Петров Д.М. КИТ-М120Б

Лабораторна робота № 3

Time-based One Time Password

Мета: Дослідити і реалізувати механізм генерації одноразових паролів TOTP.

Індивідуальне завдання

Дослідити алгоритм Time-based One Time Password. Створити програму, що реалізує механізм генерації одноразових паролів TOTP. Для додаткових балів - організувати взаємодію з мобільним додатком Google Authenticator.

Хід роботи

TOTP (Time-based One-Time Password Algorithm, RFC 6238) — OATH-алгоритм створення одноразових паролів для захищеної аутентифікації, є поліпшенням HOTP (HMAC-Based One-Time Password Algorithm). Є алгоритмом односторонньої аутентифікації — сервер засвідчується в справжності клієнта. Головна відмінність TOTP від HOTP це генерація пароля на основі часу, тобто час є параметром. При цьому зазвичай використовується не точне зазначення часу, а поточний інтервал з встановленими заздалегідь межами (наприклад, 30 секунд).

- T - дискретне значення часу, що використовується в якості параметра. (Вимірюється в одиницях , 4 байти)
- X - інтервал часу, протягом якого дійсний пароль. (За замовчуванням 30 сек.)
- T0 - початковий час, необхідний для синхронізації сторін. (За замовчуванням — час від початку UNIX ери)
- K - спільний секрет.
- CurrentTime - поточний час.

$$T = (CurrentTime - T_0)/X$$

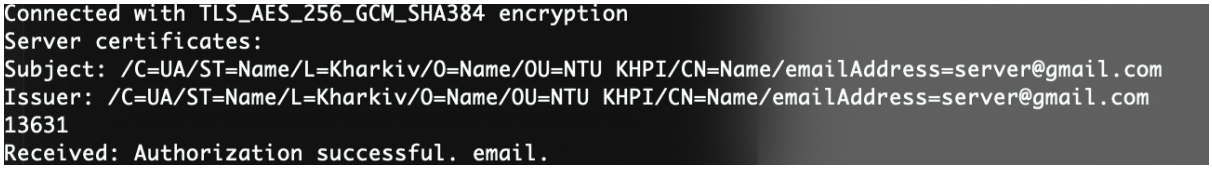
$$\mathrm{HOTP}(K,T) = Truncate(\mathrm{HMAC\text{-}SHA\text{-}1}(K,T))$$

$$\mathrm{TOTP} = \mathrm{HOTP}(K,T)$$

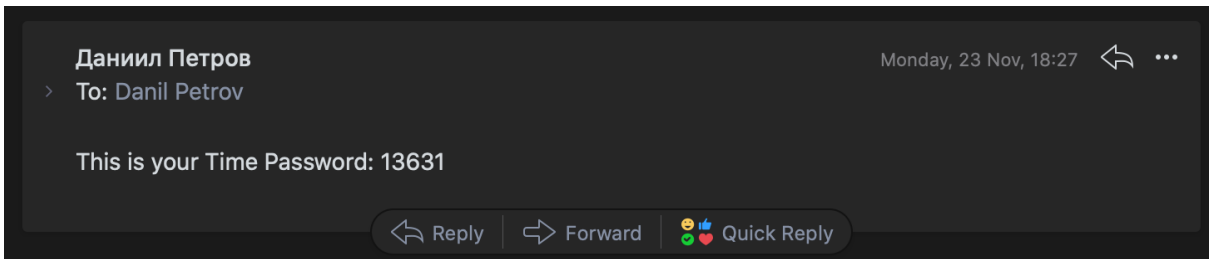
- HMAC-SHA-1(K,T) — ггенерація 20-ти байт на основі таємного ключа і часу за допомогою хеш-функції SHA-1.
- Truncate — функція вибору певним способом 5 байт.

Також варто відзначити, що на відміну від HOTP, який заснований тільки на SHA-1, TOTP може також використовувати HMAC-SHA-256, HMAC-SHA-512 та інші HMAC-хеш-функції.

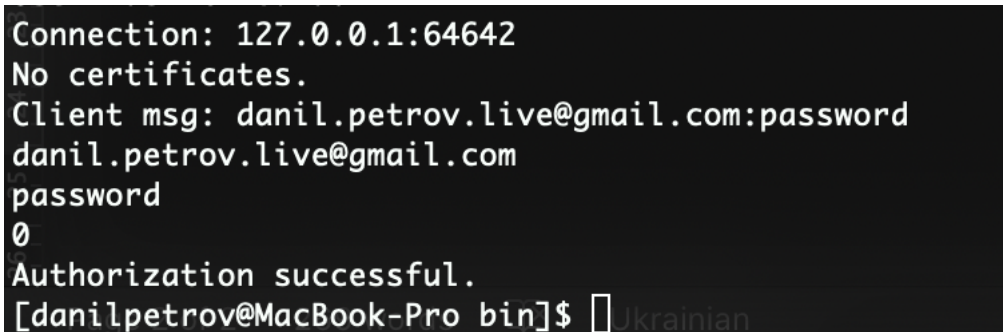
В ході лабораторної роботи було розроблено дві програми: клієнт та сервер. Клієнт проходить ідентифікацію на сервері, сервер отримує логін та пароль, перевіряє їх на наявність у базі, та потім на email, який виступає логіном, відправляє повідомлення з тимчасовим кодом який сервер генерує для кожного клієнта.



На рисунку можна побачити пароль (13631), який був відправлений клієнтові на почтову скриньку.



Повідомлення з почтової скриньки.



Сервер отримав логін (danil.petrov.live@gmail.com) та пароль (password), перевірив його через хеш функцію MD5 та згенерував тимчасовий пароль на 120 секунд: відправив його на поштову скриню і чикав код від клієнта.

Висновок

Дослідив і реалізував механізм генерації одноразових паролів TOTP.