Politechnika Wrocławska

Sprawozdanie z zajęć laboratoryjnych
Cyberbezpieczeństwo

Lab 04
Asymetryczne algorytmy szyfrowania

Tomasz Mroczko, 266604

October 29, 2023

1 Dane testowe

Użyty tekst

Do eksperymentów użyto 3 tekstów o różnych poziomach entropii:

1) **Tekst jednorodny:** Jako tekst jednorodny użyto litery 'a' powtórzonej 2000 razy.
2) **Tekst częściowo zróżnicowany:** Ciąg słów "this test is very repetetive" powtórzony 100 razy.
3) **Tekst zróżnicowany:** Fragment początku książki "1984", autorstwa George'a Orwella, w języku angielskim. Fragment został ograniczony do długości około 1700 znaków.

2 Zadania

Zadanie 1.3

Dla trzech długości klucza (512,1024,2048) oraz dla trzech ustalonych tekstów jawnych (TJ) o różnych entropiach (np. tekst jednorodny, tekst średnio zróżnicowany, tekst bardzo zróżnicowany) należy porównać entropię TJ z entropią po zaszyfrowaniu (entropią tekstu tajnego TT). Proszę przyjrzeć się również autokorelacji TT i TJ.

Przeprowadzono analizę dla *dwóch* długości klucza - 512 i 2048.

Szyfrowanie	Jednorodny	Średnio zróżnicowany	Zróżnicowany
Brak	0.00	3.00	4.21
RSA 512	5.90	7.24	7.90
RSA 2048	7.45	7.94	7.90

Table 1: Poziom entropi teksów po zaszyfrowaniu

- **Entropia** Długość klucza ma pewien wpływ na poziom entropii dla tekstu jednorodnego oraz średnio zróżnicowanego. Im dłuższy klucz tym wyższy poziom entropii. Jendak dla tekstu zróżnicowanego, poziom entropii był bardzo wysoki niezależnie od klucza.
- **Autokorelacja**
  - **Jednorodny**

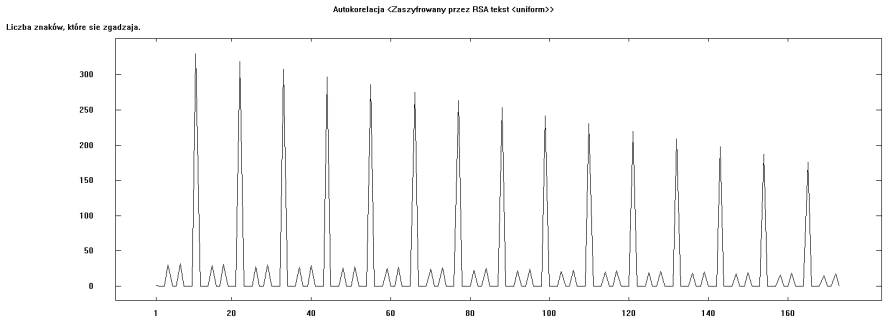

Figure 1: Autokorelacja RSA 512 dla tekstu jednorodnego

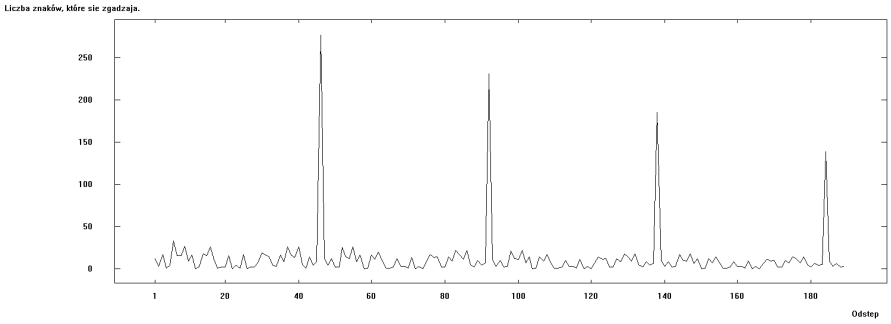

Figure 2: Autokorelacja RSA 2048 dla tekstu jednorodnego

Przy tekście jednorodnym, autokorolecja dla długości kluczy wykazuje pewien schemat. Przy kluczu o długości 512, przy przesunięciu o wielokrotność około 11 znaków, liczba zgadzających się znaków jest *bardzo* wysoka. Przy każdej kolejnej wielokrotności liczba ta jest mniejsza, jednak dalej widoczna jest bardzo duża górka na wykresie. Dla klucza 2048, tendencja jest bardzo podobna, jednak okres cyklu jest 4 krotnie dłuższy.
Przy każdym okresie liczba powtarzającyh się znaków jest coraz mniejsza, ponieważ wychodzimy poza długość tekstu. Gdyby jednorodny tekst był nieskończony, każdy 'spike' byłby tej samej wysokości.

– **Średnio zróżnicowany**

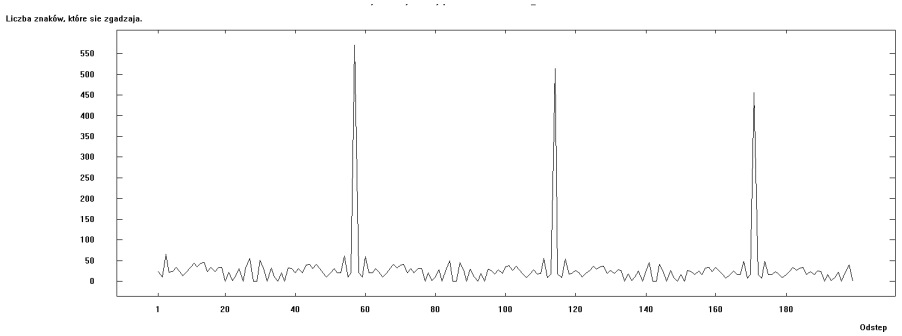

Figure 3: Autokorelacja RSA 512 dla tekstu średnio zróżnicowanego

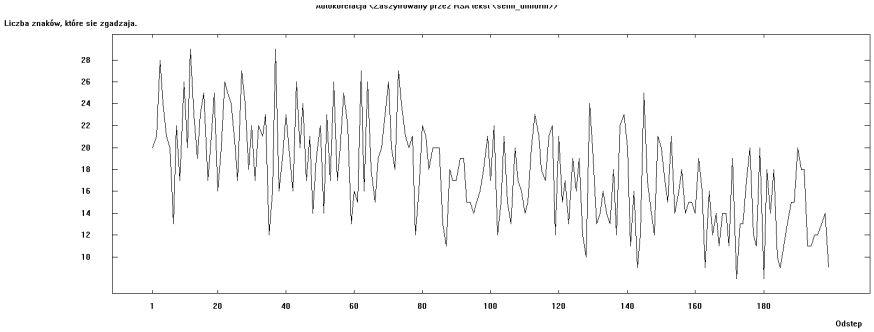

Figure 4: Autokorelacja RSA 2048 dla tekstu średnio zróżnicowanego

Dla tekstu średnio zróżnicowanego, przy kluczu długości 512bit tendencja autokorelacji jest bardzo podobna do tendencji z tekstu jednorodnego. Tym razem jednak, okres przesunięcia jest większy (około 60 znaków). Dla klucza 2048, ta tendencja znika, a autokorelacja nie wykazuje oczywistych schematów.

– **Zróżnicowany**

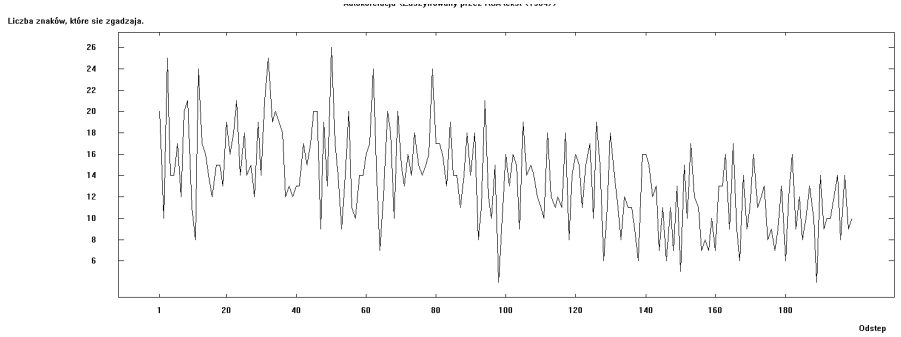

Figure 5: Autokorelacja RSA 512 dla tekstu zróżnicowanego

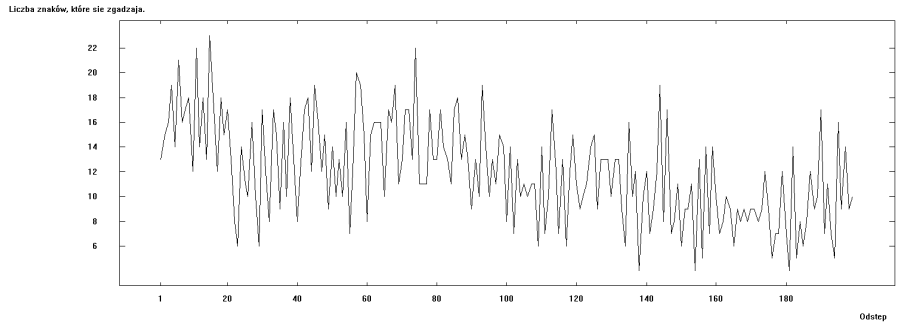

Figure 6: Autokorelacja RSA 2048 dla tekstu zróżnicowanego

Dla tekstu zróżnicowanego nie występują ewidentne powtórzenia znaków przy konkrentych przesunięciach, a wykres autokorelacji nie wykazuje schematów.

- **Zadanie 1.4**

  .Dla różnych długości klucza algorytmu RSA zmierzyć czas szyfrowania i deszyfrowania plików o rozmiarze 1MB, 2MB, 5MB (dokładność do około sekudny).

W celu wygenerowania plików powtórzono użyty wcześniej tekst zróżnicowany, i powtórzono go.

Szyfrowanie	1MB	2MB	5MB
RSA 512	0.398s	0.785s	1.891s
RSA 2048	1.115	2.142	5.535s

Table 2: Czas szyfrowania plików za pomocą RSA

Deszyfrowanie	1MB	2MB	5MB
RSA 512	5.201s	10.274s	24.804
RSA 2048	40.192s	81.120s	199.031s

Table 3: Czas deszyfrowania plików za pomocą RSA

Zadanie 1.5

Pliki z punktu 4. zaszyfrować i odszyfrować algorytmem symetrycznym próbując zaobserwować czas realizacji tych operacji.

Do przeprowadzenia eksperymentów wybrano algorytm AES, w wersji 256bit, w trybie działania CBC. Zarówno szyfrowanie jak deszyfrowanie okazały się niemal natychmiastowe (ewidentnie poniżej sekundy). Potwierdza to domysły że algorytmy symetryczne są znacznie szybsze niż asymetryczne. Po części może to wynikać ze znacznie mniejszej długości klucza używanego do szyfrowania, nawet w przypadku używania AES 256.

Zadanie 1.6

.Do kryptogramów utworzonych przy użyciu kluczy o różnej długości wprowadzić następujące zmiany: • zmienić wartość 1 bajtu,
• usunąć 1 bajt,
• usunąć kilka (kilkadziesiąt) bajtów,
• usunąć fragment równy długości modułu algorytmu (512,1024,...).
Następnie należy odszyfrować kryptogram i zaobserwować powstałe zmiany w tekście jawnym.

- **Zmiana jednego bajtu**

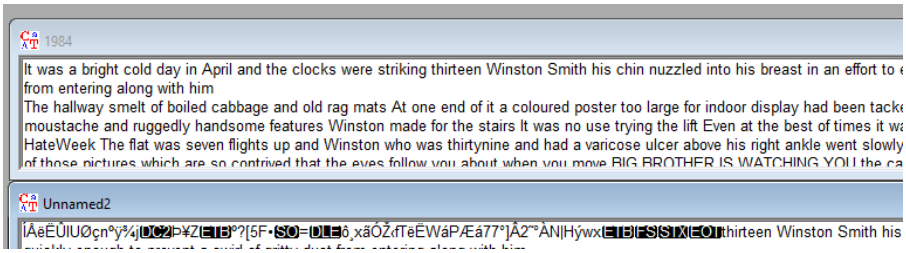

Figure 7: Efekt zmiany jednego bajtu RSA 512

W przypdaku zmiany jednego bajtu kryptogramu, zniekształceniu uległ fragment tekstu jawnego, na pozycji, w której ten bajt zmieniono. Zniekształcony został cały fragment długości bloku (64 znaki dla klucza 512 oraz 256 znaków dla klucza 2048)

- **Usunięcie długości bloku**

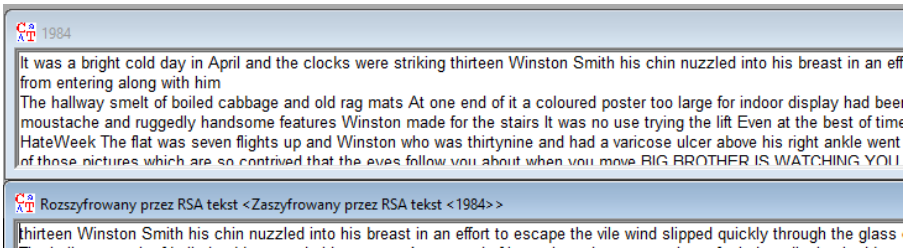

Figure 8: Efekt usunięcią z kryptogramu długości bloku

Usunięcię z kryptogramu długości bloku, spodowodowało usunięcię z tekstu jawnego długości tego bloku, bez wpływu na resztę tekstu.

Zadanie 1.7

Czy i jak długość klucza wpływa na entropię TT?

Długość klucza ma wpływ na entropię TT przy szyfrowaniu tekstów znacznie mniej zróżnicowanych niż język naturalny. Im większe zróżnicowanie TJ, tym mniejszy wpływ na poziom entropii TT ma długość klucza. Dla tekstu zróżnicowanego, nawet klucz długości 512 bit osiągnął bardzo wysoki poziom entropii.

Zadanie 1.8

Czy i jak długość klucza wpływa na autokorelację TT?

Zauważono wpływ długości klucza na autokorelację przy szyfrowaniu tekstu jednorodnego oraz średnio zróżnicowanego. Dla tekstu jednorodnego, długość klucza zwiększała okres przesunięcia dla którego występowało powtórzenie dużej ilości znaków (odległość górek na wykresie). Dla tekstu zróżnicowanego długość klucza nie miała zauważalnego wpływu na autokorelację.

Zadanie 1.9

.Czy i jak obserwowana entropia TT zależy od entropii TJ?

Entropia TT zawsze była znacznie większa od entropii tekstu jawnego. Entropia TJ ma wpływ na entropię TT, jednak dla tekstów zróżnicowanych jest bliska maksymalnej do uzyskania wartości. W przypadku sztucznych tekstów o małym zróżnicowaniu entropia jest mniejsza niż dla tekstu zróżnicowanego.

Zadanie 1.10

jak kształtuje się czas szyfrowania/deszyfrowania w zależności od długości pliku?

Zarówno dla szyfrowania jak dla deszyfrowania zaobserwowano prawie idealnie liniowy wzrost czasu operacji wraz z wielkością pliku.

Zadanie 1.11

Jak wygląda czas operacji szyfrowania/deszyfrowania algorytmem asymetrycznym w porównaniu do realizacji tych operacji algorytmem symetrycznym?

W przypadku algorytmów symetrycznych trudno było zaobserwować czas operacji, ponieważ, nawet dla pliku 5MB było to prawie natychmiastowe. Szyfrowanie oraz deszyfrowanie algorytmami asymetrycznymi było *znacznie* wolniejsze. Szczególnie operacja deszyfrowania potrafiła zająć znaczną ilość czasu (200 sekund dla pliku 5MB i klucz 2048bit).

Zadanie 1.12

Jak wyglądają zmiany w TJ przy wprowadzeniu przekłamań do TT? Jaka ich jest skala? Od czego zależy?

W przypadku zmiany jednego bajtu kryptogramu, zniekształceniu uległ fragment, w którym się ten bajt znajdował (długości klucza). Kiedy usunięto z TT fragment długości klucza, to po deszyfrowaniu, odpowiadający mu fragment TJ (długości klucza) po prostu zniknął. W obu przypadkach reszta TJ nie została zmieniona.

Zadanie 1.13

Czy można usunąć fragment z TT tak, aby pozostały tekst TJ po odszyfrowaniu był czytelny?

W przypadku kiedy usunięty fragment ma długość bloku, to zostanie on usunięty z TJ, jednak reszta tekstu pozostanie czytelna. W przypadku usunięcia liczby bajtów innej niż wielkość bloku, zniekształceniu ulegał cały TJ.

Zadanie 1.14

Jakie są wady i zalety algorytmów asymetrycznych w porównaniu do algorytmów symetrycznych?

- **Wady**
  Algorytmy asymetryczne są znacznie wolniejsze niż algorytmy symetryczne. Szyfrowanie i deszyfrowanie są bardziej skomplikowane oraz znacznie mniej wydajne.
- **Zalety** Jedną z głównych zalet jest pozbycie się potrzeby przekazania klucza wraz z wiadomością. Wpływa to pozytywnie na ich bezpieczeństwo. Każdy udostępnia swój klucz publiczny i dzięki temu bardzo wygodnie można szyfrować wiadomości za pomocą kogoś klucza publicznego.

Zadanie 1.15

W jakich zastosowaniach lepiej korzystać algorytmów asymetrycznych, a w jakich z algorytmów symetrycznych?

Algorytmy symetryczne, takie jak AES, lepiej stosować do szyfrowania danych w spoczynku, takich jak dyski i bazy danych. Używa się je także w protokołach sieciowych. Generalnie algorytmy symetryczne używa się tam gdzie występuje duża ilość danych, ponieważ są znacznie szybsze. Algorytmy asymetryczne lepiej używać tam gdzie potrzebna jest wymiana kluczy. Systemy takie jak podpisy elektroniczne, SSH, certyfikaty i autoryzacja.