл> Зберегти (File > Save)** та закрийте **Блокнот**.

Крок 5: Обчисліть новий хеш файлу Hash.txt

a. Знову натисніть кнопку **Обчислити (Calculate)** в HashCalc.

Яке значення поряд із **MD5**?.

_____
_____

Чи значення відрізняється від значення, що одержано на кроці 3?

_____
_____

ii. Поставте прапорець біля усіх типів хеш-функцій.

iii. Натисніть **Обчислити (Calculate)**

iv. Зверніть увагу, що багато типів хеш-функцій створюють хеш різної довжини. Чому?

_____
_____

Лабораторна робота №3.
Створення та збереження надійних паролей

Цілі та задачі

Зрозуміти концепцію надійного пароля.

Частина 1: Дослідження концепцій створення надійного пароля.

Частина 2: Дослідження концепцій безпечного збереження паролів.

Довідкова інформація / Сценарій

Паролі широко використовуються для захисту доступу до ресурсів. Зловмисники можуть використовувати багато методів для вивчення паролів користувачів та отримання несанкціонованого доступу до ресурсів або даних.

Щоб краще захистити себе, важливо розуміти, що робить пароль надійним і як його безпечно зберігати.

Необхідні ресурси

- ПК або мобільний пристрій з доступом до Інтернету

Частина 1: Створення надійного пароля

Надійні паролі мають відповідати вимогам, які перераховані в порядку важливості:

1. Користувач може легко запам'ятати пароль.
2. Для будь-якої іншої людини вгадати цей пароль не є тривіальною задачею.

3. Вгадати або визначити цей пароль не є тривіальною задачею для програми.

4. Пароль має бути складним, містити цифри, символи та суміш літер у верхньому та нижньому регістрах.

Виходячи з зазначеного вище списку, перша вимога, мабуть, є найважливішою, оскільки Вам потрібно Ваш пароль пам'ятати. Наприклад, пароль **#4ssFrX^-aartPOknx25_70!xAdk<d!** вважається надійним, оскільки він задовольняє останнім трьом вимогам, але його дуже важко запам'ятати.

Багато організацій вимагають, щоб паролі містили комбінацію цифр, символів та літер у нижньому та верхньому регістрах. Паролі, які відповідають цій політиці, вважаються придатними для використання, якщо вони легко запам'ятовуються. Нижче наведено приклад політики щодо пароля для типової організації:

- Довжина пароля має бути мінімум 8 символів
- Пароль повинен містити символи у верхньому і нижньому регістрах
- Пароль має містити число
- Пароль має містити неалфавітний символ

Проаналізуйте характеристики надійного пароля та загальну політику вибору паролів, наведену вище. Чому в політиці не враховуються перші два пункти? Поясніть.

_____
_____
_____
_____

Хорошою практикою створення надійних паролів є вибір чотирьох або більше випадкових слів і їх поєднання. Пароль **televisionfrogbootschurch** надійніший ніж **J0n@than#81**. Зверніть увагу, що, хоча другий пароль відповідає описаним вище правилам, програми зламу паролів дуже ефективні при визначенні цього типу пароля. Хоча багато політик створення паролів не дозволять використання першого пароля, **televisionfrogbootschurch**, він набагато надійніший ніж другий. Користувачу простіше його запам'ятати (особливо якщо він асоціюється з зображенням), він дуже довгий, і фактор випадковості ускладнює визначення такого пароля.

Використовуючи онлайн-інструмент для створення паролів, створіть паролі на основі загальної політики компанії щодо створення паролів, яка була описана вище.

5. Відкрийте веб-браузер і перейдіть на http://passwordsgenerator.net

6. Виберіть параметри, які відповідають політиці вибору пароля

7. Згенеруйте пароль

Чи легко запам'ятати згенерований пароль?

_____

_____

Використовуючи онлайн-інструмент для створення паролів, створіть паролі на основі випадкових слів. Зауважте, що оскільки слова з'єднані разом, вони не розглядаються як словарні слова.

8. Відкрийте веб-браузер і перейдіть на http://preshing.com/20110811/xkcd-password-generator/

9. Згенеруйте новий пароль з випадкових слів, натиснувши **Generate Another!** у верхній частині веб-сторінки.

10. Чи легко запам'ятати згенерований пароль?

_____
_____
_____
_____

Частина 2: Безпечне зберігання паролів

Якщо користувач вирішить використовувати менеджер паролів, на першу характеристику надійного пароля можна не зважати, оскільки користувач завжди має доступ до менеджера паролів. Зверніть увагу, що деякі користувачі довіряють свої паролі лише власній пам'яті. Менеджери паролів, як локальні, так і віддалені, використовують сховище паролів, яке може бути скомпрометовано.

Сховище менеджера паролів має бути надійно зашифровано, і доступ до нього має жорстко контролюватися. За допомогою програм для мобільних телефонів та веб-інтерфейсів, хмарні менеджери паролів надають своїм користувачам у будь-який час безперебійний доступ.

Популярним менеджером паролів є LastPass.

Створіть пробний обліковий запис LastPass:

a. Відкрийте веб-браузер і перейдіть на https://lastpass.com/

b. Натисніть **Start Trial** для створення пробного облікового запису.

c. Заповніть поля, як зазначено в інструкції.

d. Встановіть майстер-пароль. Цей пароль дає вам доступ до вашого облікового запису LastPass.

e. Завантажте та встановіть клієнта LastPass відповідно до своєї операційної системи.

f. Відкрийте клієнт і увійдіть до системи за допомогою майстер-пароля LastPass.

g. Дослідіть менеджер паролів LastPass.

Коли ви додасте паролі до LastPass, де вони зберігаються?

_____
_____

Окрім вас, щонайменше, один інший суб'єкт має доступ до паролів. Хто цей суб'єкт?

_____
_____

Хоча зберігати всі Ваші паролі в одному місці може бути досить зручно, є недоліки у цьому підході. Як Ви думаєте, які недоліки?

_____
_____
_____

Частина 2: Що тепер для Вас означає надійний пароль?

Використовуючи характеристики надійного пароля, наведені на початку цієї лабораторної роботи, виберіть пароль, який легко запам'ятати, але важко вгадати. Складність паролів важлива, якщо вона не впливає на більш важливі вимоги, такі як придатність для легкого запам'ятовування.

Якщо використовується менеджер паролів, вимога до простоти запам'ятовування може бути скасована.

Нижче наведений короткий підсумок:

Обирайте пароль, який можете легко запам'ятати.

Обирайте пароль, який ніхто не зможе асоціювати з Вами.

Обирайте різні паролі та ніколи не використовуйте один і той самий пароль для різних сервісів.

Складність паролів - це хороша практика доти, доки не виникають проблеми з їх запам'ятовуванням.

Лабораторна робота №4.
Резервне копіювання даних до зовнішнього сховища

Цілі та задачі

Резервне копіювання даних користувача.

Частина 1: Використання локального зовнішнього диску для резервного копіювання даних

Частина 2: Використання віддаленого диску для резервного копіювання даних

Довідкова інформація/Сценарій

Важливо встановити стратегію резервного копіювання, яка включає в себе відновлення даних особистих файлів.

Хоча існує багато інструментів резервного копіювання, ця лабораторна робота фокусується на Microsoft Backup Utility для виконання резервних копій на локальні зовнішні диски. У частині 2 ця лабораторна робота використовує службу Dropbox для резервного копіювання даних на віддалений або хмарний диск.

Необхідні ресурси

- ПК або мобільний пристрій з доступом до Інтернету

Частина 1: Резервне копіювання на локальний зовнішній диск

Крок 1: Початок роботи з інструментами резервного копіювання у Windows

Використання комп'ютера та організаційні вимоги визначають, як часто необхідно проводити резервне копіювання даних та тип резервної копії. Процес резервного копіювання може зайняти багато часу. Якщо ретельно дотримуватися стратегії резервного копіювання, не обов'язково кожного разу створювати резервні копії всіх файлів. Тільки ті файли, які змінилися з моменту останнього резервного копіювання, підлягають резервному копіюванню.

Microsoft Windows містить інструменти резервного копіювання, які можна використовувати для резервного копіювання файлів. У версіях, що передують Windows 8, ви можете скористатись інструментом Резервне копіювання та відновлення для резервного копіювання ваших файлів. Windows 8.1 поставляється з інструментом Історія файлів, який можна використовувати для резервного копіювання файлів у папках "Документи", "Музика", "Зображення", "Відео" та "Робочий стіл". З плином часу Історія файлів будує історію ваших файлів, що дозволяє вам повернутися і відновити певні версії файлу. Це корисна функція, якщо є пошкоджені або втрачені файли.

Windows 7 та Vista постачаються з іншим інструментом резервного копіювання, що називається **Резервне копіювання та відновлення**. Коли вибрано зовнішній диск, Windows 7 запропонує використовувати новий накопичувач як резервний пристрій. Використовуйте Резервне копіювання та відновлення для керування резервними копіями.

Щоб отримати доступ до служби Резервного копіювання та відновлення у Windows 7, виконайте наведені нижче дії.

1) Підключіть зовнішній накопичувач.

2) Запустіть службу Резервне копіювання там відновлення за допомогою наступного шляху:

Пуск > Панель керування > Резервне копіювання та відновлення

Для початку роботи з Історією файлів у Windows 8.1, виконайте наведені нижче дії:

3) Підключіть зовнішній накопичувач.

i. Увімкніть Історію файлів за допомогою наступного шляху:

Панель керування> Історія файлів> натисніть Увімкнути

Примітка: в інших операційних системах також доступні інструменти резервного копіювання. Apple OS X включає Time Machine, в той час як Ubuntu Linux включає Déjà Dup, за замовчуванням.

Крок 2: Резервне копіювання папок Документи та Зображення

Тепер, коли зовнішній диск підключений, і ви знаєте, як знайти інструмент резервного копіювання, установіть його для резервного копіювання папок Документи та Зображення щодня о 3 ранку.

a. Відкрийте **Резервне копіювання та відновлення** (Windows 7) або **Історія файлів** (Windows 8.x).

b. Виберіть зовнішній диск, який ви хочете використовувати для отримання резервної копії.

c. Вкажіть, резервну копію яких даних ви хочете створити. Для цієї лабораторної роботи виберіть папки **Документи** та **Зображення**.

d. Налаштуйте графік резервного копіювання. Для цієї лабораторної роботи, оберіть резервне копіювання кожного дня о 3 ранку.

Чому Ви вирішити робити резервне копіювання о 3 ранку?

_____
_____
_____
_____

e Запустіть резервне копіювання, натиснувши **Зберегти параметри та створити резервну копію**.

Частина 2: Резервне копіювання на віддалений диск

Крок 1: Ознайомлення з хмарними службами резервного копіювання

Іншим варіантом місця призначення резервної копії є віддалений диск. Це може бути хмарний сервіс, або просто NAS, підключений до мережі, віддалені резервні копії також дуже поширені.

a Перерахуйте кілька хмарних служб резервного копіювання.

_____
_____
_____

b Дослідіть служби, які ви зазначили вище. Чи є ці служби безкоштовними?

_____
_____
_____

c Чи залежать служби, перелічені вами, від платформи?

_____
_____
_____

d Ви можете отримати доступ до своїх даних із усіх пристроїв, якими ви володієте (настільний комп'ютер, ноутбук, планшет та телефон)?

_____
_____

Крок 2: Використання Резервного копіювання та відновлення для резервного копіювання даних у хмару

Виберіть службу, яка відповідає вашим потребам, і створіть резервну копію вашої папки «Документи» у хмарі. Зверніть увагу, що Dropbox і OneDrive дозволяють створити папку на вашому комп'ютері, яка діє як посилання на хмарний диск. Після створення, файли, скопійовані в цю папку, автоматично завантажуються в хмару за допомогою клієнту служби, який завжди працює. Ця система дуже зручна, тому що ви можете використовувати будь-які інструменти резервного копіювання за вашим вибором, щоб запланувати резервне копіювання у хмару. Щоб використовувати Резервне копіювання та відновлення Windows для резервного копіювання файлів у Dropbox, виконайте наступні дії:

a. Відвідайте сторінку http://dropbox.com та зареєструйте безкоштовний обліковий запис Dropbox.

b. Коли обліковий запис буде створено, Dropbox відображатиме всі файли, що зберігаються у вашому обліковому записі. Клацніть на **ваше ім'я** та натисніть **Встановити**, щоб завантажити та встановити відповідний клієнт Dropbox для своєї операційної системи.

c. Відкрийте завантажену програму для встановлення клієнта.

d. Після завершення установки клієнт Dropbox створить папку під назвою Dropbox всередині вашої Домашньої папки. Зверніть увагу, що будь-які файли, скопійовані до новоствореної папки, будуть автоматично скопійовані до хмарних серверів Dropbox.

е. Відкрийте **Резервне копіювання та відновлення Windows** та налаштуйте його на використання нової папки Dropbox як місця для резервного копіювання.

Міркування

1. Які переваги резервного копіювання даних на локальний зовнішній диск?

_____
_____

2. Які недоліки резервного копіювання даних на локальний зовнішній диск?

_____
_____

3. Які переваги резервного копіювання даних на хмарний диск?

_____
_____

4. Які недоліки резервного копіювання даних на хмарний диск?

_____
_____

Лабораторна робота №5.
Захист персональних даних

Цілі та задачі

Дослідіть яким є право власності на Ваші дані, якщо вони зберігаються не в локальній системі.

Частина 1: Знайомимося з правилами надання послуг

Частина 2: Чи знаєте Ви під чим підписуєтесь?

Довідкова інформація/Сценарій

Соціальні медіа та онлайн-сховища стали невід'ємною частиною життя багатьох людей. Файли, фотографії та відео використовуються разом з друзями та рідними. Співпраця онлайн та онлайн-наради проводяться на робочих місцях людьми, які знаходяться за багато миль один від одного. Можливості зберігання даних більше не обмежуються пристроями, доступними локально. Географічне положення пристроїв зберігання даних більше не є обмеженням для зберігання або резервного копіювання даних у віддалених сховищах.

В цій лабораторній роботі Ви маєте дослідити правові угоди, необхідні для використання різних онлайн-сервісів. Ви також дізнаєтеся про деякі способи захисту Ваших даних.

Необхідні ресурси

- ПК або мобільний пристрій з доступом до Інтернету

Частина 1: Знайомимося з правилами надання послуг

Якщо Ви використовуєте онлайн-сервіси для зберігання даних або спілкування з друзями чи родиною, напевно Ви уклали угоду з провайдером цих сервісів. Умови надання послуг, також відомі як "Умови використання" або "Загальні положення та умови", є юридично обов'язковим контрактом, який регулює правила взаємовідносин між Вами, Вашим провайдером та іншими особами, які користуються сервісом.

Перейдіть на веб-сайт онлайн-сервісу, який Ви використовуєте та знайдіть Угоду про умови надання послуг. Нижче наведено список найбільш популярних соціальних мереж та сервісів для онлайн-зберігання даних.

Соціальні мережі

Facebook: https://www.facebook.com/policies

Instagram: http://instagram.com/legal/terms/

Twitter: https://twitter.com/tos

Pinterest: https://about.pinterest.com/en/terms-service

Сервіси для онлайн-зберігання даних

iCloud: https://www.apple.com/legal/internet-services/icloud/en/terms.html

Dropbox: https://www.dropbox.com/terms2014

OneDrive: http://windows.microsoft.com/en-us/windows/microsoft-services-agreement

Ще раз перегляньте терміни і дайте відповіді на наступні запитання.

1) Чи маєте Ви обліковий запис у постачальника онлайн-послуг? Якщо так, чи ознайомилися Ви з Угодою про надання послуг?

_____
_____

2) Що таке політика використання даних?

_____
_____

3) Що таке налаштування конфіденційності?

_____
_____

4) Що таке Політика безпеки?_____
_____

5) Які права Ви маєте щодо своїх даних? Чи можете Ви запросити копію Ваших даних?

_____

_____

6) Що може робити постачальник послуг із даними, які Ви завантажили?

_____

_____

7) Що відбувається з вашими даними, коли Ви закриваєте свій обліковий запис?

_____

_____

Частина 2: Чи знаєте Ви під чим підписалися?

Після того, як Ви створили обліковий запис і погодились з Умовами надання послуг, чи дійсно ви знаєте, під чим підписалися?

В Частині 2 Ви дізнаєтеся, як Умови надання послуг можуть бути інтерпретовані та використані постачальниками сервісів.

Використовуйте Інтернет для пошуку інформації щодо інтерпретації Умов надання послуг.

Нижче наведено кілька прикладів статей, які допоможуть Вам розпочати роботу.

Facebook:

http://www.telegraph.co.uk/technology/social-media/9780565/Facebook-terms-and-conditions-why-you-dont-own-your-online-life.html

iCloud:

http://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/april12/have-attorneys-read-the-icloud-terms-and-conditions.html

Dropbox:

http://www.legalgenealogist.com/blog/2014/02/24/terms-of-use-change-dropbox/

Перегляньте статті та дайте відповіді на наступні запитання.

1) Що Ви можете зробити щоб захистити себе?

_____

_____

2) Що Ви можете зробити, щоб захистити свій обліковий запис і свої дані?

_____

_____

Лабораторна робота №6.
Дослідження ризиків в Інтернеті

Цілі та задачі

Дослідити дії в Інтернеті, що можуть скомпрометувати вашу безпеку чи конфіденційність.

Довідкова інформація/Сценарій

Інтернет - це вороже середовище, і ви повинні бути пильними, щоб ваші дані не були скомпрометовані. Зловмисники креативні і будуть використовувати різні методи, щоб обдурити користувачів. Ця лабораторна робота допоможе визначити ризики своєї поведінки в Інтернеті та надати поради щодо безпечного використання Інтернету.

Частина 1: Знайомимося з правилами надання послуг

Відповідайте на питання, наведені нижче, чесно та зверніть увагу, скільки балів дає кожна відповідь. Додайте всі очки до загального балу та перейдіть до Частини 2 для аналізу вашого поведінки в Інтернеті.

a) Якою інформацією ви ділитеся на сайтах соціальних мереж? _____

(1) Всією; Я покладаюся на соціальні мережі, щоб підтримувати зв'язок з друзями та родиною. (3 бали)

(2) Статті та новини, які я знаходжу чи читаю (2 бали)

(3) Це залежить від того чим і з ким я ділюся. Я відфільтровую. (1 бал)

(4) Нічим. Я не використовую соціальні мережі. (0 балів)

b) Коли ви створюєте новий обліковий запис в онлайн-службі, ви: _____

(1) Повторно використовуйте той самий пароль, який використовується в інших службах, щоб полегшити його запам'ятовування. (3 бали)

(2) Створюєте пароль, який є максимально простим, щоб ви могли його запам'ятати. (3 бали)

(3) Створюєте дуже складний пароль і зберігаєте його в службі керування паролями. (1 бал)

(4) Створюєте новий пароль, який схожий, але відрізняється від пароля, який використовується в іншій службі. (1 бал)

(5) Створюєте абсолютно новий надійний пароль. (0 балів)

c) Коли ви отримуєте електронне повідомлення з посиланнями на інші сайти: _____

(1) Ви не натискаєте на посилання, тому що ви ніколи не переходите за посиланнями, що приходять вам у електронних повідомленнях. (0 балів)

(2) Ви переходите за посиланням, тому що поштовий сервер вже просканував це повідомлення. (3 бали)

(3) Ви переходите за всіма посиланнями, якщо повідомлення надійшло від людини, яку ви знаєте. (2 бали)

(4) Ви наводите курсор миші на посилання, щоб перевірити кінцеву URL адресу перед тим як натиснути. (1 бал)

d) Під час відвідування веб-сайту відображається спливаюче вікно. У ньому говориться , що ваш комп'ютер знаходиться під загрозою, і ви повинні завантажити та встановити діагностичну програму, щоб убезпечити свій комп'ютер: _____

(1) Ви натискаєте, завантажуєте та встановлюєте програму, щоб захистити ваш комп'ютер. (3 бали)

(2) Ви перевіряєте спливаючі вікна та наводите курсор на посилання, щоб перевірити його безпечність. (3 бали)

(3) Ігноруєте повідомлення, переконавшись, що ви не натисли на нього, не завантажуєте програму та закриваєте веб-сайт. (0 балів)

e) Коли вам потрібно ввійти на веб-сайт своєї фінансової установи, щоб виконати щось, ви: _____

(1) Вводите свою реєстраційну інформацію негайно. (3 бали)

(2) Ви перевіряєте URL, щоб переконатися, що це заклад, який вам потрібен, перед введенням будь-якої інформації. (0 балів)

(3) Ви не використовуєте онлайн-банкінг або будь-які онлайн-фінансові послуги. (0 балів)

f) Ви прочитали про програму і вирішите спробувати її. Ви шукаєте в Інтернеті та знаходите пробну версію на невідомому сайті, ви:_____

(1) Негайно завантажуєте та встановлюєте програму. (3 бали)

(2) Шукайте більше інформації про автора програми, перш ніж завантажувати її. (1 бал)

(3) Не завантажуєте та не встановлюєте програму. (0 балів)

g) Ви знаходите USB-флешдиск на шляху до роботи, ви: _____

(1) Берете його та підключаєте до комп'ютера, щоб переглянути його вміст. (3 бали)

(2) Берете його та підключаєте до комп'ютера, щоб стерти його вміст перед використанням. (3 бали)

(3) Берете його та підключаєте до комп'ютера, щоб запустити антивірусне сканування, перш ніж повторно використовувати його для власних файлів (3 бали)

(4) Не піднімаєте його. (0 балів)

h) _____ Вам потрібно підключитися до Інтернету, і ви знаходите відкриту точку доступу Wi-Fi. Ви: _____

(1) Підключаєтеся до неї та користуєтеся Інтернетом. (3 бали)

(2) Не підключаєтеся до неї та чекаєте на появу надійного з'єднання з Інтернетом. (0 балів)

(3) Підключаєтеся до неї та встановлюєте VPN на надійний сервер перед надсиланням будь-якої інформації. (0 балів)

Частина 2: Проаналізуйте свою поведінку в Інтернеті

Чим більша ваша сума балів, тим менш безпечною є ваша поведінка в Інтернеті. Вашою метою повинна бути 100% безпека, якої ви зможете досягти, звертаючи увагу на всі свої дії онлайн. Це дуже важливо, оскільки лише одна помилка може поставити під загрозу ваш комп'ютер та дані.

Додайте бали з Частини 1. Запишіть свою суму балів. __

0: Ви дуже безпечно поводите себе в Інтернеті.

0-3: Ви частково безпечно поводите себе в Інтернеті, але все одно повинні трохи змінити свою поведінку, щоб вона була повністю безпечною.

3-17: Ваша поведінка у Інтернеті небезпечна і ви ризикуєте поставити себе під загрозу.

18 або більше: Ваша поведінка в Інтернету дуже небезпечна і ваші дані будуть скомпрометовані.

Нижче наведено кілька важливих порад щодо безпеки онлайн.

a) Чим більшою кількістю інформації ви ділитеся в соціальних мережах, тим більше ви дозволяєте зловмисникові дізнатись про вас. Маючи більше знань про вас, зловмисник може створити набагато більш спрямовану атаку. Наприклад, якщо ви поділитеся з світом інформацією про те, що ви були на автомобільних перегонах, зловмисник зможе надіслати вам електронного листа від імені компанії, що відповідальна за продажу квитків на перегони. Оскільки ви нещодавно були на цьому заході, повідомлення буде виглядати більш надійним.

b) Повторне використання паролів - це погана практика. Якщо ви повторно використовуєте пароль у службі, що знаходиться під контролем зловмисників, вони можуть успішно спробувати увійти під вашим обліковим записом у інші служби.

c) Електронні листи можуть легко підробити, щоб вони виглядали надійно. Підроблені електронні листи часто містять посилання на шкідливі сайти

або шкідливе програмне забезпечення. Візьміть за правило не натискати на вкладенні посилання з листів, отриманих електронною поштою.

d) Не погоджуйтесь на встановлення небажаного програмного забезпечення, особливо якщо його пропонують вам на веб-сторінці. Дуже малоймовірно, що ця веб-сторінка матиме для вас законне та безпечне програмне забезпечення. Настійно рекомендується закрити браузер та використати інструменти операційної системи, щоб перевірити наявність оновлень.

e) Шкідливі веб-сторінки легко можна зробити схожими на веб-сайт банку або фінансової установи. Перш ніж натискати посилання або надавати будь-яку інформацію, двічі перевірте URL-адресу, щоб переконатися, що це правильна веб-сторінка.

f) Коли ви дозволяєте програмі запускатись на вашому комп'ютері, ви даєте їй багато можливостей. Добре подумайте перш ніж запускати програму. Проведіть невелике дослідження, щоб переконатися, що компанія або особа, відповідальна за програму, є серйозним та законним автором. Завантажуйте цю програму лише з офіційного веб-сайту компанії чи особи.

g) USB-накопичувачі та флешки містять мініатюрний контролер, що дозволяє комп'ютерам з ними спілкуватися. Цей контролер можна заразити і навчити встановлювати шкідливе програмне забезпечення на комп'ютер. Оскільки шкідливе програмне забезпечення розміщується безпосередньо в контролері USB, а не в області даних, то видалення даних або антивірусне сканування не виявить зловмисне програмне забезпечення.

h) Зловмисники часто розгортають підроблені точки доступу Wi-Fi, щоб заманити користувачів. Оскільки атакуючий має доступ до всієї інформації, переданої через скомпрометовану точку доступу, користувачі, підключені до цієї точки доступу, піддаються ризику. Ніколи не використовуйте невідомі точки Wi-Fi, не шифруючи трафік через VPN. Ніколи не передавайте конфіденційні дані, такі як номери кредитних карток, під час використання невідомої мережі (дротова або бездротова).

Міркування

Проаналізувавши свою поведінку в Інтернеті, які зміни ви б зробили, щоб захистити себе в Інтернеті?

_____
_____
_____
_____

Лабораторна робота №7.
Пошук персональних даних

Цілі та задачі

Дослідіть у кого є право власності на ваші дані, якщо вони зберігаються не в локальній системі.

Частина 1: Знайомимося з правилами надання послуг

Частина 2: Чи знаєте ви під чим підписуєтесь?

Довідкова інформація / Сценарій

Соціальні медіа та онлайн-сховища стали невід'ємною частиною життя багатьох людей. Файли, фотографії та відео використовуються спільно з друзями та рідними. Співпраця онлайн та онлайн-наради проводяться на робочих місцях людьми, які знаходяться за багато миль один від одного. Можливості зберігання даних більше не обмежуються пристроями, доступними локально. Географічне положення пристроїв зберігання даних більше не є обмеженням для зберігання або резервного копіювання даних у віддалених сховищах.

В цій лабораторній роботі ви маєте дослідити правові угоди, які необхідні для використання різних онлайн-сервісів. Ви також дізнаєтеся про деякі способи захисту ваших даних.

Необхідні ресурси

- ПК або мобільний пристрій з доступом до Інтернету

Частина 1: Знайомимося з правилами надання послуг

Якщо ви використовуєте онлайн-сервіси для зберігання даних або спілкування з друзями чи родиною, напевно ви уклали угоду з провайдером цих сервісів. Умови надання послуг, також відомі як "Умови використання" або "Загальні положення та умови", є юридично обов'язковим контрактом, який регулює правила взаємовідносин між вами, вашим провайдером та іншими особами, які користуються сервісом.

Перейдіть на веб-сайт онлайн-сервісу, який ви використовуєте та знайдіть Угоду про умови надання послуг. Нижче наведено список найбільш популярних соціальних мереж та сервісів для онлайн-зберігання даних.

Соціальні мережі

Facebook: https://www.facebook.com/policies

Instagram: http://instagram.com/legal/terms/

Twitter: https://twitter.com/tos

Pinterest: https://about.pinterest.com/en/terms-service

Сервіси для онлайн-зберігання даних

iCloud: https://www.apple.com/legal/internet-services/icloud/en/terms.html

Dropbox: https://www.dropbox.com/terms2014

OneDrive: http://windows.microsoft.com/en-us/windows/microsoft-services-agreement

Ще раз перегляньте умови і дайте відповіді на наступні запитання.

a. Чи маєте ви обліковий запис у постачальника онлайн-послуг? Якщо так, чи ознайомилися ви з Угодою про надання послуг?

_____
_____
_____

b. Що таке політика використання даних?

_____
_____
_____

c. Що таке налаштування конфіденційності?

_____
_____
_____

d. Що таке Політика безпеки?

_____
_____
_____

e. Які права ви маєте щодо своїх даних? Чи можете ви запросити копію ваших даних?

_____
_____
_____

f. Що може робити постачальник послуг із даними, які ви завантажили?

_____
_____
_____

g. Що відбувається з вашими даними, коли ви закриваєте свій обліковий запис?

_____
_____
_____

Частина 2: Чи знаєте ви під чим підписалися?

Після того, як ви створили обліковий запис і погодились з Умовами надання послуг, чи дійсно ви знаєте, під чим підписалися?

В Частині 2 ви дізнаєтеся, як Умови надання послуг можуть бути інтерпретовані та використані постачальниками сервісів.

Використовуйте Інтернет для пошуку інформації щодо інтерпретації Умов надання послуг.

Нижче наведено кілька прикладів статей, які допоможуть Вам розпочати роботу.

acebook:

http://www.telegraph.co.uk/technology/social-media/9780565/Facebook-terms-and-conditions-why-you-dont-own-your-online-life.html

iCloud:

http://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/april12/have-attorneys-read-the-icloud-terms-and-conditions.html

Dropbox:

http://www.legalgenealogist.com/blog/2014/02/24/terms-of-use-change-dropbox/

Перегляньте статті та дайте відповіді на наступні запитання.

a. Що ви можете зробити шоб захистити себе?

_____
_____
_____
_____

b. Що ви можете зробити, щоб захистити свій обліковий запис і свої дані?

_____
_____
_____

Лабораторна робота №8.
Використання цифрових підписів

Цілі та задачі

Зрозуміти концепції цифрового підпису.

Частина 1: Продемонструвати використання цифрових підписів.

Частина 2: Продемонструвати перевірку цифрового підпису.

Довідкова інформація / Сценарій

Цифровий підпис - це математичний метод, який використовується для перевірки автентичності та цілісності цифрового повідомлення. Цифровий підпис є еквівалентом рукописного підпису. Цифрові підписи можуть бути набагато більш безпечними. Мета цифрового підпису полягає в тому, щоб запобігти підробці та інперсоніфікації цифрових повідомлень. У багатьох країнах, включаючи Сполучені Штати, цифрові підписи мають таке ж юридичне значення, як і традиційні форми підписаних документів. Уряд Сполучених Штатів тепер публікує електронні версії бюджетів, законів і законопроектів Конгресу з цифровими підписами.

Необхідні ресурси

- ПК або мобільний пристрій з доступом до Інтернету

Part 4: Використання цифрових підписів

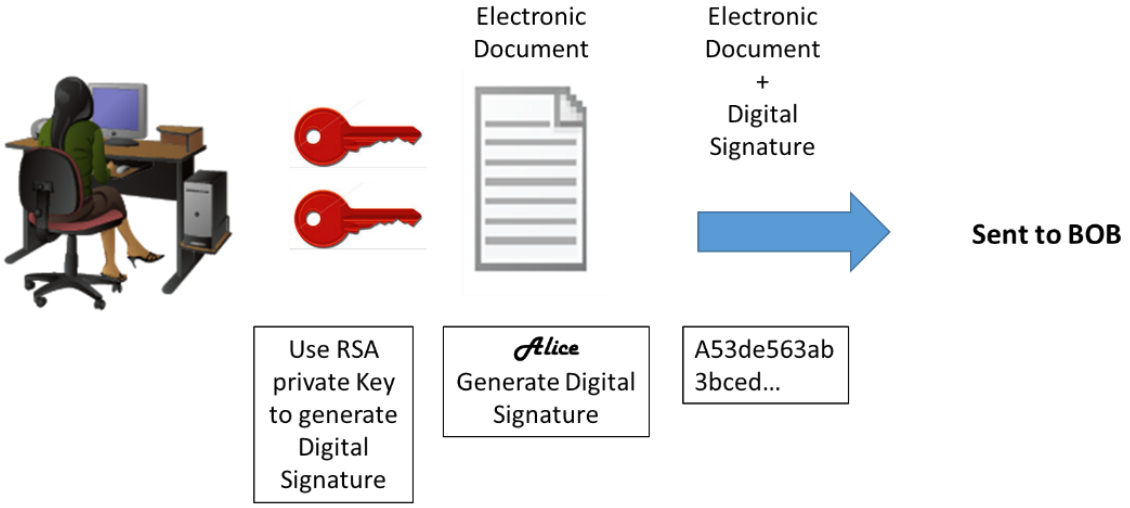
У цій частині ви будете використовувати веб-сайт для перевірки підпису документа між Алісою і Бобом. Аліса і Боб використовують одну пару закритих і відкритих ключів RSA. Кожен з них використовує свій закритий ключ для підписання юридичного документа. Потім вони відправляють документи один одному. І Аліса, і Боб можуть перевірити підпис один одного відкритим ключем. Вони також повинні домовитися про спільну відкриту експоненту для розрахунку.

Таблиця 1 - Відкритий і закритий ключі RSA

Відкритий ключ RSA	d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a30c428b39e3362fb3779a497eceaea37100f264d7fb9fb1a97fbf621133de55fdcb9b1ad0d7a31b379216d79252f5c527b9bc63d83d4ecf4d1d45cbf843e8474babc655e9bb6799cba77a47eafa838296474afc24beb9c825b73ebf549
Закритий ключ RSA	47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095793c12bae1e09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5ba629d25ccf72a5ceb8a8da038906c84dcdb1fe677dffb2c029fd8926318eede1b58272af22bda5c5232be066839398e42f5352df58848adad11a1
Відкрита експонента	10001

Step 1: Підпишіть документ.

Аліса підписує юридичний документ і відправляє його Бобу з використанням відкритих і закритих ключів RSA, показаних в таблиці вище. Тепер Бобу доведеться перевірити цифровий підпис Аліси, щоб довіряти справжності електронного документа.



Step 2: Перевірте цифровий підпис.

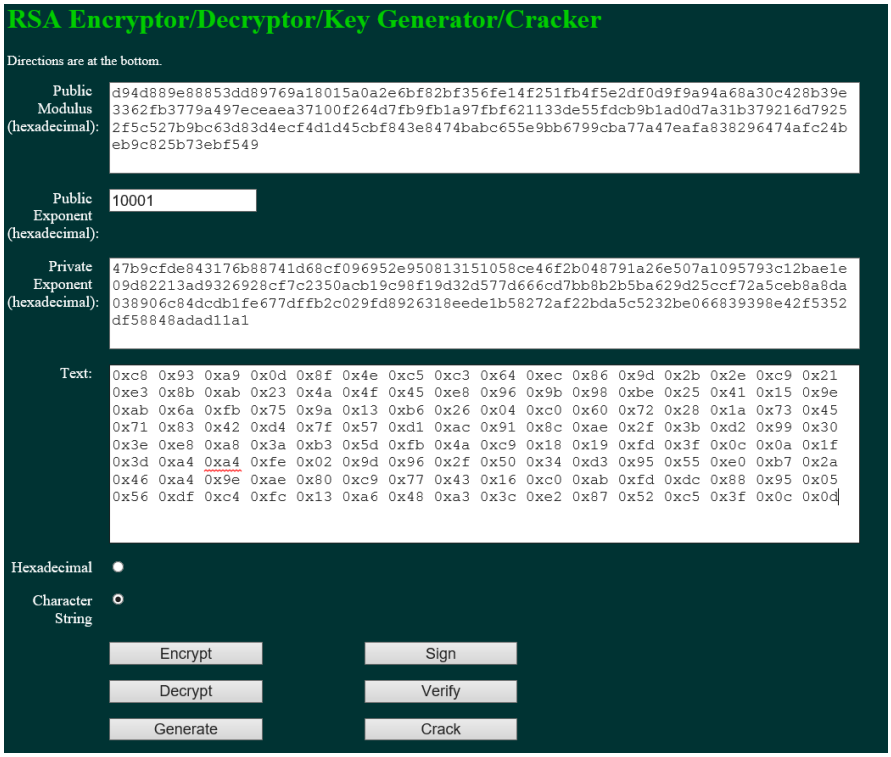
Боб отримує документ з цифровим підписом, показаним в таблиці нижче.

Таблиця 2 - Цифровий підпис Аліси

Цифровий підпис Аліси
0xc8 0x93 0xa9 0x0d 0x8f 0x4e 0xc5 0xc3 0x64 0xec 0x86 0x9d 0x2b 0x2e 0xc9 0x21 0xe3 0x8b 0xab 0x23 0x4a 0x4f 0x45 0xe8 0x96 0x9b 0x98 0xbe 0x25 0x41 0x15 0x9e 0xab 0x6a 0xfb 0x75 0x9a 0x13 0xb6 0x26 0x04 0xc0 0x60 0x72 0x28 0x1a 0x73 0x45 0x71 0x83 0x42 0xd4 0x7f 0x57 0xd1 0xac 0x91 0x8c 0xae 0x2f 0x3b 0xd2 0x99 0x30 0x3e 0xe8 0xa8 0x3a 0xb3 0x5d 0xfb 0x4a 0xc9 0x18 0x19 0xfd 0x3f 0x0c 0x0a 0x1f 0x3d 0xa4 0xa4 0xfe 0x02 0x9d 0x96 0x2f 0x50 0x34 0xd3 0x95 0x55 0xe0 0xb7 0x2a 0x46 0xa4 0x9e 0xae 0x80 0xc9 0x77 0x43 0x16 0xc0 0xab 0xfd 0xdc 0x88 0x95 0x05 0x56 0xdf 0xc4 0xfc 0x13 0xa6 0x48 0xa3 0x3c 0xe2 0x87 0x52 0xc5 0x3f 0x0c 0x0d

Перейдіть за посиланням http://nmichaels.org/rsa.py, щоб використати онлайн-інструмент RSA для перевірки справжності цифрового підпису Аліси.

Таблиця 3 - Онлайн інструмент цифрового підпису



a. Скопіюйте і вставте **відкриті** і **закриті** ключі з Таблиці 1 вище у поля **Public Modulus** і **Private Exponent** на сайті, як показано на рисунку вище.

b. Переконайтеся, що значення Public Exponent дорівнює 10001.

c. Вставте цифровий підпис Аліси з Таблиці 2 в поле з написом на веб-сайті, як показано вище.

d. Тепер Боб може перевірити цифровий підпис, натиснувши кнопку **Verify** знизу веб-сайту. Чий підпис ідентифіковано?

_____

_____ _____

Step 3: Створіть підпис для відповіді.

Боб отримує і перевіряє електронний документ і цифровий підпис Аліси. Тепер Боб створює електронний документ і генерує свій власний цифровий підпис, використовуючи закритий ключ RSA в Таблиці 1 (Примітка: ім'я Боба великими літерами).

Таблиця 4 - Цифровий підпис Боба

Цифровий підпис Боба
0x6c 0x99 0xd6 0xa8 0x42 0x53 0xee 0xb5 0x2d 0x7f 0x0b 0x27 0x17 0xf1 0x1b 0x62 0x92 0x7f 0x92 0x6d 0x42 0xbd 0xc6 0xd5 0x3e 0x5c 0xe9 0xb5 0xd2 0x96 0xad 0x22 0x5d 0x18 0x64 0xf3 0x89 0x52 0x08 0x62 0xe2 0xa2 0x91 0x47 0x94 0xe8 0x75 0xce 0x02 0xf8 0xe9 0xf8 0x49 0x72 0x20 0x12 0xe2 0xac 0x99 0x25 0x9a 0x27 0xe0 0x99 0x38 0x54 0x54 0x93 0x06 0x97 0x71 0x69 0xb1 0xb6

0x24 0xed 0x1c 0x89 0x62 0x3d 0xd2 0xdf 0xda 0x7a 0x0b 0xd3 0x36 0x37 0xa3 0xcb 0x32 0xbb 0x1d 0x5e 0x13 0xbc 0xca 0x78 0x3e 0xe6 0xfc 0x5a 0x81 0x66 0x4e 0xa0 0x66 0xce 0xb3 0x1b 0x93 0x32 0x2c 0x91 0x4c 0x58 0xbf 0xff 0xd8 0x97 0x2f 0xa8 0x57 0xd7 0x49 0x93 0xb1 0x62

Боб посилає Алісі електронний документ і цифровий підпис.

Step 4: Перевірте цифровий підпис.

a. Скопіюйте і вставте **відкриті** і **закриті** ключі з Таблиці 1 вище у поля **Public Modulus** і **Private Exponent** на сайті, як показано на рисунку вище.

b. Переконайтеся, що значення Public Exponent дорівнює 10001.

c. Вставте цифровий підпис Боба з Таблиці 4 в поле з написом на веб-сайті, як показано вище.

d. Тепер Аліса може перевірити цифровий підпис, натиснувши кнопку **Verify** знизу веб-сайту. Чий підпис ідентифіковано?

_____
_____

Part 5: Створіть свій власний цифровий підпис

Тепер, коли ви бачите, як працюють цифрові підписи, ви можете створити свій власний цифровий підпис.

Step 1: Створіть нову пару RSA-ключів.

Перейдіть на інструмент веб-сайту і створіть новий набір відкритих і закритих ключів RSA.

a. Видаліть вміст полів з написами **Public Modulus**, **Private Modulus** і **Text**. Просто використовуйте мишу, щоб виділити текст і натисніть клавішу delete на клавіатурі.

b. Переконайтеся, що поле «Public Exponent» має значення **10001**.

c. Створіть новий набір ключів RSA, натиснувши кнопку **Generate** в правому нижньому кутку веб-сайту.

d. Скопіюйте нові ключі в Таблицю 5.

Таблиця 5 - Нові ключі RSA

Відкритий ключ	
Закритий ключ	

e. Тепер введіть своє повне ім'я в поле з написом **Text** і натисніть **Sign**.

Таблиця 6 - Персональний цифровий підпис

Персональний цифровий підпис	

Part 6: Обміняйтеся і перевірте цифрові підписи

Тепер ви можете використовувати цей цифровий підпис.

Step 1: Обміняйтеся вашими новими відкритими і закритими ключами в Таблиці 5 з вашим партнером по лабораторній роботі.

a. Запишіть відкриті і закриті ключі RSA свого партнера з його Таблиці 5

b. Запишіть обидва ключа в таблиці нижче.

Таблиця 7 - Ключі RSA партнера по лабораторній роботі

Відкритий ключ	
Закритий ключ	

c. Тепер обміняйтеся цифровими підписами з Таблиці 6. Запишіть цифровий підпис в таблиці нижче.

Цифровий підпис партнера по лабораторній роботі	

Step 2: Перевірте цифровий підпис партнера по лабораторній роботі

a. Щоб підтвердити цифровий підпис свого партнера, вставте його або її відкриті і закриті ключі до відповідних полів, помічених **Public and Private modulus** на веб-сайті.

b. Тепер вставте цифровий підпис в поле з написом **Text**.

c. Тепер перевірте його або її цифровий підпис, натиснувши кнопку verify.

d. Що відображається в текстовому полі?

_____

_____

ЗМІСТ