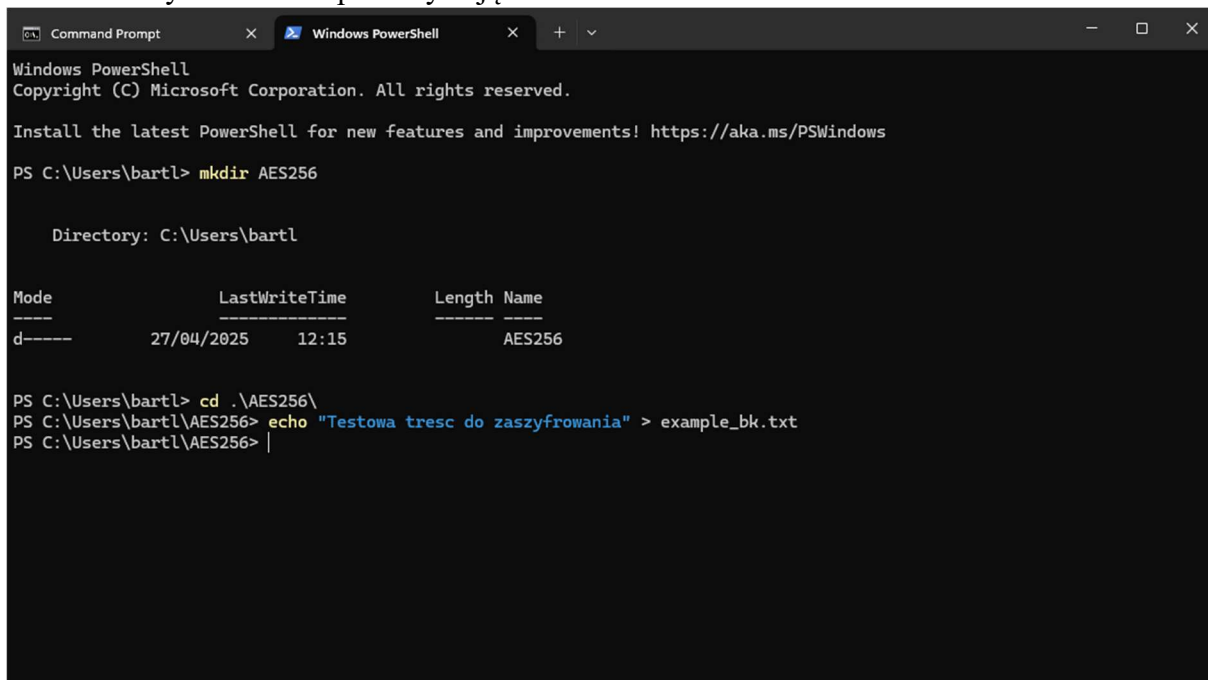


INSTRUKCJA LABORATORYJNA NUMER 3	
Przedmiot: Zagrożenia bezpieczeństwa systemów	Tok: 2024/2025
Cel praktyczny zajęć: Kryptografia w praktyce - Szyfrowanie i deszyfrowanie pliku z użyciem Open SSL.	

Scenariusz ćwiczenia

Celem ćwiczenia jest zapoznanie ze sposobem procesu zabezpieczania informacji poprzez szyfrowanie plików przy użyciu algorytmu AES-256.

1. Zainstaluj OpenSSL, dla Windows możesz pobrać instalator ze strony:
<https://slproweb.com/products/Win32OpenSSL.html>
2. Dodaj go do zmiennej środowiskowej, żeby działał w CMD
3. Utwórz nowy folder oraz plik używając CMD



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

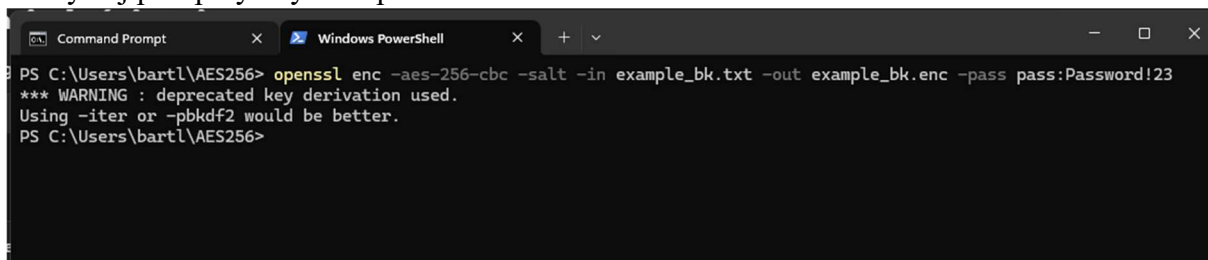
PS C:\Users\bartl> mkdir AES256

Directory: C:\Users\bartl

Mode                LastWriteTime         Length Name
----                -
d-----          27/04/2025   12:15             AES256

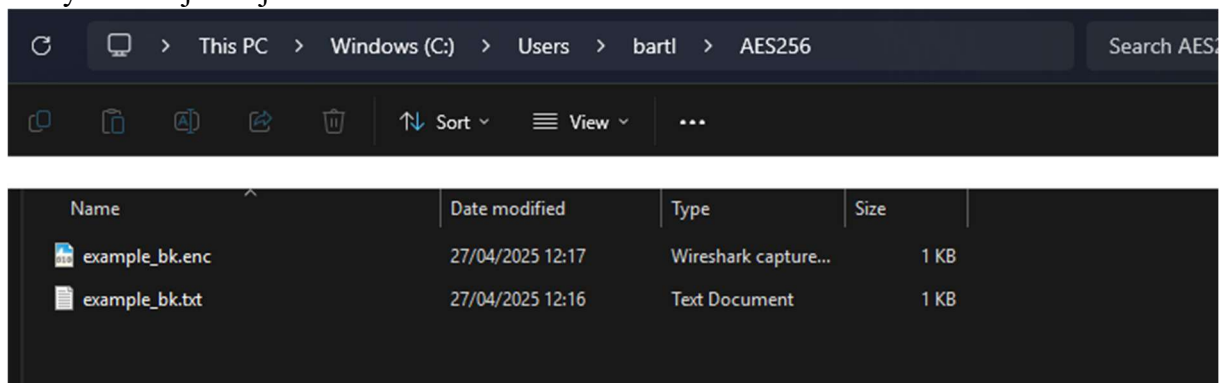
PS C:\Users\bartl> cd .\AES256\
PS C:\Users\bartl\AES256> echo "Testowa tresc do zaszyfrowania" > example_bk.txt
PS C:\Users\bartl\AES256> |
```

4. Zaszyfruj plik przy użyciu Open SSL



```
PS C:\Users\bartl\AES256> openssl enc -aes-256-cbc -salt -in example_bk.txt -out example_bk.enc -pass pass:Password!23
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
PS C:\Users\bartl\AES256>
```

Wynikiem operacji powinno być utworzenie pliku tekstowego oraz jego zaszyfrowanej wersji



5. Odszyfruj plik i sprawdź czy jego treść jest zgodna z plikiem pierwotnym.
6. Wygeneruj SHA-256 dla pliku pierwotnego i odszyfrowanego, zweryfikuj czy hashe są takie same, jeśli tak to co to oznacza? Możesz użyć polecenia:
`openssl dgst -sha256 example_bk.txt`
7. Zmień losowy bajt w zaszyfrowanym pliku i spróbuj go odszyfrować, jaki jest efekt operacji i dlaczego?

Pytania do ćwiczenia:

- Co to jest funkcja skrótu i do czego jej używamy? Jakie cechy powinna mieć dobra funkcja skrótu?
- Co to jest Open SSL i jakie jest jego praktyczne zastosowanie?
- Co by się stało, gdybyśmy nie stosowali funkcji skrótu przy transmisji danych?
- Czym jest Certyfikat SSL? Do czego jest używany?
- Co to jest szyfrowanie symetryczne?
- Dlaczego używamy soli (-salt) podczas szyfrowania plików?
- Co się stanie, jeśli podamy złe hasło przy deszyfrowaniu pliku? Czy plik się odszyfruje? Jeśli nie, co wtedy otrzymamy?
- Czym różni się szyfrowanie danych od haszowania danych? Czy możliwe jest odzyskanie oryginalnych danych z hasza?
- Jakim poleceniem odszyfrowałeś plik w ćwiczeniu?
- W jaki sposób sprawdzałeś integralność danych po odszyfrowaniu?
- Czy zmiana choćby jednego znaku w zaszyfrowanym pliku wpływa na wynik odszyfrowania? Dlaczego?

Po zakończonej pracy nie zapomnij przesłać wybranych pakietów oraz odpowiedzi!