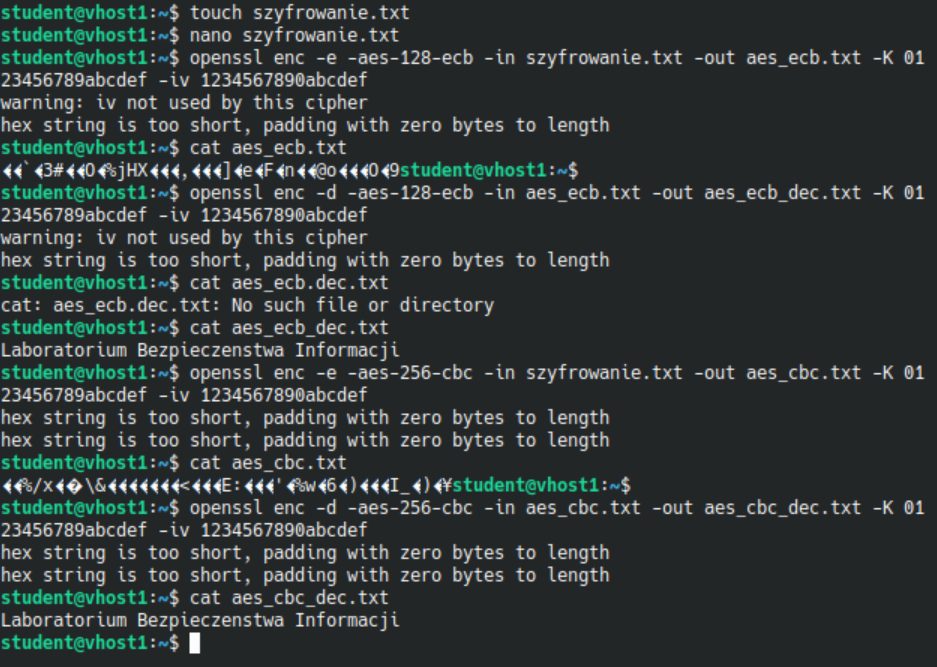
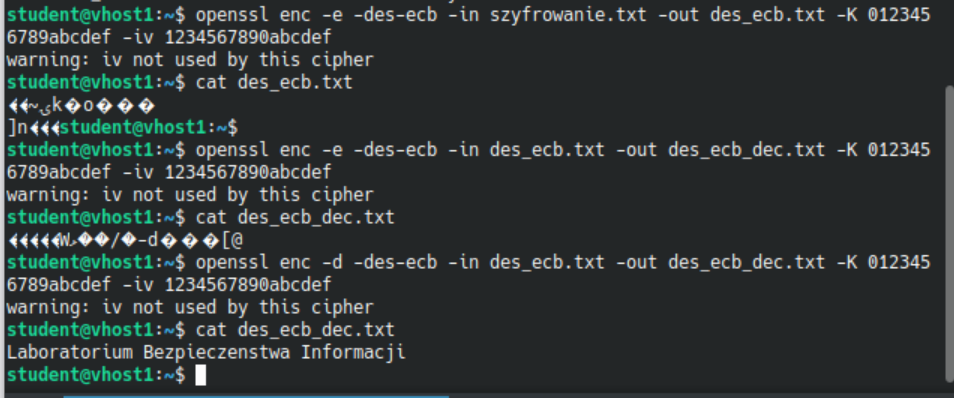
**Jakub Dudek**

**Sprawozdanie Laboratorium 4**

**P.4.1. Zwróć uwagę na komunikaty na rys. 4.1. Dlaczego tak się dzieje? Czy wszystkie tryby wymagają wektora inicjalizującego? Udokumentuj w sprawozdaniu szyfrowanie i deszyfrowanie pliku przy użyciu wybranych algorytmów szyfrujących i trybów pracy.**

****

****

****

Komunikaty oznaczają, że używa za krótki klucz. Przy aes-128 klucz musi mieć 32 znaki.

Nie wszystkie tryby wymagają wektora inicjalizującego.

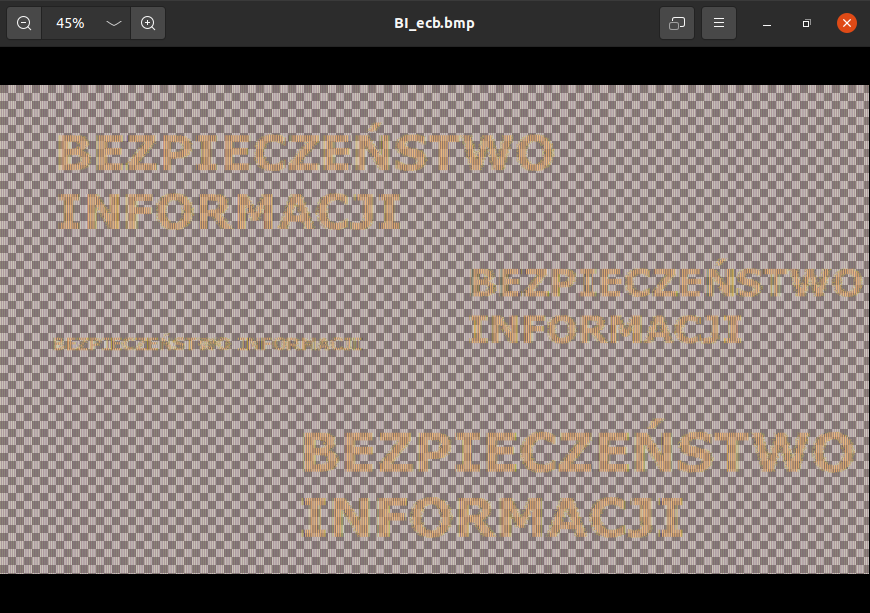
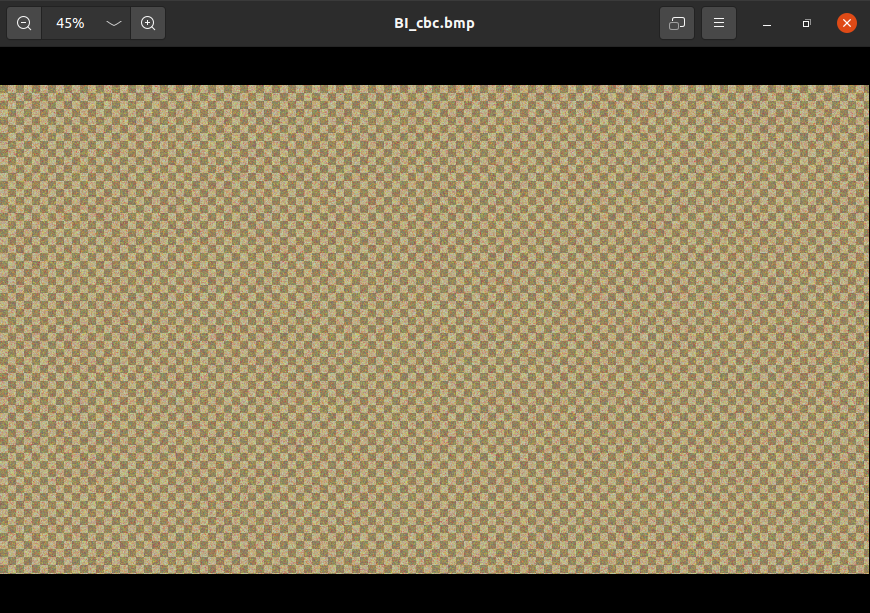
**P.4.2. Zaszyfruj i odszyfruj plik stosując opcje -base64 i -salt. Opisz, co uzyskasz stosując te opcje. Jaka opcja umożliwi podanie klucza szyfrującego w linii polecenia.**

-base64 używa kodowania tekstowego base64,

-salt generuje losowo klika dodatkowych danych w kluczu, bez użycia soli to samo hasło zawsze generuje ten sam tajny klucz

Podanie hasła szyfrowania umożliwia -pass.

**P.4.3. Wyświetl zawartość zaszyfrowanych plików graficznych. Umieść je w sprawozdaniu. Omów uzyskane wyniki. Uzasadnij zauważone charakterystyczne cechy poszczególnych wyników w zależności od zawartości pliku graficznego. Czy we wszystkich szyfrogramach są takie same i dlaczego? Przeanalizuj swoje obserwacje i opisz je w sprawozdaniu**

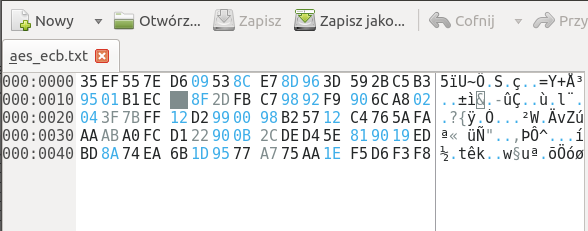
****

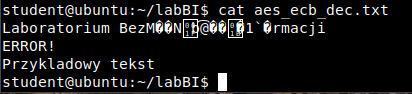
****

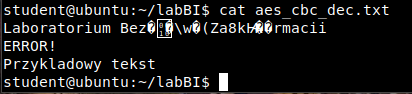
Przy jednolitym tle po szyfrowaniu z wykorzystaniem trybu ECB są widoczne napisy.

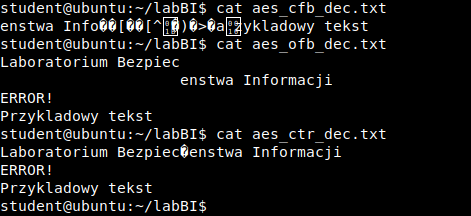
**P.4.4. Oznacz miejsce wprowadzenia przekłamania i zamieść tą informacje w sprawozdaniu. Ile danych jesteś w stanie odczytać po odszyfrowaniu uszkodzonych plików zaszyfrowanych algorytmem szyfrującym pracującym w trybie ECB, CBC, CFB, OFB, CTR? Opisz, jakiego algorytmu użyłeś. Wyjaśnij uzyskane wyniki. Wyciągnij wnioski z przeprowadzonego badania i opisz je w sprawozdaniu.**

****

****

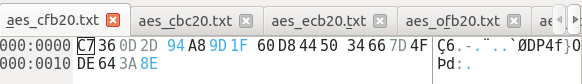
****

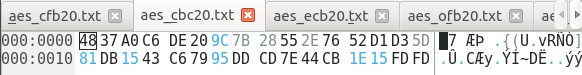
****

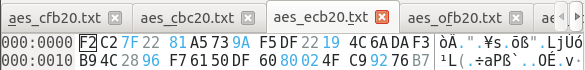
****

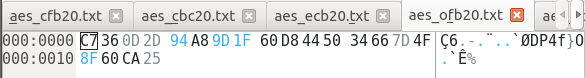
Użyto algorytmu AES. Przy użyciu trybu CTR i po wprowadzeniu przekłamania jest możliwość odczytania największej ilości danych po odszyfrowaniu.

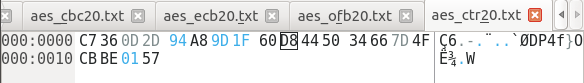
**P.4.5. Użyj trybów ECB, CBC, CFB, OFB, CTR do zaszyfrowania plików. W tym przypadku możesz użyć dowolnego algorytmu. Określ, które z trybów wymagają uzupełniania bloków. W sprawozdaniu umieść zrzut ekranu prezentujący wyniki oraz wyjaśnij, dlaczego niektóre z trybów pracy algorytmów szyfrujących nie wymagają uzupełnienia oraz określ, co z tego wynika.**

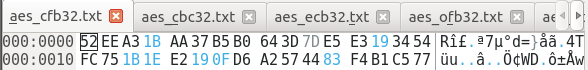


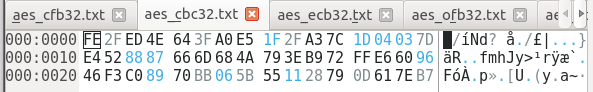




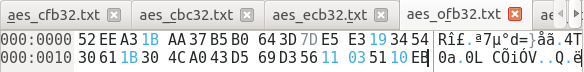
****

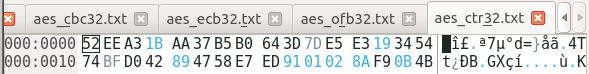


****

****

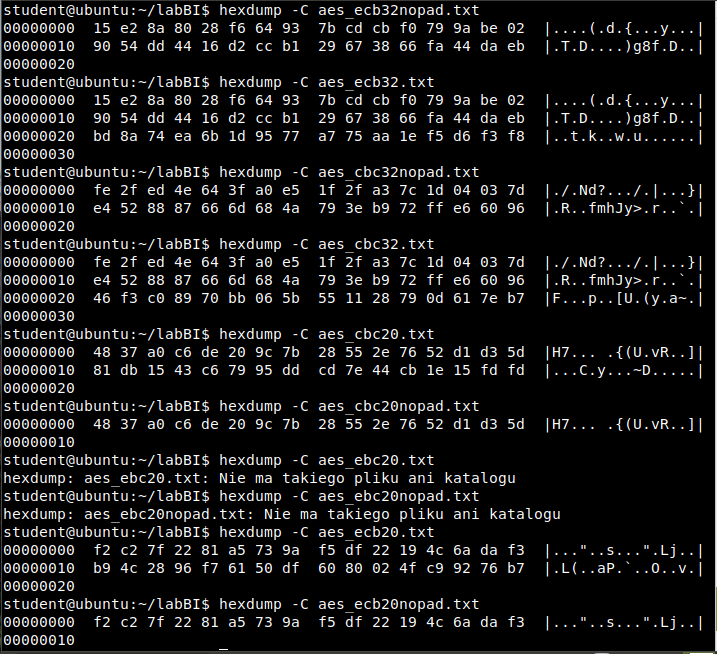
****

****

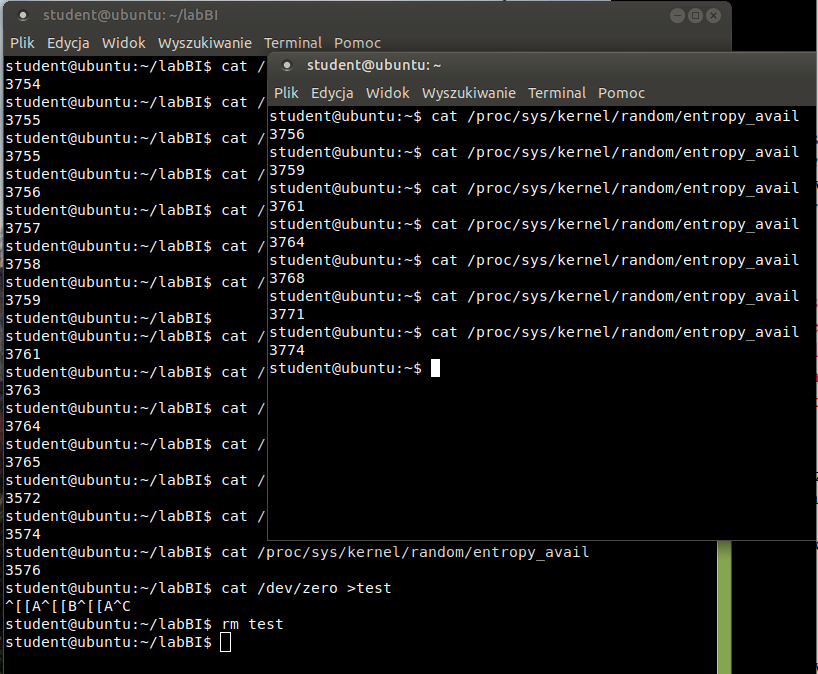
****

Tryb CBC oraz ECB wymagają uzupełnienia bloków.

**P.4.6. W celu sprawdzenia, co jest dodawane podczas uzupełniania do rozmiaru pełnego bloku należy ponownie wykonać szyfrowanie plików o rozmiarze 20 i 32 bajty z wykorzystaniem algorytmów AES i DES w trybie wymagającym uzupełniania bloków. Niestety odszyfrowanie plików automatycznie usunie dopełnienie, uniemożliwiając nam jego podgląd. Aby rozwiązać ten problem podczas odszyfrowania użyj opcji –nopad. Do wyświetlenia plików użyj następnie polecenia hexdump. Przykładowe działanie polecenia pokazano na Rys. 4.3. Omów, co zostało dodane do poszczególnych plików w celu uzupełnienia do rozmiaru pełnych bloków. Wyjaśnij mechanizm dopełniania bloków dla algorytmu AES i DES.**



**P.4.7. Proszę kilkukrotnie wywołać polecenia. Następnie proszę  
poruszać myszą, po czym należy wykonać kolejną serie odczytów entropii. Podobne doświadczenie wykonaj po użyciu klawiatury do przepisania fragmentu tekstu. Proszę również sprawdzic jak wpływają na entropie operacje dyskowe. Można użyć polecenia cat /dev/zero >test, które będzie w sposób ciągły zapisywało zera do pliku generując operacje dyskowe. Uwaga! Po zakończeniu należy usunąć utworzony plik test! Wnioski i obserwacje z niniejszego ćwiczenia proszę zamieścić w sprawozdaniu.**



Operacje dyskowe szybko zwiększają liczbę bitów liczb losowych zgromadzonych aktualnie w systemie. Ruch myszą oraz przepisanie tekstu nie zwiększył ich tak jak operacja dyskowa.

**P.4.8. Uruchom polecenie kilka razy. Zaobserwuj, że w pewnym momencie przestanie odpowiadać bezzwłocznie. Konieczne będzie oczekiwanie na wynik polecenia. Zaobserwuj, co się stanie, jeśli podczas oczekiwania nie będziesz wykonywać żadnych czynności w systemie, co jeśli będziesz poruszać myszą, używać klawiatury, wykonywać operacje dyskowe. Obserwacje i wnioski z przeprowadzonego badania umieść w sprawozdaniu.**

Przy wykonywaniu czynności w systemie, szybciej zwiększa się czas oczekiwania na wynik polecenia.