МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки комп’ютерної та програмної інженерії

Кафедра безпеки інформаційних технологій

**Blockchain-технології**

**Лабораторна робота №4**

Тема: HMAC. Код автентифікації повідомлень на основі хешування.

Тривалість заняття: 90 хв.

Київ 2023

**Тема:** HMAC. Код автентифікації повідомлень на основі хешування.

**Мета:** Ознайомитись з методом роботи HMAC.

**Теоретичні відомості**

HMAC (скорочення від [англ.](https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) hash-based message authentication code, код автентифікації повідомлень на основі хешування, або від [англ.](https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) keyed-hash message authentication code, код автентифікації повідомлень на основі хешування з ключем) — механізм перевірки цілісності інформації, що передається або зберігається в ненадійному середовищі. Подібні способи є невід'ємною і необхідною частиною світу відкритих обчислень і комунікацій.

HMAC використовує хеш-функцію разом з секретним ключем, що дозволяє створити унікальний код для кожного повідомлення, який можна використовувати для перевірки автентичності повідомлення. Хеш-функція використовується для створення контрольної суми повідомлення, а секретний ключ додає додатковий рівень безпеки, так як лише особа з доступом до секретного ключа зможе створити коректний HMAC.

Механізми, які надають такі перевірки цілісності на основі секретного ключа, зазвичай називають кодом автентичності повідомлення ([MAC](https://uk.wikipedia.org/wiki/MAC-%D0%BF%D1%96%D0%B4%D0%BF%D0%B8%D1%81)). Як правило, МАС використовується між двома сторонами, які поділяють секретний ключ для перевірки автентичності інформації, переданої між цими сторонами. Цей стандарт визначає MAC.

Код перевірки автентичності повідомлення (MAC) – це криптографічний метод, який використовується для забезпечення цілісності та автентичності повідомлення. Він включає використання секретного ключа для створення фіксованого тегу розміру, який додається до повідомлення. Потім одержувач може перевірити цілісність повідомлення, повторно обчисливши тег з використанням того ж ключа та порівнявши його з отриманим тегом. Якщо теги збігаються, це означає, що повідомлення не було змінено.

Алгоритм MAC приймає як вхідні дані повідомлення і секретний ключ і створює тег. Безпека алгоритму MAC залежить від його базової конструкції. Існує кілька типів алгоритмів MAC, включаючи алгоритми із симетричним ключем, алгоритми на основі хешів та алгоритми на основі блокового шифру.

Одним із широко використовуваних алгоритмів MAC є код автентифікації повідомлень на основі хешів (HMAC). HMAC – це особлива конструкція для MAC, яка базується на криптографічній хеш-функції. Він забезпечує підвищену безпеку, порівняно з традиційними алгоритмами MAC, за рахунок включення додаткових кроків при обчисленні тега.

Основна відмінність між MAC та HMAC полягає у способі обчислення тега. В алгоритмі MAC тег зазвичай обчислюється шляхом застосування криптографічної функції безпосередньо до повідомлення та секретного ключа. Навпаки, HMAC використовує складнішу конструкцію, яка включає два проходи хеш-функції, а також використання внутрішнього та зовнішнього заповнення.

Конструкція HMAC забезпечує кілька переваг у плані безпеки. По-перше, він забезпечує захист від певних типів атак, таких як атаки з розширенням довжини, які можна використовувати для підробки дійсних тегів MAC для змінених повідомлень. Включаючи секретний ключ до обчислення тега, HMAC не дозволяє зловмиснику легко генерувати дійсні теги, не знаючи ключа.

По-друге, HMAC забезпечує більш високий рівень безпеки, порівняно з традиційними алгоритмами MAC. Це пов'язано з додатковою складністю, пов'язаною з двопрохідним обчисленням та використанням заповнення. Ці додаткові кроки ускладнюють зловмиснику використання будь-яких слабких місць у базовій хеш-функції.

Крім того, HMAC призначений для роботи з будь-якою криптографічною хеш-функцією, що робить його гнучким вибором для програм MAC. Він набув широкого поширення в різних протоколах і стандартах, включаючи IPsec, SSL/TLS та SSH.

Щоб проілюструвати різницю між MAC та HMAC, розглянемо наступний приклад. Припустимо, ми маємо алгоритм MAC, який використовує секретний ключ для обчислення тега для повідомлення. Алгоритм просто застосовує хеш-функцію до конкатенації ключа та повідомлення. З іншого боку, HMAC використовує два проходи хеш-функції, а також операції заповнення та XOR для обчислення тега. Ця додаткова складність робить HMAC захищенішим від певних типів атак.

Конструкція HMAC підвищує безпеку MAC завдяки включенню додаткових кроків у обчислення тега. Він забезпечує стійкість до певних типів атак та забезпечує більш високий рівень безпеки порівняно з традиційними алгоритмами MAC. HMAC широко використовується в різних протоколах та стандартах, що робить його цінним інструментом для забезпечення цілісності та справжності повідомлень.

Коли зловмисник перехоплює повідомлення та додає власні шкідливі блоки, це може призвести до вразливості в безпеці зв'язку. Ця вразливість може бути використана для порушення цілісності та справжності повідомлення. В області кібербезпеки цей сценарій має відношення до вивчення кодів автентифікації повідомлень (MAC) і HMAC (коди автентифікації повідомлень на основі хешів).

Код перевірки автентичності повідомлення (MAC) – це криптографічний метод, який використовується для перевірки цілісності та автентичності повідомлення. Він включає секретний ключ, спільно використовуваний відправником і одержувачем, який використовується для створення тега або коду, що додається до повідомлення. Цей тег є доказом того, що повідомлення не було змінено під час передачі.

Однак, якщо зловмисник перехопить повідомлення та додасть свої власні шкідливі блоки, він потенційно може змінити вихідне повідомлення або додати шкідливий контент без виявлення. Це може призвести до різних ризиків та вразливостей безпеки, таких як:

1. Цілісність повідомлення. Додаючи власні шкідливі блоки, зловмисник може змінити вихідний вміст повідомлення. Це може призвести до того, що одержувач прийме та обробить підроблене повідомлення як легітимне, що може призвести до несанкціонованих дій або пошкодження даних.

Наприклад, розглянемо сценарій, у якому фінансова установа надсилає повідомлення про переказ коштів з одного рахунку на інший. Якщо зловмисник перехопить повідомлення і додасть власні шкідливі блоки, він зможе змінити номери рахунків або суму переказу. У результаті кошти можуть бути переведені на непередбачений рахунок або неправильну суму, що призведе до фінансових втрат або шахрайства.

2. Обхід автентифікації. Додаючи власні шкідливі блоки, зловмисник може маніпулювати процесом аутентифікації та оминати заходи безпеки. Це може дозволити їм отримати несанкціонований доступ до систем чи ресурсів.

Наприклад, уявіть сценарій, в якому користувач надсилає запит на сервер, який включає токен автентифікації, згенерований з використанням MAC. Якщо зловмисник перехоплює повідомлення та додає власні шкідливі блоки, він може змінити токен або додати підроблений токен, щоб уникнути процес аутентифікації. Це може надати їм несанкціонований доступ до конфіденційної інформації або привілейованих дій.

3. Довіра та репутація. Коли зловмисник успішно перехоплює та модифікує повідомлення, це може підірвати довіру та репутацію системи зв'язку. Користувачі можуть втратити впевненість у здатності системи захистити свої дані та можуть сумніватися у безпечному спілкуванні.

Щоб зменшити вразливість, що виникає внаслідок перехоплення повідомлення зловмисником та додавання власних шкідливих блоків, дуже важливо використовувати надійні алгоритми MAC та методи безпечного керування ключами. Ці заходи допомагають забезпечити цілісність та справжність повідомлення, що ускладнює підробку вмісту зловмисниками.

Коли зловмисник перехоплює повідомлення та додає свої власні шкідливі блоки, це може призвести до вразливостей у цілісності повідомлення, обході автентичності та довіри. Розуміння цих уразливостей та впровадження надійних методів MAC може допомогти захистити системи зв'язку від таких атак.

Основною метою MAC є виявлення будь-яких несанкціонованих модифікацій повідомлення. Додаючи MAC-адресу до повідомлення, відправник може гарантувати, що одержувач зможе перевірити цілісність при отриманні. Якщо під час надсилання до повідомлення вносяться будь-які зміни, MAC-адреса не співпадатиме, вказуючи на те, що повідомлення було підроблено.

MAC засновані на криптографічних хеш-функціях та секретних ключах. Хеш-функція - це математичний алгоритм, який приймає вхідні дані та виробляє вихідні дані фіксованого розміру, які називають хеш-значенням або дайджестом. Ключ є секретом, загальним для відправника та одержувача, і він використовується для генерації MAC.

Щоб створити MAC, відправник застосовує хеш-функцію до повідомлення та секретного ключа. Отримане значення хеш додається до повідомлення, формуючи MAC. Потім відправник передає повідомлення та MAC-адресу одержувачу.

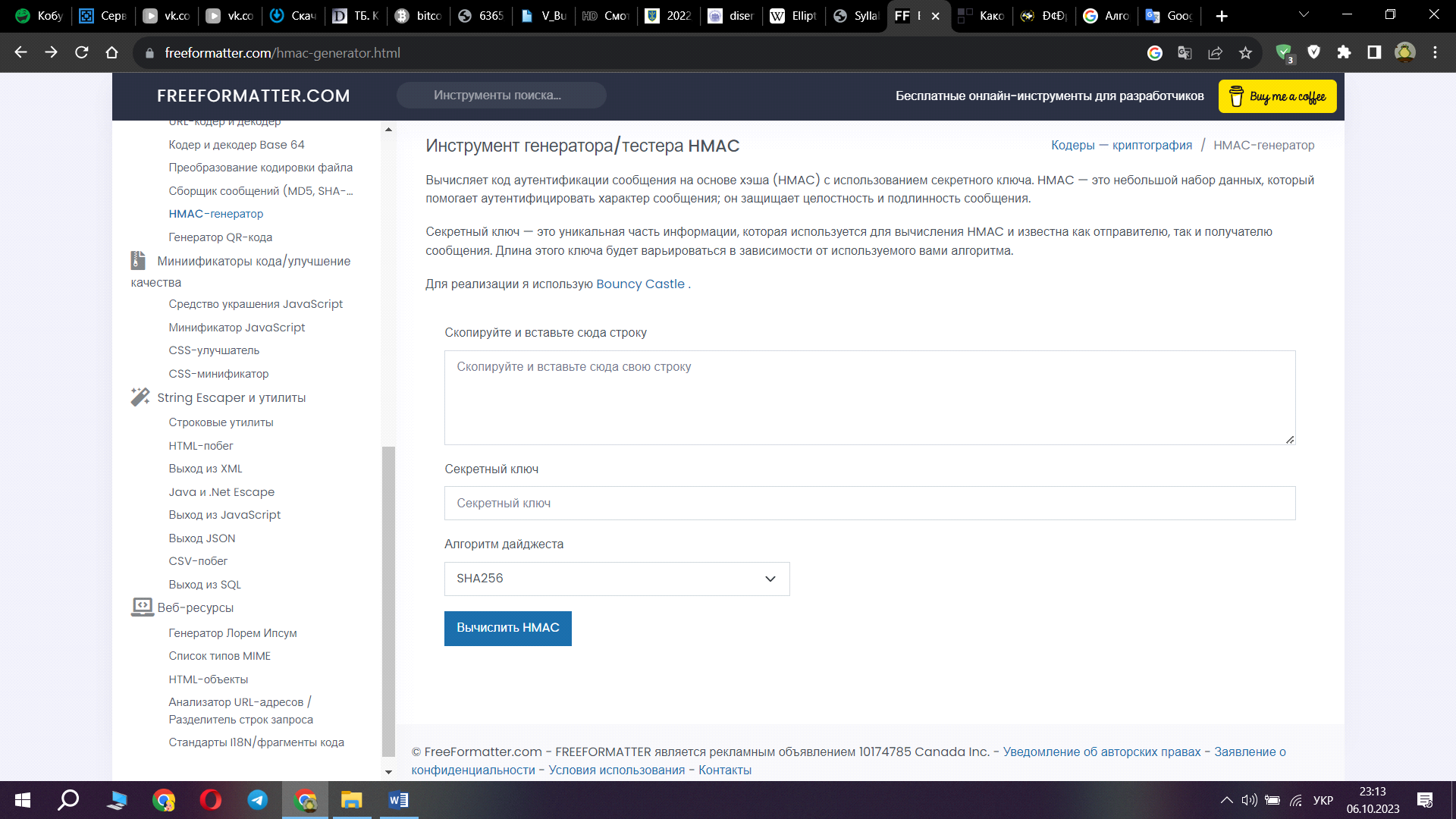
Отримавши повідомлення, одержувач перераховує MAC-адресу, використовуючи ту ж хеш-функцію та секретний ключ. Якщо перерахована MAC-адреса збігається з отриманою MAC-адресою, одержувач може бути впевнений, що повідомлення не було змінено та походить від очікуваного відправника. Якщо MAC-адреси не співпадають, одержувач знає, що повідомлення було підроблено або надійшло не з очікуваного джерела.

MAC-адреси забезпечують високий рівень безпеки, оскільки вони ґрунтуються на властивостях криптографічних хеш-функцій. Ці функції спроектовані як односторонні, що означає, що обчислювально неможливо визначити вихідне введення по хеш-значенню. Крім того, навіть невелика зміна у вхідних даних призведе до значної зміни хеш-значення, що робить вкрай малоймовірним, що зловмисник зможе змінити повідомлення без виявлення.

Одним із широко використовуваних алгоритмів MAC є HMAC (код аутентифікації повідомлень на основі хешів). HMAC поєднує властивості криптографічної хеш-функції з секретним ключем для забезпечення підвищеної безпеки. Він широко використовується в різних протоколах та додатках безпеки, включаючи IPsec, SSL/TLS та SSH.

Код автентифікації повідомлення (MAC) у кібербезпеці призначений для забезпечення цілісності та справжності повідомлення. Він надає одержувачу засоби для перевірки того, що повідомлення не було змінено під час передачі і що воно виходить із надійного джерела. MAC засновані на криптографічних хеш-функціях та секретних ключах та забезпечують високий рівень захисту від несанкціонованих модифікацій.

**Завдання**

1. Використовуючи інтернет-браузер встановлений у вас на комп’ютері перейдіть по посиланню <https://www.freeformatter.com/hmac-generator.html>
   * 1. 
2. На цьому сайті в рядок куди потрібно вставити свій текст напишіть наступне повідомлення « Я Прізвище та Ім’я студент/студентка Національного Авіаційного Університету»
3. Як секретний ключ вкажіть номер вашої групи
4. В рядку Алгоритм дайджест виберіть SHA1, потім натисніть кнопку обчислити. Отримані результати занесіть до таблиці.
5. Далі вирахуйте HMAC за допомогою всіх наявних алгоритмів на сайті не змінюючи текс та секретний ключ, отримані результати занесіть до таблиці.
6. додати таблицю
7. Зробіть порівняння отриманих результатів обчислення.
8. Отримані результати занесіть до звіту.
9. Зробіть висновки та занесіть до звіту.

**Контрольні питання**

1. Що таке HMAC?
2. Яким чином працює HMAC?
3. Яким чином можна використовувати HMAC в кібербезпеці?
4. Що таке хеш-функція?
5. Які переваги забезпечує конструкція HMAC в плані безпеки?