ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ВЕБ-СЕРВІСУ ДЛЯ ХМАРНОГО ЗБЕРІГАННЯ ТА ОБМІНУ ФАЙЛІВ

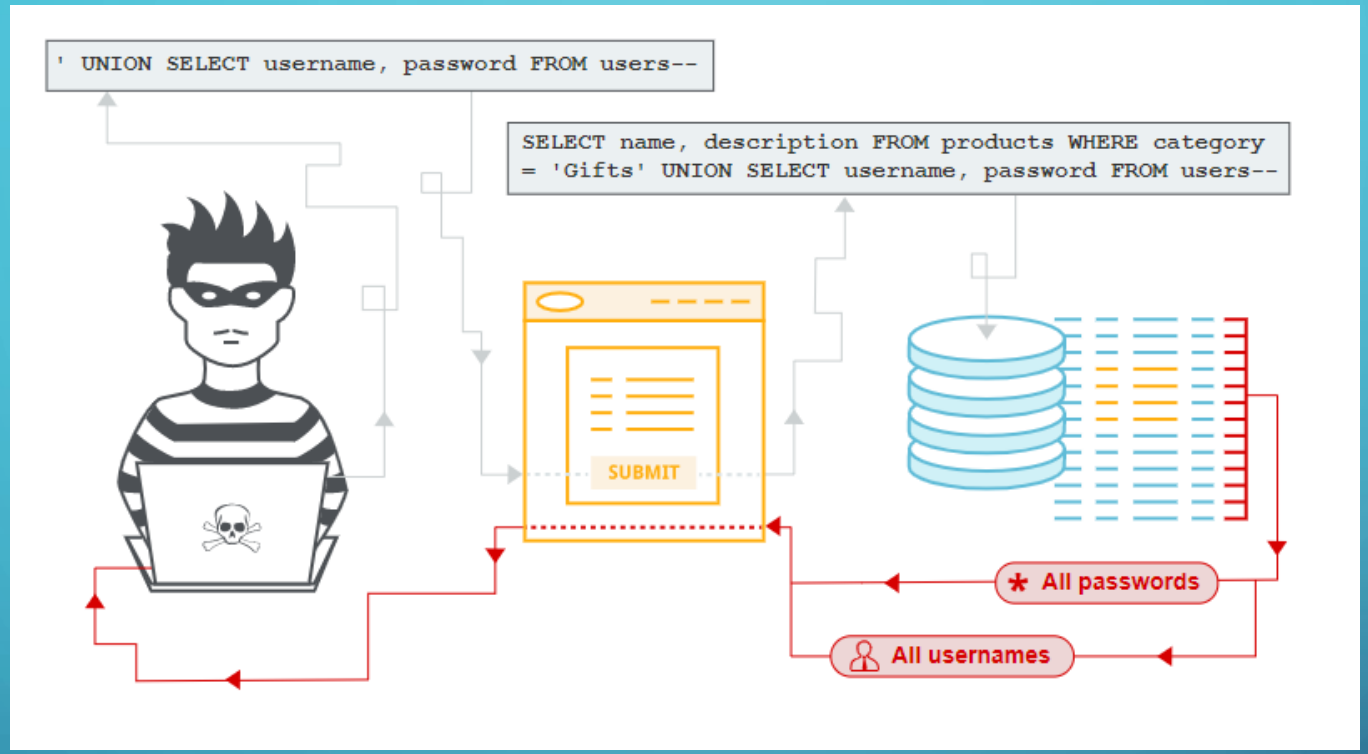
ВИКОНАЛА: СТУДЕНТ ГР. КІТ-М119Б ЩЕРБІНІНА Є.М.

КЕРІВНИК: ПРОФ. ФІЛОНЕНКО А.М.

СПИСОК НАЙБІЛЬШ ПОПУЛЯРНИХ ВРАЗЛИВОСТЕЙ ВЕБ-ЗАСТОСУНКІВ:

- ін'єкції (Injections);
- недоліки системи аутентифікації і зберігання сесій (Broken Authentication and Session Management);
- незахищеність критичних даних (Sensitive Data Exposure);
- впровадження зовнішніх XML-сутностей (XXE);
- порушення контролю доступа (Broken Access Control);
- похибки в конфігуруванні (Security Misconfiguration);
- міжсайтовий скриптинг - XSS (Cross Site Scripting);
- небезпечна десеріалізація (Insecure Deserialization);
- використання компонентів з відомими вразливостями (Using Components with Known Vulnerabilities);
- недостатнє логування та моніторінг;
- небезпечні прямі посилання на об’єкти (Insecure Direct Object References);
- відсутність функції контроля доступу (Missing Function Level Access Control);
- межсайтова підробка запитів (Cross-Site Request Forgery, CSRF/XSRF);
- неперевірені переадресації та пересилання (Unvalidated Redirects and Forwards).

SQL-ІН'ЄКЦІЇ



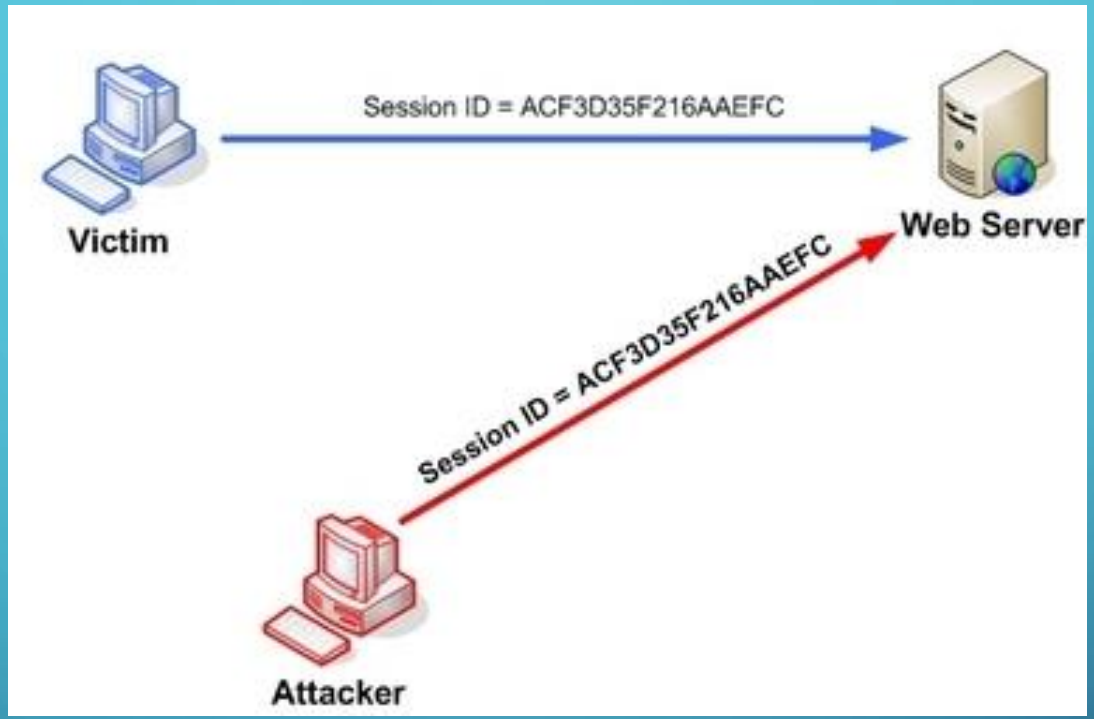
Дозволяє зловмиснику:

- отримати доступ до бази даних
- додавати змінювати та видаляти інформацію
- переглянути конфіденційну інформацію інших користувачів

Способи захисту:

- використання Object-relational mapping (ORM)
- використання параметрів в якості значень запиту
- використання валідаторів вхідних даних

НЕДОЛІКИ СИСТЕМИ АУТЕНТИФІКАЦІЇ І ЗБЕРІГАННЯ СЕСІЙ



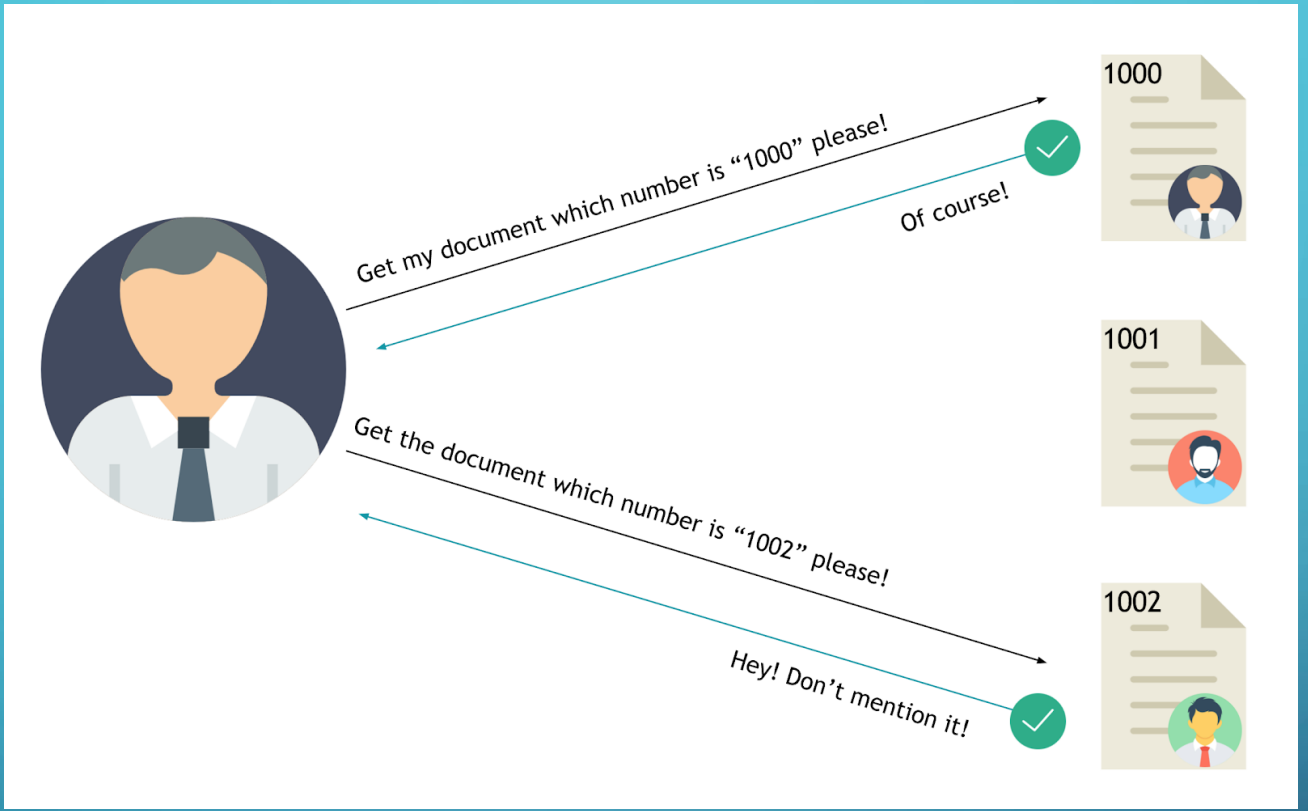
Дозволяє зловмиснику:

- отримати доступ до захищеної високочутливої інформації
- викрасти особисті дані
- вести шахрайську діяльність від лиця іншої особи

Способи захисту:

- використання багатофакторної автентифікації
- впровадження перевірки слабких паролів
- використання захищеного вбудованго менеджера сеансів на стороні сервера, який генерує новий ідентифікатор сесії

НЕБЕЗПЕЧНІ ПРЯМІ ПОСИЛАННЯ НА ОБ'ЄКТИ




```
https://insecure-website.com/customer_account?customer_number=132355
```

Дозволяє зловмиснику:

- отримати доступ до інформації інших користувачів методом перебору
- викрасти особисті дані

Способи захисту:

- використання хеша для заміни прямого ідентифікатора
- використання унікальних ідентифікаторів, які неможливо перебирати

НЕЗАХИЩЕНІСТЬ КРИТИЧНИХ ДАНИХ

Дозволяє зловмиснику:

- отримати доступ до конфеденційної інформації
- викрасти особисті дані
- впливати та змінювати таку інформацію

Способи захисту:

- використання протоколу HTTPS
- криптографічний захист даних (шифрування та хешування)

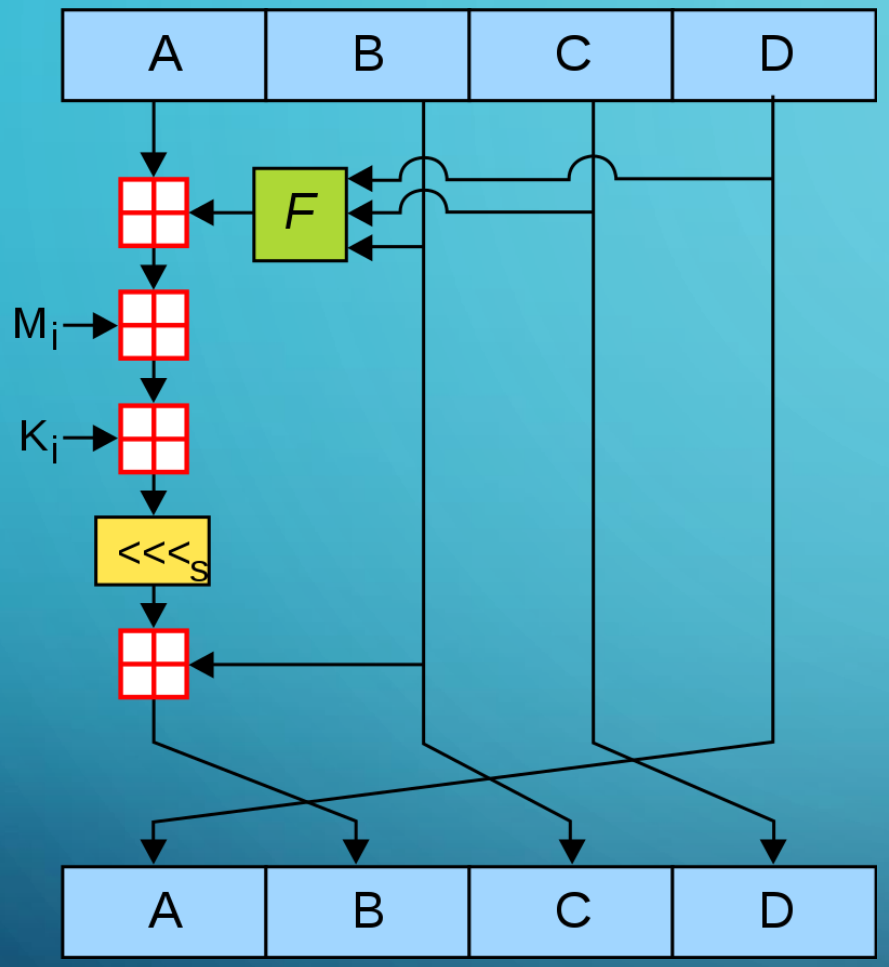
ВЛАСТИВОСТІ ХЕШ-ФУНКЦІЇ

- хеш-функція має нескінченну область визначення;
- хеш-функція має кінцеву область значень;
- вона незворотня;
- зміна вхідного потоку інформації на один біт змінює близько половини всіх біт вихідного потоку, тобто результату хеш-функції.

ВИМОГИ ДО ХЕШ-ФУНКЦІЇ

- незворотність: для заданого значення хеш-функції m повинно бути обчислювально-нездійсненним знайти блок даних X, для якого H (X) = m;
- стійкість до колізій: для заданого повідомлення M має бути обчислювально нездійсненним підібрати інше повідомлення N, для якого H (N) = H(M);
- стійкість до атак перебору (прямий перебір і перебір по словнику).

MD5

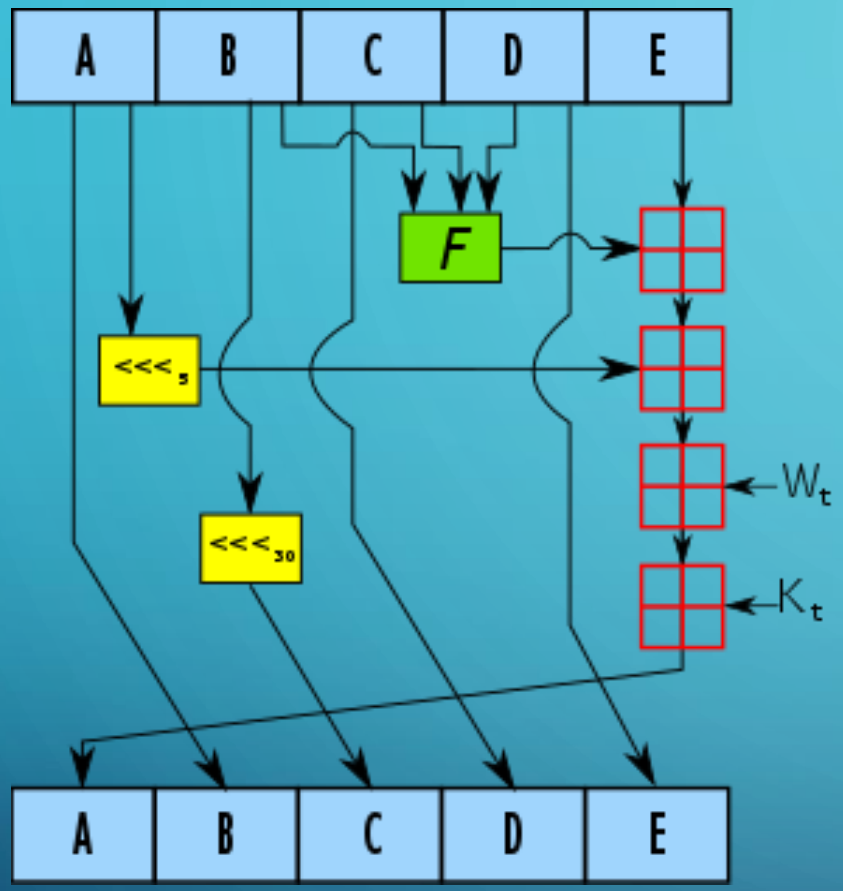


Крок 1. Вирівнювання початкових даних
L` = 512xN + 448
Крок 2. Додавання довжини повідомлення.
Крок 3. Ініціалізація буфера
Крок 4. Циклічна процедура обчислення
Крок 5. Результат обчислень

Приклади MD5-хешей:
MD5("md5") = 1BC29B36F623BA82AAF6724FD3B16718
MD5("md4") = C93D3BF7A7C4AFE94B64E30C2CE39F4F
MD5("") = D41D8CD98F00B204E9800998ECF8427E

F - нелінійна функція. Mi позначає 32-бітний блок вхідного повідомлення, а Ki - 32-бітну константу. <<< s позначає циклічний зсув вліво на s біт. ⊞ позначає складання по модулю 2^32. F залежить від раунду, Ki і s змінюються кожну операцію.

SHA1



Крок 1. Вирівнювання початкових даних
L` = 512xN + 448
Крок 2. Додавання довжини повідомлення.
Крок 3. Ініціалізація буфера
Крок 4. Циклічна процедура обчислення
Крок 5. Результат обчислень

Приклади SHA1-хешей:

SHA-1("sha") = d8f4590320e1343a915b6394170650a8f35d6926
SHA-1("Sha")= ba79baeb9f10896a46ae74715271b7f586e74640
SHA-1("") = da39a3ee5e6b4b0d3255bfef95601890afd80709

F - нелінійна функція. Wt позначає 32-бітний блок вхідного повідомлення, а Kt - 32-бітну константу. <<< позначає циклічний зсув вліво на n біт. ⊞ позначає складання по модулю 2^32. F залежить від раунду, Kt змінюється кожну операцію.

ПОРІВНЯННЯ SHA1 З MD5

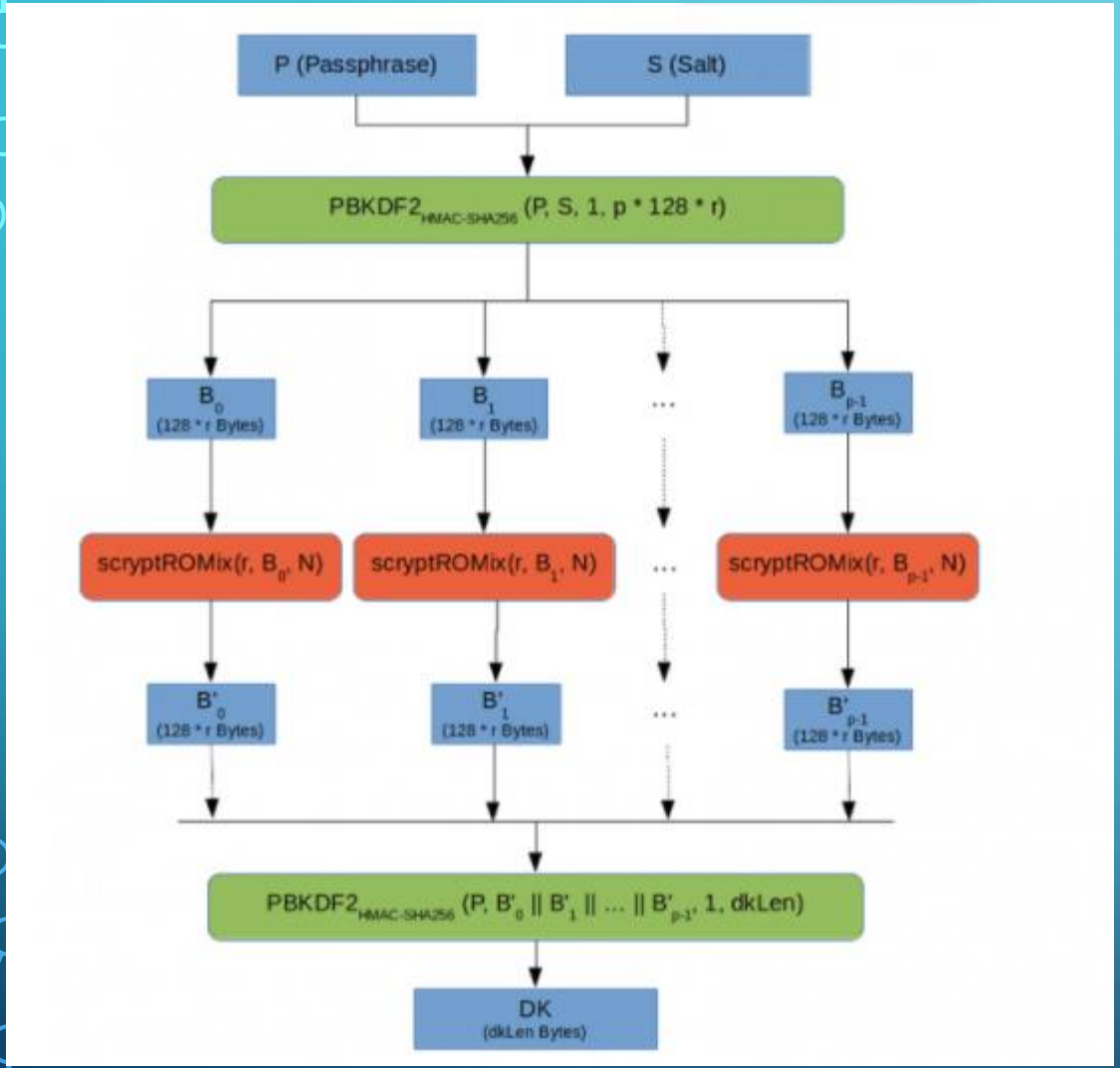
Схожість:

- чотири етапи;
- кожна дія додається до раніше отриманого результату;
- розмір блоку обробки становить 512 біт;
- обидва алгоритми виконують складання по модулю 2^{32}, вони розраховані на 32-х бітну архітектуру.

Відмінності:

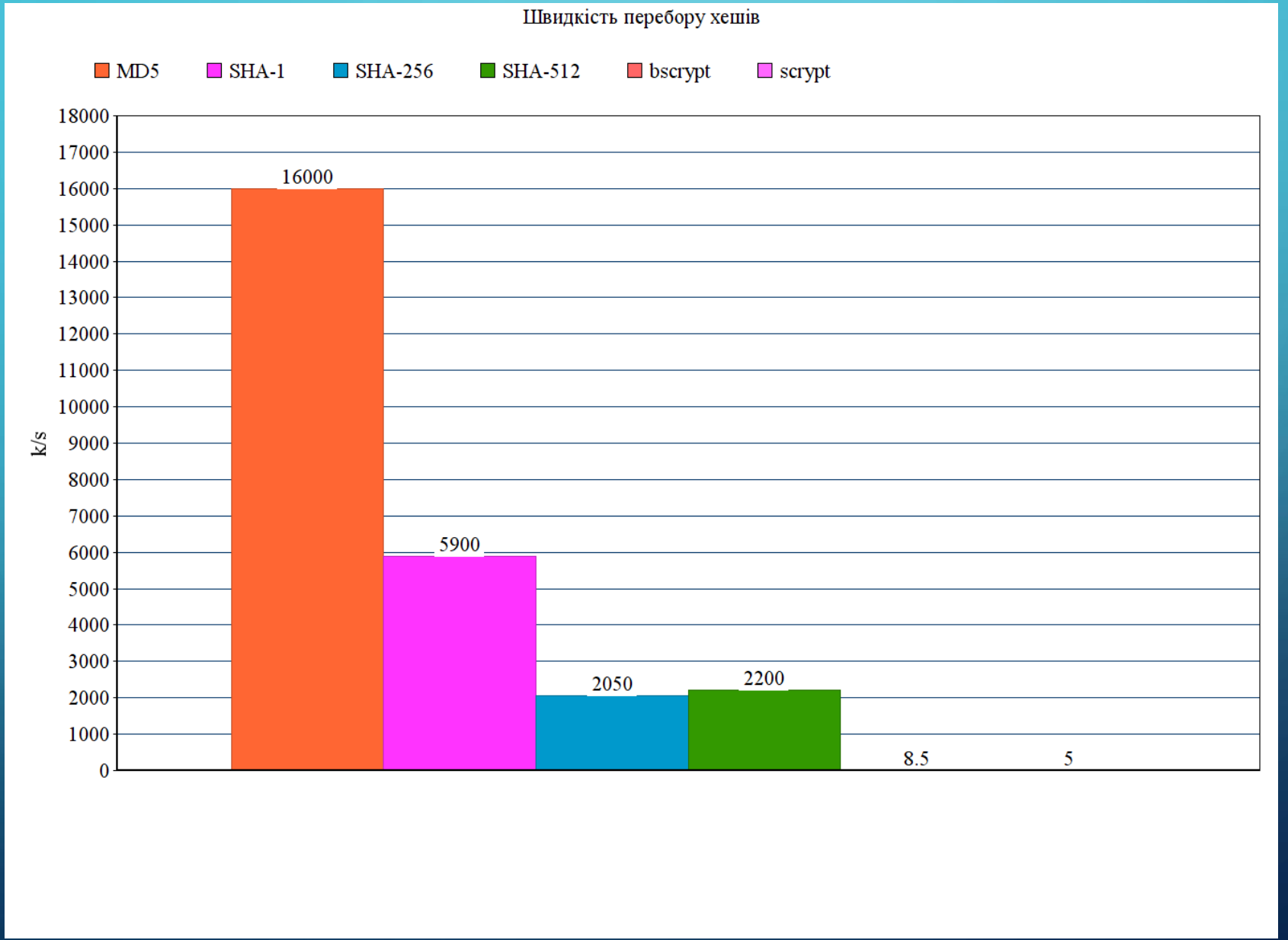
- у SHA-1 на четвертому етапі використовується та ж функція f, що і на другому етапі;
- в MD5 у кожній дії використовується унікальна адитивна константа. У SHA-1 константи використовуються повторно для кожної із чотирьох груп;
- у SHA-1 додана п'ята змінна;
- SHA-1 використовує циклічний код виправлення помилок;
- в MD5 чотири різних елементарних логічних функції, в SHA-1 – три;
- в MD5 довжина дайджесту становить 128 біт, в SHA-1 - 160 біт;

SCRYPT

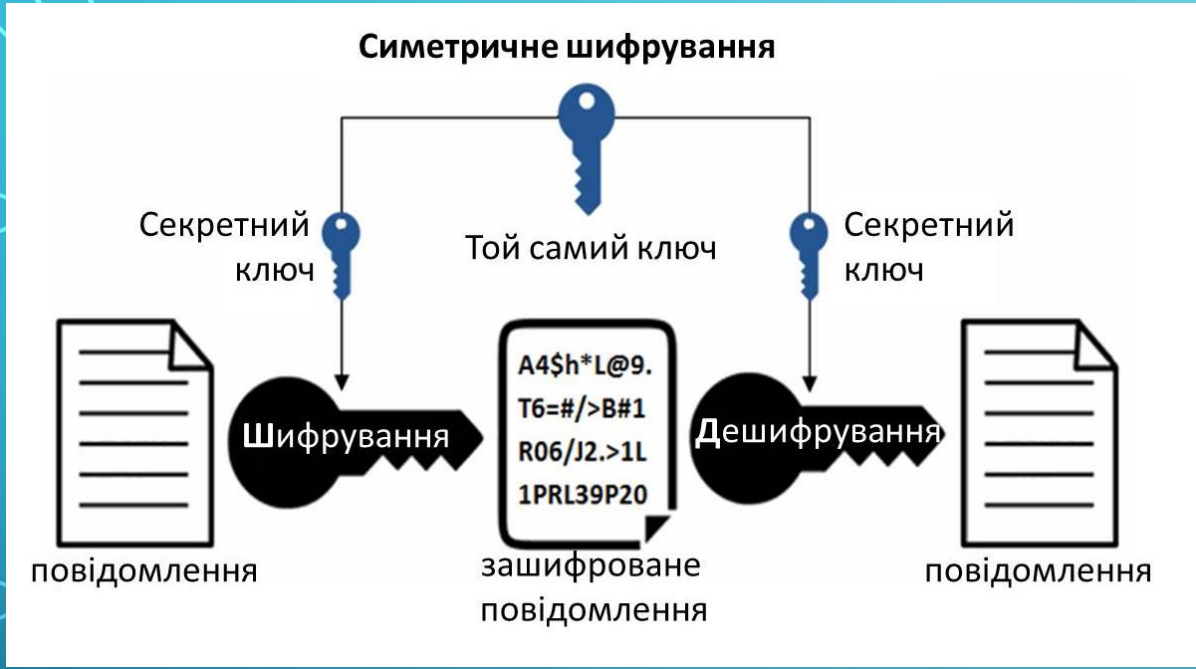


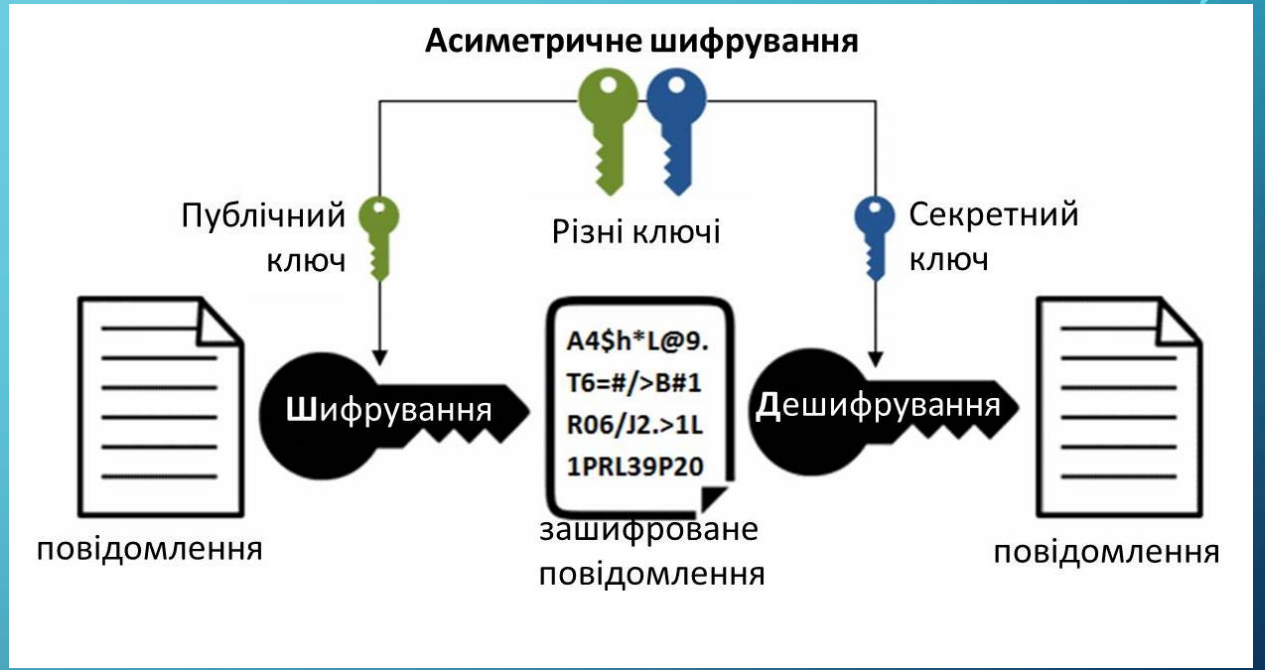
Крок 1. Генерація солі
Крок 2. Застосування псевдовипадкової функції, яка генерує p = 128*r випадкових байт-блоків.
Крок 3. Використання функції змішування (Smix/ROMix) для змішування блоків.
Крок 4. Об’єднання отриманих блоків для генерації ключа потрібної довжини

АНАЛІЗ РОЗГЛЯНУТИХ МЕТОДІВ



ШИФРУВАННЯ ФАЙЛІВ





- DES (Data Encryption Standard),
- AES (Advanced Encryption Standard),
- Triple-DES,
- Rijandel

- DSA (Digital Signature Algorithm),
- ECDSA (Elliptic Curve DSA),
- RSA (Rivest-Shamir-Adleman)

ВИСНОВОК

У роботі розглянуті найпоширеніші загрози веб-застосунків за версією OWASP, проведено аналіз найпоширеніших методів хешування паролів, описані переваги та недоліки кожного метода, виділено найбезпечніший та найбільш актуальний метод. Проведено огляд існуючих методів шифрування бази даних. Розроблено базу даних для зберігання інформації користувача, обрано спосіб зберігання файлів у сховищі. Створено веб-сервіс для хмарного зберігання та інтегровано до нього обраний спосіб захисту.

ДЯКУЮ ЗА УВАГУ