Laboratorium 3

Szyfrowanie poczty - PGP

W sprawozdaniu zamieść zrzuty ekranu z istotnych etapów oraz odpowiedzi na pytania.

Taki symbol onacza, że trzeba w sprawozdaniu dodać zrzut ekranu (najczęściej 1) z wyniku działania polecenie.

Taki symbol oznacza, że należy dodać opis (najczęściej 1 zdanie) z wyniku działania polecenia.

Wstęp

PGP jest oprogramowaniem, które w łatwy sposób pozwala na korzystanie ze współczesnych algorytmów kryptograficznych w celu zabezpieczenia korespondencji a także ochrony wszelkich innych danych w formie elektronicznej. Skrót PGP w języku angielskim rozwijamy jako "Preety Good Privacy", co w tłumaczeniu na nasz ojczysty język oznacza „Całkiem niezłą prywatność". Śmiało można powiedzieć, że stopień prywatności oferowany przez PGP jest o wiele wyższy, niż mogło by to wynikać z samej nazwy.

Philip Zimmermann stworzył PGP, by umożliwić szeroki dostęp do kryptografii. Pierwsza popularna wersja, PGP 2.3a z 1993 roku, wykorzystywała algorytm RSA do zarządzania kluczami i szyfr IDEA, z maksymalną długością klucza RSA do 1024 bitów. Wersje 2.x rozwijano mimo sporów patentowych, a Massachusetts Institute of Technology przejął ich dystrybucję. W 1995 roku powstało PGP Inc., a wersja PGP 5.0, w odpowiedzi na ograniczenia patentowe, wprowadziła nowe algorytmy (DSS/Diffie-Hellman, 3DES, CAST, SHA-1). Aby obejść przepisy eksportowe USA, kod PGP drukowano i przewożono do Europy. W 1997 roku firmę PGP Inc. kupiło Network Associates Inc., które rozwinęło PGP o funkcje VPN, certyfikaty X.509 i szyfrowanie dysków. Zimmermann odszedł z NAI w 2001 roku i obecnie angażuje się w rozwój OpenPGP.

Źródło: https://jacobriggs.io/blog/posts/how-do-pgp-keys-work-6

I. Przygotowanie środowiska pracy

1. Przygotuj maszynę wirtualną z systemem Kali Linux. (**rekomendacja:** VMware Workstation Pro)

> Możesz skorzystać z gotowej maszyny wirtualnej dostępnej na stronie Kali Linux lub samodzielnie zainstalować i skonfigurować system – wybór należy do Ciebie.

2. Uruchom maszynę wirtualną.

> Jeżeli skorzystałeś z gotowej maszyny wirtualnej, domyślne dane logowania to: **kali/kali**

3. Otwórz terminal w Kali Linux.

4. Wykonaj aktualizację repozytoriów:

```
sudo apt update
```

5. Zainstaluj klienta pocztowego Mozilla Thunderbird.

```
sudo apt install thunderbird -y
```

6. Uruchom klienta i połącz się ze swoim kontem pocztowym.

II. Praca z GnuPGP

> Program GnuPGP jest domyślnie zainstalowany w systemie Kali Linux.

1. Po połączeniu z kontem przejdź do terminala Kali Linux.

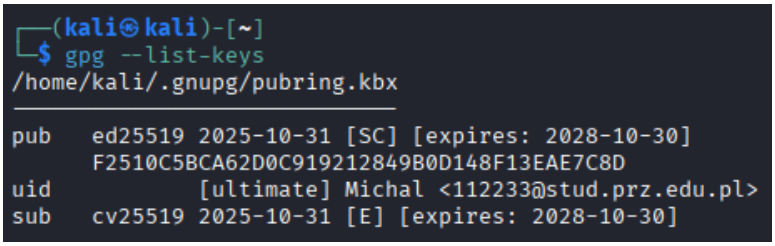
2. Wygeneruj klucz, używając następującego polecenia:

```
gpg --gen-key
```

   a. Jak nazwę podaj: `u_twój_numer_indeksu` **(np. u112233).**
   b. Wprowadź adres email, dla którego chcesz wygenerować klucz.
   c. Upewnij się, że dane są poprawne, i zatwierdź operację, wpisując literę "O".
   d. Wymyśl i wpisz hasło zabezpieczające Twój klucz.

3. Wyświetl listę posiadanych kluczy:

```
gpg --list-keys
```



Opis linia po linii:

`/home/kali/.gnupg/pubring.kbx` – lokalizacja pliku kontenera kluczy publicznych (KBX). To standardowe miejsce, gdzie GnuPG trzyma publiczne klucze dla tego użytkownika (`~/.gnupg`).

`pub ed25519 2025-10-31 [SC] [expires: 2028-10-30]` – klucz główny (publiczny).

- `pub` – klucz publiczny (primary public key).
- `ed25519` – algorytm kryptograficzny Ed25519 (EdDSA na krzywej Curve25519 wykorzystywany zwykle do podpisywania i certyfikowania). Nowoczesny, szybki i bezpieczny algorytm.
- `2025-10-31` – data utworzenia klucza.
- `[SC]` – możliwe zastosowania:
    - `S (Sign)` – do podpisywania danych i innych kluczy,
    - `C (Certify)` – do certyfikowania własnych subkluczy i tożsamości.
- `[expires: 2028-10-30]` – data wygaśnięcia klucza głównego.

`F2510C5BCA62D0C919212849B0D148F13EAE7C8D` – tzw. fingerprint (odcisk palca) Twojego klucza głównego — unikalny 40-znakowy identyfikator. Służy do jednoznacznego potwierdzenia, że klucz należy do Ciebie. Przy weryfikacji klucza między osobami zawsze porównuje się właśnie ten fingerprint, np. przez telefon lub na spotkaniu.

`uid [ultimate] Michal 112233@stud.prz.edu.pl` – identyfikator użytkownika (User ID) powiązany z tym kluczem.

- `uid` — identyfikator użytkownika przypisany do klucza (imię + e-mail).
- `[ultimate]` — oznacza najwyższy poziom zaufania lokalnego (trust) przypisany do tego klucza w Twojej bazie. Poziom ultimate informuje GPG, że całkowicie ufasz właścicielowi tego klucza — w tym przypadku sobie. Jest to ustawienie domyślne dla własnych kluczy i pozwala systemowi uznać wszystkie podpisy wykonane tym kluczem za w pełni wiarygodne.

`sub cv25519 2025-10-31 [E] [expires: 2028-10-30]` – subklucz (podrzędny) powiązany z Twoim kluczem głównym.

- `sub` – subkey (klucz podrzędny).
- `cv25519` – algorytm Curve25519 – używany do szyfrowania (a nie podpisywania).
- `2025-10-31` — data utworzenia subklucza (ta sama co główny).
- `E (Encrypt)` — subklucz służy do szyfrowania (czyli inni będą używać tego subklucza do szyfrowania wiadomości dla Ciebie).
- `[expires: 2028-10-30]` – data wygaśnięcia subklucza (zwykle taka sama jak głównego).

Reasumując, mamy zestaw nowoczesnych kluczy GPG:

Typ klucza	Algorytm	Funkcja	Ważny do	Użycie
Główny (pub)	Ed25519	Podpisywanie i certyfikacja	2028-10-30	[SC]
Subklucz (sub)	Curve25519	Szyfrowanie	2028-10-30	[E]

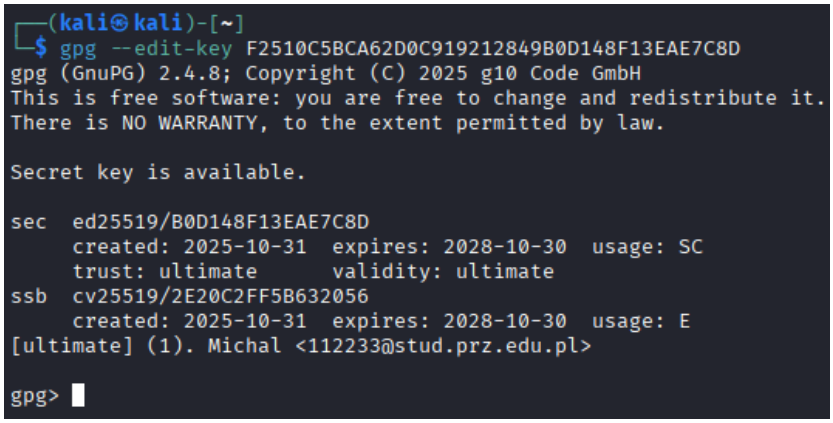
- To konfiguracja zalecana przez GnuPG — klucz główny do podpisów i subklucz do szyfrowania.
- Głównego klucza używasz do podpisywania innych kluczy, wiadomości lub potwierdzania swojej

tożsamości.
- Subklucz (E) służy do odbierania zaszyfrowanych wiadomości — inni użyją jego publicznej części, żeby zaszyfrować wiadomość tylko dla Ciebie.
- Twój fingerprint to najważniejszy identyfikator przy wymianie kluczy.

4. Skopiuj swój fingerprint.

5. Wejdź w edycję klucza:

```
gpg --edit-key fingerprint
```



6. Zobacz dostępne polecenia. W interaktywnym edytorze wpisz:

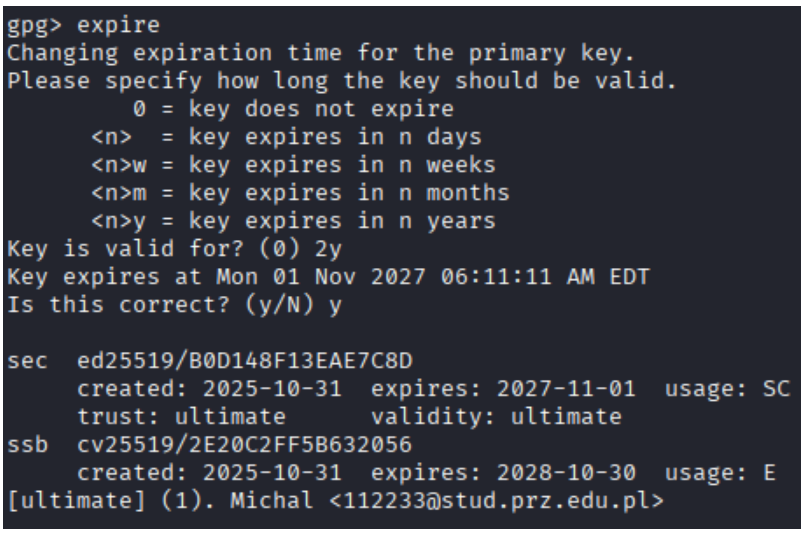
```
help
```

7. Zmień datę wygaśnięcia klucza:

```
expire
```

8. Ustaw nowy okres ważności – przykładowo na 2 lata (zatwierdź, gdy GPG o to poprosi):

```
2y
```



9. Wyjdź z edytora i zapisz:

```
quit
```

10. Wyeksportuj publiczny klucz (binarnie):

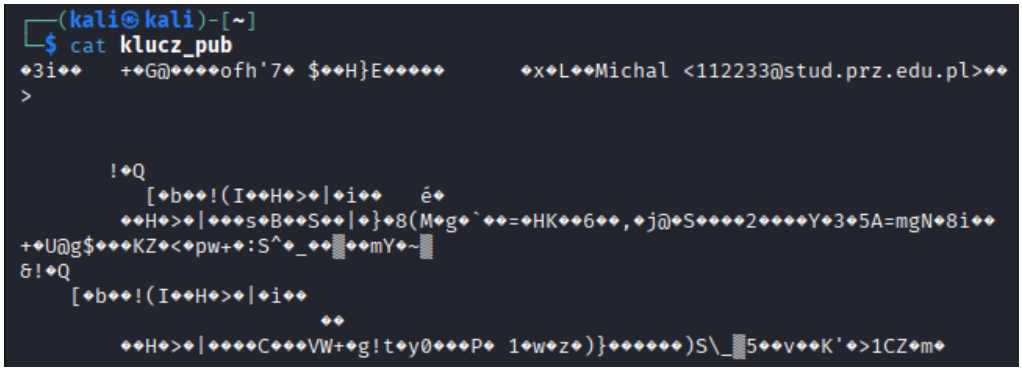
```
gpg --output twój_nr_indeksu.gpg --export fingerprint
```

11. Sprawdź, czy plik rzeczywiście powstał:

```
ls
```

12. Odczytajmy zawartość pliku

```
cat twój_nr_indeksu.gpg
```



Jak widzisz, klucz jest zapisany w postaci surowych bajtów (format binarny). Wygenerujmy go teraz w czytelniejszym formacie ASCII.

13. Wyeksportuj ten sam klucz w formacie ASCII:

```
gpg -a --output twój_nr_indeksu.asc --export fingerprint
```

14. Wyświetl zawartość w ASCII:

```
cat twój_nr_indeksu.asc
```

Tym razem klucz jest znacznie czytelniejszy – to ten sam klucz, tylko zakodowany Base64 z nagłówkami i CRC.

Kiedy czego użyć?

- ASCII: wysyłka mailem, publikacja na stronie/GitHub, wklejanie do formularzy/komunikatorów.
- Binarny: lokalne backupy (zajmuje mniej miejsca niż ASCII), automatyzacja i transfer kanałami „binary-safe” (SCP/SFTP/HTTPS/pendrive).

Przejdźmy do kluczowej części instrukcji – wymiany kluczy w celu zaszyfrowania wiadomości.

15. Wymień się z sąsiadem plikami kluczy `.asc`.

16. Zaimportuj otrzymany klucz:

```
gpg -import otrzymany_klucz.asc
```

```
u112233@112233:~$ gpg --import public.asc
gpg: klucz B0D148F13EAE7C8D: klucz publiczny „Michal <112233@stud.prz.edu.pl>” wczytano do zbioru
gpg: Ogółem przetworzonych kluczy: 1
gpg:          dołączono do zbioru: 1
```

17. Sprawdź, czy został dodany:

```
gpg --list-keys
```

```
u112233@112233:~$ gpg --list-keys
/home/u112233/.gnupg/pubring.kbx
--------------------------------
pub   ed25519 2025-10-31 [SC] [wygasa: 2027-11-01]
      F2510C5BCA62D0C919212849B0D148F13EAE7C8D
uid     [    nieznane   ] Michal <112233@stud.prz.edu.pl>
sub   cv25519 2025-10-31 [E] [wygasa: 2028-10-30]
```

Fingerprint, ze względu na długość, jest nieco uciążliwy do weryfikacji.

18. Wyświetl fingerprint w formie czytelnej dla człowieka (przydatne do weryfikacji np. przez telefon):

```
gpg -fingerprint fingerprint
```

```
┌──(kali㉿kali)-[~]
└─$ gpg --fingerprint 112233@stud.prz.edu.pl
pub   ed25519 2025-10-31 [SC] [expires: 2028-10-30]
      F251 0C5B CA62 D0C9 1921  2849 B0D1 48F1 3EAE 7C8D
uid           [ultimate] Michal <112233@stud.prz.edu.pl>
sub   cv25519 2025-10-31 [E] [expires: 2028-10-30]
```

19. Porównaj fingerprint z sąsiadem – upewnij się, że identyfikatory w pełni się zgadzają.

Jak już zauważyłeś, poziom zaufania dla zaimportowanego klucza jest nieokreślony. Ponieważ przed chwilą potwierdziłeś z sąsiadem jego poprawność, ustaw odpowiedni poziom zaufania.

20. Przejdź do trybu edycji klucza. Użyj poniższej komendy:

```
gpg --edit-key fingerprint_klucza_zaimportowanego
```

21. Ustaw zaufanie `trust` i wybierz poziom zaufania (`4 = I trust fully`).

22. Wyjdź z trybu edytora.

23. Sprawdź, czy poziom zaufania się zmienił.

24. Utwórz plik tekstowy:

```
nano wiadomosc.txt
```

25. Wpisz treść przykładowej wiadomości:

```
Witaj,

Mam na imię: imię naziwsko.
Mój nr indeksu: nr_indeksu

Oto moja zaszyfroana wiadomość dla nr_indeksu_odbiorcy.

Pozdrawiam
mój_nr_indeksu
```

26. Zapisz i zamknij edytor.

27. Zaszyfruj wiadomość dla odbiorcy (ASCII):

```
gpg --output wiadomosc.asc --armor --encrypt --recipient adres@odbiorcy wiadomosc.txt
```

28. Sprawdź, czy zaszyfrowano:

```
cat wiadomosc.asc
```

Powinien pojawić się blok `-----BEGIN PGP MESSAGE-----`

29. Wymieńcie się z sąsiadem zaszyfrowanymi plikami `.asc`.

30. Po otrzymaniu od sąsiada wiadomości – odszyfruj ją:

```
gpg --output odszyfrowana_wiadomosc.txt --decrypt wiadomosc.asc
```

31. A następnie odczytaj:

```
cat odszyfrowana_wiadomosc.txt
```

III. OpenPGP w kliencie pocztowym Thunderbird

W programie Mozilla Thunderbird opcja OpenPGP jest zintegrowana bezpośrednio, bez potrzeby instalowania dodatkowych wtyczek.

1. Aby wygenerować parę kluczy, kliknij prawym przyciskiem myszy na swoje konto i wybierz `Settings`.

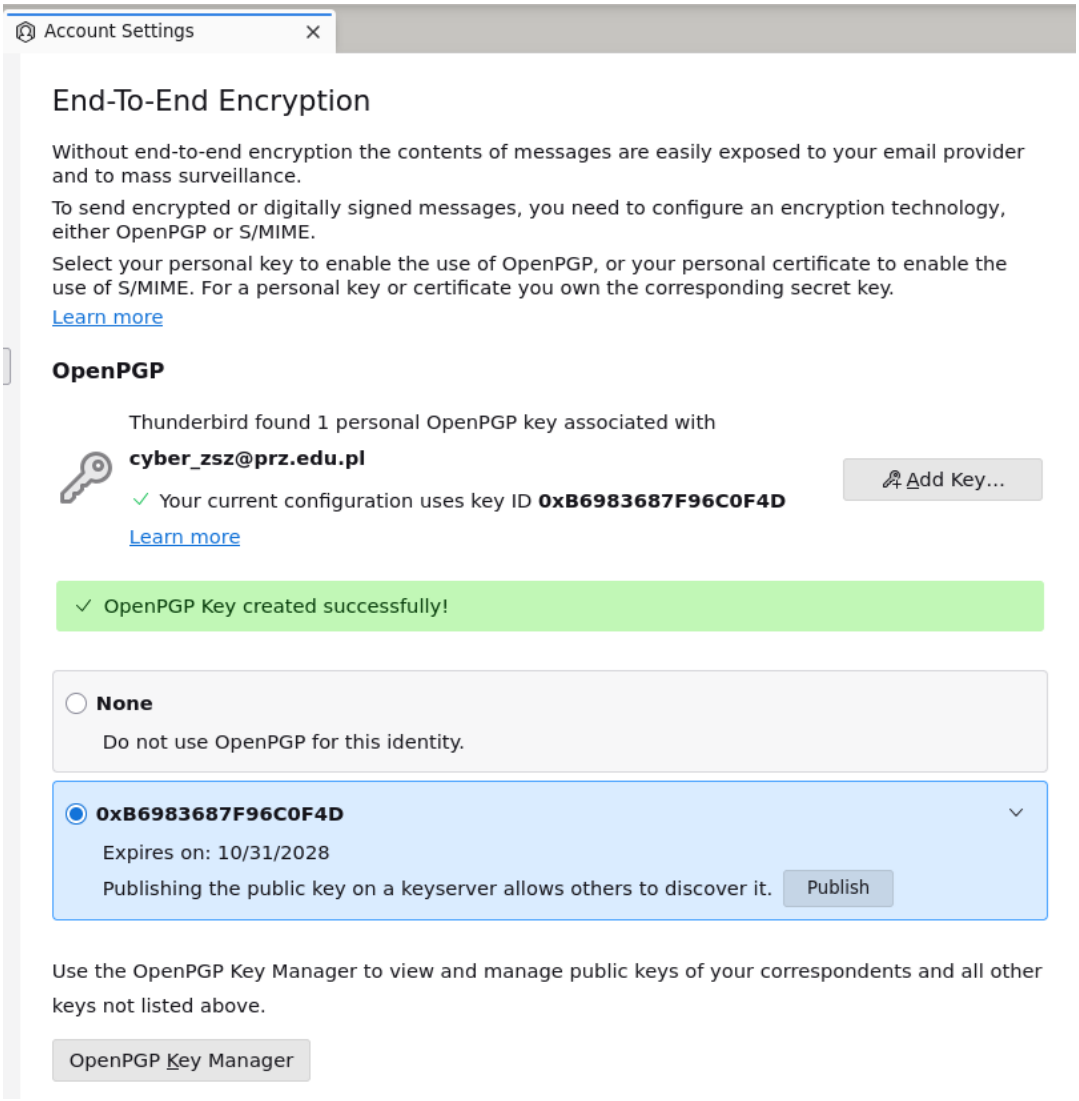
2. Przejdź do zakładki „End-To-End Encryption” i wybierz `Add Key...`.

3. Wybierz `Create a New OpenPGP Key`.

4. Ustaw czas wygaśnięcia klucza, a następnie kliknij `Generate Key`.

5. Zatwierdź, klikając `Confirm`.

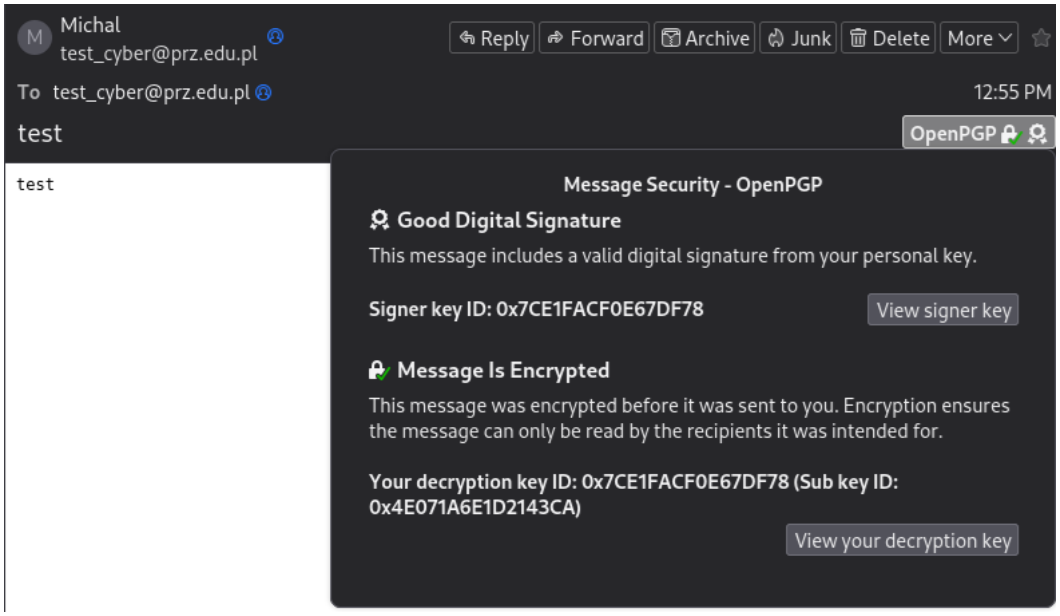
6. Po poprawnym dodaniu klucza powinieneś zobaczyć efekt podobny do poniższego przykładu.



7. Wybierz `OpenPGP Key Manager`, a następnie dwukrotnie kliknij na swój klucz.

8. Wykonaj zrzut ekranu otwartego okna i umieść go w sprawozdaniu.

9. Przetestuj, wysyłając wiadomość do samego siebie.



10. Aby wyeksportować klucz publiczny, kliknij prawym przyciskiem myszy na swoje konto i wybierz `Settings -> End-To-End Encryption -> OpenPGP Key Manager`. Następnie kliknij prawym przyciskiem na swój klucz i wybierz opcję `Export Public Key(s) to File`.

ZADANIE

Podobnie jak na poprzednich zajęciach wyślij zaszyfrowanego i podpisanego maila na adres cyber_zsz@prz.edu.pl