

Міністерство освіти і науки України  
Національний технічний університет «ХПІ»  
Навчально-науковий інститут комп'ютерних наук та інформаційних  
технологій  
Кафедра комп'ютерної інженерії та програмування

## **ЗВІТ**

з лабораторної роботи № 8  
з дисципліни «Сучасні технології безпечного програмування»  
**«TIME-BASED ONE TIME PASSWORD»**

Виконав:  
студент гр. КН-Н9226  
Кулик Д.І.

Перевірив:  
Бульба С. С.

**Мета роботи:** Дослідити і реалізувати механізм генерації одноразових паролів TOTP.

### Індивідуальне завдання

Time-based One Time Password. Створити програму, що демонструє роботу розробленого алгоритму. Організувати взаємодію з мобільним додатком Google Authenticator.

### Хід роботи

TOTP означає Time-based One-Time Passwords і є поширеною формою двофакторної автентифікації (2FA). Унікальні цифрові паролі генеруються за стандартизованим алгоритмом, який використовує поточний час як вхідні дані. Паролі на основі часу доступні в автономному режимі та забезпечують зручність і підвищену безпеку облікового запису, якщо використовувати їх як другий фактор.

### Важливі фрагменти програми

Приведена нижче функція оновлює тимчасовий пароль у файлі (див. рис. 1)

```
def task():
    log.debug('Generating TOTP...')
    totp = get_totp_token(config.SECRET)
    write_to_file(totp, config.FILENAME)
    log.debug(f'Wrote new TOTP [{totp}] to file.')

def set_background_update():
    scheduler = BackgroundScheduler()
    job = scheduler.add_job(task, 'interval', seconds=config.INTERVAL)
    job.func()
    scheduler.start()
```

**Рисунок 1** – Реалізоване оновлення TOTP

Приведені нижче функції генерують ТОТР (див. рис. 2)

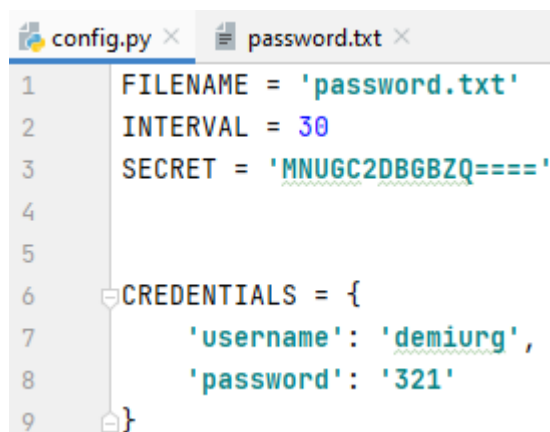
```
def get_hotp_token(secret, intervals_no):
    key = base64.b32decode(secret, True)
    msg = struct.pack(">Q", intervals_no)
    h = hmac.new(key, msg, hashlib.sha1).digest()
    o = o = h[19] & 15
    h = (struct.unpack(">I", h[o:o + 4])[0] & 0x7fffffff) % 1000000
    return h

def get_totp_token(secret):
    x = str(get_hotp_token(secret, intervals_no=int(time.time()) // INTERVAL))
    while len(x) != 6:
        x += '0'
    return x
```

Рисунок 2 – Генерація ТОТР

```
if __name__ == '__main__':
    set_background_update()
    login()
    entered_code = enter_code()
    while not validate(entered_code):
        entered_code = input('Невірний код! Спробуйте ще раз:\n')
    print('Авторизація пройшла успішно!')
```

Рисунок 3 – Перевірка на ТОТР



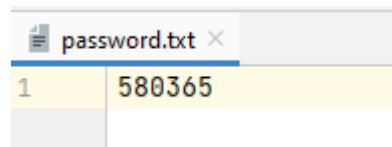
```
config.py x password.txt x
1 FILENAME = 'password.txt'
2 INTERVAL = 30
3 SECRET = 'MNUGC2DBGBZQ===='
4
5
6 CREDENTIALS = {
7     'username': 'demiurg',
8     'password': '321'
9 }
```

Рисунок 5 – Файл config.py

## Результати роботи програми

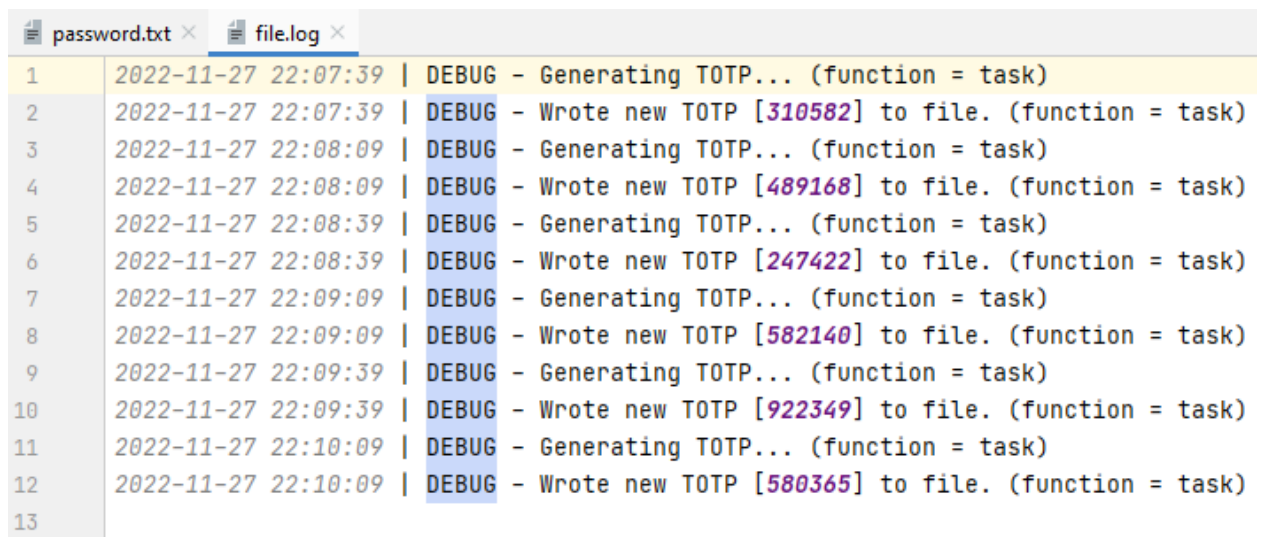
```
C:\Users\Daniil\PycharmProjects\stbp\Scripts\python.exe C:/Users/Daniil/PycharmProjects/stbp/LABS/kuLyk08/main.py
Введіть нікнейм: dem1urg
Введіть пароль: 321
Введіть код верифікації: 46263
Невірний код! Спробуйте ще раз:
fkweio
Невірний код! Спробуйте ще раз:
580365
Авторизація пройшла успішно!
```

Рисунок 6 – Результат виконання програми



1	580365
---	--------

Рисунок 7 – Файл password.txt



	password.txt	file.log
1		2022-11-27 22:07:39   DEBUG - Generating TOTP... (function = task)
2		2022-11-27 22:07:39   DEBUG - Wrote new TOTP [310582] to file. (function = task)
3		2022-11-27 22:08:09   DEBUG - Generating TOTP... (function = task)
4		2022-11-27 22:08:09   DEBUG - Wrote new TOTP [489168] to file. (function = task)
5		2022-11-27 22:08:39   DEBUG - Generating TOTP... (function = task)
6		2022-11-27 22:08:39   DEBUG - Wrote new TOTP [247422] to file. (function = task)
7		2022-11-27 22:09:09   DEBUG - Generating TOTP... (function = task)
8		2022-11-27 22:09:09   DEBUG - Wrote new TOTP [582140] to file. (function = task)
9		2022-11-27 22:09:39   DEBUG - Generating TOTP... (function = task)
10		2022-11-27 22:09:39   DEBUG - Wrote new TOTP [922349] to file. (function = task)
11		2022-11-27 22:10:09   DEBUG - Generating TOTP... (function = task)
12		2022-11-27 22:10:09   DEBUG - Wrote new TOTP [580365] to file. (function = task)
13		

Рисунок 8 – Файл log.file

**Висновки:** в результаті виконання лабораторної роботи було досліджено і реалізовано механізм генерації одноразових паролів TOTP.