



## **Wydział Studiów Strategicznych i Technicznych**

Kierunek: Informatyka, rok II, semestr III (2021/2022)

### **LABORATORIUM NR 3**

### **PODSTAWY KRYPTOGRAFII**

Prowadzący: dr Piotr Dobosz

**Zespół laboratoryjny:**

Magdalena Szafrajska, nr albumu: 18345

# Spis treści

<b>Cel ćwiczenia</b>	<b>2</b>
<b>Informacje wstępne</b>	<b>2</b>
<b>Użyte narzędzia i aplikacje</b>	<b>3</b>
<b>Przebieg ćwiczenia</b>	<b>3</b>
Instalacja wymaganego oprogramowania	3
Zestawy danych do szyfrowania	3
Analiza działania metod szyfrowania	4
SZYFR CEZARA	4
Przebieg analizy - tekst nr 1	5
Przebieg analizy - tekst nr 2	7
Wady i zalety metody szyfru Cezara	9
SZYFR ZAMIANY	9
Przebieg analizy - tekst nr 1	10
Przebieg analizy - tekst nr 2	11
Wady i zalety metody szyfru zamiana	13
DODAWANIE BITÓW	14
Przebieg analizy - tekst nr 1	14
Przebieg analizy - tekst nr 2	15
Wady i zalety metody dodawania bitów	17
XOR	17
Przebieg analizy - tekst nr 1	18
Przebieg analizy - tekst nr 2	19
Wady i zalety metody XOR	21
DES z ECB	21
Przebieg analizy - tekst nr 1	22
Przebieg analizy - tekst nr 2	24
Wady i zalety metody szyfru DES z ECB	25
DES z CBC	26
Przebieg analizy - tekst nr 1	26
Przebieg analizy - tekst nr 2	27
Wady i zalety metody szyfru DES z CBC	29
AES	29
Przebieg analizy - tekst nr 1	30
Przebieg analizy - tekst nr 2	31
Wady i zalety metody szyfru AES	34
RSA	35
Przebieg analizy - tekst nr 1	35
Przebieg analizy - tekst nr 2	38
Wady i zalety metody szyfru RSA	40
RSA z AES	41
Przebieg analizy - tekst nr 1	41
Przebieg analizy - tekst nr 2	48
Wady i zalety metody szyfru RSA z AES	56
<b>Wnioski</b>	<b>57</b>

# Cel ćwiczenia

Podstawowym celem zadania jest analiza działania najpopularniejszych technik szyfrowania dokumentów.

## Informacje wstępne

W dzisiejszych czasach szyfrowanie oraz poświadczanie swojej tożsamości zaczyna odgrywać jedną z najważniejszych ról (o ile nie największą). Ludzie coraz bardziej przyzwyczajają się do wygody użytkowania zdobyczy nauki, takich jak płatności elektroniczne, przesyłanie danych do chmury obliczeniowej, dzielenie się danymi poufnymi z najbliższymi przy pomocy systemu rozproszonych danych itp. Przed projektantami tego typu rozwiązań stoi coraz większe wyzwanie, a przy okazji coraz większa odpowiedzialność.

Na dzień dzisiejszy wykorzystuje się wiele dość popularnych rozwiązań, które są wystarczające by zapewnić zarówno poufność danych, jak i ich integralność. W celu zabezpieczania informacji przydają się:

1. **szыfrowanie symetryczne** - wykorzystują do szyfrowania i odszyfrowania ten sam klucz szyfrujący, który w związku z tym musi być chroniony. Są to np.:
  - a. Szyfr Cezara – zastępujący poszczególne litery alfabetu innymi wg określonego przesunięcia
  - b. Szyfr Vigenere'a – swoje działanie opiera na tablicy Trithemiusa
  - c. Szyfr DES (Data Encryption Standard) – szyfruje bloki 64-bitowe przy użyciu 56 bitowego klucza symetrycznego
  - d. Szyfr AES (advanced encryption standard) – to współczesny szyfr symetryczny blokowy wykorzystujący klucze o długości 128, 192 i 256 bitów.
2. **szыfrowanie asymetryczne**
  - a. RSA – wykorzystywane np. przy połączeniach SSH)

Szyfry symetryczne dzielimy na:

- Blokowe – dzielące tekst na bloki o określonej długości, z których każdy szyfrowany jest oddzielnie.
- Strumieniowe – generujące ciąg szyfrujący o długości równej szyfrowanej wiadomości.

Wszystkie typy szyfrowania bazują na kilku istotnych elementach. Jednym z nich jest klucz, który służy do szyfrowania oraz deszyfrowania danych. W historycznym już kodzie Cezara tę rolę pełni określona liczba znaków, o którą należy dokonać przesunięcie. Nowoczesne kody wykorzystują specjalne hasła do utajniania oraz odtajniania tekstu. Natomiast w szyfrowaniu komputerowym kodem jest ściśle ustalony ciąg bitów, np. klucz 40-bitowy, 128-bitowy czy 256-bitowy.

Metody opisane w niniejszej pracy stanowią jedne z podstawowych metod kryptograficznych, które w przeciągu ostatnich kilku dziesięcioleci znalazły szerokie zastosowanie praktyczne w mechanizmach ochrony i zapewnienia integralności danych, protokołach autoryzacyjnych, oraz w systemach elektronicznych podpisów cyfrowych.

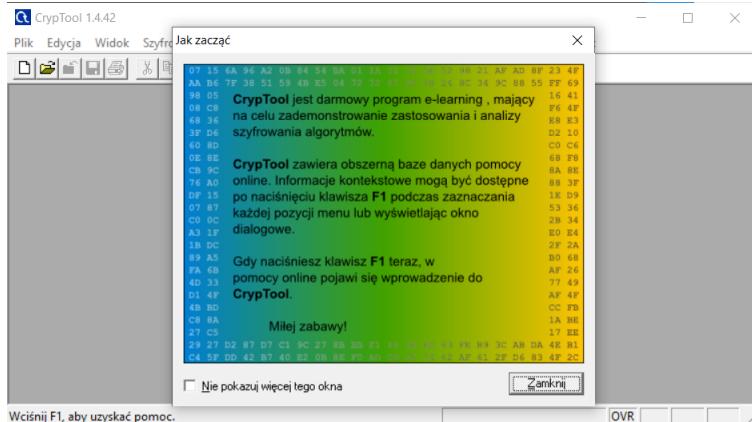
# Użyte narzędzia i aplikacje

- system Windows 10 Home w wersji 21H1 (64-bitowy)
- program CryptTool (<https://www.cryptool.org/en/ct1/downloads>) - darmowy program e-learningowy, mający na celu zademonstrowanie zastosowania i analizy szyfrowania algorytmów.

## Przebieg ćwiczenia

### Instalacja wymaganego oprogramowania

Zainstalowałem na komputerze program CryptTool w wersji 1.4.42.



### Zestawy danych do szyfrowania

Do analizy wskazanych w dalszej części metod szyfrowania wybrałem dwa różne pliki tekstowe.

- Tekst nr 1 to fragment przemyśleń Marka Aureliusza, (Księga III, punkty 1 i 2). Skorzystałem ze źródła darmowych treści dostępnych pod adresem:  
<https://wolnelektury.pl/katalog/lektura/rozmyslania-marek-aureliusz.html>

#### Analizowany tekst nr 1:

Marek Aureliusz, Księga III, punkty 1 i 2

1. Nie tylko to powinno się wziąć pod rozważę, że co dnia zużywa się życie i pozostaje coraz mniejsza jego częścią, ale i to, że gdyby się miało żyć bardzo długo, to jest niepewne, czy starczy równej na dalszą przyszłość bystrości potrzebnej do zrozumienia wypadków i do zrozumienia nauki, mającej na celu badanie spraw boskich i ludzkich. Gdy się bowiem zacznie dzieciścieć, pozostałe wprawdzie zdolność oddychania i karmienia się, i tworzenia wyobrażeń, i pożądanie itd., ale gaśnie zdolność władania sobą samym i umiejętności zdawania sobie sprawy z obowiązków, i porządkowania zjawisk, i zdolność osądzenia, czy już należy stąd wynieść się samemu, i to wszystko, co w wysokim stopniu wymaga umysłu wyćwiczonego. Należy się więc spieszyc, i to nie tylko dlatego, że każdej chwili bliżsi stajemy się śmierci, ale i dlatego, że ustaje zdolność wnikania w zdarzenia i ich zrozumienia.

2. Należy i nad tym się zastanawiać, że i w zjawiskach wtórnego tworów natury jest coś miłego i pociągającego. Np. gdy się chleb piecze, otrzymuje pewne pęknienia. Te więc pęknienia, jakkolwiek istnieją przecież wbrew zapowiedzi sztuki piekarskiej, jakoś nęczę swym widokiem i dodają w sposób sobie właściwy chęci do jedzenia. Także figi, gdy są najdroższe, pękają. I oliwek zupełnie dojrzałych zbliżające się psucie dodaje jakiegoś swoistego uroku owocowi. I kłosy, gdy się w dół schylają, i zmarszczone czoło lwa, i pianka leżąca się z pyska dzików, i innych wiele objawów, które są dalekie od piękności, gdyby im się przypatrzyć każdemu z osobna, przecież służą ku ozdobie i małe są duszy, ponieważ są dalszym ogniwem tworów natury, tak że jeżeli ktoś odczuwa i ma głębsze zrozumienie

tego, co się dzieje w wszechświecie, temu prawie wszystkie objawy wtórne będą się wydawały jakieś małe i zharmonizowane. Ten będzie z nie mniejszą przyjemnością patrzyć na rzeczywiste paszczę dzikich zwierząt, jak na te, które — naśladowując — pokazują malarze i rzeźbiarze. I staruszki, i starca pewien rozwitk i urok, i wdzięk młodzieńczy u chłopiat będzie mógł oglądać rozumnym swym okiem. I inne liczne podobne zjawiska nie każdemu będą małe, lecz tylko temu, kto się naprawdę zżyje z naturą i jej dziełami.

- Tekst nr 2 to fragment wstępku książki “Enigma, bliżej prawdy” autorstwa Marka Grajka.

### Analizowany tekst nr 2:

Marek Grajek, “Enigma bliżej prawdy”

Bibliografia tekstów poświęconych historii złamania szyfrów niemieckiej Enigmy obejmuje setki pozycji i rozciąga się na kilkadziesiąt stron druku, zasługując zapewne na wydanie w osobnej książce.

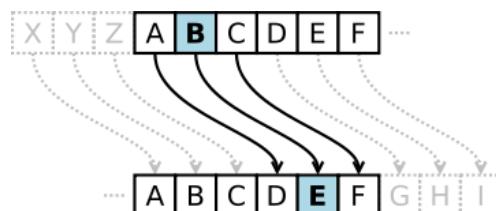
Popularność zagadnienia doprowadziła do powstania enigmologii; dziedziny wiedzy łączącej elementy nauk historycznych, wojskowych oraz matematyki i kryptologii. Dyscyplina ta w naturalny sposób wykształciła swoją awangardę - grono badaczy zajmujących się zawodowo lub hobbystycznie problematyką związaną z Enigmą. Istnieje kilka tradycyjnych oraz elektronicznych periodyków, sytuujących enigmologię w centrum zainteresowania. Rzeczywiste wydarzenia stały się kanwą, na której osnuto fabułę kilku filmów i wielu powieści, niektórych o charakterze dokumentalnym, innych - sensacyjnym. Po kilkudziesięcioletnim okresie kamuflowania prawdy, w ostatnim dziesięcioleciu XX wieku, archiwa zasypały historyków odtajnionymi dokumentami z epoki, pozostawiając jednakże pobudzające wyobraźnię luki w wiedzy o operacjach z Enigmą w tle. Tysiące stron internetowych zawierają mnóstwo informacji dotyczących historii maszyny, jej szyfrów i losów ludzi z nimi związanych, mieszając fakty i fikcję w sposób prawie nie pozwalający ich odróżnić.

## Analiza działania metod szyfrowania

Każdą z metod szyfrowania przeanalizowałam na podstawie szyfrowania na dwóch zestawach danych, po czym dokonałam ich odszyfrowania celem sprawdzenia poprawności działania przykładowu.

### 1. SZYFR CEZARA

Szyfr Cezara (szyfr przesuwający) zastępuje każdą literę tekstu jawnego inną, przesuniętą względem litery kodowanej o stałą liczbę pozycji w alfabetie. Na rysunku szyfr z przesunięciem równym 3, tak więc B w tekście jawnym jest podmieniane w szyfrogramie na E (rozpatrywany jest alfabet łaciński).



źródło: [https://pl.wikipedia.org/wiki/Szyfr\\_Cezara](https://pl.wikipedia.org/wiki/Szyfr_Cezara)

Szyfr Cezara bardzo łatwo jest opisać w sposób matematyczny. Kolejnym literom alfabetu łacińskiego przyporządkujmy liczby od 0 do 25.

Oznaczenie  $a \ mod \ b$  oznacza resztę z dzielenia liczby całkowitej  $a$  przez dodatnią liczbę całkowitą  $b$ . Szyfr Cezara może teraz być zdefiniowany wzorem:

$$C = (n + k) \ mod \ 26,$$

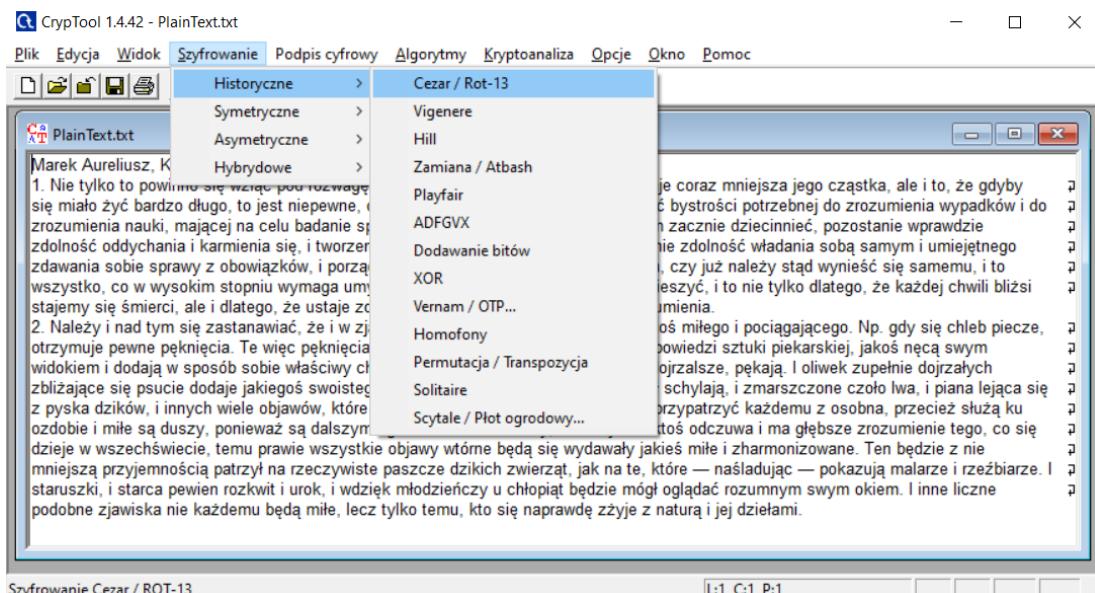
gdzie  $k$  jest kluczem szyfrowania,  $n$  jest numerem litery, którą szyfrujemy, a  $C$  jest numerem litery po zaszyfrowaniu.

Każdą zaszyfrowaną wiadomość trzeba kiedyś rozszyfrować. W szyfrze Cezara znajdujemy literę stojącą w alfabetie trzy miejsca bliżej, czyli stosujemy ten sam algorytm szyfrowania z innym kluczem. Do szyfrowania używamy klucza +3, a do rozszyfrowania klucza -3. Gdy znamy klucz szyfrowania, to znamy też klucz rozszyfrowania, jest to ten sam klucz, jeśli pominiemy jego znak. Deszyfrowanie odbywa się według wzoru:

$$C = (n - k) \bmod 26.$$

## Przebieg analizy - tekst nr 1

- Stworzyłam nowy plik o nazwie *PlainText.txt* z przygotowanym plikiem do analizy i wybrałam metodę szyfrowania.



- Zaszyfrowałam plik metodą Cezara z ustawieniami jak na poniższym screenie. Wybrałam przesunięcie o 13 pozycji w prawo a więc literze "A" (pierwszej pozycji w alfabetie) w tekście jawnym będzie w zaszyfrowanym tekście odpowiadała litera oddalona od niej o 13 pozycji w prawo a zatem litera "N".

Zdecydowałam się na takie właśnie przesunięcie, gdyż szyfr Cezara z przesunięciem 13, tzw. ROT13, jest nadal obecnie stosowany jako prosta metoda ukrycia treści (np. puenty dowcipów i zakończeń fabuły – tzw. spoilerów), szeroko rozpowszechniona w systemach Unix.

Wprowadzenie klucza: Cezar / ROT-13

**Opis**

**Klucz**

Szyfr Cezara jest monoalfabetycznym szyfrem zamiany, w którym znaki tekstu są mapowane na znaki szyfru przez przesunięcie. Wartością przesunięcia jest klucz. Możesz wprowadzić klucz jako liczbę lub jako pojedynczy znak alfabetu.

Rot-13 jest specjalnym wariantem, w którym klucz posiada ustaloną wartość równą połowie długości alfabetu tekstu jawnego. Ten wariant jest możliwy tylko gdy drugie

**Wybierz wariant**

Caesar

Rot-13

**Opcje interpretacji znaków alfabetu**

Wartość pierwszego znaku alfabetu = 0 (n.p.: "A" = 0)

Wartość pierwszego znaku alfabetu = 1 (n.p.: "A" = 1)

**Klucz wprowadzany jako**

Znak alfabetu

Wart. liczbową

**Informacja o szyfrowaniu**

Przesunięcie 13

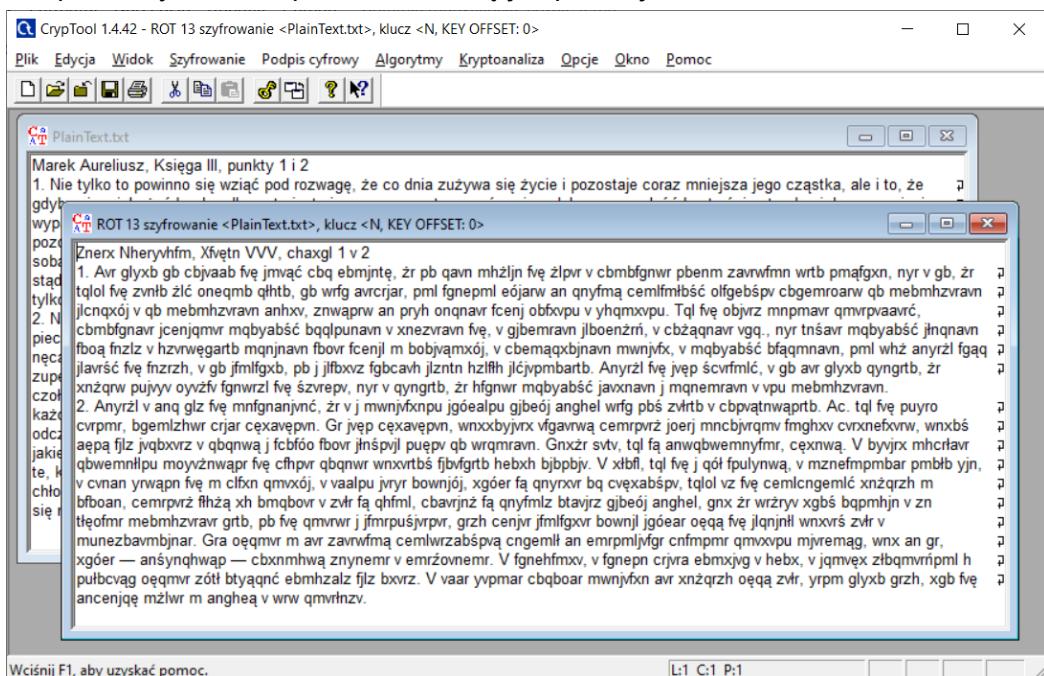
Mapowanie alfabetu(26 znaków)

z:

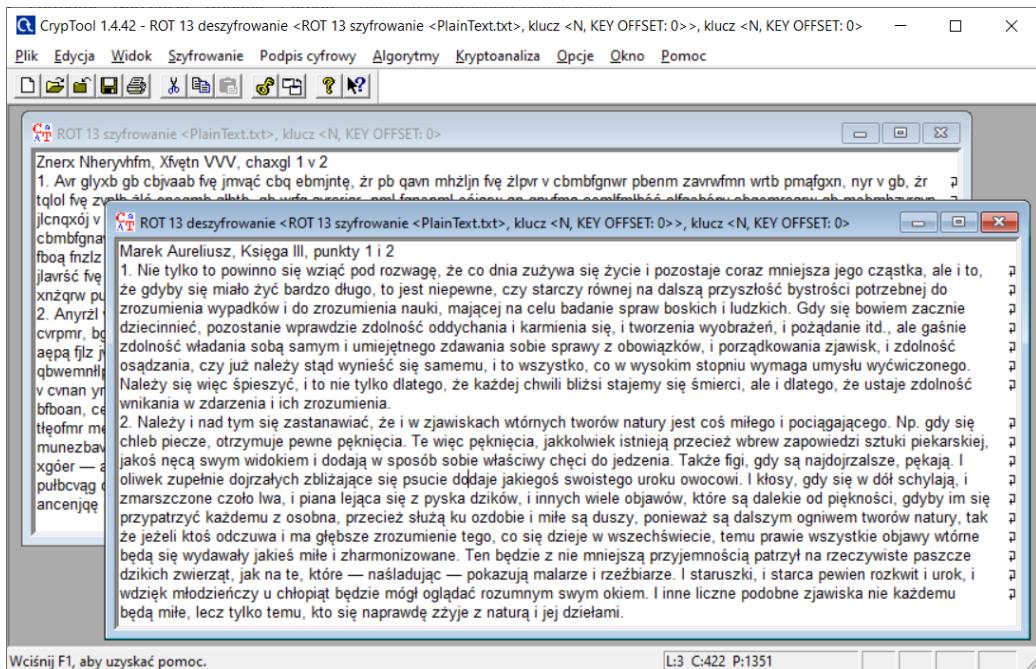
do:

**Szyfruj** **Deszyfruj** **Opcje tekstu** **Anuluj**

- Plik po zaszyfrowaniu przedstawiał się jak poniżej.

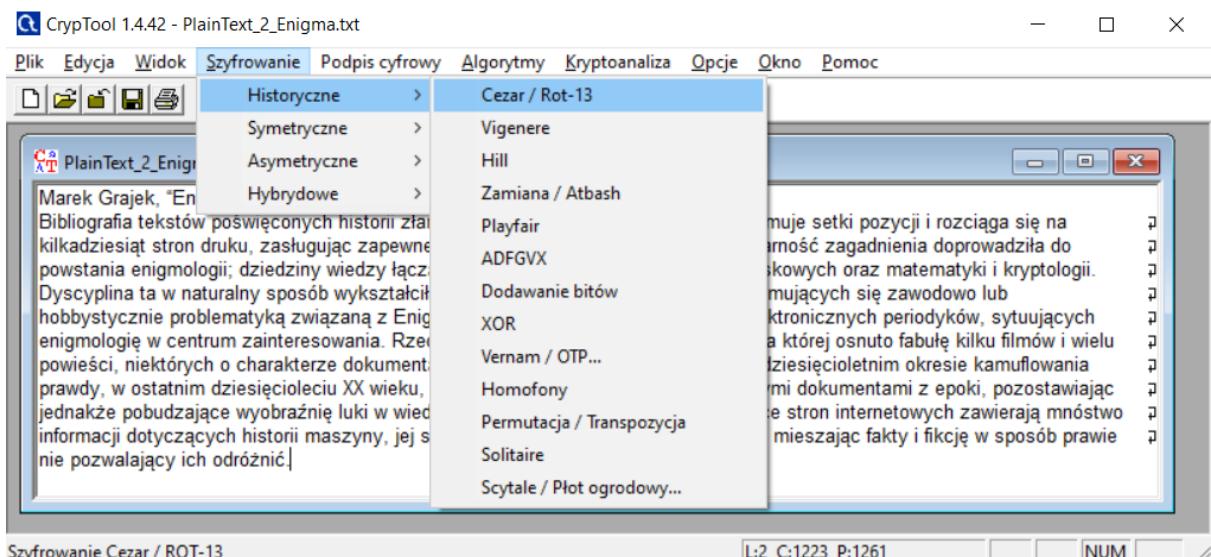


- Następnie deszyfrowałam plik używając tych samych ustawień a więc przesunięcia o 13.

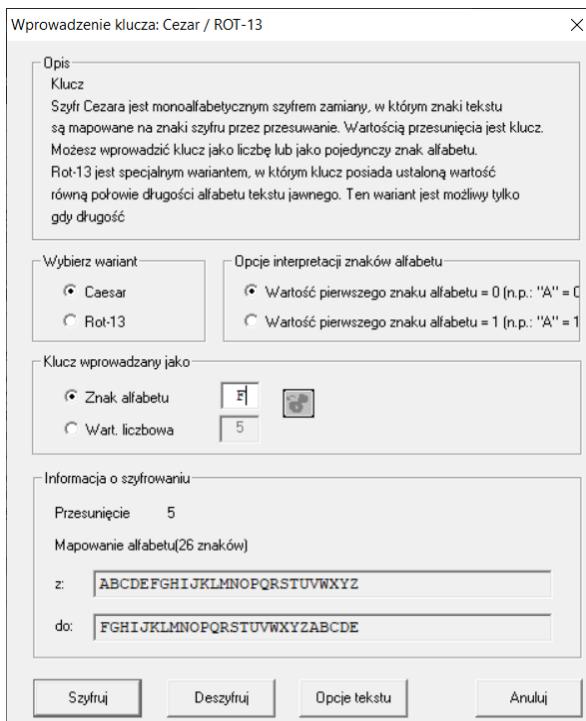


## **Przebieg analizy - tekst nr 2**

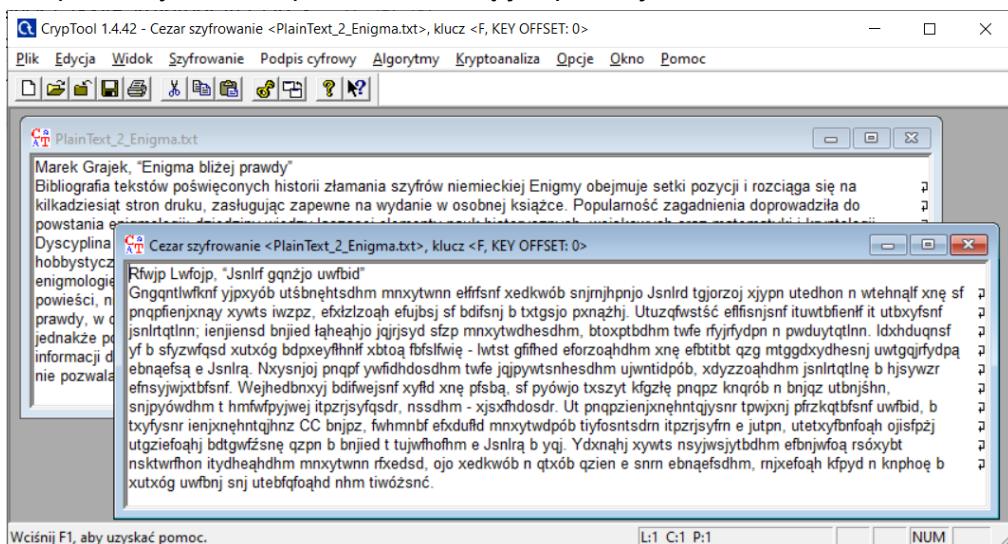
- Stworzyłam nowy plik o nazwie *PlainText\_2\_Enigma.txt* z przygotowanym plikiem do analizy i wybrałam odpowiednią metodę szyfrowania.



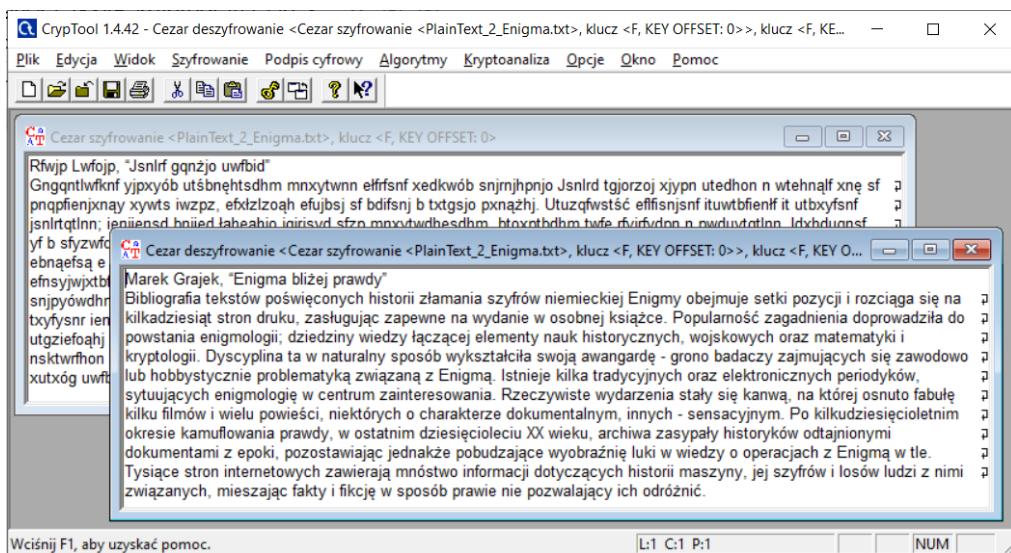
- Zaszyfrowałam plik metodą Cezara z ustawieniami jak na poniższym screenie. Wybrałam przesunięcie o 5 pozycji w prawo a więc literze "A" (pierwszej pozycji w alfabetie) w tekście jawnym będzie w zaszyfrowanym tekście odpowiadała litera oddalona od niej o 5 pozycji w prawo a zatem litera "F".



- Plik po zaszyfrowaniu przedstawał się jak poniżej.



- Następnie deszyfrowałam plik używając tych samych ustawień a więc przesunięcia o 5.



Jak widać, w drugim pliku deszyfrowanie również przebiegło pomyślnie i plik został odtworzony w nienaruszonym stanie.

## Wady i zalety metody szyfru Cezara

### WADY

- Szyfr Cezara, tak jak każda technika podmieniająca pojedyncze litery alfabetu na inne, nie oferuje żadnego bezpieczeństwa komunikacji. Jest to największa wada tej metody.
- Bezpieczeństwo zależne jest od długości klucza: litery leżące w odległości równej długości klucza są szyfrowane tym samym szyfrem Cezara.
- Pominięcie przy szyfrowaniu wszelkich znaków nie będących literami (w tym cyfr). W zależności od treści szyfrowanego pliku, może to być wysoce podatne na nasłuchiwanie.
- Podatność na tak zwaną analizę częstości. Przykład języka angielskiego pokaże na czym ona polega: po zbadaniu dłuższego tekstu w języku angielskim, można zauważać, że najczęściej występującą literą jest „E”, następnie w kolejności są „T” oraz „A” i tak dalej. W celu odszyfrowania wiadomości należy sprawdzić jak często w zaszyfrowanym tekście występuje dany symbol lub litera. Jeśli przykładowo najczęściej występującą literą jest „B”, prawdopodobnie następuje ona „E”. Podobnie sprawdza się pozostałe litery i tak jeśli drugą najczęściej występującą literą jest „C”, oznacza to że prawdopodobnie następuje literę „T” itd.

### ZALETY

- Zaletą jest prostota algorytmu szyfrowania. Korzystanie z szyfru Cezara jest stosunkowo proste i dostępne dla osób niewykwalifikowanych.
- Łatwość wymiany i uzgodnienia klucza.

## 2. SZYFR ZAMIANY

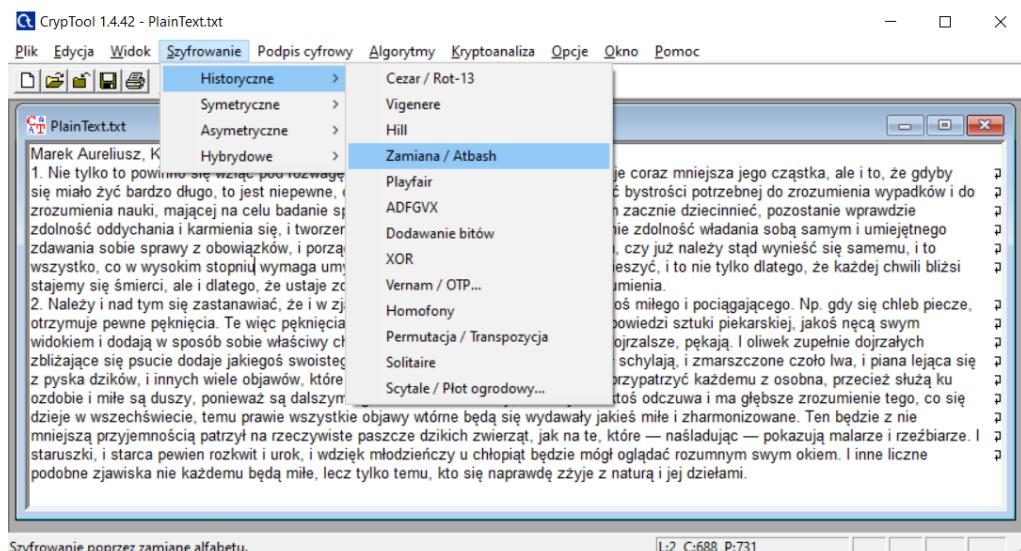
Szyfr ten polega, najprościej mówiąc, na zamianie liter w kluczu. Chcąc zaszyfrować wyraz zamieniamy po kolei każdą literę, na jej odpowiednik w kluczu.

Szyfr zamiana szyfruje poprzez zamianę odpowiednich par znaków na podstawie klucza. Klucz używany do szyfrowania to lista liczb dodatnich (istnieje możliwość dopuszczenia liczb ujemnych.) Szyfrowanie polega na tym, że dla każdego znaku jest

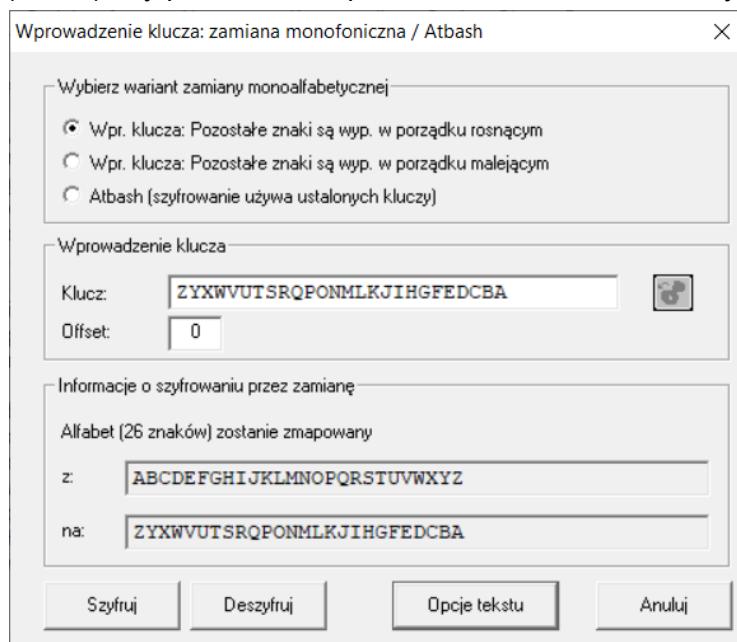
wykonywana zamiana jego razem ze znakiem położonym  $k$  pozycji dalej.  $k$  jest to  $i$ -ta liczba pobrana z klucza. W związku z tym, że pobierana wartość z klucza może nie istnieć to należy pobrać wtedy wartość  $k \bmod \text{długość klucza}$ . Podobnie należy postępować podczas zamiany, gdy nie istnieje pozycja  $i + k$  należy zamienić  $i$ -ty znak z  $i + k \bmod \text{długość tekstu}$ .

## Przebieg analizy - tekst nr 1

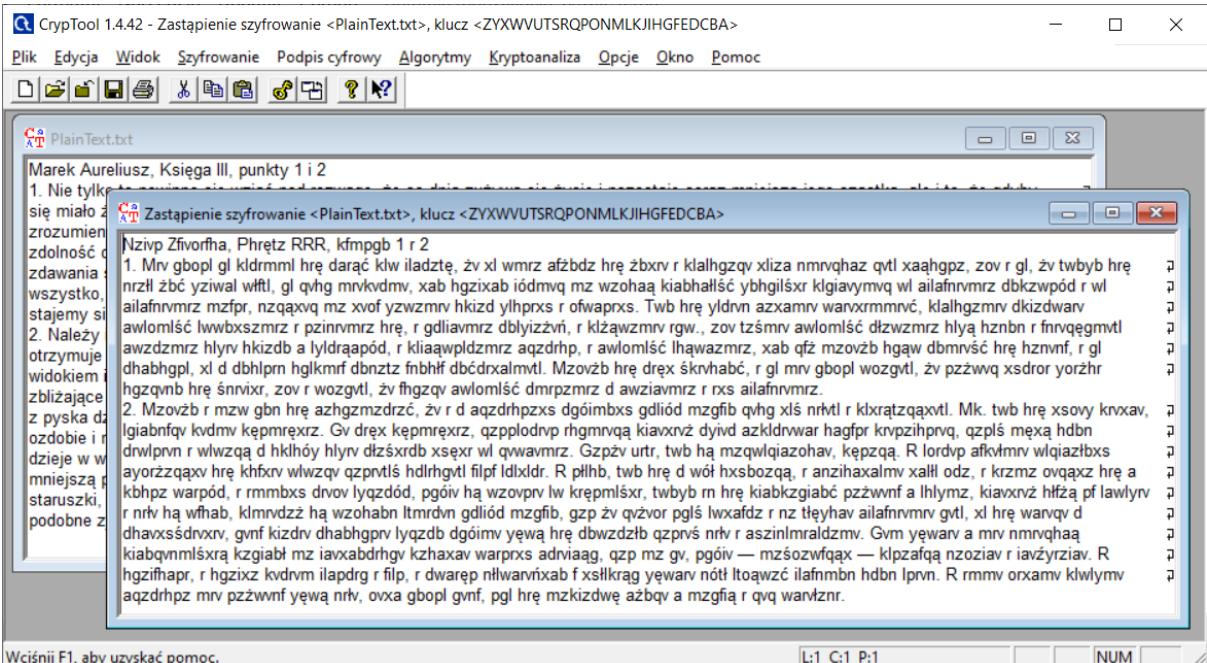
- Na przygotowanym pliku z tekstem jawnym rozpoczęłam szyfrowanie metodą zamiany.



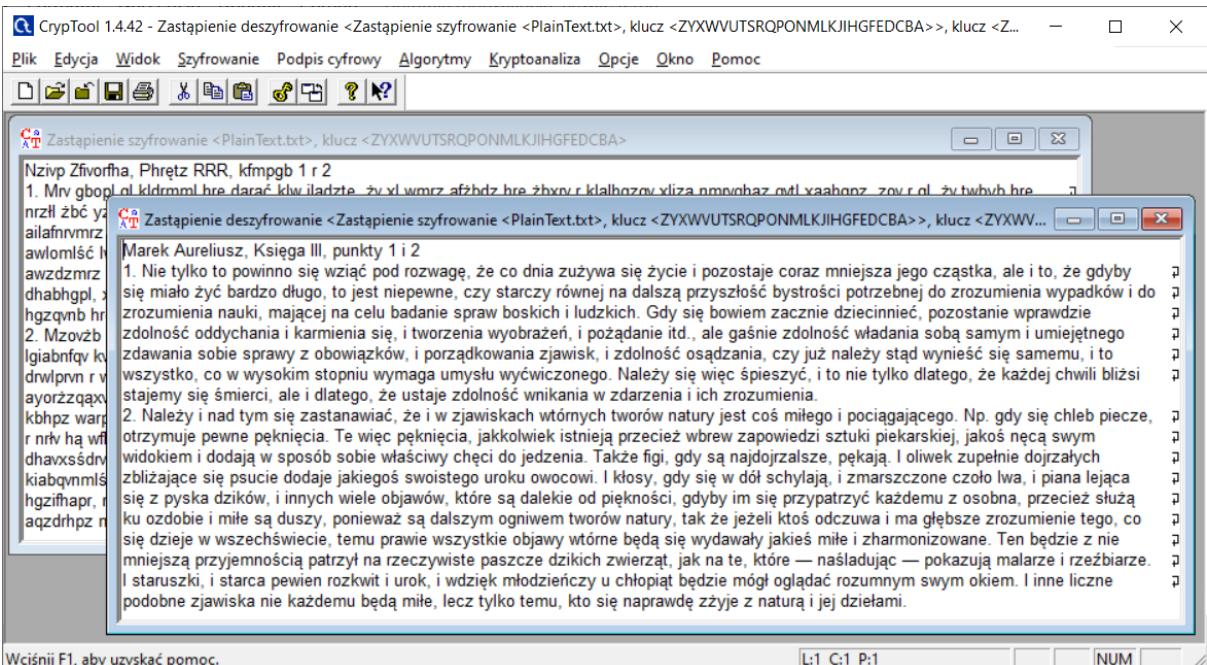
- Zastosowałam parametry jak poniżej na zrzucie ekranu, a więc przykładowo literze "A" odpowiada litera "Z" itd. Nie stosowałam opcjonalnego przesunięcia klucza (Offset) aby przetestować podstawowe działanie metody.



- Plik po zaszyfrowaniu wyglądał jak poniżej.



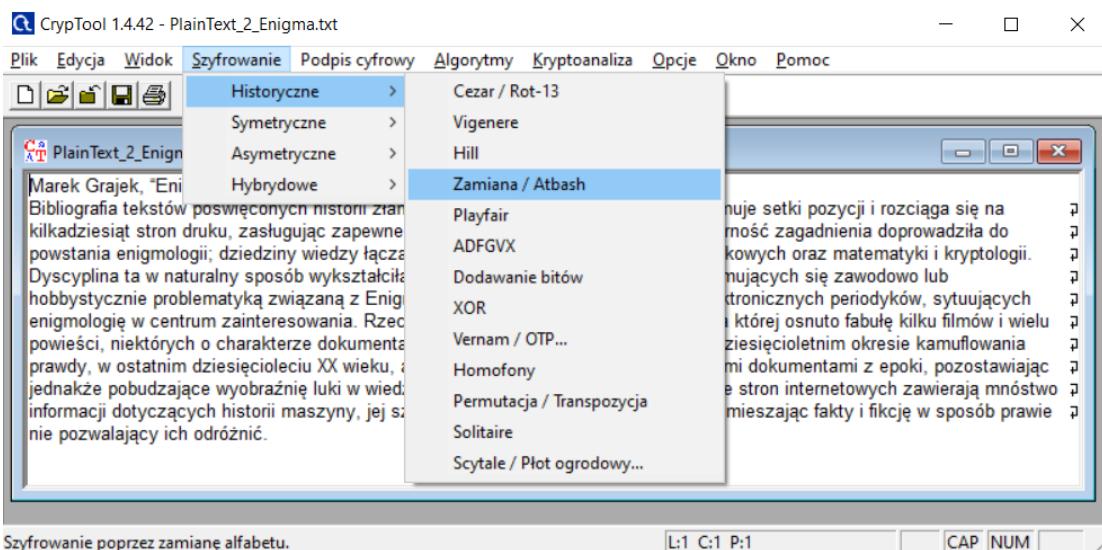
- Następnie deszyfrowałem plik używając tych samych ustawień co przy szyfrowaniu.



Jak widać, deszyfrowanie przebiegło pomyślnie i plik został odtworzony w nienaruszonym stanie.

## Przebieg analizy - tekst nr 2

- Na przygotowanym pliku z tekstem jawnym rozpoczęłam szyfrowanie metodą zamiany.



- Zastosowałam parametry jak poniżej na zrzucie ekranu. Dla odmiany od pierwszego tekstu analizowanego ta metoda, zastosowałam przesunięcie o 4 (Offset = 4).

Wprowadzenie klucza: zamiana monofoniczna / Atbash

Wybierz wariant zamiany monoalfabetycznej

- Wpr. klucza: Pozostałe znaki są wyp. w porządku rosnącym
- Wpr. klucza: Pozostałe znaki są wyp. w porządku malejącym
- Atbash (szfrowanie używa ustalonych kluczy)

Wprowadzenie klucza

Klucz:	Z Y X W V U T S R Q P O N M L K J I H G F E D C B A	
Offset:	4	

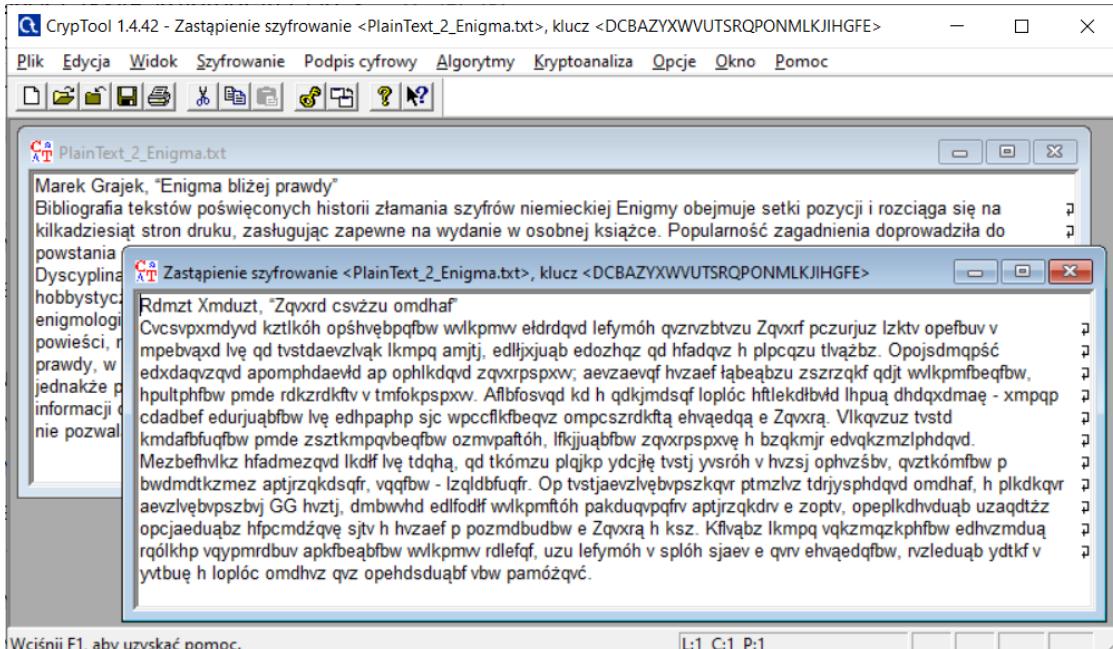
Informacje o szyfrowaniu przez zamianę

Alfabet (26 znaków) zostanie zmapowany

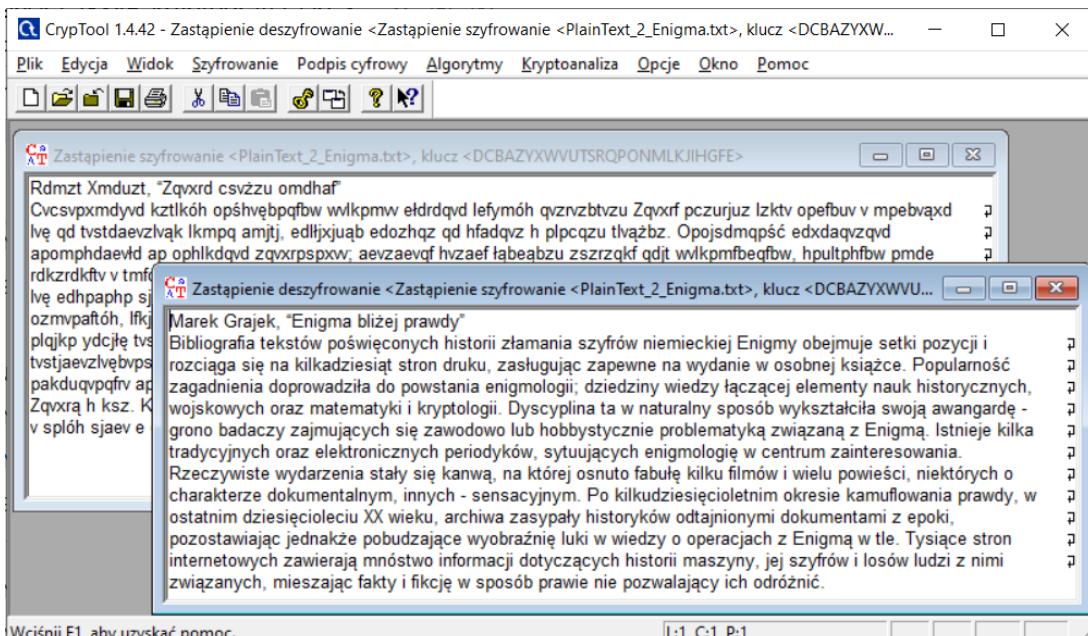
z:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
na:	D C B A Z Y X W V U T S R Q P O N M L K J I H G F E

Szyfruj
Deszyfruj
Opcje tekstu
Anuluj

- Plik po zaszyfrowaniu wyglądał jak poniżej.



- Następnie deszyfrowałam plik używając tych samych ustawień co przy szyfrowaniu.



Jak widać, deszyfrowanie przebiegło pomyślnie i plik został odtworzony w nienaruszonym stanie.

## **Wady i zalety metody szyfru zamiana**

WADY

- Szyfrowanie metodą zamiany, podobnie jak szyfr Cezara, nie oferuje żadnego bezpieczeństwa komunikacji. Jest to największa wada tej metody.
  - Inną wadą jest pominięcie przy szyfrowaniu wszelkich znaków nie będących literami (w tym cyfr). W zależności od treści szyfrowanego pliku, może to być wysoce podatne na odszyfrowanie.

ZALETY

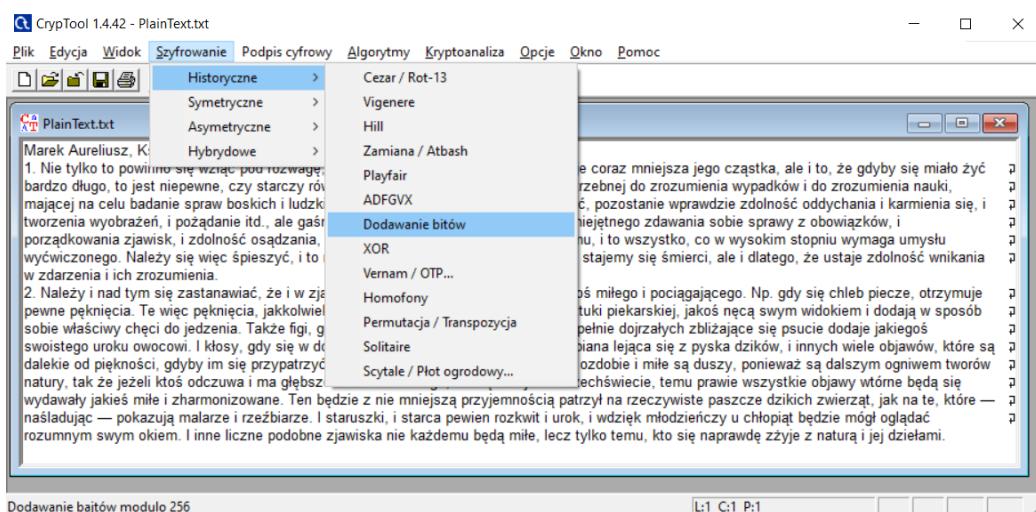
- Zaletą jest prostota i szybkość metody.

### 3. DODAWANIE BITÓW

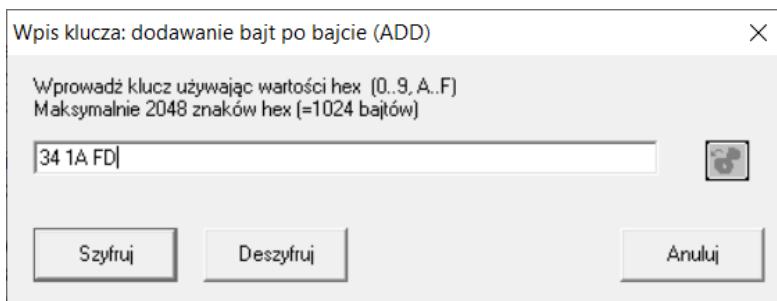
Tę metodę szyfrowania nazywamy inaczej dopełnianiem bloków danych (ang. padding). Polega ona na dodawaniu pewnych uzgodnionych wartości na końcu przesyłanych wiadomości. Informacja o użytym standardzie dopełniania musi zostać przekazana do odbiorcy. To pozwala mu określić (po odszyfrowaniu szyfrogramu) gdzie kończy się oryginalna wiadomość, a zaczynają się nieistotne bajty dopełnienia. Jedyną wadą dopełniania bloków jest fakt, że nawet jeśli wiadomość zawiera odpowiednią liczbę bajtów (całkowitą wielokrotność długości jednego bloku), to dopełnienie i tak musi zostać dodane, aby zagrawantować, że odbiorca będzie w stanie zrozumieć wiadomość. Zwykle dodawany jest jeszcze jeden blok, zawierający jedynie nieistotne bajty dopełnienia.

#### Przebieg analizy - tekst nr 1

- Na przygotowanym pliku z tekstem jawnym rozpoczęłam szyfrowanie metodą dodawania bitów.



- Zastosowałam parametry jak poniżej na zrzucie ekranu, a więc klucz o wartości: 34 1A FD.



- Plik po zaszyfrowaniu wyglądał jak poniżej.

Marek Aureliusz, Księga III, punkty 1 i 2  
1. Nie tylko to powinno się wziąć pod uwagę, że co dnia zużywa się życie i pozostaje coraz mniejsza jego częstka, ale i to, że gdyby się miało żyć bardziej długo, to jest niepowie, mającej na celu badanie spraw tworzenia wyobrażeń, i pożądanie porządkowania zjawisk, i zdolność wyćwiczonego. Należy się więc w zdarzeniu i ich zrozumieniu.  
2. Należy i nad tym się zastanawiać, kiedyś kiedyś chcieli do jedzenia pewne pęknienia. Te wiec poknieni sobie wyobrażeń i zharmonizowane, wydawały jakieś mile i zharmonizowane, naśladowując — pokazują malarze rozumnym swym okiem. I inne l

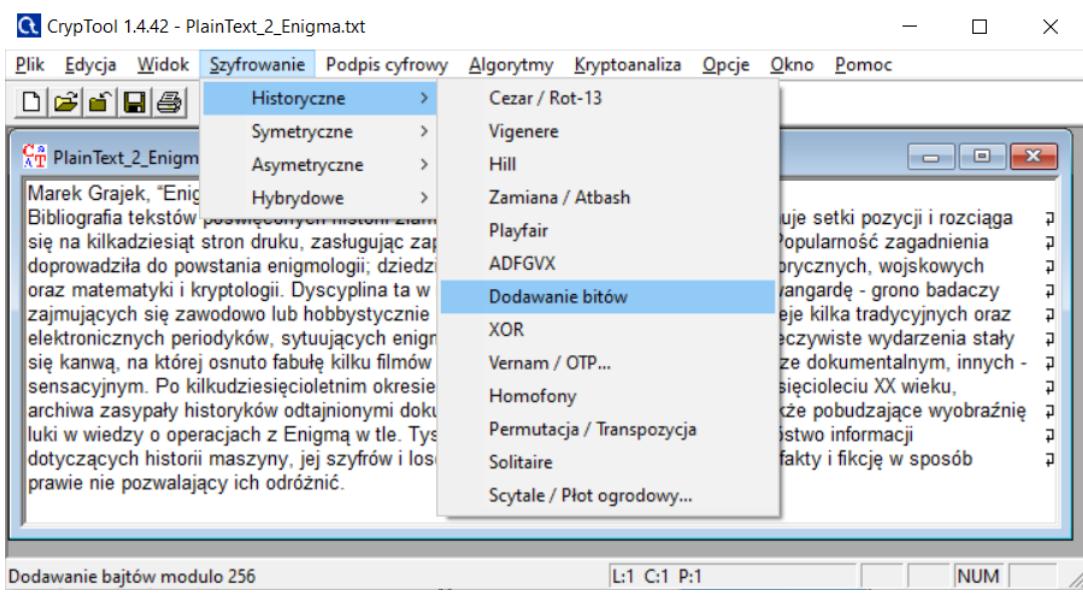
- Następnie deszyfrowałem plik używając tego samego klucza: 34 1A FD - co jest dodatkowo widoczne w górnej części okna z rozszyfrowaną wiadomością.

Marek Aureliusz, Księga III, punkty 1 i 2  
1. Nie tylko to powinno się wziąć pod uwagę, że co dnia zużywa się życie i pozostaje coraz mniejsza jego częstka, ale i to, że gdyby się miało żyć bardziej długo, to jest niepowie, czysty z równej na dalszą prędkością potrzebnej do zrozumienia wypadków i do zrozumienia nauki, mającej na celu badanie spraw boskich i ludzkich. Gdy się bowiem zacznie dziedziczenie, pozostanie wprawdzie zdolność oddychania i karmienia się, i tworzenia wyobrażeń, i pożądanie itd., ale gąsienica zdolność владания sobą samym i umiejętności zdawania sobie sprawy z obowiązków, i porządkowania zjawisk, i zdolność osiądzania, czy już należy stąd wynieść się samemu, i to wszystko, co w wysokim stopniu wymaga umysłu wyćwiczonego. Należy się więc śpieszyć, i to nie tylko dlatego, że każdej chwili bliźniaczej się śmiert, ale i dlatego, że ustąpi zdolność wnikania w zdarzenia i ich zrozumienia.  
2. Należy i nad tym się zastanawiać, że i w zjawiskach tychowych twór natury jest coś milego i pociągającego. Np. gdy się chleb pieczę, otrzymuje pewne pęknienia. Te wiec pęknienia, jakkolwiek istnieją przecież w bławie zapowiedzi sztuki piekarskiej, jakoś sązym wiadomkiem i dodają w sposób sobie właściwy chęci do jedzenia. Także figi, gdy są najdroższe, pękają. I oliwek zupełnie dorżałych zbliżających się puscie dodaje jakiegoś swoistego uroku owocowi. I klosy, gdy się w dół schylają, i zmarszczone czoło lwa, i piana leżąca z pyska dzików, i innych wielu owabiów, które są daleko od piękności, gdyby im się przypatrzyć każdemu z osobna, przecież służą ku ozobie i mile są duszy, ponieważ są dalszym ogniem tychowych twórów natury, tak że jeżeli ktoś odczuwa i ma głębokie zrozumienie tego, co się dzieje w wszelkim temu prawie wszystkie objawy wtórne będą się wydawały jakieś mile i zharmonizowane. Ten będzie z nie mniejszą przyjemnością patrzyć na rzeczywiste paszcze dzikich zwierząt, jak na te, które — naśladowując — pokazują malarze i rzeźbiarze. I starszus, i starca pewien rozwitki i urok, i wdzięk młodzienicy w chłopiąt będzie mógł oglądać rozumnym swym okiem. I inne liczne podobne zjawiska nie każdemu będą mile, lecz tylko temu, kto się naprawdę zczyje z naturą i jej dziełami.

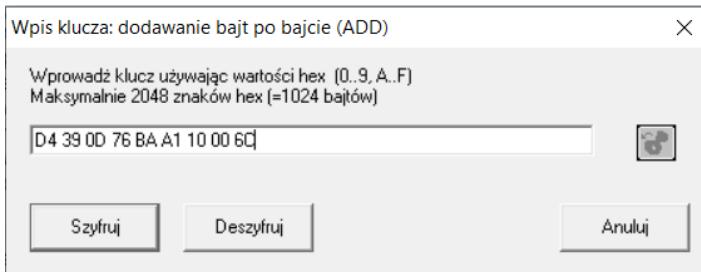
Jak widać, deszyfrowanie przebiegło pomyślnie i plik został odtworzony w nienaruszonym stanie.

## Przebieg analizy - tekst nr 2

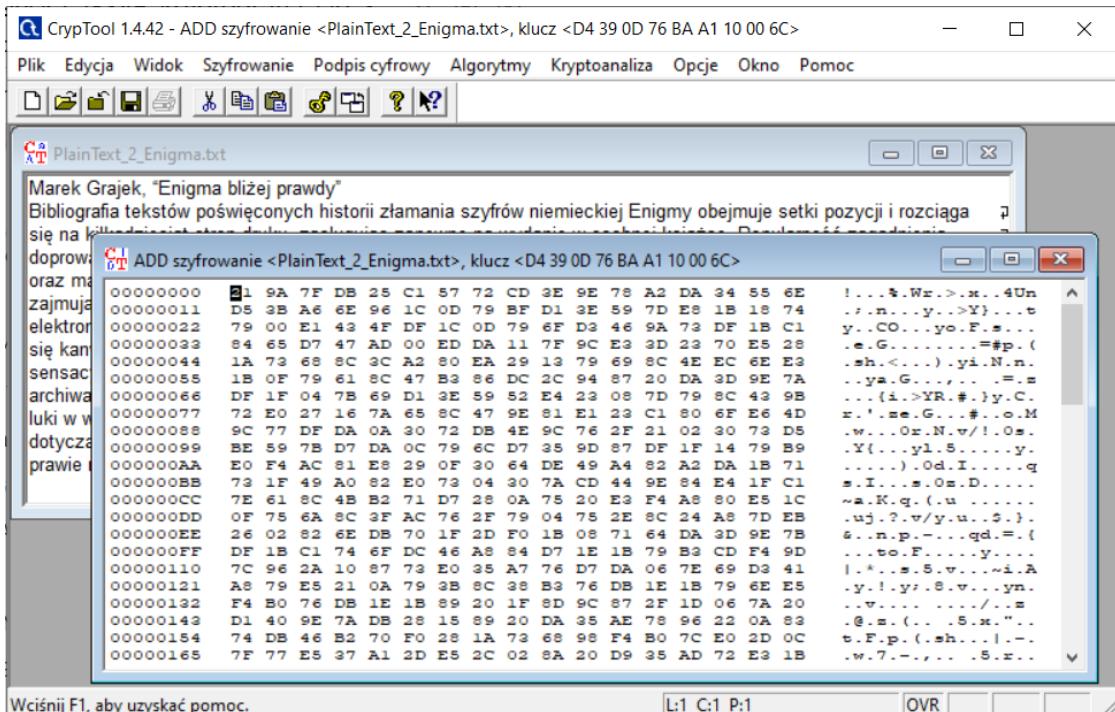
- Na przygotowanym pliku z tekstem jawnym rozpoczęłam szyfrowanie metodą dodawania bitów.



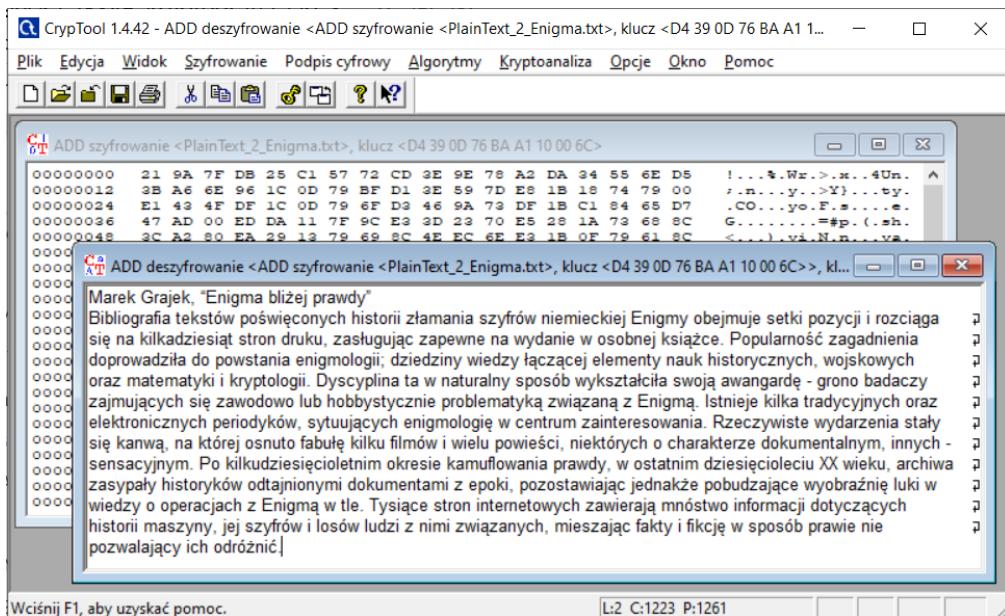
- Zastosowałem parametry jak poniżej na zrzucie ekranu, a więc klucz o wartości: D4 39 0D 76 BA A1 10 00 6C.



- Plik po zaszyfrowaniu wyglądał jak poniżej.



- Następnie deszyfrowałem plik używając tego samego klucza: D4 39 0D 76 BA A1 10 00 6C - co jest dodatkowo widoczne w górnej części okna z rozszyfrowaną wiadomością.



Jak widać, deszyfrowanie przebiegło pomyślnie i plik został odtworzony w nienaruszonym stanie.

## Wady i zalety metody dodawania bitów

### WADY

- Używanie ogólnie przyjętych standardów dopełniania jest wygodnym sposobem gwarantowania poprawnej długości szyfrowanych danych.
- Jedyną wadą szyfrowania metodą dodawania bitów jest fakt, że nawet jeśli wiadomość zawiera odpowiednią liczbę bajtów (całkowitą wielokrotność długości jednego bloku), to dopełnienie i tak musi zostać dodane, aby zagrawantować, że odbiorca będzie w stanie zrozumieć wiadomość. Zwykle dodawany jest jeszcze jeden blok, zawierający jedynie nieistotne bajty dopełnienia.

### ZALETY

- Używanie ogólnie przyjętych standardów dopełniania jest wygodnym sposobem gwarantowania poprawnej długości szyfrowanych danych.

## 4. XOR

XOR jest rodzajem symetrycznego szyfru strumieniowego. Jego działanie opiera się na działaniu logiki matematycznej XOR czyli alternatywie rozłącznej. Operator XOR przyjmuje wartość 1 na wyjściu, gdy wartości na wejściach są różne, a więc gdy dokładnie jedno z dwóch wejść niesie logiczną wartość prawdy. Poniżej jego tablica prawdy:

$$\begin{array}{l}
 \mathbf{0 \text{ XOR } 0 = 0} \\
 \mathbf{0 \text{ XOR } 1 = 1} \\
 \mathbf{1 \text{ XOR } 0 = 1} \\
 \mathbf{1 \text{ XOR } 1 = 0}
 \end{array}$$

W szyfrze XOR algorytm sumuje kolejne bajty tekstu jawnego i sekretnego klucza o dowolnej długości za pomocą działania XOR. Po wykorzystaniu ostatniego bajtu klucza, przechodzi się z powrotem do pierwszego bajtu. W celu odszyfrowania postępuje się w taki

sam sposób, czyli dodaje się kolejne bajty klucza do kolejnych bajtów szyfrogramu za pomocą operacji XOR.

Każdy znak, obraz, element wyświetlony na ekranie komputera ma swoją interpretację w systemie dwójkowym. Przykładowo, interpretacja słowa „szyfr” w systemie dwójkowym:

„szyfr” = 01110011,01111010,01111001,01100110,01110010

Jeśli chcielibyśmy zaszyfrować to słowo i do zaszyfrowania użyjemy pojedynczej litery „c” której dwubitowa interpretacja wynosi 01100011 nasz szyfr będzie wyglądał następująco:

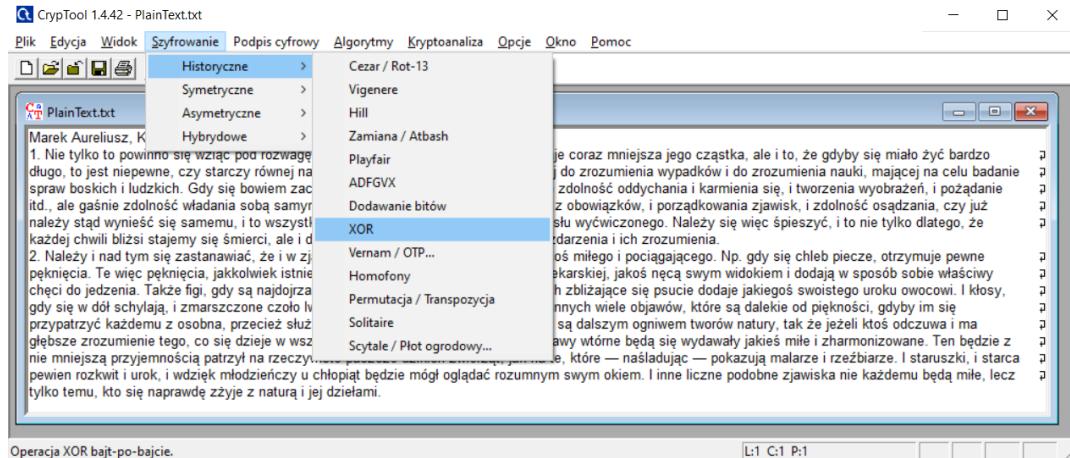
01110011,01111010,01111001,01100110,01110010 – szyfr  
⊕ 01100011,01100011,01100011,01100011,01100011 – ccccc  

---

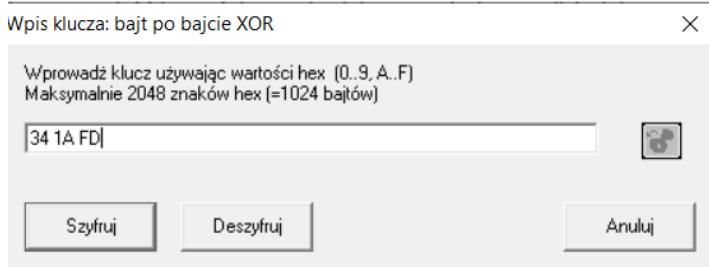
00010000,00011001,00011010,00000101,00010001 –

## Przebieg analizy - tekst nr 1

- Na przygotowanym pliku z tekstem jawnym rozpoczęłam szyfrowanie metodą XOR.



- Zastosowałam parametry jak poniżej na zrzucie ekranu, a więc klucz o wartości: 34 1A FD (identyczny co przy metodzie dodawania bitów dla pierwszego tekstu).



- Plik po zaszyfrowaniu wyglądał jak poniżej, zaszyfrowana wiadomość, pomimo użytego identycznego klucza co w metodzie dodawania bitów, wyglądała całkiem inaczej.

CrypTool 1.4.42 - XOR szyfrowanie <PlainText.txt>, klucz <34 1A FD>

Plik Edycja Widok Szyfrowanie Podpis cyfrowy Algorytmy Kryptoanaliza Opcje Okno Pomoc

**C1 XOR szyfrowanie <PlainText.txt>, klucz <34 1A FD>**

```
00000000  79 7B 8F 51 71 DD 75 6F 8F 51 76 94 41 69 87 18 3A B6 47 73 17 53 7B DD 7D 53 B4 18 3A 8D y(.Qq.uo.Qv.Ai...:G.s(.).S... At.8c...:(.>>..T.Qi.Mv.[i.:i.
0000001E  41 74 96 40 63 DD 05 3A 94 14 28 F0 3E 2B D3 14 54 94 81 3A 89 4D 76 96 5B 3A 89 5B 3A 8D At.8c...:(.>>..T.Qi.Mv.[i.:i.
0000003C  5B 6D 94 52 74 82 16 69 94 DE 5A 4E 73 43 D3 3A 8D 5B 7E DD 46 75 87 43 7B 92 DE 86 DD [m.Zb.i...:NsD:[~.Fu.C(.).6.
0000005A  5B 6D 94 52 74 82 16 69 94 DE 5A 4E 73 43 D3 3A 8D 5B 7E DD 46 75 87 43 7B 92 DE 86 DD .m.Zb.i...:NsD:[~.Fu.C(.).6.
00000076  44 75 7B 69 88 70 88 47 99 92 46 7B 87 44 79 92 89 8D 7F 97 47 60 9C 44 70 98 83 75 DD Du.(i.Ug.y...:A(.G...:W...:.
00000096  57 60 44 47 6E 86 55 36 DD 50 76 14 73 DD 40 75 D1 14 A5 98 14 7D 99 4D 78 84 14 69 94 W.DG.U6.U6...:U...:Gu...:M...:i.
000000B4  DE 3A 90 5D 7B 42 4D FC DD 56 7B 5F 50 60 92 14 7E 4E 41 7D 92 18 3A 89 5B 3A 97 .:J(N:BM..Vi.P...:NA) M...:i.
000000D2  S1 69 89 14 74 94 51 6A 9A 47 74 98 18 3A 9E 42 69 DD 47 6E 9C 46 79 87 4D 2A 8F C7 6D 93 Qi...:t.Qj.Cb...:Ne.Gn.Fy.Mi.m.
000000F0  S1 70 DD 5B 7B DD 50 7B 47 60 44 14 6A 8F 42 69 AA 92 FC DD 56 63 88 40 65 92 Qp.Z(F.(G'D...:3.Nc.N...:Vc.Qh.
0000010E  A8 79 94 14 6A 92 40 68 87 51 78 93 51 70 DD 50 75 DD 4E 68 92 45 67 90 5D 7F 98 8D 7B DD .y..:j.Sh.Qs.Qp.Fu.Nh.No.J...:i.
0000012C  43 63 8D 55 7B 96 47 C6 DD 5D 3A 59 5B 3A 87 46 75 87 41 77 94 51 74 94 55 3A 93 55 6F 96 cc.U...:m]::[~.Fu.Aw.Qb.U:Uo.
0000014K  5D 36 DD 55 7B 97 8D 79 98 55 3A 93 55 3A 98 51 76 88 14 78 9C 50 7B 93 5D 7F DD 47 6A 8F 16.Y...:y.^:Uz.Qw...:x.P(.).Gj.
00000165  55 6D 75 7B 9E 5C 73 98 5C 3A 94 14 76 88 50 60 96 5D 79 9C 50 7A BA 50 63 DD 47 6A 8F Um.Vu...:s.\.:v.P...:ly...:Pc.Gs.
00000186  14 73 92 43 73 89 55 3A 87 46 79 98 5A 73 98 14 7E 87 5D 7F 9C 5D 78 93 5D 7F 18 15 8A 8D .x.cs.Y...:Uy.Zs...:~.I...:l...
000001A4  50 92 47 6E 86 55 74 98 50 60 96 5D 79 9C 50 7A BA 50 63 DD 47 6A 8F 14 69 92 8D 12 [m.Zb.i...:NsD:[~.Fu.Zs...:m.Fu...:Q...:Pu.Zu...
000001C2  80 7E 54 57 72 8C 8A 79 9C 14 73 DD 59 7B 8F 59 79 88 73 9C 44 69 94 DE 36 6D 5D 80 89 P...:W...:Z...:i...:Ys...:m...:j...
000001E0  43 75 8F 4E 7E 83 7D 7B DD 43 63 82 56 68 9C 88 7C OC 18 3A 94 14 6A 92 8A 93 55 74 94 Cu.M...:i...:Co.Vh...:~.j...:Us...
000001FE  S1 3A 94 40 7D 3E 16 3A 9C 55 77 DD 53 75 61 5A 73 95 14 60 99 55 76 93 5B 68 18 14 6D 4E Q:~.Q...:X...:Si...:z...:m...
0000021C  55 7E 9C 5A 7C 9C 14 69 82 56 A3 DD 47 77 90 40 77 DD 5D 3A 88 53 73 98 5E F0 80 73 7F 9A U...:Zs...:i...:V...:G...:Mv...:i...:Z...
0000023A  5B 3A 87 50 7B 8A 55 74 94 55 3A 8E 5B 78 94 51 3A 8E 44 68 9C 43 63 DD 4E 3A 92 56 75 A [:P(U...:U...:[~.Q...:Dh.Cc.N...:Vu...
00000255  SD A3 87 5F E9 CA 18 3A 94 14 6A 92 46 60 44 50 71 92 43 79 93 5D 7B DD 4E 70 9C 43 73 8E J...:_.:...:j.DFQg.C(.).J...:Np.Cs...
00000276  5F 36 DD 5D 3A 87 50 75 91 5A 78 61 D2 3A 92 47 A3 99 4E 7B 93 5D 7B D1 14 79 87 4D 3A 97 _6]::Pu.Zu...:G...:N...:I...:J...:y.M...
00000294  41 A5 DD 55 7B 91 51 A5 84 14 69 59 8D 7D 43 63 93 5D 7F 61 D2 3A 8E 5D F0 DD 47 7B 90 A...:Z(Q...:i...:~.Cc.J.a...:i...:G...
000002B2  S1 77 88 15 3A 94 14 6E 92 14 6D 4E 63 82 40 71 92 18 3A 9E 5B 3A 8A 14 6D 84 47 7A 96 Qw...:...:n...:m...:Nc.Qg...:i...:i...:m...
000002D0  SD 77 DD 47 6E 82 14 70 84 42 A3 74 77 96 50 78 7D 44 63 82 40 71 92 18 3A 9E 5B 3A 8A 14 6D 84 D2 94 Iw.Gn.Dt.A...:Mv...:Aw...:m...:m...
000002E2  S1 69 18 15 3A 94 14 6E 92 14 74 94 81 3A 89 47 64 76 86 5B 3A 99 55 78 89 51 7D 92 18 3A 92 42 W...:Z...:i...:Q...:M...:i...:j...
0000030C  SE 69 18 15 3A 94 14 6E 92 14 74 94 81 3A 89 47 64 76 86 5B 3A 99 55 78 89 51 7D 92 18 3A 92 42 Ne...:i...:Q...:e...:Q...:M...:i...:j...
00000323  S1 3A 96 55 55 99 51 70 DD 57 72 5A 5D 76 94 14 75 91 51 85 8E 5D 3A 8E 40 7B 87 51 77 84 Q:~.U...:Op.Wr...:i...:x...:i...:8...:Q...
00000345  14 69 94 3E 61 59 73 99 46 79 94 18 2A 9C 57 7F DD 5D 3A 99 55 78 89 51 7D 92 18 3A 42 i...:ax...:Fy...:~.X...:i...:X...:i...:B...
00000366  S1 3A 88 47 6E 9C 5E 7E DD 4E 7E 92 52 74 92 A3 FC DD 43 74 94 5F 7B 93 5D 7B DD 43 74 87 Q:~.Gn...:~.Nx...:...:Ct...:i...:C...
00000384  50 7B 8F 4E 7F 93 5D 7B 5D 5A 54 57 72 DD 4E 65 62 9E 46 90 5D 7F 92 5D 7B DD 39 10 CF P(.N...:J...:Wz.Nh.No.J...:i...:9...
000002A2  1A 3A B2 55 76 98 5B 62 63 5D 3A 95 55 7D 40 63 90 14 69 90 DE 3A 87 55 69 89 55 74 9C .:U...:c...:U...:~.c...:i...:i...:U...
000003C0  43 73 9C 5D 3E 6D BB 7F 5D 5A 5A 14 60 97 58 6D 46 91 9C 57 72 DD 43 6E 0E 46 74 84 Cs...:6...:i...:~.Um.Gg.Wr.Cn.Ft...
000003DE  57 72 DD 40 6D 92 46 89 5A 14 74 8C 40 6F 8E 40 3A 97 51 69 89 14 79 92 8A 3A 90 5D A9 98 Wr...:m...:F...:t...@M...:Q...:y...:i...
000003FC  S2 75 DD 5D 5A 5D 7B 59 94 8D 7D 5C 5E A3 92 51 7D 92 1A 3A B3 44 34 DD 52 7E 84 14 69 94 Su...:i...:y...:~.Q...:i...:D4...:S...:i...
0000041A  DE 3A 9E 5C 76 98 5B 8A 2D 5D 7B 5E 4E 7F D1 14 75 89 46 60 84 59 6F 97 51 3A 8D 51 6D 92 .:U...:V...:i...:N...:u.F...:Yo.Q...:Qm...
00000426  S1 3A 8D DE 71 93 5D F0 92 5D 7B D3 14 4E 98 14 6D 94 DE 79 DD 44 F0 96 5A 73 17 57 73 9C Q...:q...:i...:R...:m...:i...:D...:Zs...:W...
00000456  18 3A 97 55 71 96 5B 76 8A 5D 7F 96 14 73 8E 40 74 94 51 70 44 14 6A 8F 4E 7F 9E 5D 7F 42 .:Uq.[v...:...:s...:e...:Qp.D...:j...:N...:i...:B...
```

Wciśnij F1, aby uzyskać pomoc.

- Następnie deszyfrowałem plik używając tych samych ustawień

CrypTool 1.4.42 - XOR deszyfrowanie <XOR szyfrowanie <PlainText.txt>, klucz <34 1A FD>>, klucz <34 1A FD>

Plik Edycja Widok Szyfrowanie Podpis cyfrowy Algorytmy Kryptoanaliza Opcje Okno Pomoc

**C1 XOR deszyfrowanie <XOR szyfrowanie <PlainText.txt>, klucz <34 1A FD>>, klucz <34 1A FD>**

**C1 XOR deszyfrowanie <XOR szyfrowanie <PlainText.txt>, klucz <34 1A FD>>, klucz <34 1A FD>**

Mark Aurelius, Księga III, punkty 1 i 2

1. Nie tylko to powinno się wziąć pod uwagę, że co dnia zużywa się życie i pozostaje coraz mniejszość jego częścią, ale i to, że gdyby się miało żyć bardzo długo, to jest niepewne, czy starczy równej na dalszą przyszłość szybkości potrzebnej do zrozumienia wypadków i do zrozumienia nauki, mającej na celu badania spraw boskich i ludzkich. Gdy się bowiem zacznie dziesiątki, pozostanie uprawdzie oddychania i karmienia się, i tworzenia wyobrażeń, i poządzania itd., ale gaśnie zdolność владania sobą samym i umiejętnego zdawania sobie sprawy z obowiązków, i porządkowania zjawisk, i zdolności osiądzania, czy już należy stąd wynieść się samemu, i to wszystko, co wysokim stopniu wymaga umysłu wyćwiczonego. Należy się więc spieszyć, i to nie tylko dlatego, że każdej chwili bliżej stajemy się śmierci, ale i dlatego, że staje się zdolność wnikania w zdarzenia i ich zrozumienia.

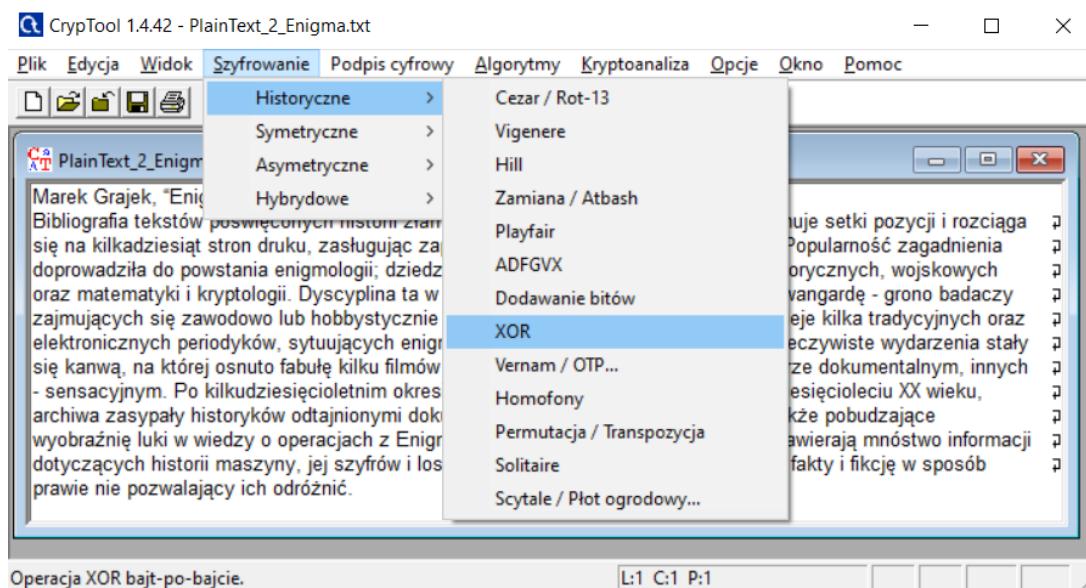
2. Należy i nad tym zastanawać, że i w zjawiskach wtórnego tworów natury jest coś mięsigo i pociągającego. Np. gdy się chleb piecze, otrzymuje pewne pekińciki. Te wień pekińcja, jakkolwiek istnieją przeciw wbrew zapowiedzi stuleci piekarskiej, jakoś nowy widokiem i dodają w sposób sobie właściwy chęci do jedzenia. Także figi, gdy są najdroższe, pękają. I ołówk zupełnie dojrzały zbliżający się psucie dodaje jakiegoś swoistego uroku owocowi. I klosy, gdy się w dół schylają, i zmarszczone czoło lwa, i piana leżąca się z pyska dzików, i innych wiele objawów, które są dalekie od piękności, gdyby im się przypatrzyć każdemu z osobna, przecież służą ku ozdobie i mięs są duszy, ponieważ są dalszym ogniwem tworów natury, tak że jeżeli ktoś odczuwa i ma głębsze zrozumienie tego, co się dzieje w wszechświecie, temu prawie wszystkie objawy wtórne będą się wydawały jakieś mięs i zharmonizowane. Ten będzie z nie mniejszą przyjemnością patrzyć na rzeczywiste paszczę dzików zwierząt, jak na te, które — naśladując — pokazują malarze i rzeźbiarze. I staruszki, i starca pewien rozwitk i urok, i wdzięk młodzienicy u chłopięt będzie mógł oglądać rozumnym swym okiem. I inne liczne podobne zjawiska nie każdemu będą mięs, lecz tylko temu, kto się naprawdę zżyje z naturą i jej dziełami.

Wciśnij F1, aby uzyskać pomoc.

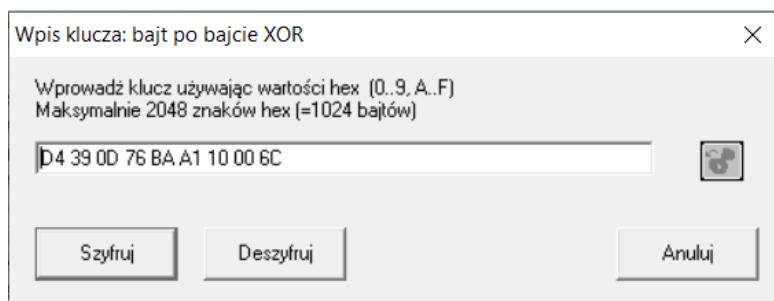
Jak widać, deszyfrowanie przebiegło pomyślnie i plik został odtworzony w nienaruszonym stanie.

## Przebieg analizy - tekst nr 2

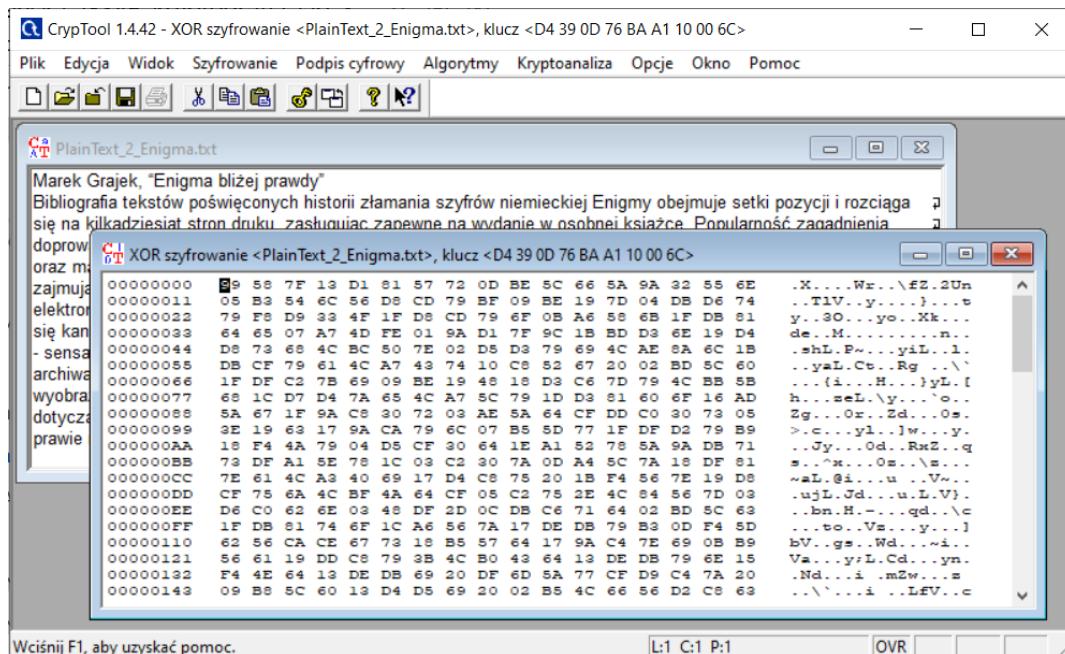
- Na przygotowanym pliku z tekstem jawnym rozpoczęłam szyfrowanie metodą XOR.



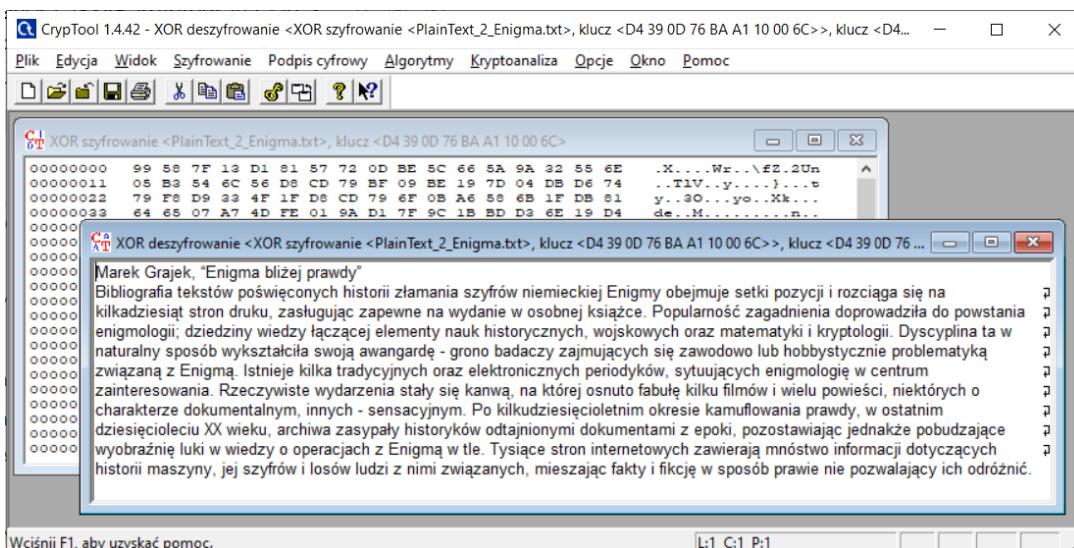
- Zastosowałam parametry jak poniżej na zrzucie ekranu, a więc klucz o wartości: D4 39 0D 76 BA A1 10 00 6C.



- Plik po zaszyfrowaniu wyglądał jak poniżej.



- Następnie deszyfrowałam plik używając tych samych ustawień co przy szyfrowaniu a więc klucza D4 39 0D 76 BA A1 10 00 6C.



Jak widać, deszyfrowanie przebiegło pomyślnie i plik został odtworzony w nienaruszonym stanie.

## Wady i zalety metody XOR

### WADY

- Proste szyfrowanie XOR jest względnie łatwe do złamania. Jego zabezpieczenia nie są lepsze niż klasycznych szyfrów wieloalfabetowych. Przy użyciu komputera, odkrycie tekstu jawnego zajmuje stosunkowo niewiele czasu.
- Jeśli szyfrujemy literę za pomocą siebie samej to efekt będzie zawsze ten sam czyli 00000000, to bardzo ważna informacja która ułatwia atakującemu złamanie szyfru.
- Jest podatny na atak znanego tekstu jawnego.
- Samo w sobie, używając stale powtarzającego się klucza, szyfr XOR można w prosty sposób złamać za pomocą analizy częstotliwości. Jeśli można odgadnąć treść wiadomości lub poznać ją w inny sposób, można ujawnić klucz.
- Jest możliwe przerzucanie dowolnych bitów w odszyfrowanym tekście jawnym poprzez manipulowanie tekstem zaszyfrowanym. Nazywa się to plastycznością i jest to cecha bardzo niepożądana w krypto systemie, nie odnosi się do zdolności atakującego do odczytania zaszyfrowanej wiadomości a do możliwości jej modyfikacji.

### ZALETY

- Jest łatwy do wdrożenia, a operacja XOR jest tania obliczeniowo.
- Prosty, powtarzający się XOR jest czasami używany do ukrywania informacji w przypadkach, gdy nie jest wymagane żadne szczególne zabezpieczenie (szyfr XOR jest często używany w złośliwym oprogramowaniu komputerowym, aby utrudnić inżynierię wstępnej).

## 5. DES z ECB

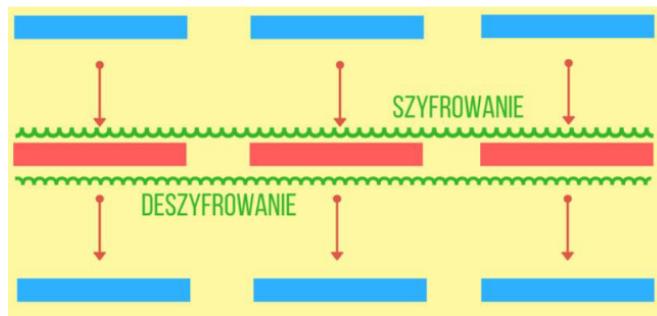
Szyfr blokowy DES operuje na n-bitowych paczkach (blokach) danych tekstu jawnego, który przy pomocy sparametryzowanej kluczem prywatnym funkcji szyfrującej odwracany jest na n-bitowy blok tekstu zaszyfrowanego (szyfrogram). W chwili, gdy długość tekstu jawnego jest większa od n, stosuje się kilka różnych trybów działania.

Zarówno do szyfrowania, jak i deszyfrowania stosuje się ten sam algorytm. Klucz jest 64-bitowy, przy czym informacja użyteczna zajmuje 56 bitów (co ósmy bit w ciągu klucza jest bitem parzystości).

DES pracuje w czterech trybach pracy. Dwa z nich ECB i CBC przeanalizuję w obrębie tego laboratorium.

W trybie elektronicznej książki kodowej (Electronic Codebook – ECB) każdy z bloków tekstu kodowany jest oddzielnie, w taki sam sposób deszyfrowane są szyfrogramy.

Zapewnia to przeprowadzenie wielu wątków w tym samym czasie. Elektroniczna książka kodowa to zbiór pewnych fraz i odpowiadających im fraz po zakodowaniu. Jeśli dla danego klucza (a szyfrujemy tym samym kluczem) utworzymy wszystkie możliwe teksty jawne i ich kryptogramy w efekcie otrzymamy „książkę kodową”. Książek kodowych będzie tyle ile możliwych kluczy dla danego szyfru.



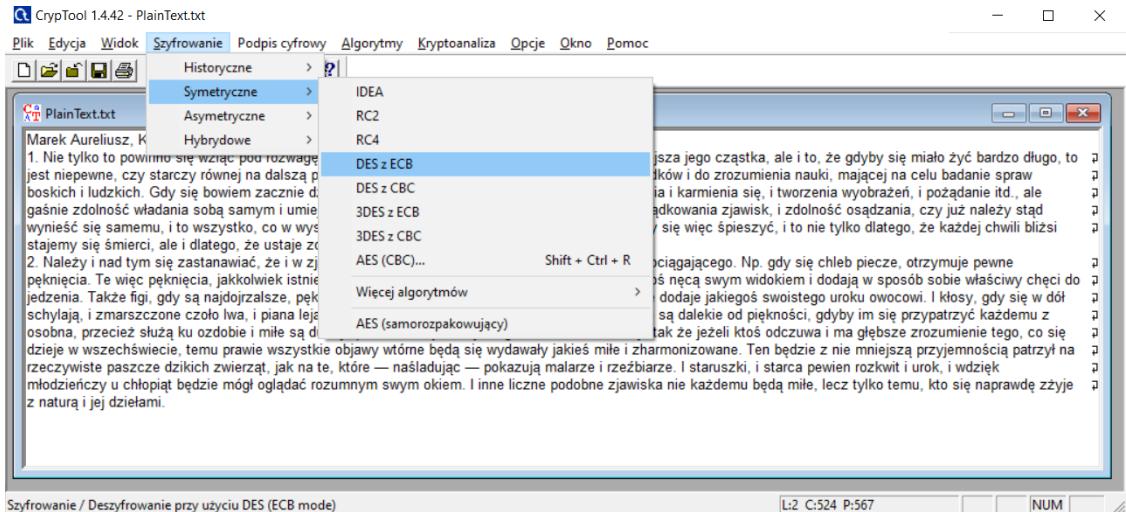
Źródło: prezentacja [agh.edu.pl](http://agh.edu.pl)

Najważniejsze właściwości ECB:

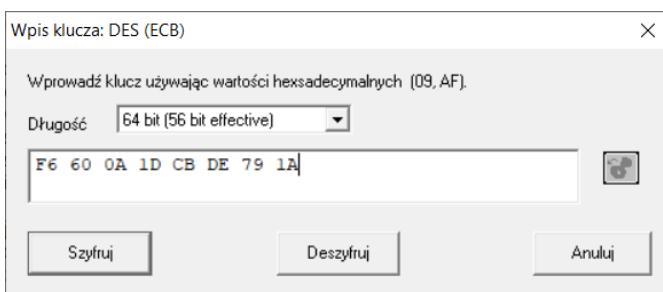
- Szyfr blokowy DES w trybie ECB szyfruje tekst jawnego w blokach n-bitowych o stałym rozmiarze (zazwyczaj  $n=64$ ).
- Wiadomości przekraczające n bitów dzieli się na n-bitowe bloki i szyfruje każdy osobno.
- Wiadomość, która ma być zaszyfrowana musi być wyrównana do długości równej wielokrotności długości jednego bloku.
- Zależności łańcuchowe: bloki są szyfrowane niezależnie od innych bloków. Zmiana kolejności bloków tekstu zaszyfrowanego powoduje zmianę kolejności bloków tekstu jawnego.
- Ma zastosowanie w szyfrowaniu baz danych.

### Przebieg analizy - tekst nr 1

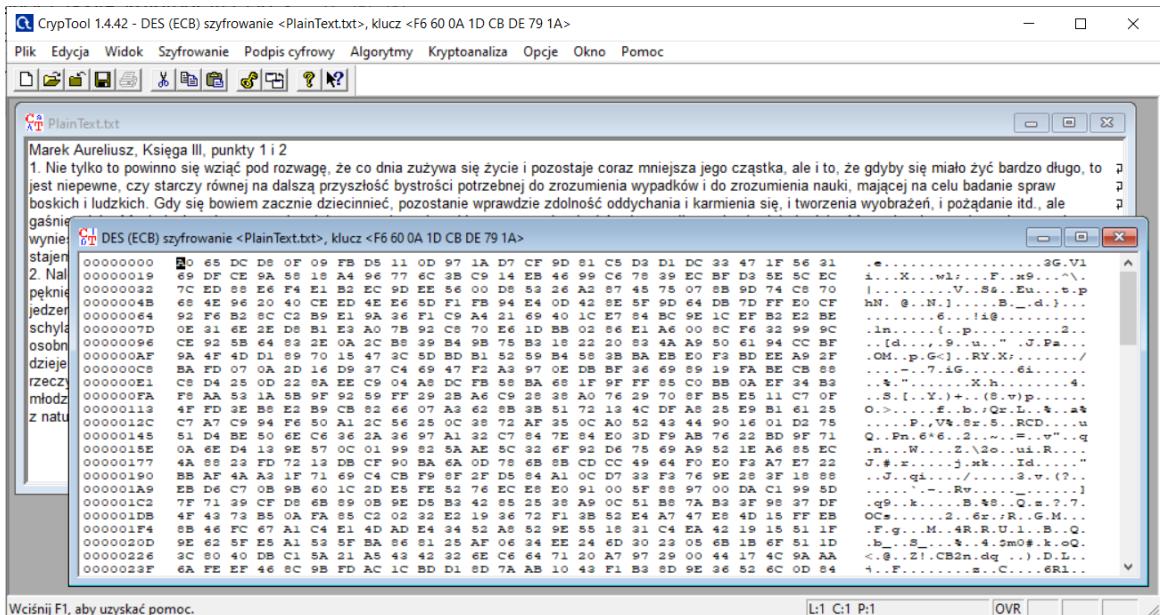
- Na przygotowanym pliku z tekstem jawnym rozpoczęłam szyfrowanie metodą DES z ECB.



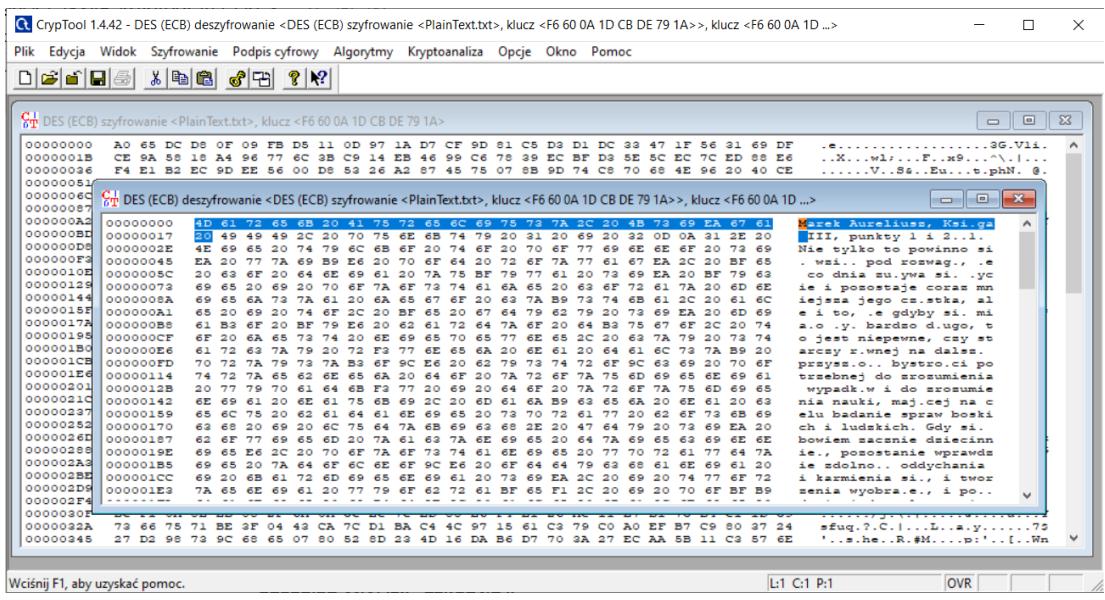
- Zastosowałem parametry jak poniżej na zrzucie ekranu, używając 64-bitowego klucza F6600A1DCBDE791A.



- Plik po zaszyfrowaniu wyglądał jak poniżej.



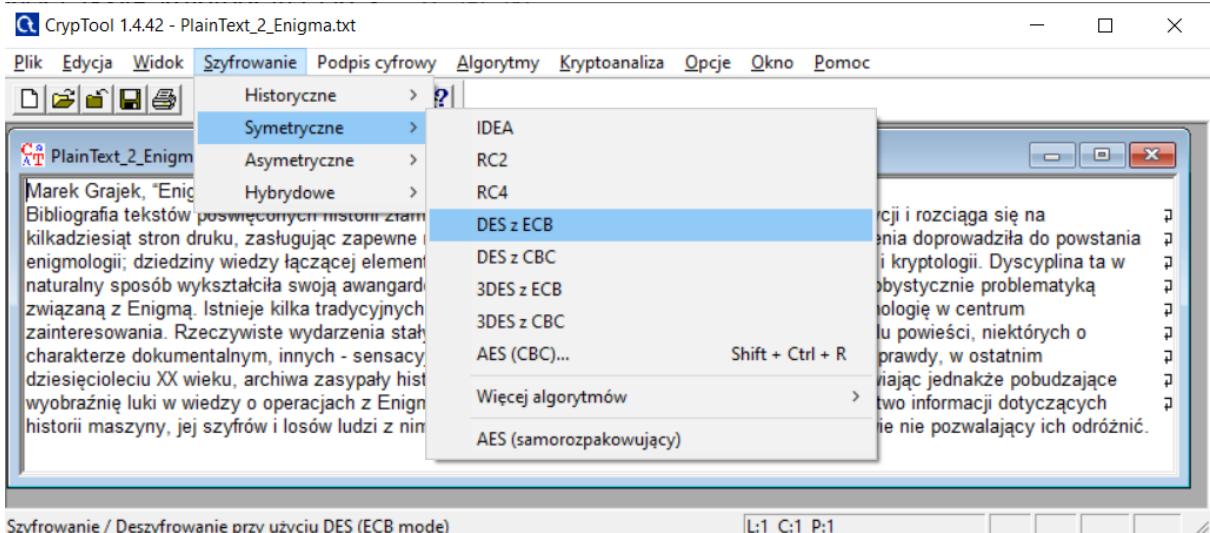
- Następnie deszyfrowałem plik używając tych samych ustawień 64-bitowego klucza F6600A1DCBDE791A.



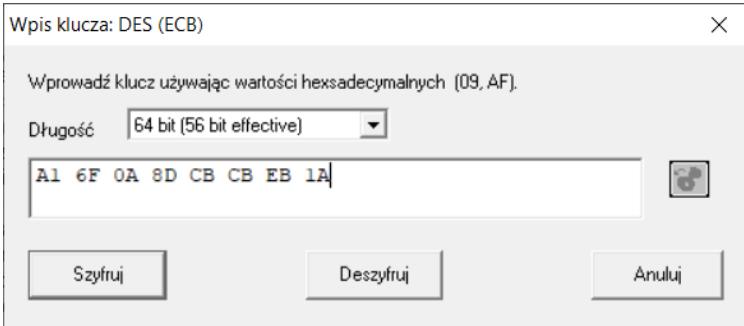
Jak widać, deszyfrowanie przebiegło pomyślnie i plik został odtworzony w nienaruszonym stanie. W prawej części okna z deszyfrowaniem widać tekst jawnny.

## Przebieg analizy - tekst nr 2

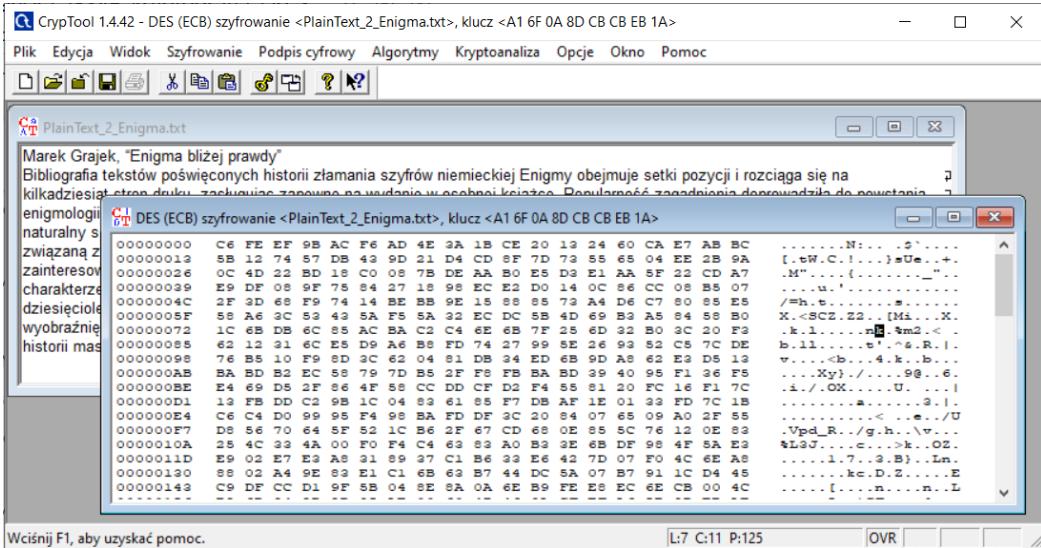
- Na przygotowanym pliku z tekstem jawnym rozpoczęłam szyfrowanie metodą DES z ECB.



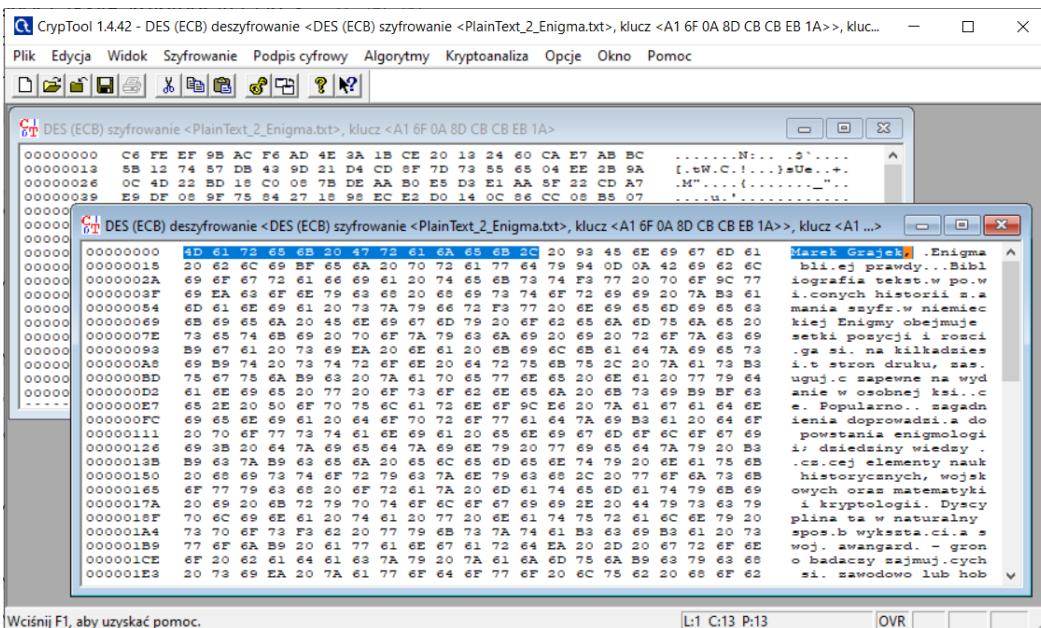
- Zastosowałam parametry jak poniżej na zrzucie ekranu, używając 64-bitowego klucza A1 6F 0A 8D CB CB EB 1A.



- Plik po zaszyfrowaniu wyglądał jak poniżej.



- Następnie deszyfrowałam plik używając tych samych ustawień



Jak widać, deszyfrowanie przebiegło pomyślnie i plik został odtworzony w nienaruszonym stanie. W prawej części okna z deszyfrowaniem widać tekst jawnny.

## **Wady i zalety metody szyfru DES z ECB**

WADY

- Szyfr blokowy DES w trybie ECB jest podatny na ataki „metodą powtórzenia”.
- Możliwa jest modyfikacja kryptogramu bez znajomości klucza.
- Metoda ta nie zawiera mechanizmu informowania o tym, że jakąś wiadomość wstawiono lub usunięto.

## ZALETY

- Utrata lub uszkodzenie pojedynczych bloków nie ma wpływu na możliwość deszyfrowania pozostałych.
- Nadaje się do szyfrowania baz danych

## 6. DES z CBC

Szyfr DES w trybie wiązania bloków zaszyfrowanych (Cipher Block Chaining – CBC) wymaga dodatkowego n-bitowego wektora, którym inicjalizuje się początkową ("zerową") wartość szyfrogramu. Postaci szyfrogramów dla poszczególnych bloków wiadomości otrzymuje się w wyniku przekształcania funkcją szyfrującą kolejnych bloków tekstu jawnego, które dodatkowo sumuje się modulo 2 z blokiem szyfrogramu z kroku poprzedzającego. W ten sposób uzyskuje się szyfrogram zależny od całej historii sesji szyfrowania.

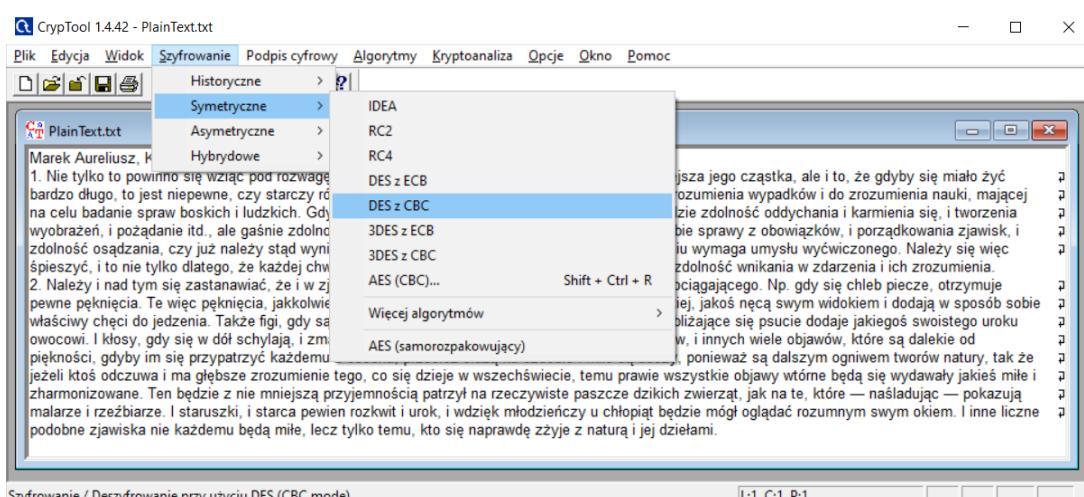
W tym tzw. "trybie wiązania bloków zaszyfrowanych", na danym bloku tekstu jawnego jest przed zaszyfrowaniem wykonywana różnica symetryczna z zaszyfrowaną wiadomością z poprzedniego bloku. Wynik tej operacji jest następnie szyfrowany za pomocą zwykłego klucza. Deszyfrowanie może odbywać się z wykorzystaniem wielu wątków równocześnie (szyfrowanie w tym trybie przeprowadzane jest z wykorzystaniem tylko jednego wątku).

Najważniejsze właściwości CBC:

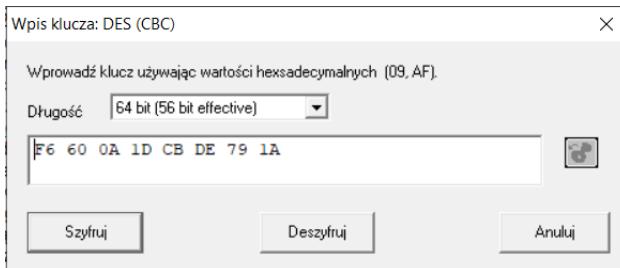
- Takie same bloki tekstu jawnego mają różne kryptogramy.
- Zmiana bitu wewnętrz jednego bloku prowadzi do zmiany tekstu po deszyfrowaniu tylko w danym bloku i następnym.
- Nie można usunąć żadnego bloku z kryptogramu.
- Wiadomość, która ma być zaszyfrowana musi być wyrównana do długości równej wielokrotności długości jednego bloku.

### Przebieg analizy - tekst nr 1

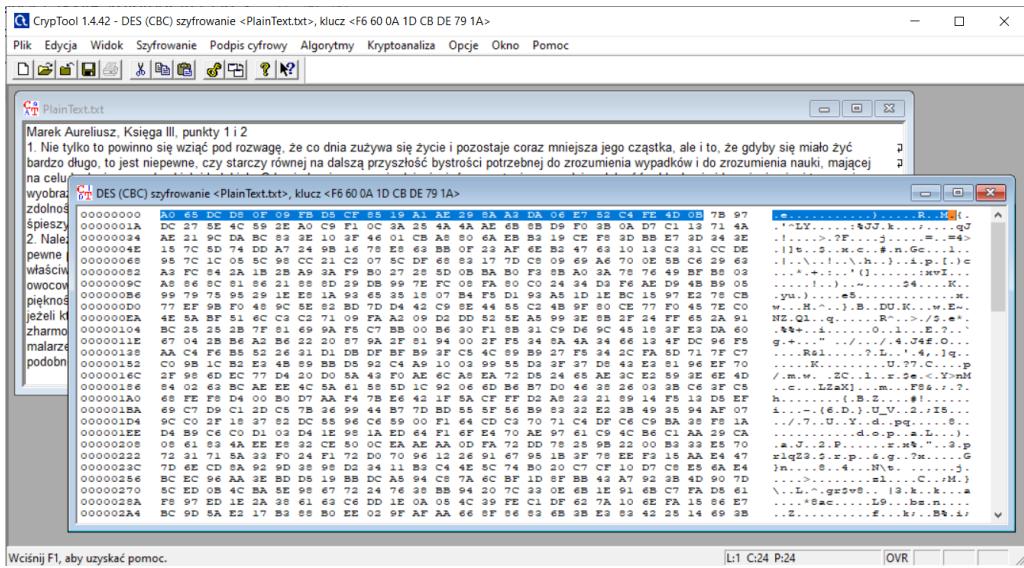
- Na przygotowanym pliku z tekstem jawnym rozpoczęłam szyfrowanie metodą DES z CBC.



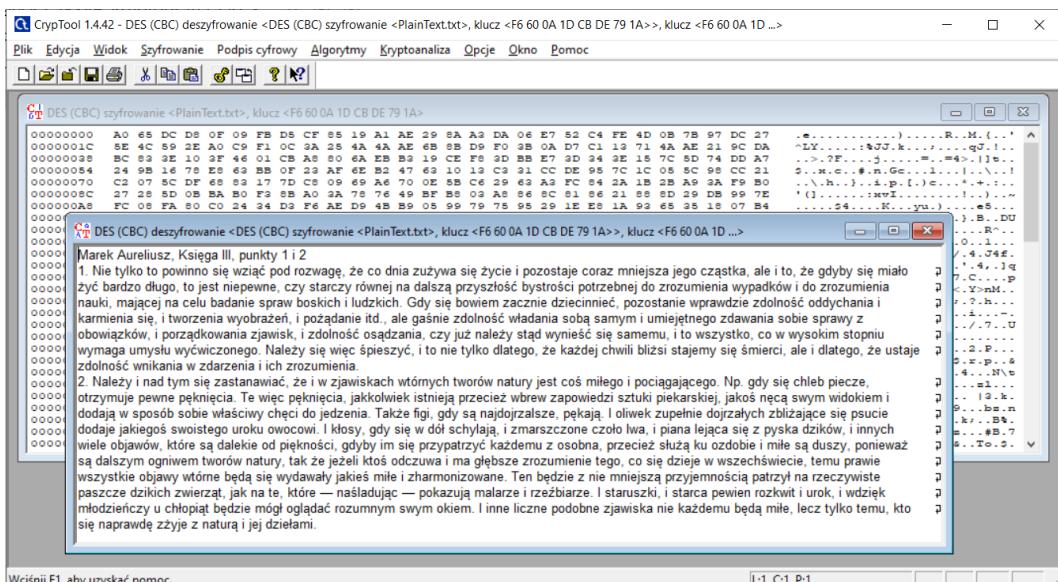
- Zastosowałem parametry jak poniżej na zrzucie ekranu, używając tym razem analogicznie jak przy metodzie DES z ECB 64-bitowego Klucza F6600A1DCBDE791A.



- Plik po zaszyfrowaniu wyglądał jak poniżej.



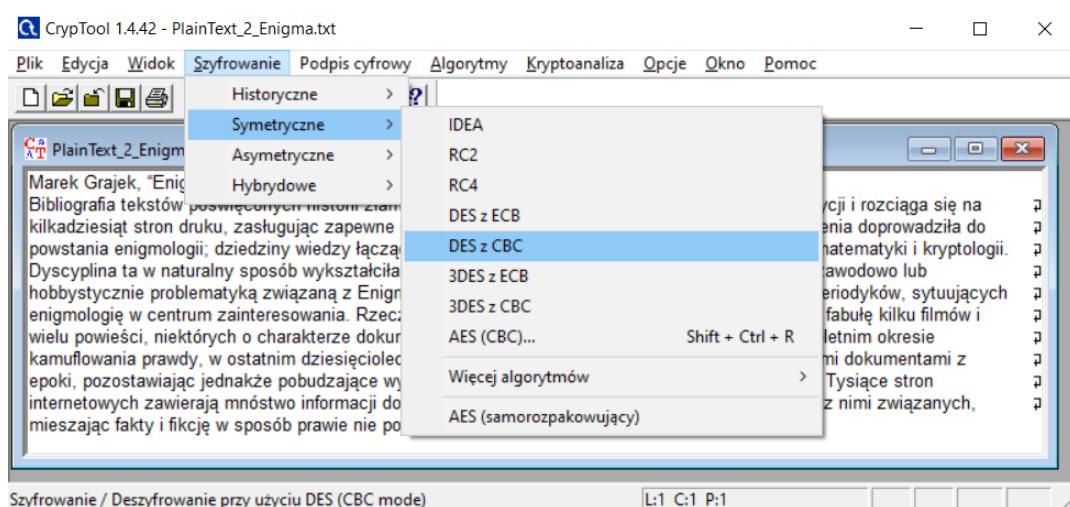
- Następnie deszyfrowałem plik używając tych samych ustawień 64-bitowego klucza F6600A1DCBDE791A.



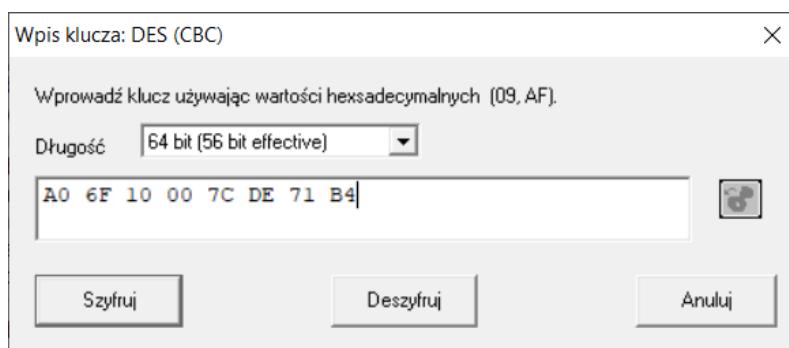
Jak widać, deszyfrowanie przebiegło pomyślnie i plik został odtworzony w nienaruszonym stanie.

## Przebieg analizy - tekst nr 2

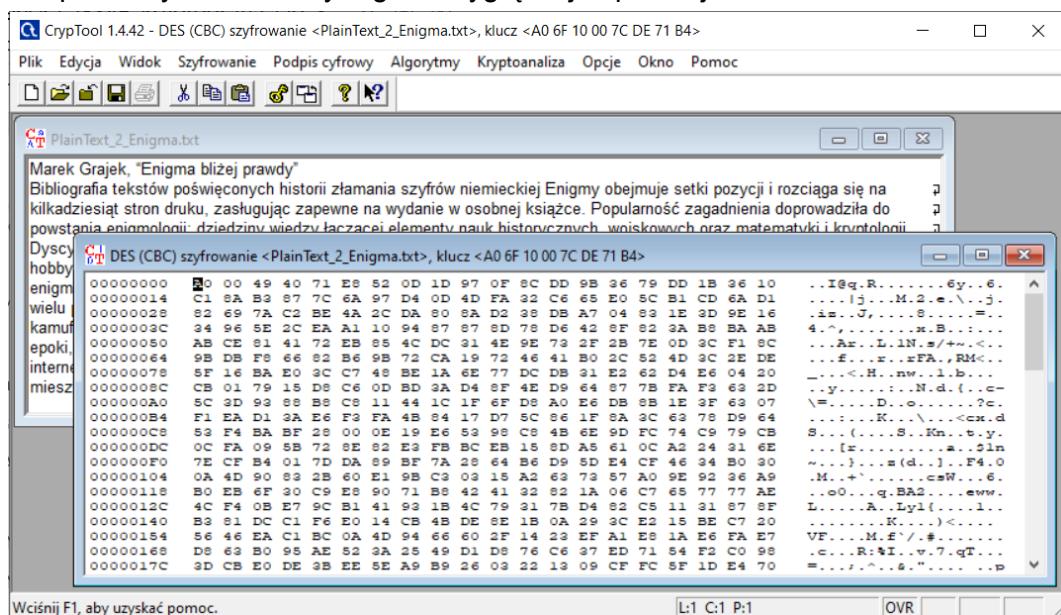
- Na przygotowanym pliku z tekstem jawnym rozpoczęłam szyfrowanie metodą DES z CBC.



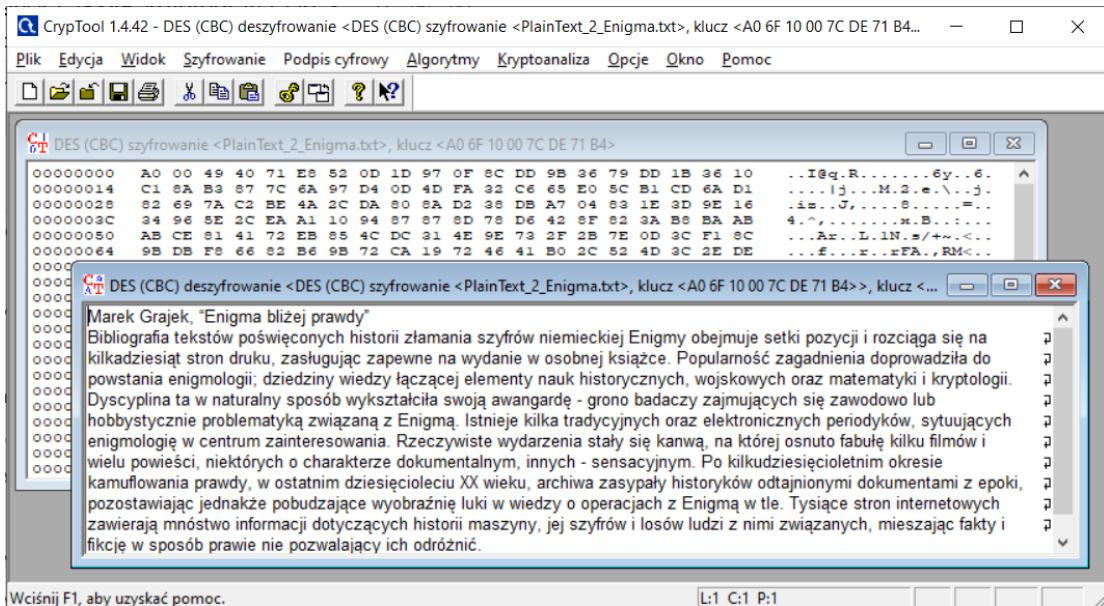
- Zastosowałam parametry jak poniżej na zrzucie ekranu, używając tym razem analogicznie jak przy metodzie DES z CBC 64-bitowego klucza A0 6F 10 00 7C DE 71 B4.



- Plik po zaszyfrowaniu szyfrogram wyglądał jak poniżej.



- Następnie deszyfrowałem plik używając tych samych ustawień



Jak widać, deszyfrowanie przebiegło pomyślnie i plik został odtworzony w nienaruszonym stanie.

## **Wady i zalety metody szyfru DES z CBC**

### **WADY**

- Nieodporny na zakłóczenia (dodatkowy bit lub utrata jednego bitu psują dalszy przekaz).
- Zakłamanie jednego bitu tekstu jawnego (na przykład w wyniku błędu w transmisji) powoduje uszkodzenie wszystkich kolejnych bloków szyfrogramu i nie można odszyfrować go w przyszłości.
- Zakłamanie jednego bitu szyfrogramu powoduje uszkodzenie jedynie dwóch odszyfrowanych bloków tekstu jawnego.
- Nie można usunąć żadnego bloku z kryptogramu.
- Nie nadaje się do szyfrowania baz danych.

### **ZALETY**

- takie same bloki tekstu jawnego mają różne kryptogramy
- zmiana bitu (przekłamanie) wewnętrz jednego bloku prowadzi do zmiany tekstu po deszyfrowaniu tylko w danym bloku i następnym.

## **7. AES**

Metoda szyfrowania danych AES (zwana również Rijndael) to szyfr blokowy z kluczem symetrycznym. Do szyfrowania i deszyfrowania danych za pomocą AES wykorzystywany jest sekretny klucz o długości 128 lub 192 lub 256 bitów. W zależności od długości klucza zmianie podlega wyłącznie liczba rund, która dla kluczy 128 bitowych wynosi 10, dla kluczy 192 bitowych 12, oraz 14 dla kluczy o długości 256 bitów.

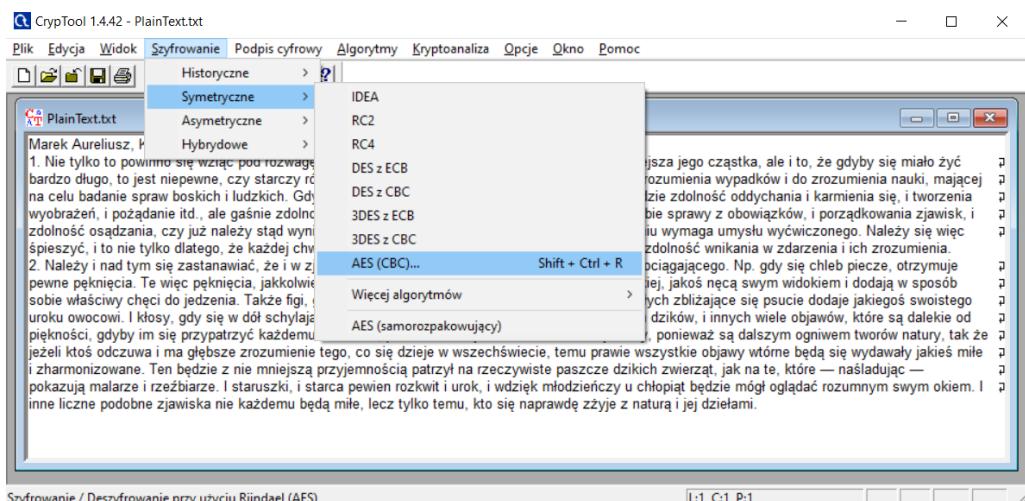
AES szyfruje dane, które otrzymuje w blokach bitów, w przeciwieństwie do szyfrowania bit po bicie. Używa on różnych długości kluczy. Im większy rozmiar klucza, tym więcej zasobów zużyje, więc można śmiało powiedzieć, że mniej wydajny system będzie częściej używał 128-bitowych kluczy AES zamiast swoich 256-bitowego odpowiednika. Na

przykład, jeśli w telefonie używany jest 256-bitowy klucz szyfrowania AES, bateria może rozładowywać się szybciej niż przy 128-bitowej wersji tego samego standardu szyfrowania.

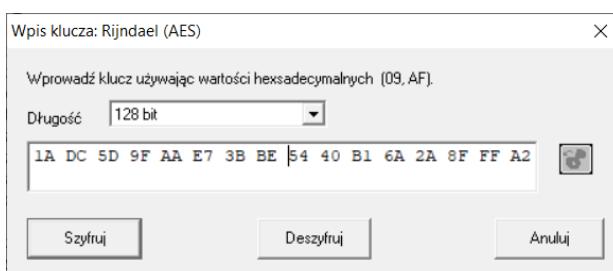
Pierwszym krokiem szyfrowania AES jest rozdzielenie danych na bloki. Każdy z tych bloków zawiera kolumnę 4 na 4 złożoną z 128 bitów lub 16 bajtów. Biorąc pod uwagę, że jeden bajt składa się z 8 bitów, mamy  $16 \times 8 = 128$  bitów, co jest rozmiarem bloku.

## Przebieg analizy - tekst nr 1

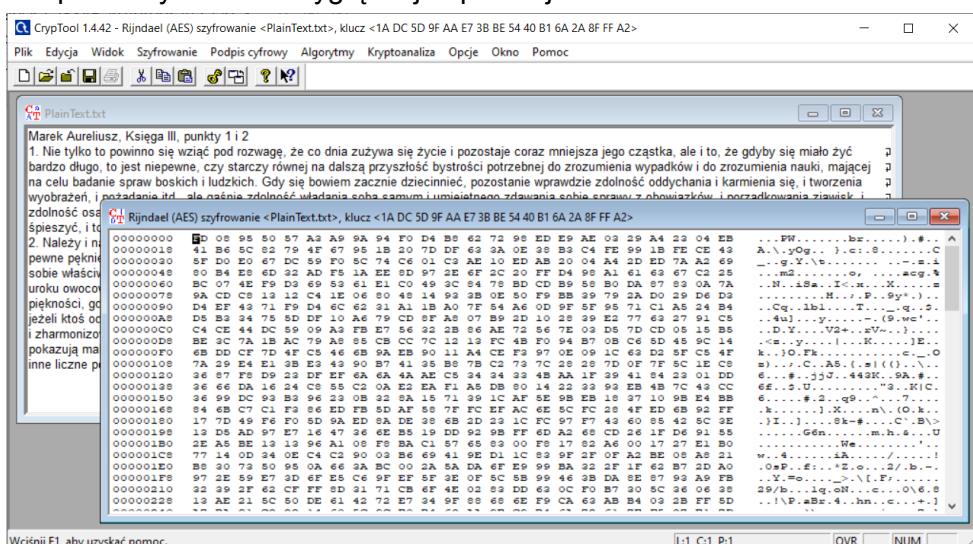
- Na przygotowanym pliku z tekstem jawnym rozpoczęłam szyfrowanie metodą AES.



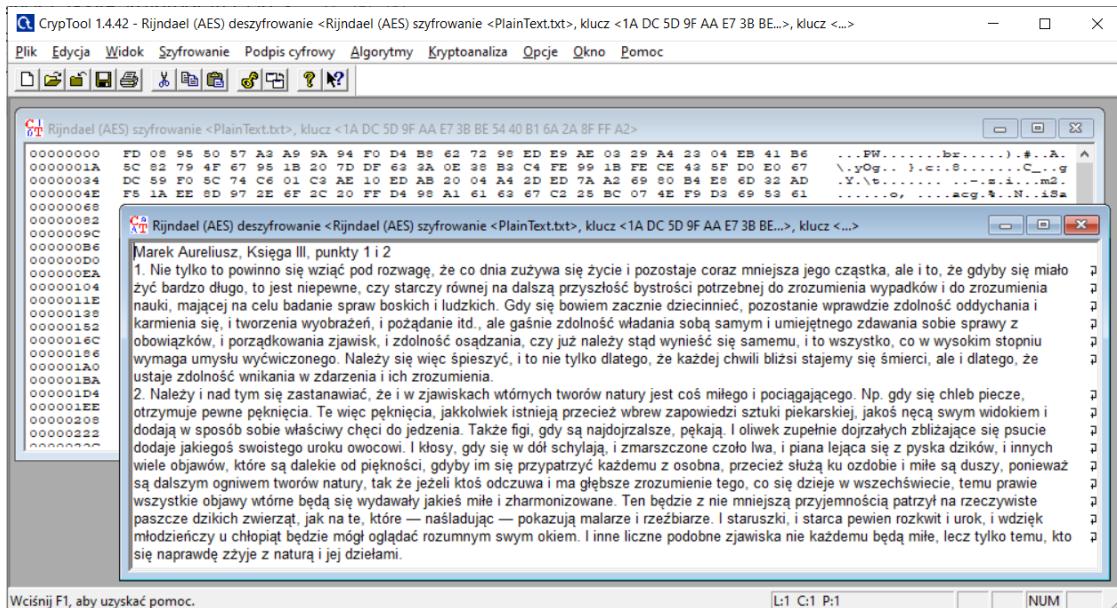
- Zastosowałam parametry jak poniżej na zrzucie ekranu, używając 128-bitowego klucza 1ADC5D9FAAE73BBE5440B16A2A8FFFA2.



- Plik po zaszyfrowaniu wyglądał jak poniżej.



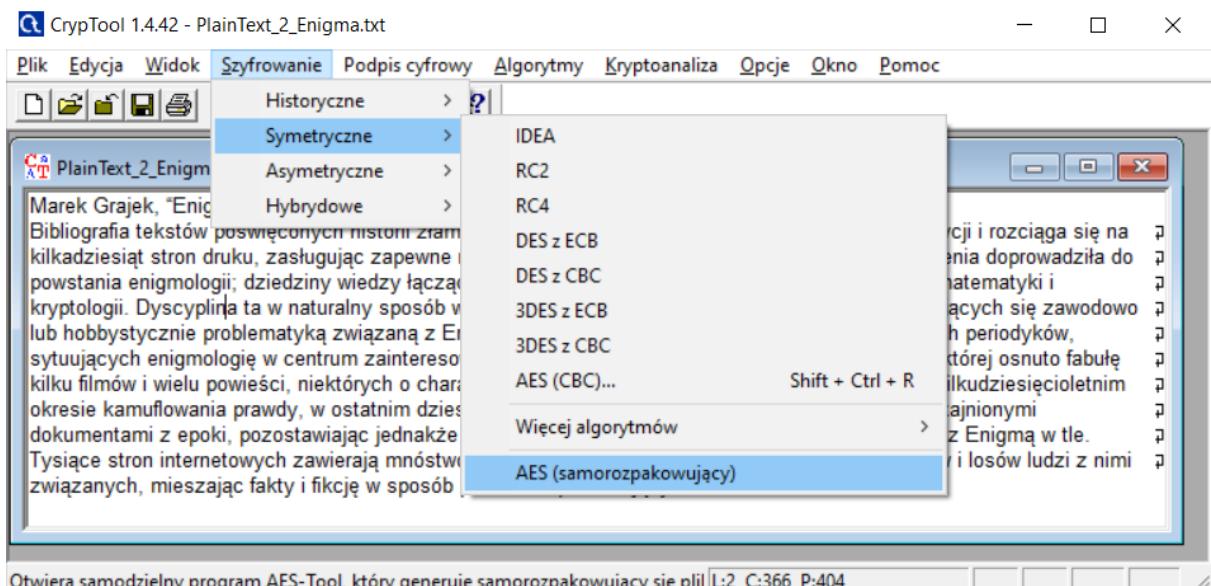
- Następnie deszyfrowałem plik używając tych samych ustawień



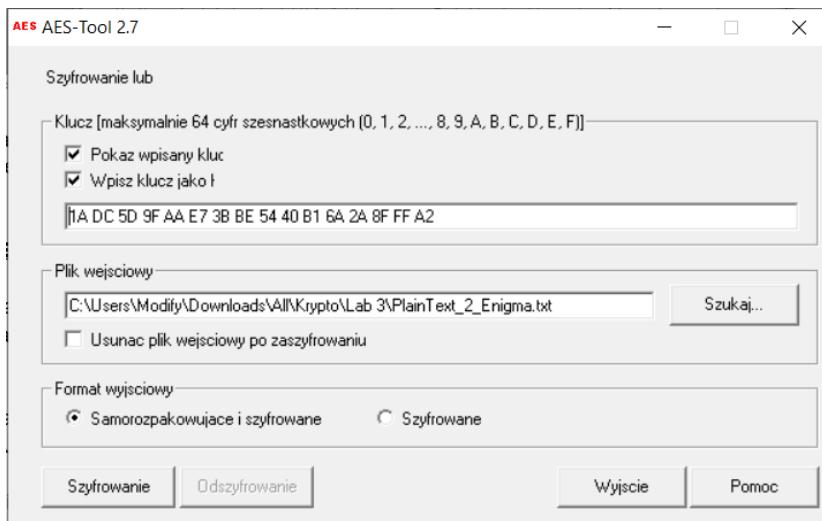
Jak widać, deszyfrowanie przebiegło pomyślnie i plik został odtworzony w nienaruszonym stanie.

## Przebieg analizy - tekst nr 2

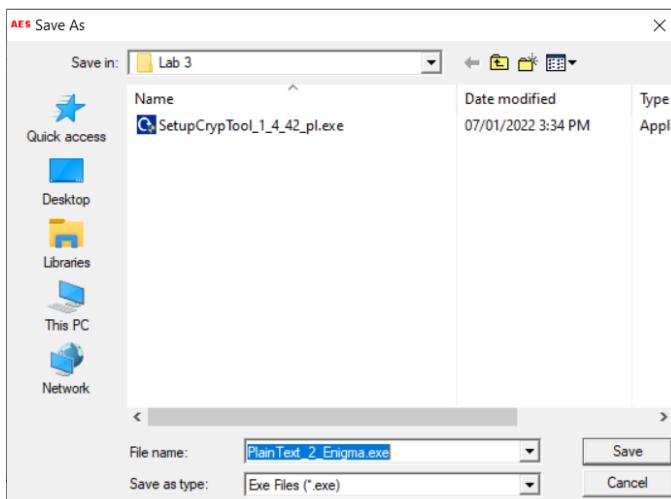
- Na przygotowanym pliku z tekstem jawnym rozpoczęłam szyfrowanie metodą AES. Tym razem skorzystałam z drugiej dostępnej w programie CrypTool opcji, mianowicie metody AES samorzatkowującego.



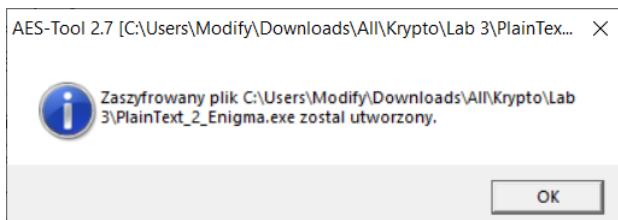
- Otworzyło się okno zewnętrznego programu AES-Tool 2.7. Zastosowałam parametry jak poniżej na zrzucie ekranu, używając tego samego klucza co przy pierwszym analizowanym tekście czyli 1ADC5D9FAAE73BBE5440B16A2A8FFA2.



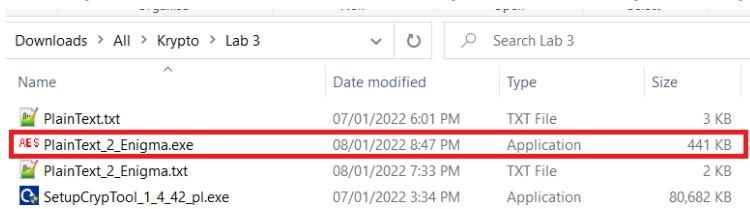
- Wybrałem miejsce zapisu zaszyfrowanego pliku.



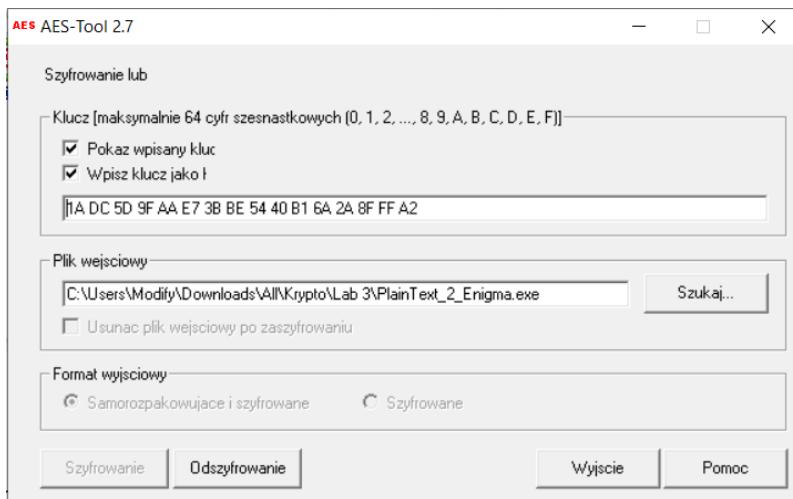
Otrzymałam informację o pomyślnym utworzeniu zaszyfrowanego pliku.



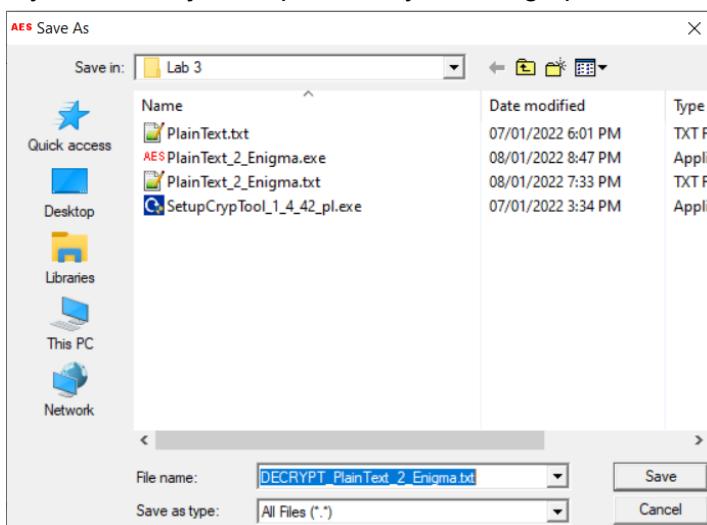
Rzeczywiście, plik został utworzony we wskazanym na dysku lokalnym miejscu.



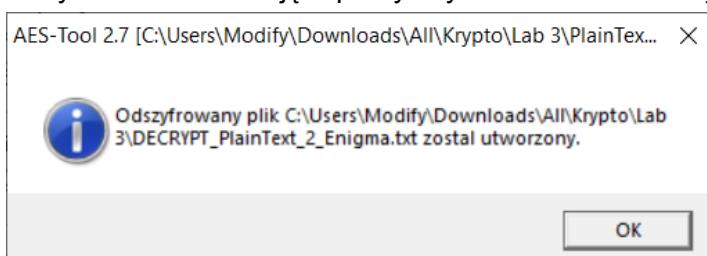
- Po uruchomieniu pliku .exe wpisałam wymagany klucz:  
1ADC5D9FAAE73BBE5440B16A2A8FFFA2



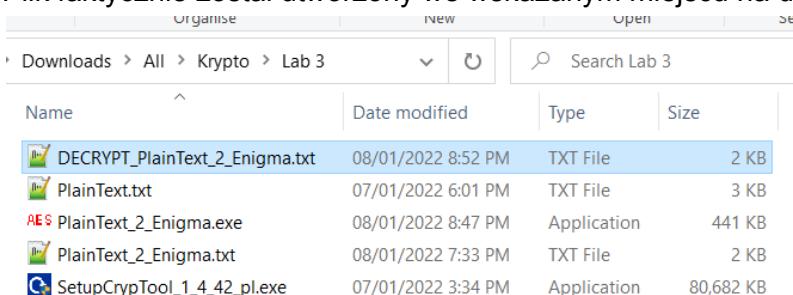
- Wybrałem miejsce zapisu deszyfrowanego pliku.



Otrzymałam informację o pomyślnym utworzeniu deszyfrowanego pliku.



Plik faktycznie został utworzony we wskazanym miejscu na dysku lokalnym.



- Plik po deszyfrowaniu wyglądał jak poniżej.

The screenshot shows a Notepad++ window with the file 'DECRYPT\_PlainText\_2\_Enigma.txt' open. The text content is as follows:

```

1 Marek Grajek, "Enigma bliżej prawdy"
2 Bibliografia tekstów poświęconych historii złamania szyfrów niemieckiej Enigmy obejmuje
setki pozycji i rozciąga się na kilkadziesiąt stron druku, zasługując zapewne na wydanie
w osobnej książce. Popularność zagadnienia doprowadziła do powstania enigmologii;
dziedziny wiedzy łączącej elementy nauk historycznych, wojskowych oraz matematyki i
kryptologii. Dyscyplina ta w naturalny sposób wykształciła swoją awangardę - grono
badaczy zajmujących się zawodowo lub hobbystycznie problematyką związaną z Enigma.
Istnieje kilka tradycyjnych oraz elektronicznych periodyków, sytuujących enigmologię w
centrum zainteresowania. Rzeczywiste wydarzenia stały się kanwą, na której osnuto fabułę
kilku filmów i wielu powieści, niektórych o charakterze dokumentalnym, innych -
sensacyjnym. Po kilkudziesięcioletnim okresie kamuflowania prawdy, w ostatnim
dziesięcioleciu XX wieku, archiwa zasypały historyków odtajnionymi dokumentami z epoki,
pozostawiając jednakże pobudzające wyobraźnię luki w wiedzy o operacjach z Enigmą w tle.
Tysiące stron internetowych zawierają mnóstwo informacji dotyczących historii maszyny,
jej szyfrów i losów ludzi z nimi związanych, mieszając fakty i fikcję w sposób prawie nie
pozwalający ich odróżnić.

```

Normal text file | length : 1,260 | lines : 2 | Ln:1 Col:1 Pos:1 | Windows (CR LF) | ANSI | INS

Jak widać, deszyfrowanie przebiegło pomyślnie i plik został odtworzony w nienaruszonym stanie.

## Wady i zalety metody szyfru AES

### WADY

- Największą wadą AES jest klucz - jak go bezpiecznie przesłać innej stronie wymiany.
- Używana jest stosunkowo prosta arytmetyka, co potencjalnie jest łatwiejsze do zaatakowania niż np. duże liczby proste na których oparty jest RSA.
- W celu przyspieszenia działania aplikacji, można zdecydować się na wcześniejsze przeliczenie wszystkich funkcji zawartych w różnych rundach algorytmu AES, a następnie zastąpienie tych obliczeń zwykłym podstawianiem danych z uzyskanych tabel. Wadą tego rozwiązania jest znaczne zwiększenie rozmiaru aplikacji. Wielkość kodu aplikacji może wzrosnąć z kilku do kilkudziesięciu kilobajtów, w zależności od długości używanego sekretnego klucza.

### ZALETY

- Szybka i bezpieczna metoda szyfrowania.
- Łatwy do wdrożenia niezależnie od miejsca docelowego (implementacja sprzętowa jest podobno łatwiejsza niż oprogramowanie)
- Jest w stanie odszyfrować chronione dane tak szybko, jak jest w stanie je zaszyfrować.
- Fakt, że obsługuje trzy długości klucza, zapewnia pewną elastyczność w zakresie bezpieczeństwa i szybkości (wydajności).
- Wszystkie trzy typy kluczy są wystarczająco długie, co sprawia, że AES jest niemożliwym celem ataku brutalnego.
- Do tej pory żaden atak kryptograficzny nie działał przeciwko AES.
- Zużywa mniej pamięci i mocy obliczeniowej niż inne popularne standardy szyfrowania (takie jak DES).
- AES jest na tyle elastyczny, że pozwala łączyć go z kilkoma innymi protokołami bezpieczeństwa, takimi jak TKIP, WPA2, WEP, ale także innymi typami szyfrowania, takimi jak SSL.
- Jego elastyczność umożliwia korzystanie z niej w szerokiej gamie produktów, od codziennych aplikacji, takich jak WhatsApp lub Signal do wojskowych systemów

bezpieczeństwa, a nawet sprzętu. Można go znaleźć praktycznie wszędzie, biorąc pod uwagę fakt, że rząd USA zdefiniował go jako standard.

- AES jest praktycznie nieprzenikniony - wykorzystuje algorytm sieciowy z podstawieniem permutacji (algorytm SPN) w celu zastosowania kilku rund szyfrowania w celu ochrony danych.
- AES to nie tylko pierwszy, ale także jedyny publicznie dostępny szyfr, który został zatwierdzony przez NSA (National Security Agency) do ochrony ścisłe tajnych danych.

## 8. RSA

RSA jest obecnie jednym z najpopularniejszych algorytmów szyfrowania asymetrycznego. Może być stosowany zarówno do szyfrowania wiadomości jak i do podpisów cyfrowych. RSA został zaprojektowany przez Ron'a Rivest'a, Adi Shamir'a i Leonard'a Adleman'a w roku 1977 - nazwa powstała właśnie od nazwisk twórców.

Algorytm RSA umożliwia utworzenie dwóch powiązanych kluczy: publicznego oraz prywatnego, a następnie wykorzystywanie ich w celu ochrony treści przekazywanych wiadomości. Klucz publiczny jest powszechnie znany i każdy może za jego pomocą zaszyfrować dowolną wiadomość. Natomiast jedynie posiadacz klucza prywatnego może odszyfrować otrzymane szyfrogramy. Analogicznie, posiadacz klucza prywatnego może używać go do szyfrowania danych, pozwalając w ten sposób każdemu posiadaczowi odpowiadającego mu klucza publicznego odszyfrować je.

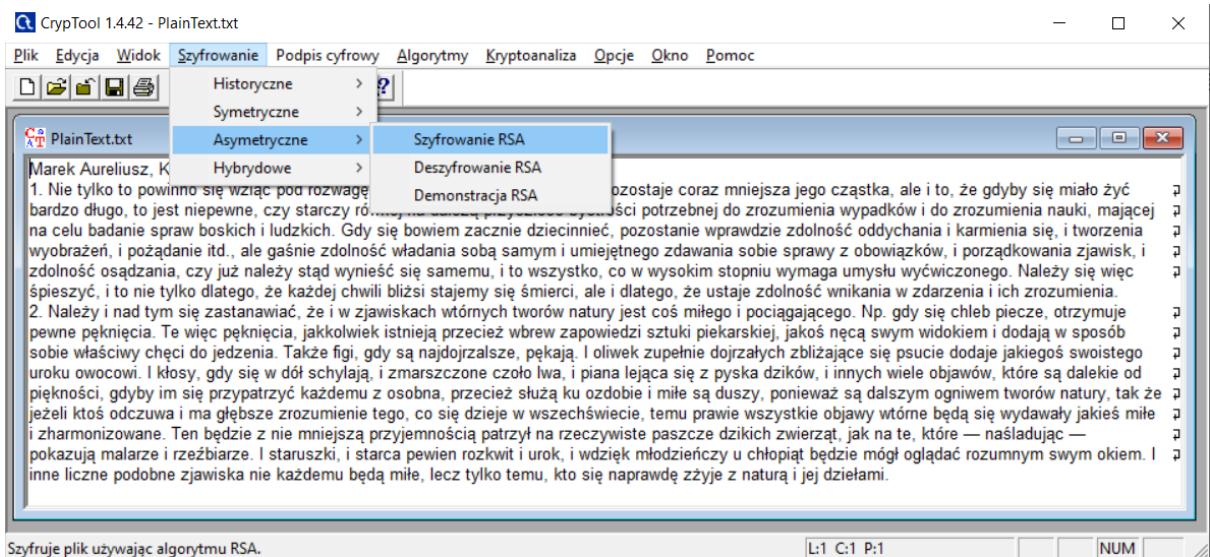
System RSA umożliwia bezpieczne przesyłanie danych w środowisku, w którym może dochodzić do różnych nadużyć. Bezpieczeństwo opiera się na zagadnieniach faktoryzacji dużych liczb złożonych, a konkretniej trudności rozkładu dużych liczb na czynniki pierwsze.

Algorytm RSA składa się z trzech podstawowych kroków:

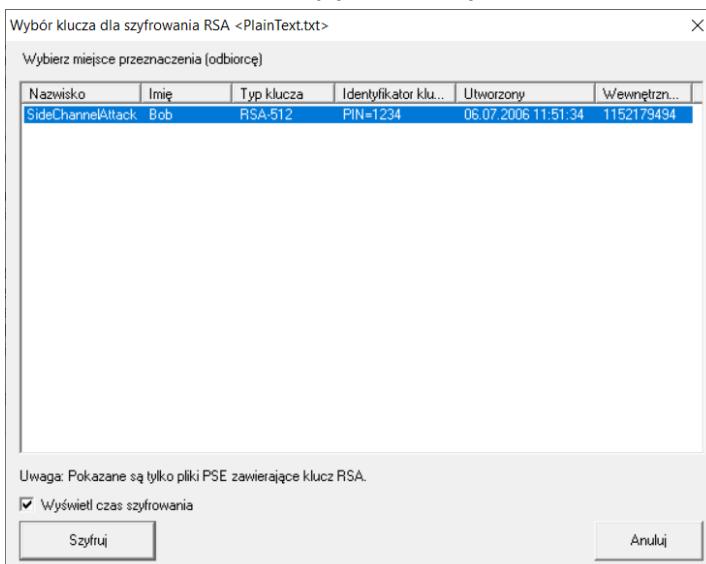
1. Generacja klucza publicznego i tajnego. Klucz publiczny jest przekazywany wszystkim zainteresowanym i umożliwia zaszyfrowanie danych. Klucz tajny umożliwia rozszyfrowanie danych zakodowanych kluczem publicznym. Jest trzymany w ścisłej tajemnicy.
2. Użytkownik po otrzymaniu klucza publicznego, np. poprzez sieć Internet, koduje za jego pomocą swoje dane i przesyła je w postaci szyfru RSA do adresata dysponującego kluczem tajnym, np. do banku, firmy komercyjnej, tajnych służb. Klucz publiczny nie musi być chroniony, ponieważ nie umożliwia on rozszyfrowania informacji - proces szyfrowania nie jest odwracalny przy pomocy tego klucza. Zatem nie ma potrzeby jego ochrony i może on być powierzany wszystkim zainteresowanym bez ryzyka złamania kodu.
3. Adresat po otrzymaniu zaszyfrowanej wiadomości rozszyfrowuje ją za pomocą klucza tajnego.

### Przebieg analizy - tekst nr 1

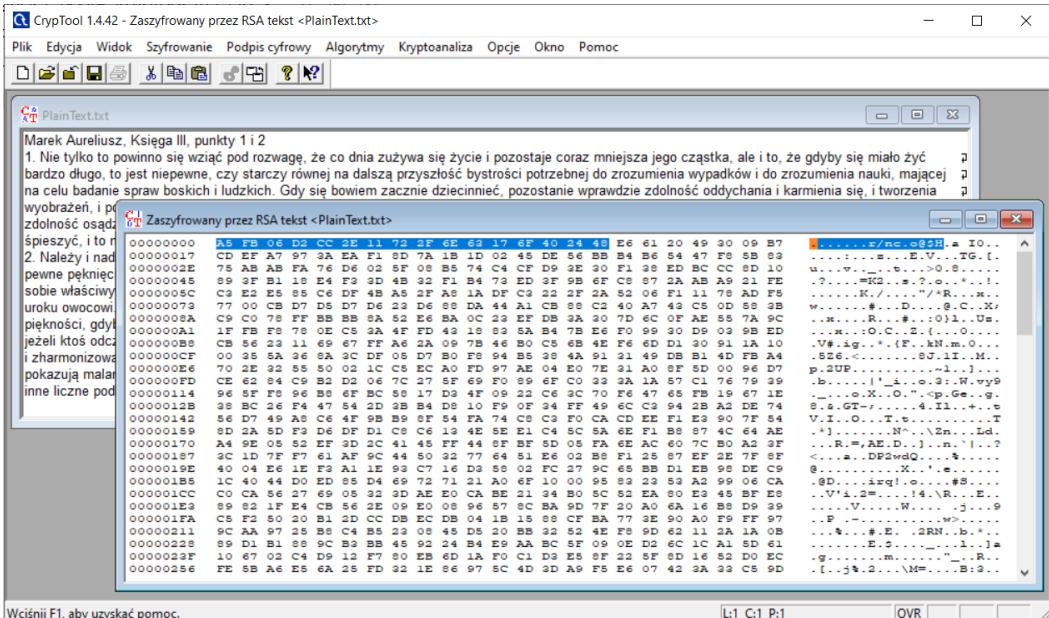
- Na przygotowanym pliku z tekstem jawnym rozpoczęłam szyfrowanie metodą RSA.



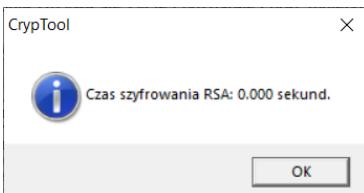
- Zastosowałam parametry jak poniżej na zrzucie ekranu z typem klucza RSA-512.



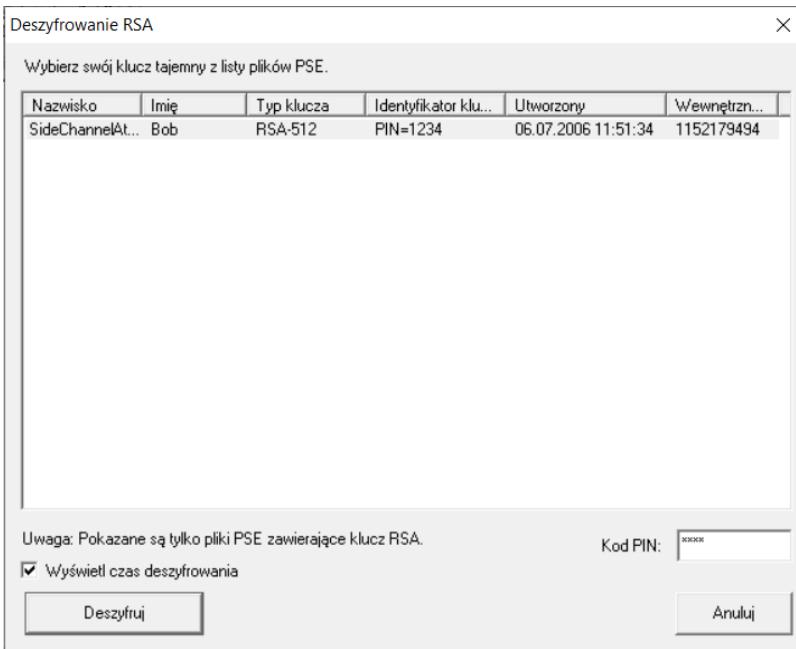
- Plik po zaszyfrowaniu wyglądał jak poniżej.



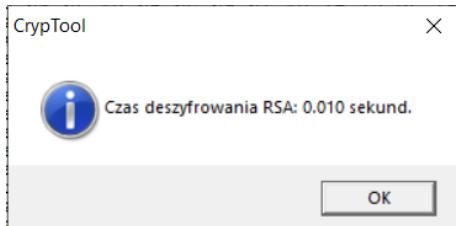
Czas szyfrowania był tak mały, że procesor przyjął go za zero.



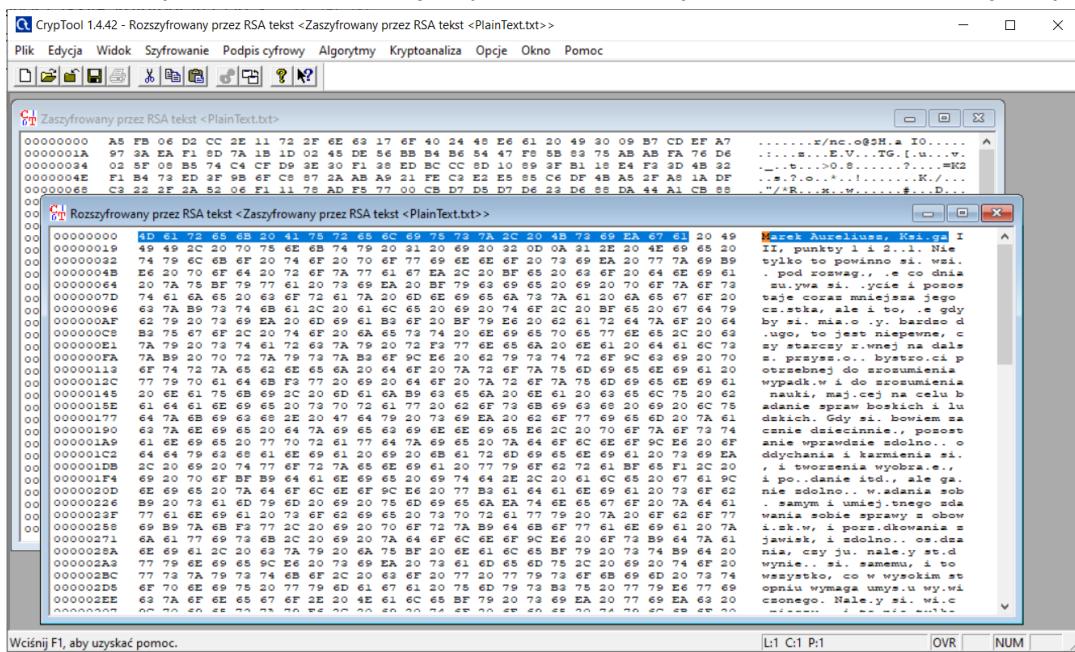
- Następnie deszyfrowałam plik używając tych samych ustawień oraz klucza prywatnego (PIN) podanego w parametrach deszyfrowania.



Tym razem czas deszyfrowania był nadal bliski zeru niemniej różny od zera.

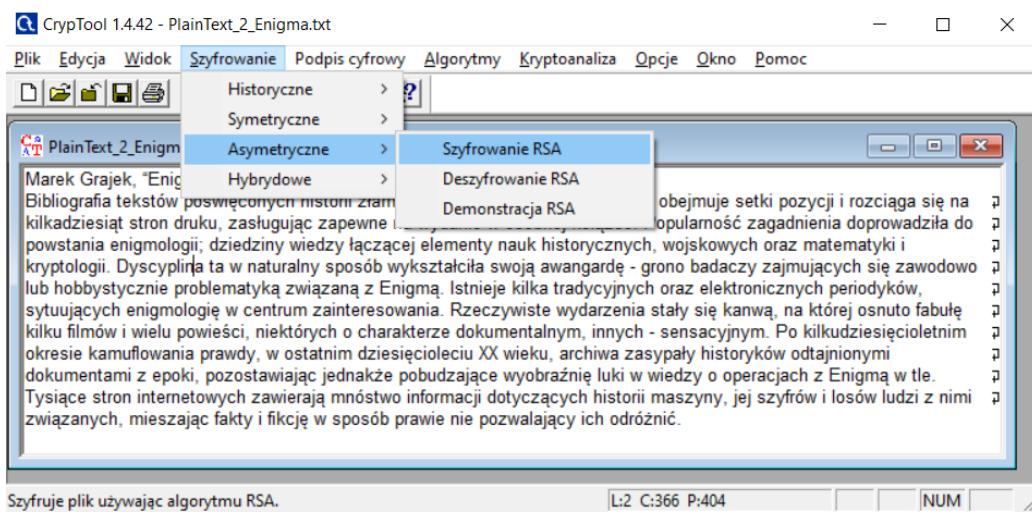


- Jak widać, deszyfrowanie przebiegło pomyślnie i plik został odtworzony w nienaruszonym stanie. W prawej części okna z deszyfrowaniem widać tekst jawnny.

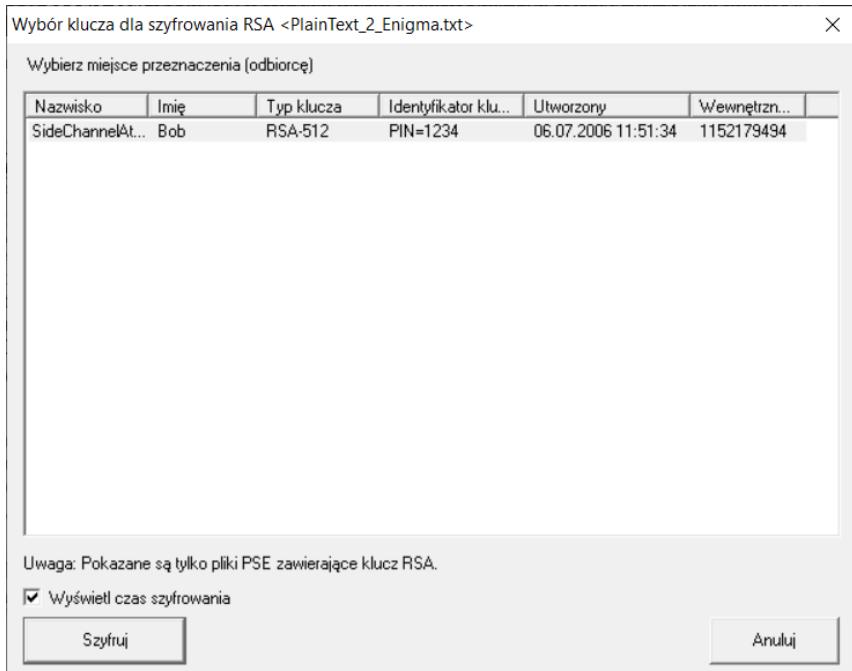


## Przebieg analizy - tekst nr 2

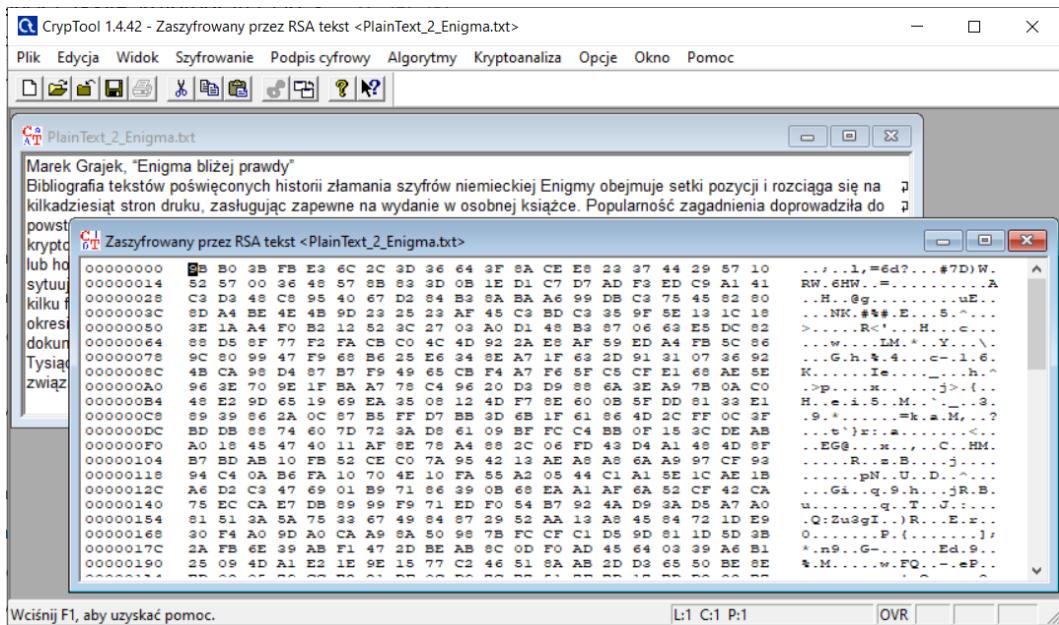
- Na przygotowanym pliku z tekstem jawnym rozpoczęłam szyfrowanie metodą RSA.



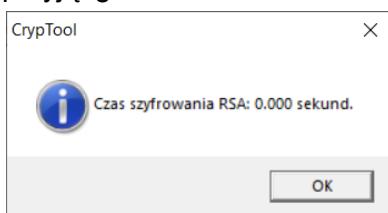
- Zastosowałam parametry jak poniżej na zrzucie ekranu z typem klucza RSA-512 i wyświetleniem czasu szyfrowania.



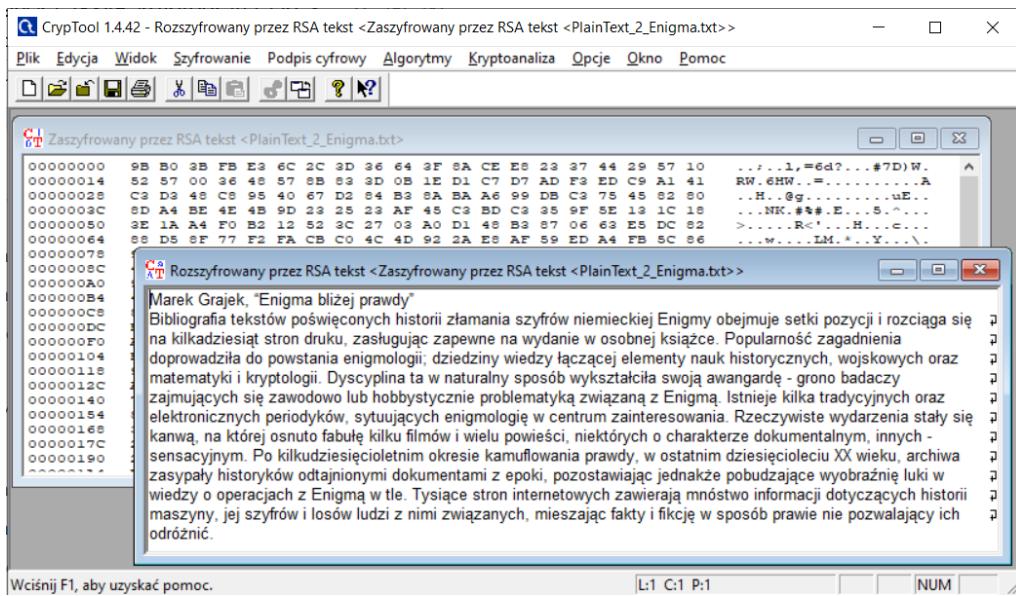
- Plik po zaszyfrowaniu wyglądał jak poniżej.



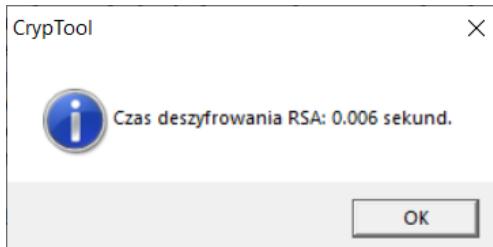
Podobnie jak przy pierwszej analizie, czas szyfrowania był tak mały, że procesor przyjął go za zero.



- Następnie deszyfrowałam plik używając tych samych ustawień oraz klucza prywatnego (PIN) podanego w parametrach deszyfrowania.



Tym razem czas deszyfrowania był nadal bliski零u niemniej różny od zero. Minimalnie krótszy też niż przy pierwszej analizie co było zapewne spowodowane długością tekstu do zaszyfrowania a zatem mniejszym plikiem.



Jak widać, deszyfrowanie przebiegło pomyślnie i plik został odtworzony w nienaruszonym stanie. W prawej części okna z deszyfrowaniem widać tekst jawnego.

## Wady i zalety metody szyfru RSA

### WADY

- Algorytm RSA jest deterministyczny (jego działanie jest całkowicie zdeterminowane przez warunki początkowe), wobec tego szyfr ten jest podatny na ataki z wybranym tekstem jawnym. Można zaszyfrować wiele wiadomości za pomocą znanego klucza publicznego, więc napastnik może odgadnąć zawartość wcześniejszych przechwyconych zaszyfrowanych wiadomości, przez porównywanie ich z wiadomościami utworzonymi przez siebie.
- Szyfrogram iloczynu dwóch tekstów jawnych jest taki sam jak iloczyn dwóch szyfrogramów, które odpowiadają tym tekstom.
- Potencjalnym zagrożeniem dla RSA jest skonstruowanie komputera kwantowego, którego moc obliczeniowa będzie w stanie w zadowalającym czasie dokonać rozkładu dużych liczb na czynniki pierwsze.
- Wadą RSA jest także jego powolne działanie w porównaniu do AES, winowającą czego są duże liczby proste.

### ZALETY

- Główną zaletą natomiast algorytmu RSA jest jego „bezpieczeństwo”, wykorzystywanie klucza od długości 4k bitów prawie eliminuje możliwość ingerencji w treść przesyłanych informacji.

- RSA jest trudny do złamania, gdyż rozłożenie liczby n na jej czynniki (wartości p i q) jest bardzo trudne (jest to prawda tylko dla dużych pierwszych. To, że muszą być one duże i jednocześnie pierwsze, sprawia pewną trudność, gdyż nie ma algorytmów uzyskiwania takich liczb).
- Możliwość tworzenia podpisów elektronicznych z użyciem tych samych kluczy, które służą do szyfrowania. Do uzyskania podpisu używany jest klucz prywatny, a każda osoba dysponująca kluczem publicznym może stwierdzić, czy rzeczywiście autorem wiadomości jest właściciel klucza prywatnego.

## 9. RSA z AES

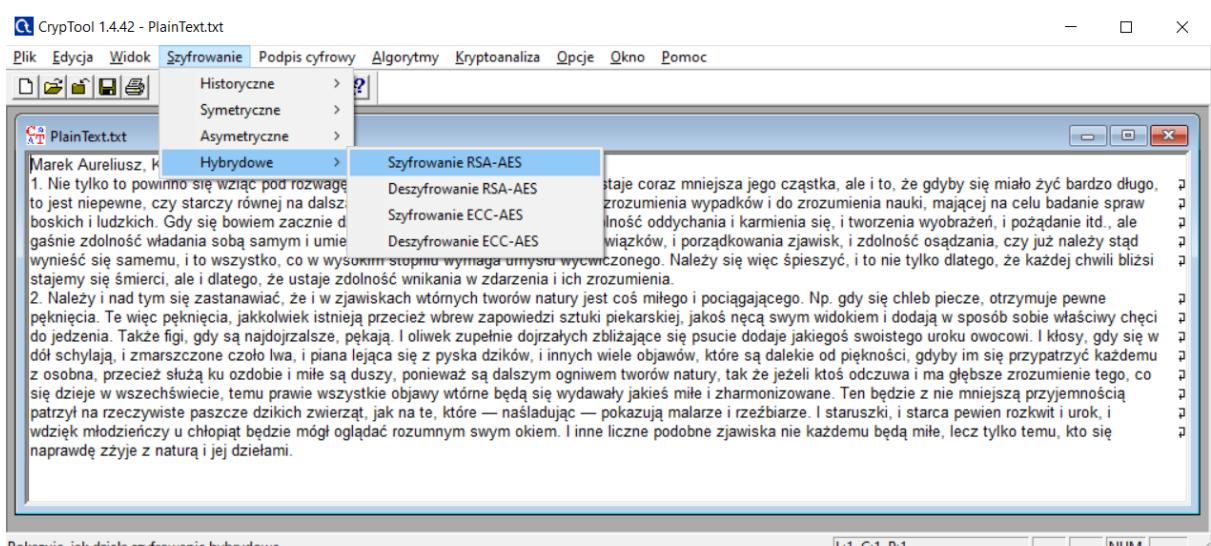
Zastanawiano się czy da się uzyskać stopień zabezpieczenia przesyłanej informacji taki jak daje nam algorytm RSA oraz szybkość szyfrowania/odszyfrowania tejże informacji tak jak przy AES. Okazało się, że tak. Powstał algorytm będący hybrydą obu wspomnianych, tzw. hybrid encryption. Algorytm ten polega na kombinacji silnych stron obu algorytmów, w celu połączenia ich zalet oraz prawie całkowitej eliminacji wad. Możemy to osiągnąć przesyłając klucz AES służący do szyfrowania i odszyfrowania informacji obok tejże informacji.

Wykorzystywanie AES dla szyfrowania i odszyfrowania informacji ma największą zaletę, której w tym momencie potrzebujemy – szybkość działania. Pomimo, że wadą AES jest ogólny poziom bezpieczeństwa w porównaniu do RSA, to jednak eliminujemy ją w kolejnym kroku: klucz AES przesyłany obok zaszyfrowanej informacji szyfrujemy parą kluczy RSA znanej tylko stronom wymieniającym się informacją. Wynikiem tej operacji będzie przesłanie w bezpieczny sposób klucza AES który później służy do odszyfrowania wiadomości.

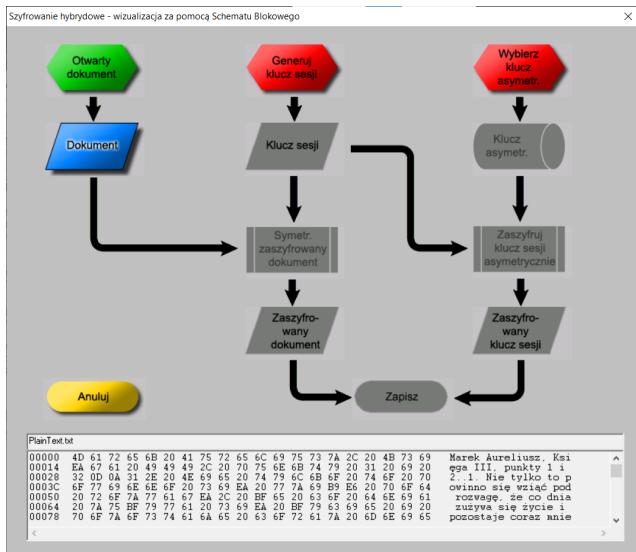
Dorzucając do klucza AES jakiś losowy challenge całkowicie eliminuje ataki typu bruteforce, nawet jeśli atakującemu udaje się zorganizować atak typu man-in-the-middle – możliwość powtórzenia się challenge o odpowiedniej długości jest znikoma.

### Przebieg analizy - tekst nr 1

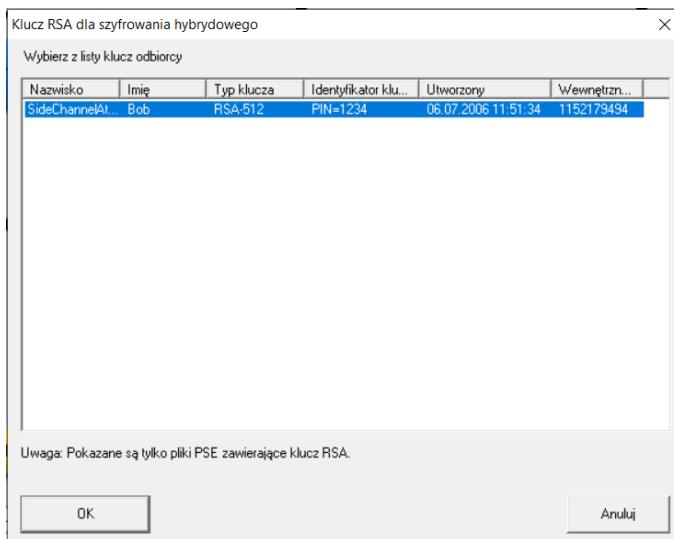
- Na przygotowanym pliku z tekstem jawnym rozpoczęłam szyfrowanie metodą RSA z AES.



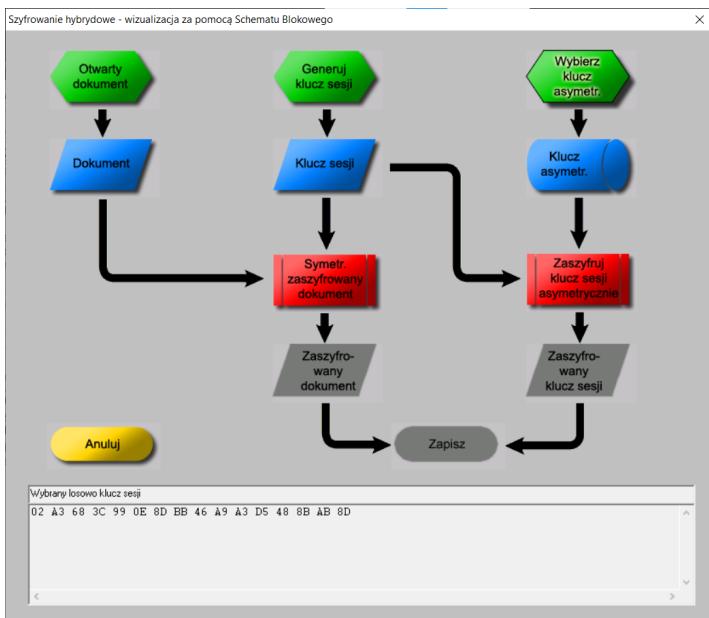
- Do zaszyfrowania otworzyłam okno jak poniżej.



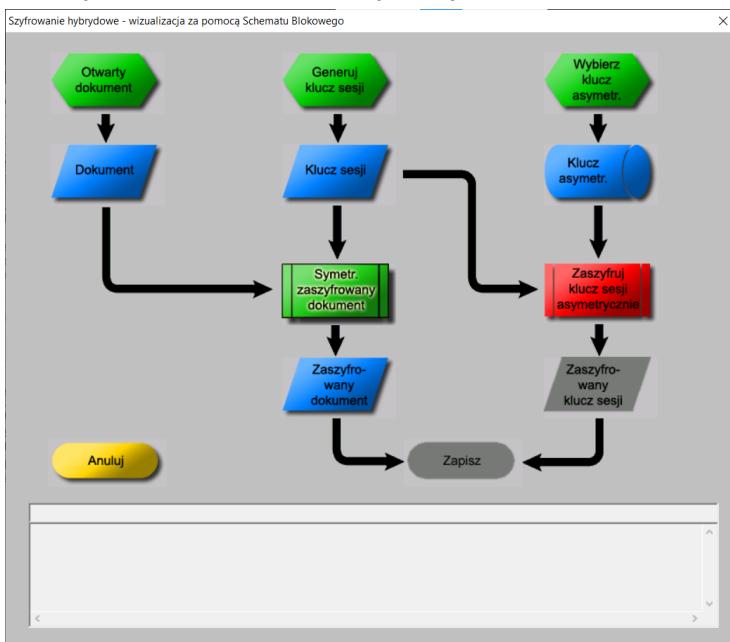
- Wygenerowałem następujące wymagane wstępne dane:
  - wybierałem klucz asymetryczny



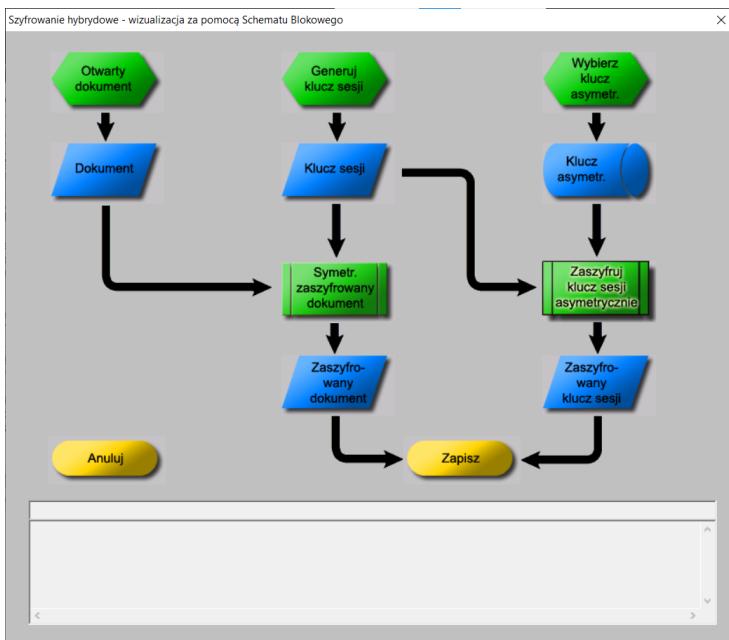
- losowy klucz sesji: 02 A3 68 3C 99 0E 8D BB 46 A9 A3 D5 48 8B AB 8D



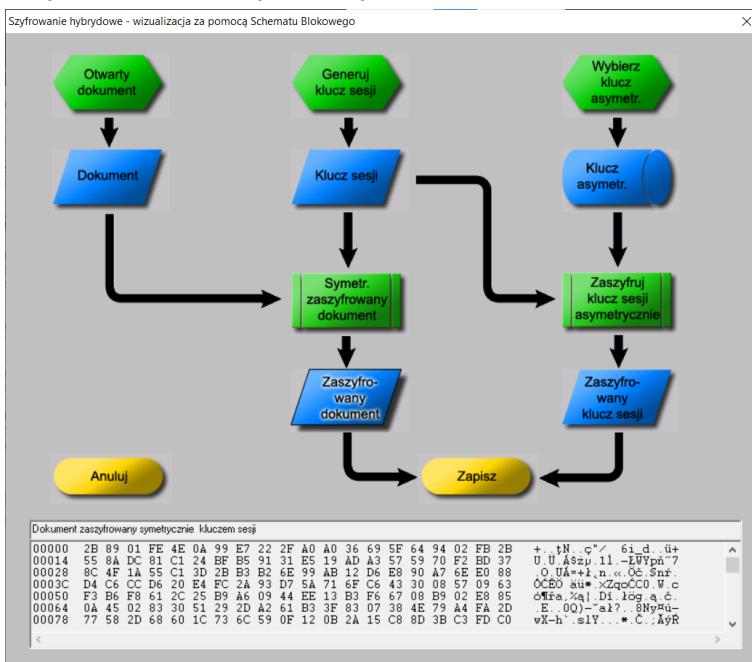
- Zaszyfrowałem dokument symetrycznie



- Zaszyfrowałem klucz sesji asymetrycznie

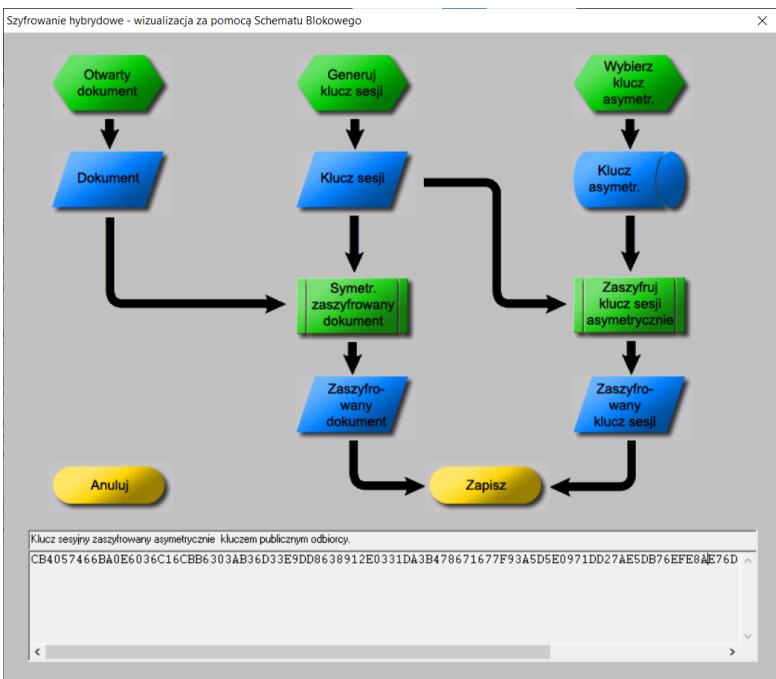


- Wyświetlilam zaszyfrowany dokument



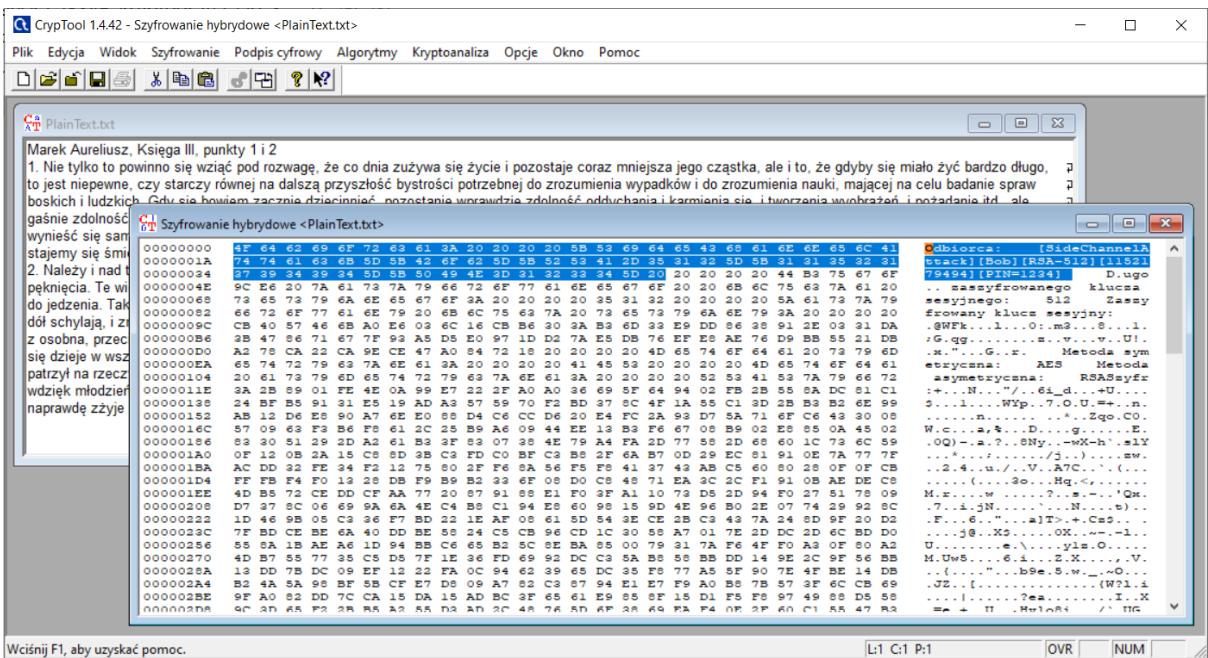
- Wyświetlilam klucz sesyjny zaszyfrowany asymetrycznie kluczem publicznym odbiorcy:

CB4057466BA0E6036C16CBB6303AB36D33E9DD8638912E0331DA3B478671677  
F93A5D5E0971DD27AE5DB76EFE8AE76D9BB5521DBA278CA22CA9ECE47A084  
7218



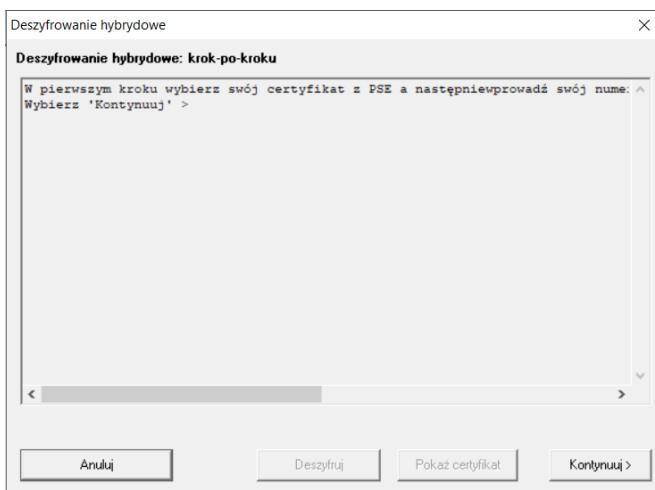
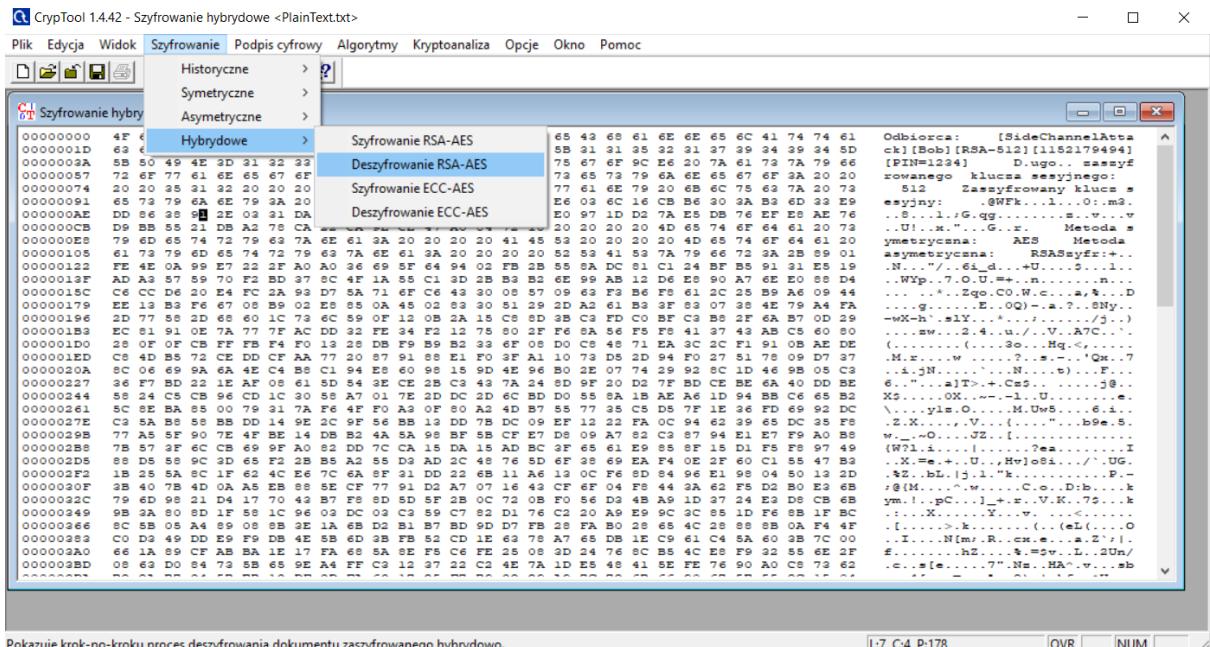
- Zapisałam wszystkie wygenerowane informacje.

- Plik po zaszyfrowaniu wyglądał jak poniżej.

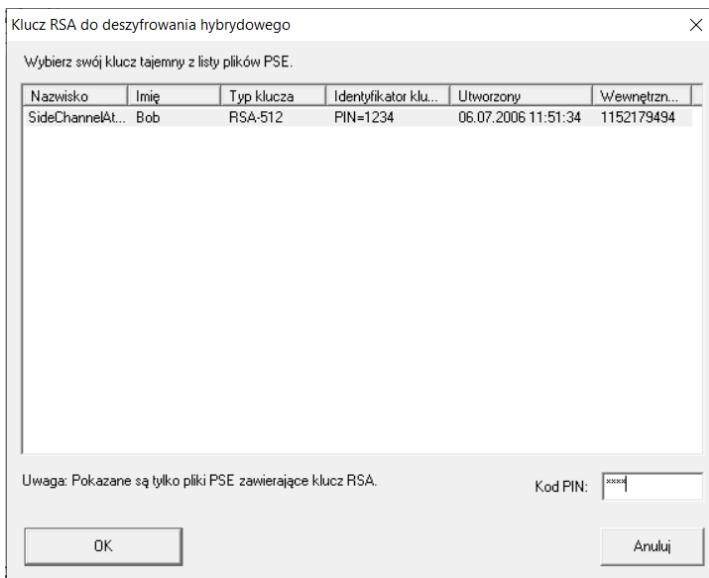


Widać w treści wprowadzone ustawienia klucza RSA (m.in. odbiorca) oraz informację o obu użytych do szyfrowania hybrydowego metodach.

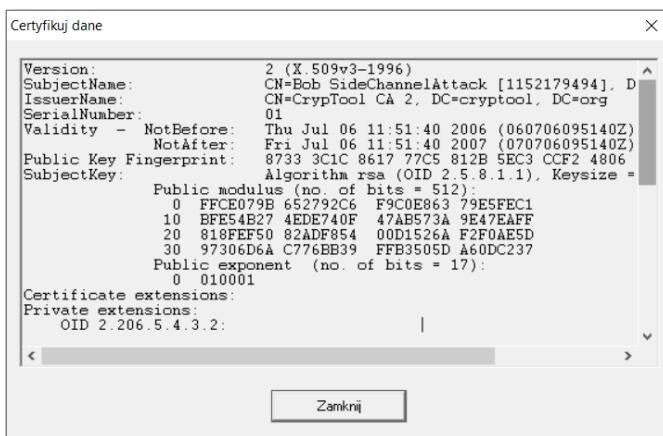
- Następnie przystąpiłem do deszyfrowania szyfrogramu.



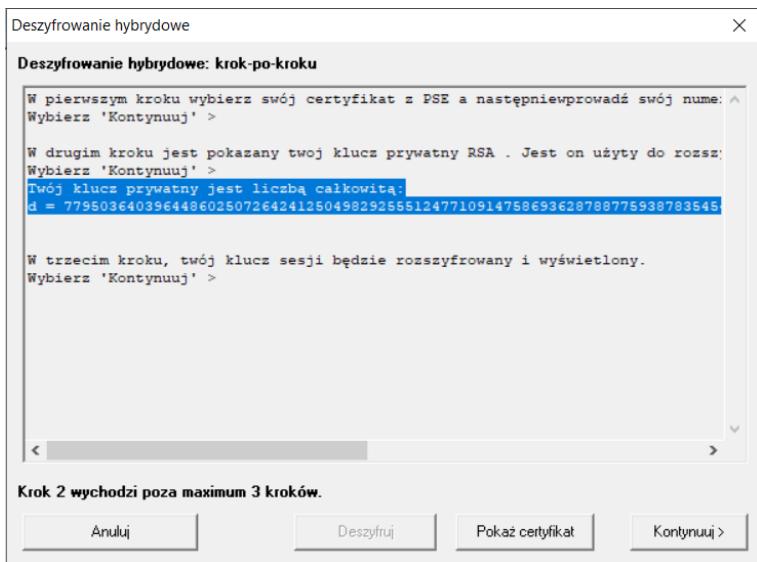
- W pierwszym kroku wybrałem swój certyfikat z PSE oraz wprowadziłem swój numer PIN (1234).



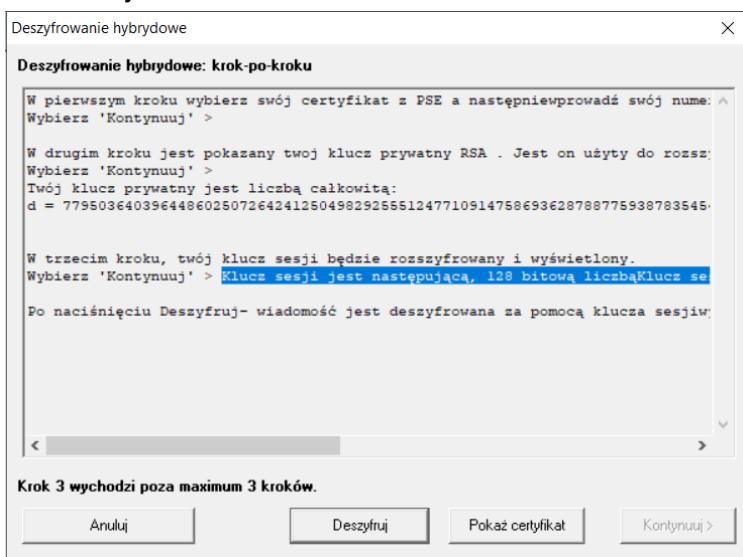
- Dzięki temu miałam możliwość przeczytania mojego klucza prywatnego RSA z pliku PSE.



- W drugim kroku pokazano mi mój klucz prywatny RSA. Został on użyty do rozszyfrowania klucza sesyjnego.  
Twój klucz prywatny jest liczbą całkowitą:  
 $d =$   
7795036403964486025072642412504982925551247710914758693628788775938  
7835454193820408779009965640493205588280774002827039042768160696523  
49394563092391797657



- W trzecim kroku mój klucz sesji został rozszyfrowany i wyświetlony.  
Klucz sesji jest następującą, 128 bitową liczbą.  
Klucz sesji: 02 A3 68 3C 99 0E 8D BB 46 A9 A3 D5 48 8B AB 8D



- W ostatnim kroku deszyfrowałem wiadomość za pomocą klucza sesji. W wyniku tego została wyświetlona rozszyfrowana wiadomość w oknie głównym.

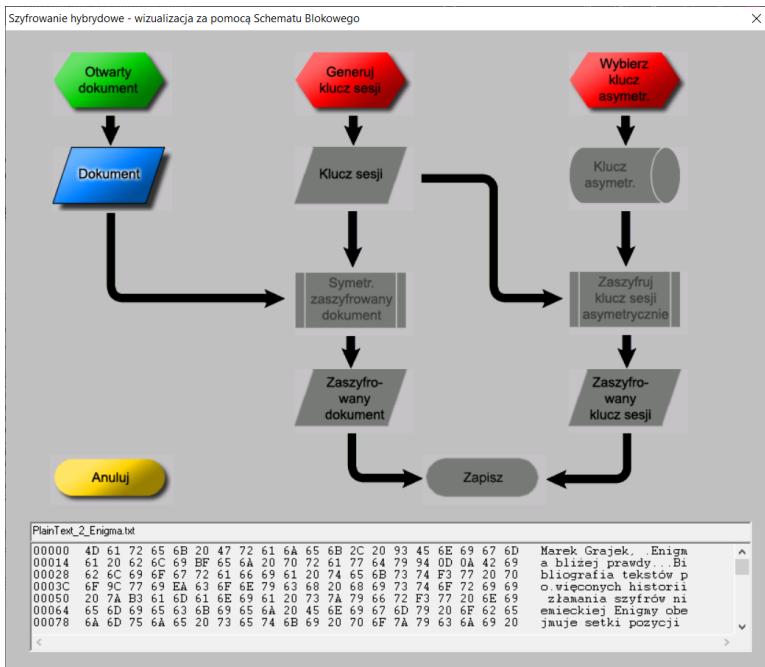
Jak widać, deszyfrowanie przebiegło pomyślnie i plik został odtworzony w nienaruszonym stanie. W prawej części okna z deszyfrowaniem widać tekst jawnny.

## Przebieg analizy - tekst nr 2

- Na przygotowanym pliku z tekstem jawnym rozpoczęłam szyfrowanie metodą RSA z AES.

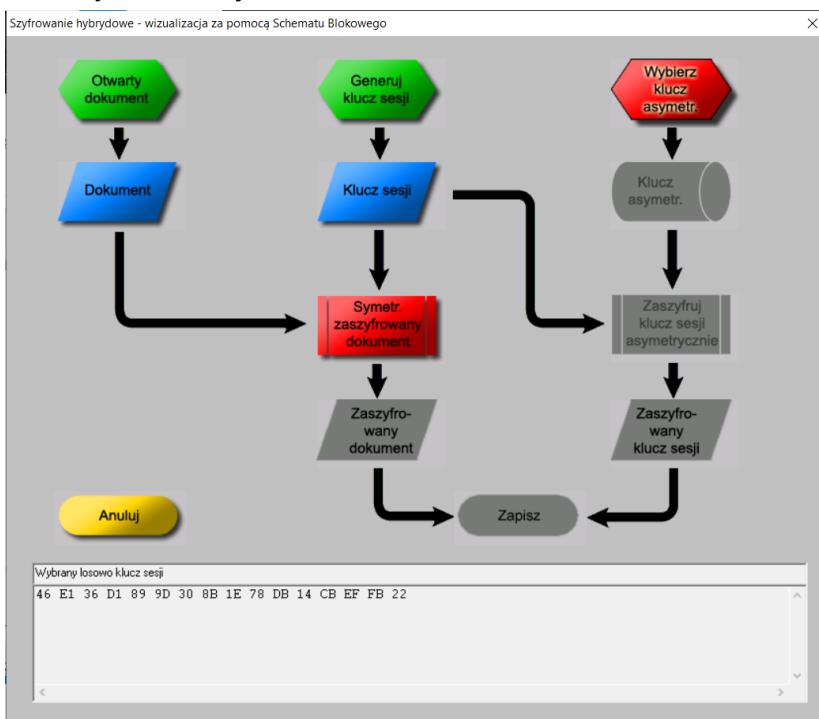
The screenshot shows the CrypTool 1.4.42 application window. The menu bar at the top includes 'Plik', 'Edycja', 'Widok', 'Szyfrowanie' (selected), 'Podpis cyfrowy', 'Algorytmy', 'Kryptoanaliza', 'Opcje', 'Okno', and 'Pomoc'. The 'Szyfrowanie' menu is open, displaying sub-options: 'Historyczne', 'Symetryczne', 'Asymetryczne', 'Hybridowe' (selected), and 'Szyfrowanie RSA-AES'. A detailed description of hybrid encryption is visible in the main pane, mentioning RSA-AES and ECC-AES algorithms. The status bar at the bottom indicates 'Pokazuje, jak działa szyfrowanie hybrydowe.' and shows keyboard input fields.

- Do zaszyfrowania otworzyło mi się okno jak poniżej.

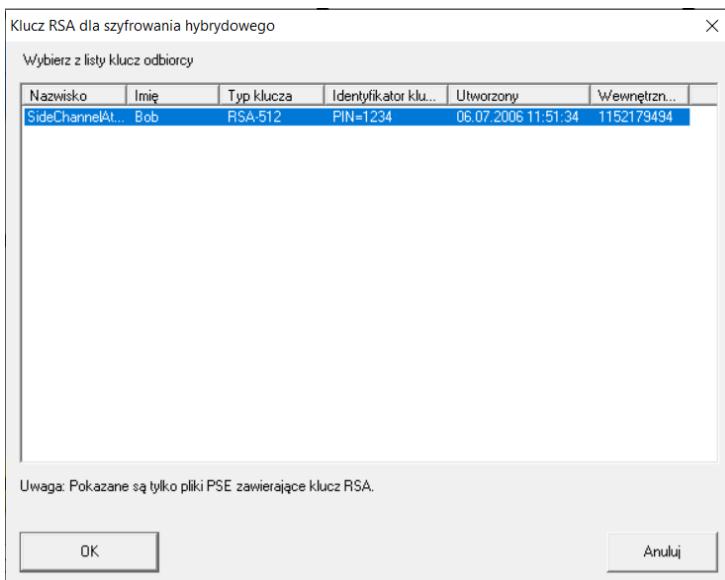


- Wygenerowałem następujące wymagane wstępne dane:

- losowy klucz sesji: 46 E1 36 D1 89 9D 30 8B 1E 78 DB 14 CB EF FB 22



- klucz asymetryczny



Klucz publiczny dla: Bob SideChannelAttack

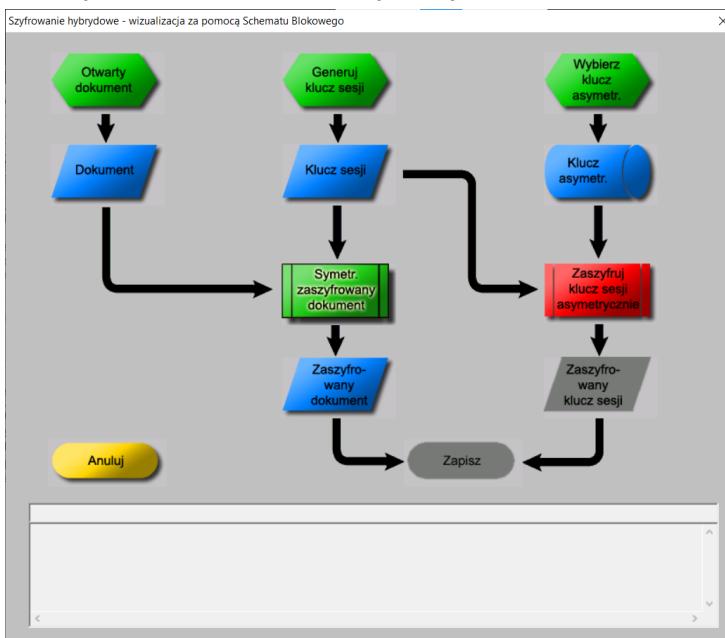
Modulus: 133975846635708615201590770183928841622787789785271967822598  
392386431002915255007207383566873210619482065892816993509135  
68653993056674407415318295312450103

Wykładnik: 65537

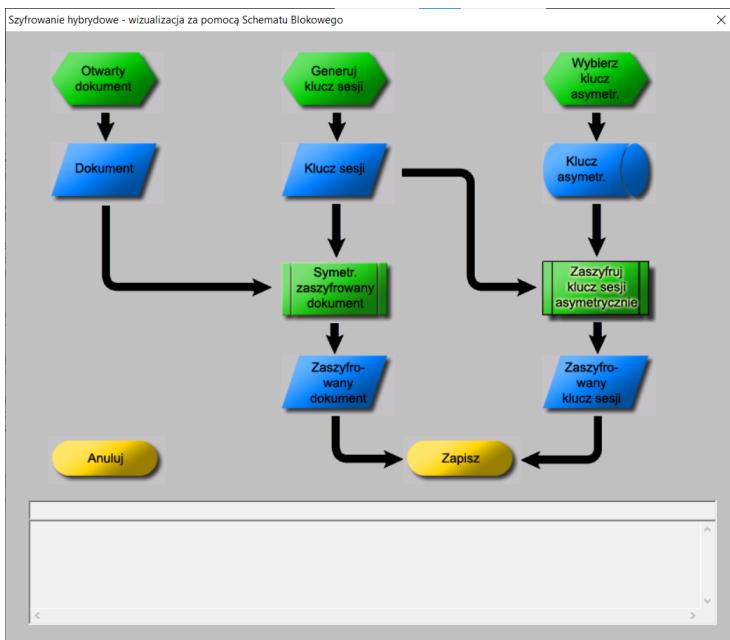
System liczbowy

Oct     Dec     Hex

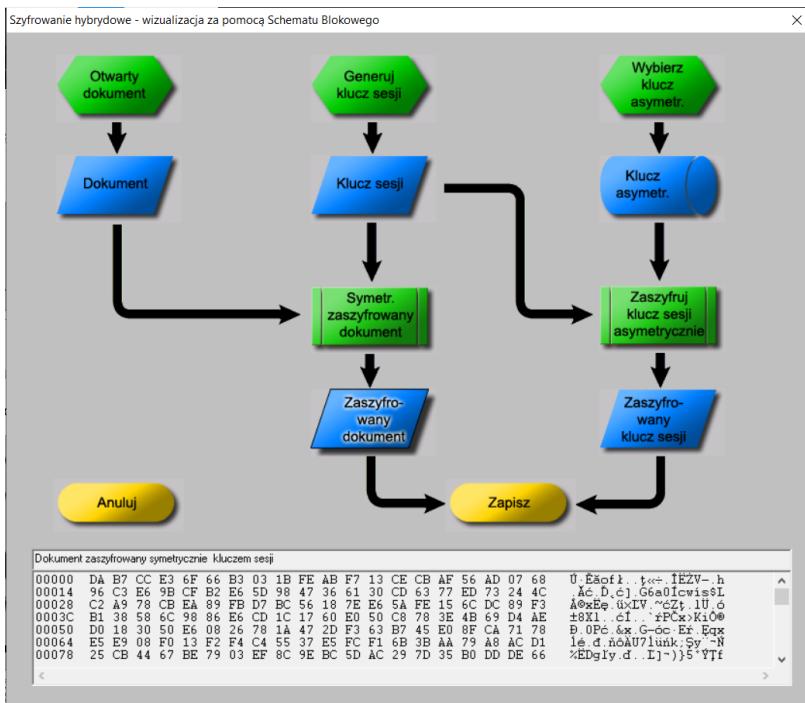
### - Zaszyfrowałem dokument symetrycznie



### - Zaszyfrowałem klucz sesji asymetrycznie

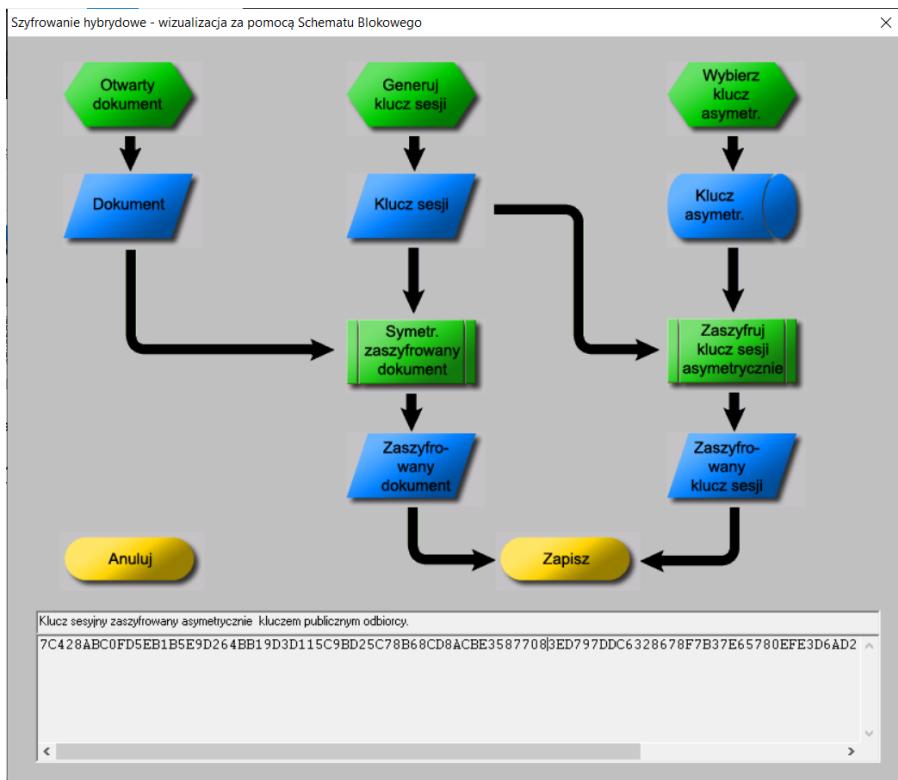


- Wyświetliłam zaszyfrowany dokument



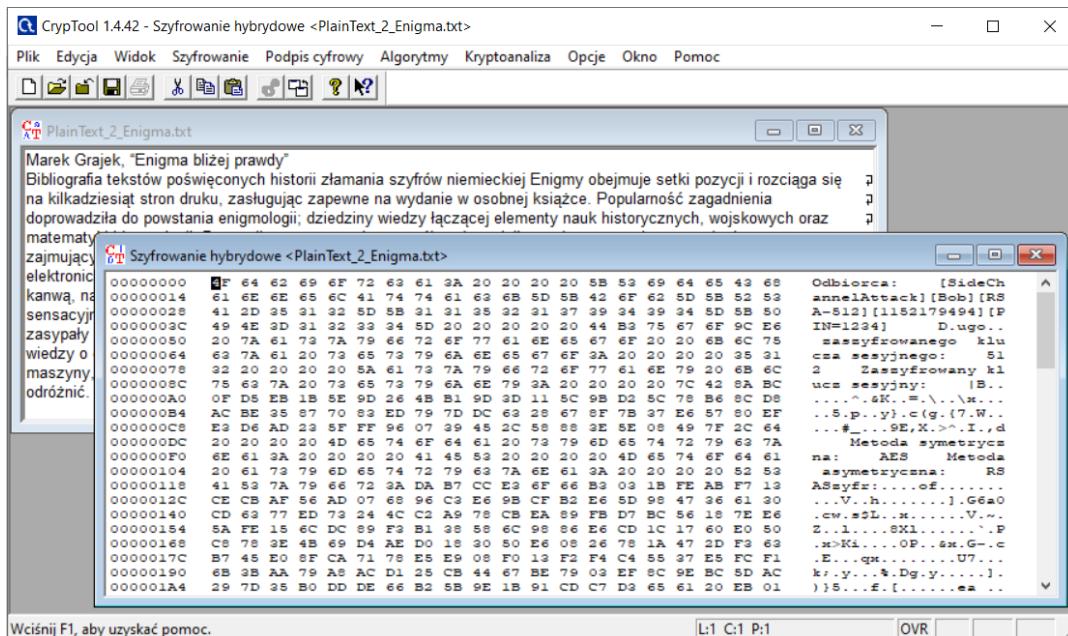
- Wyświetliłam klucz sesyjny zaszyfrowany asymetrycznie kluczem publicznym odbiorcy:

7C428ABC0FD5EB1B5E9D264BB19D3D115C9BD25C78B68CD8ACBE35877083ED797DDC6328678F7B37E65780EFE3D6AD235FFF960739452C58883E5E08497F2C64



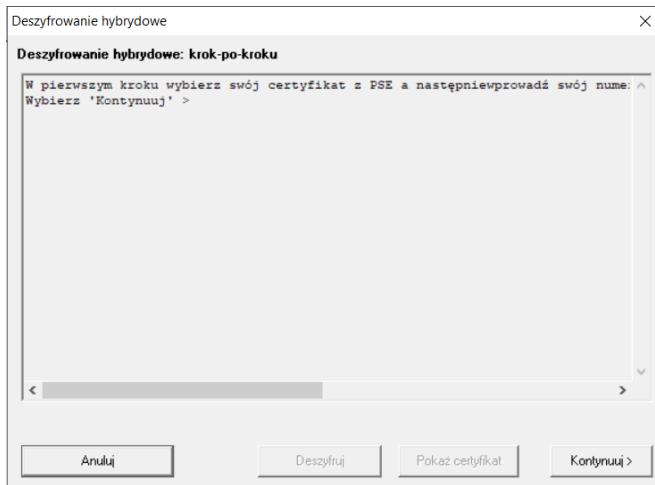
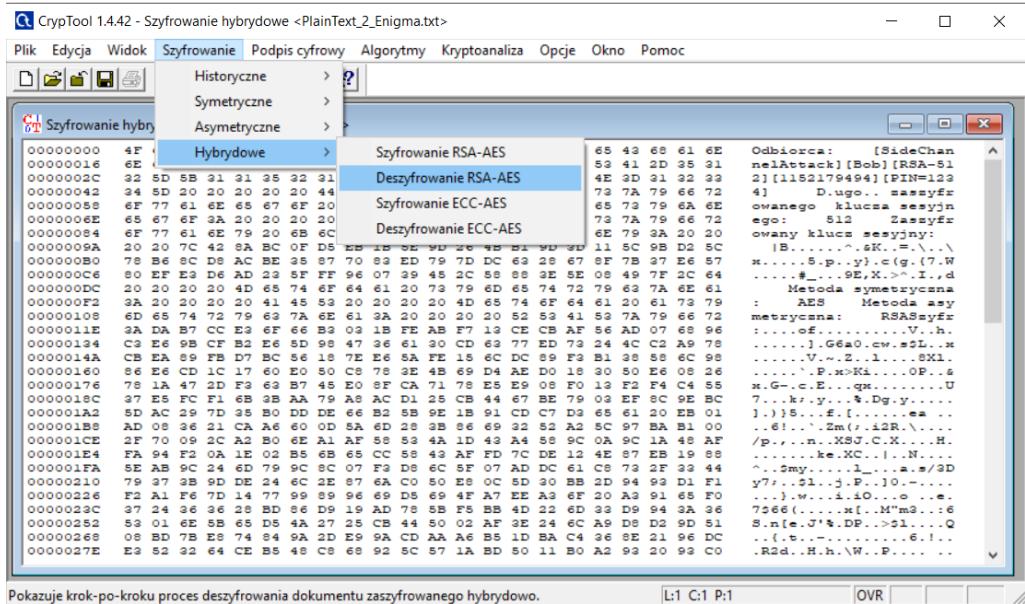
- Zapisałam wszystkie wygenerowane informacje.

- Plik po zaszyfrowaniu wyglądał jak poniżej.

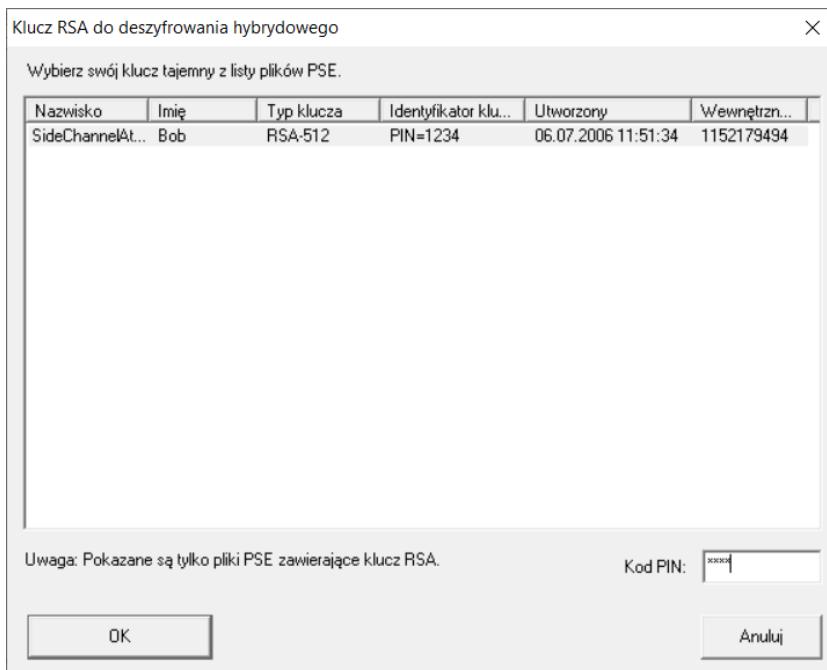


Widac w treści wprowadzone ustawienia klucza RSA (m.in. odbiorca) oraz informację o obu użytych do szyfrowania hybrydowego metodach.

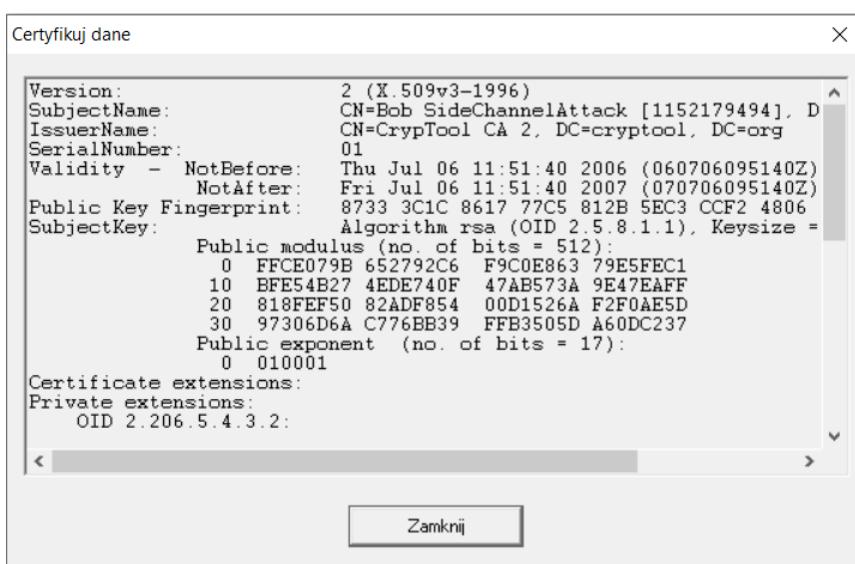
- Następnie przystąpiłem do deszyfrowania szyfrogramu.



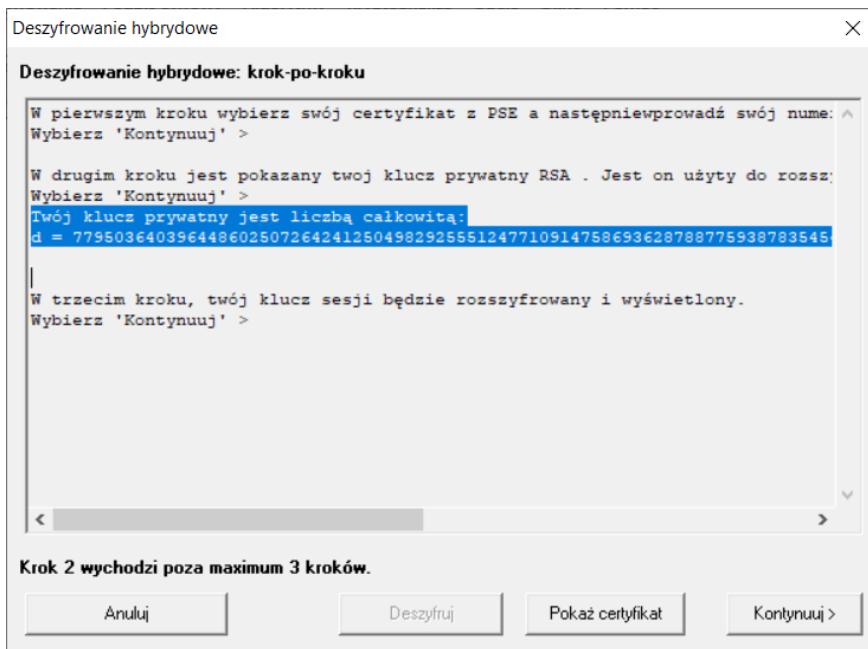
- W pierwszym kroku wybrałem swój certyfikat z PSE oraz wprowadziłem swój numer PIN (1234).



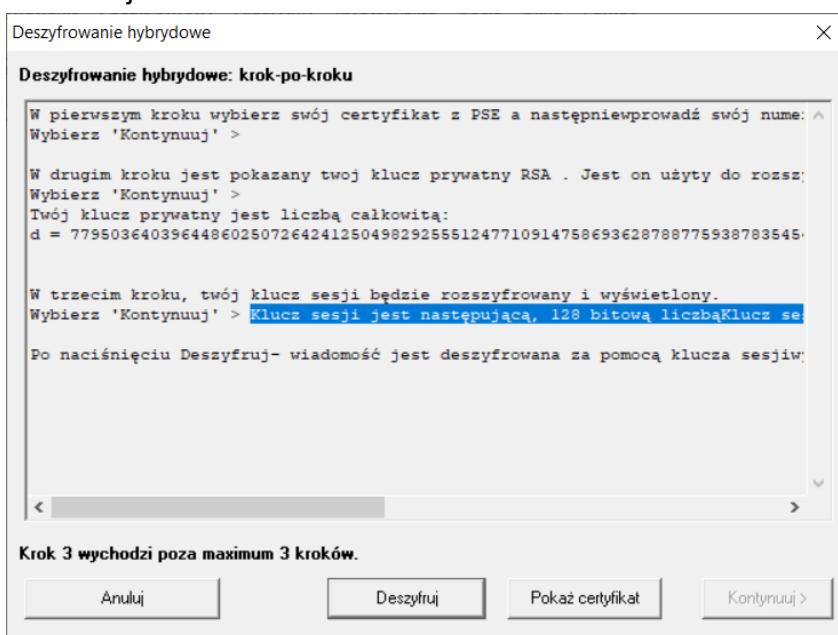
- Dzięki temu miałam możliwość przeczytania mojego klucza prywatnego RSA z pliku PSE.



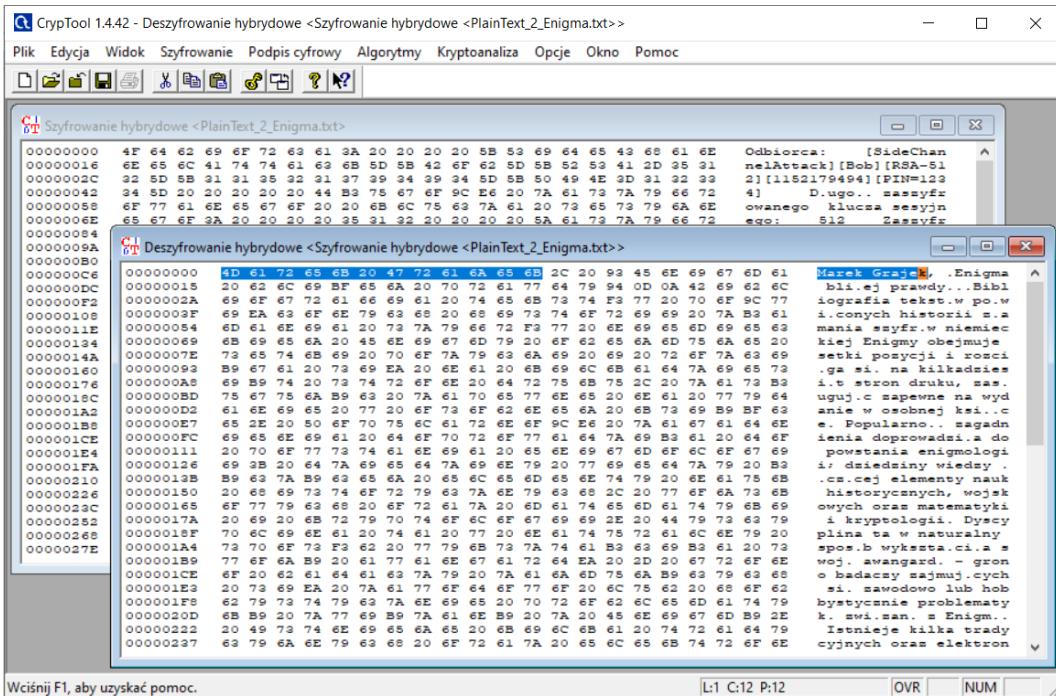
- W drugim kroku pokazano mi mój klucz prywatny RSA. Został on użyty do rozszyfrowania klucza sesyjnego. Co ciekawe, jest on identyczny jak przy pierwszej analizie zupełnie innego tekstu.  
Twój klucz prywatny jest liczbą całkowitą:  
 $d =$   
779503640396448602507264241250498292551247710914758693628788775938  
7835454193820408779009965640493205588280774002827039042768160696523  
49394563092391797657



- W trzecim kroku mój klucz sesji został rozszyfrowany i wyświetlony.  
Klucz sesji jest następującą, 128 bitową liczbą.  
Klucz sesji: 46 E1 36 D1 89 9D 30 8B 1E 78 DB 14 CB EF FB 22



- W ostatnim kroku deszyfrowałem wiadomość za pomocą klucza sesji. W wyniku tego została wyświetlona rozszyfrowana wiadomość w oknie głównym.



Jak widać, deszyfrowanie przebiegło pomyślnie i plik został odtworzony w nienaruszonym stanie. W prawej części okna z deszyfrowaniem widać tekst jawnny.

## Wady i zalety metody szyfru RSA z AES

### WADY

- Algorytm ten polega na kombinacji silnych stron obu algorytmów, w celu połączenia ich zalet oraz prawie całkowitej eliminacji wad przez co ciężko w tym momencie wskazać jakąkolwiek wadę tej metody.

### ZALETY

- Wysoki stopień zabezpieczenia przesyłanej informacji z jednocześnie dużą szybkością szyfrowania/odszyfrowania tejże informacji.

# Wnioski

Istnieje wiele metod szyfrowania, na tym laboratorium przeanalizowałam działanie najpopularniejszych z nich. Zaliczały się one do jednej z dwóch głównych rodzajów metod szyfrowania: symetrycznego i asymetrycznego.

**Historyczne szyfry**, takie jak Cezara lub zamiany, musiały umożliwiać szyfrowanie i deszyfrowanie przez człowieka, a więc opierać się na relatywnie prostych operacjach. Tak jak każda technika podmieniająca pojedyncze litery alfabetu na inne, nie oferują one żadnego bezpieczeństwa komunikacji. Informacje można deszyfrować nawet bez użycia komputera. Jest to największa wada tych metod.

**Metody symetryczne** (AES) wydają się szybsze od asymetrycznych, niemniej ich podstawową wadą jest klucz - jak go bezpiecznie przesyłać innej stronie wymiany. Klucz jest jeden - zarówno do szyfrowania jak i deszyfrowania informacji.

**Symetryczny szyfr strumieniowy** (XOR) ma liczne wady i jest względnie łatwy do złamania. Jego zabezpieczenia nie są lepsze niż klasycznych szyfrów wieloalfabetowych. Przy użyciu komputera, odkrycie tekstu jawnego zajmuje stosunkowo niewiele czasu. Podobnie jak w szyfrach historycznych, jego siła tkwi w prostocie działania.

Stosowanie **symetrycznych szyfrów blokowych**, które przeanalizowałam, a więc DES z ECB i DES z CBC, wiąże się z bezpieczeństwem użycia tych samych bitów sekretnego klucza do zaszyfrowania takich samych fragmentów tekstu jawnego.

Wykorzystanie jednego deterministycznego algorytmu szyfrującego do zakodowania pewnej ilości identycznych danych wejściowych, daje w wyniku powtarzające się dane wyjściowe. Stwarza to niebezpieczeństwo dla użytkowników szyfrów blokowych.

Ewentualny napastnik mógłby wyciągnąć dużo informacji znając rozkład powtarzających się takich samych fragmentów wiadomości, nawet jeśli nie zdołaby całkowicie złamać szyfru i poznać całego tekstu jawnego.

Przy **metodach asymetrycznych** (RSA) zauważałam delikatnie dłuższy proces odszyfrowywania szyfrogramu co potwierdza ich założenia. Wykorzystują one parę kluczy szyfrujących, jeden (publiczny) do szyfrowania a drugi (prywatny) do odszyfrowania. Działają przez to zwykle dużo wolniej niż szyfry symetryczne ale zapewniają większe bezpieczeństwo.

Najbezpieczniejszym sposobem szyfrowania wydaje się **hybryda RSA z AES**. Ta kombinacji silnych stron obu algorytmów, w celu połączenia ich zalet oraz prawie całkowitej eliminacji wad daje nam metodę niemal doskonałą.

Podsumowując, dzisiejsze wymagania bezpieczeństwa ograniczają nas do stosowania najpotężniejszych z poruszanych metod szyfrowania. Symetryczne algorytmy szyfrowania są znacznie szybsze i wymagają mniejszej mocy obliczeniowej, ale ich główną słabością jest właściwa i bezpieczna dystrybucja klucza. Walorami asymetrycznych algorytmów szyfrowania jest ich wyższy poziom bezpieczeństwa i wygoda używania. Nie wymagają też przekazywania tajnych kluczy.