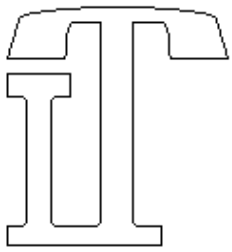


INSTYTUT TELEKOMUNIKACJI

POLITECHNIKA WARSZAWSKA

KRZYSZTOF SZCZYPIORSKI, KONRAD WRONA

VIVALDI

SYSTEM OCHRONY INFORMACJI

Warszawa, czerwiec 1996

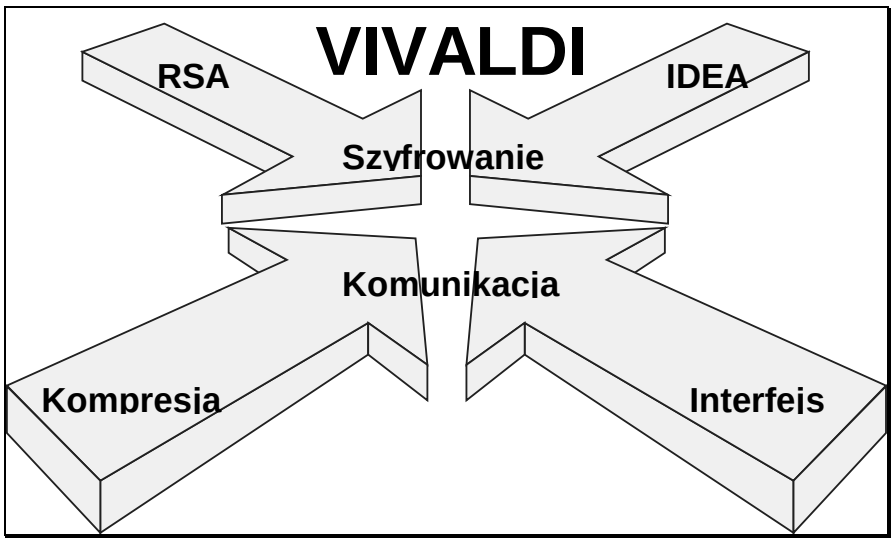
Spis treści:

Antonio Vivaldi (1678 - 1741) włoski skrzypek, kompozytor, jeden z najlepszych, najzdolniejszych muzyków późnego baroku. Pozostawił po sobie ponad 700 kompozycji, odkrytych dopiero w połowie XIX wieku, podczas prac nad manuskryptami Bacha.

**"Na świecie istnieją dwa rodzaje kryptografii:
kryptografia, która powstrzyma twoją młodszą siostrę przed czytaniem twoich plików
i kryptografia, która powstrzyma instytucje rządowe przed czytaniem twoich plików.
Ta książka jest o tej ostatniej."**

Bruce Schneier "Applied Cryptography ..."

Wprowadzenie



Vivaldi jest hybrydowym systemem kryptograficznym[1] - wykorzystującym zarówno asymetryczne jak i symetryczne algorytmy kryptograficzne.

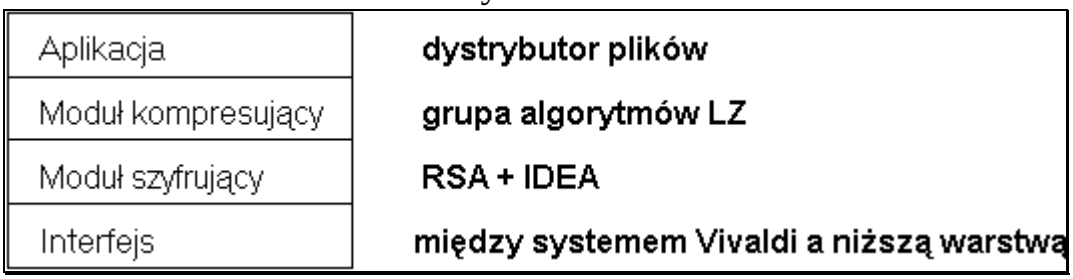
Asymetrycznym algorytmem jest algorytm klucza publicznego RSA (Rivest - Shamir - Adleman), symetrycznym - algorytm IDEA (International Data Encryption Algorithm) międzynarodowy standard - następca legendarnego DES-a (Data Encryption Standard).

W Vivaldim wbudowana jest także kompresja - zaimplementowano trzy algorytmy należące do grupy Lempel-Ziv.

[1] kryptosystemem

1. BUDOWA systemu Vivaldi. Opis algorytmów i implementacji

Rysunek 1



Rysunek 1 prezentuje hierarchię warstw zaimplementowanych w programie.

Na szczycie znajduje się **aplikacja** - dystrybutor plików, w środku **moduł kompresji**, niżej **moduł szyfrujący**, na samym dole **interfejs z niższą warstwą**. Ułożenie warstwy kompresji ponad warstwą szyfrującą jest związane z analizą probabilistyczną ciągów generowanych przez szyfr IDEA. Ciągi te charakteryzują się dużym rozproszeniem, niską korelacją - a zatem **kompresja po zaszyfrowaniu nie jest efektywna**.

1.1 Aplikacja

1.1.1 Zadanie

Sterowanie procesem dystrybucji plików.

1.1.2 Opis

Zorientowana przyjaźnie dla użytkownika aplikacja umożliwia sterowanie procesami szyfrowania i kompresowania plików. Uwzględniono cztery kombinacje usług dla dystrybuowanych plików: kompresja i szyfrowanie, tylko kompresja, tylko szyfrowanie, brak kompresji i brak szyfrowania (kopiowanie).

1.1.3 Implementacja

Język C (kompilator Borland C++ 3.1). Prymitywy dotyczące obsługi ekranu zostały napisane na poziomie asemblera (wbudowanego w kompilator).

1.2 Moduł kompresji

1.2.1 Zadanie

Kompresja plików - eliminacja powtórzeń (redundancji), wstępna ochrona informacji.

1.2.2 Opis algorytmów kompresji

Wszystkie zastosowane algorytmy kompresji są modyfikacjami metody słownikowej. Idea tego rozwiązania polega na kodowaniu ciągów symboli za pomocą odwołań do słownika zawierającego takie ciągi. Im dłuższy ciąg znaków uda się zastąpić indeksem do słownika, tym większy będzie stopień kompresji.

1.3 Moduł szyfrujący

1.3.1 Zadanie

Kryptograficzna ochrona przekazywanych plików. Generacja podpisów cyfrowych.

1.3.2 Wstępny opis kryptosystemu

1.3.2.1 Szyfrowanie

Implementacje programowe i sprzętowe RSA są około 100-1000 razy wolniejsze od implementacji algorytmów symetrycznych takich jak DES, czy IDEA. Dlatego też w praktyce buduje się **systemy hybrydowe (mieszane)** ([PEM93], [SZCZYP95], [ZIMMER93]).

W systemie Vivaldi algorytm RSA jest używany do ochrony klucza sesyjnego (dla algorytmu IDEA). **Proces szyfrowania** wiadomości (pliku) przez system Vivaldi przebiega następująco:

1. Weź klucz publiczny odbiorcy.
2. Wygeneruj losowy klucz sesyjny (dla IDEA).
3. Zaszyfruj plik kluczem sesyjnym (IDEA).
4. Zaszyfruj klucz sesyjny kluczem publicznym odbiorcy (RSA).

Proces odszyfrowania jest odwrotny:

1. Weź klucz prywatny odbiorcy.
2. Odszyfruj klucz sesyjny kluczem prywatnym odbiorcy (RSA).
3. Odszyfruj plik kluczem sesyjnym (IDEA).

1.3.2.1 Generacja podpisu cyfrowego

Podpis cyfrowy służy do uwierzytelnienia nadawcy.

W systemie Vivaldi do tworzenia podpisów cyfrowych używany jest algorytm RSA i funkcja skrótu MD5.

Proces generacji podpisu:

1. Weź klucz prywatny nadawcy.
2. Dokonaj skrótu wiadomości (algorytm MD5).
3. Zaszyfruj skrót kluczem prywatnym.

Zaszyfrowany skrót jest podpisem.

Proces weryfikacji podpisu:
1. Weź klucz publiczny nadawcy.
2. Odszyfruj kluczem publicznym podpis.
3. Dokonaj skrótu wiadomości (algorytm MD5).
4. Porównaj wyniki czynności przeprowadzonych w punktach 3 i 4.

Jeśli wyniki są identyczne podpis jest prawdziwy. Jeśli nie jest fałszywy.

1.3.7 Tryby pracy algorytmu IDEA

1.3.7.1 Electronic Code Book Mode - ECB

(Tryb elektronicznej książki kodowej)

Najprostszy, a zarazem najmniej bezpieczny, tryb pracy algorytmu. Każdy 64-bitowy blok danych jest szyfrowany niezależnie, przy użyciu tego samego klucza. Termin "książka kodowa" jest używany dlatego, gdyż przy danym kluczu dla każdego 64-bitowego bloku danych istnieje jednoznacznie określona zaszyfrowana wiadomość. Jest to odpowiednik gigantycznej książki kodowej.

Metoda idealna do szyfrowania krótkich wiadomości (np. kluczy). Mało bezpieczna dla długich wiadomości o regularnej strukturze.

1.3.7.2 Cipher Block Chaining Mode - CBC

(Tryb dowiązywania zaszyfrowanych bloków)

Danymi wejściowymi dla algorytmu szyfrującego jest wynik funkcji XOR poprzedniego 64-bitowego bloku szyfru i następnego bloku tekstu jawnego. Jeżeli identyczny blok tekstu jawnego pojawi się kilkakrotnie w strumieniu wejściowym, za każdym razem otrzymany blok szyfrogramu będzie różny.

1.3.7.3 Cipher Feedback Mode - CFB

(Tryb ze sprzężeniem zwrotnym z szyfrogramu)

Na raz przetwarzanych jest N bitów danych wejściowych. Poprzedzający szyfrogram jest używany jako dane wejściowe dla algorytmu szyfrującego w

celu otrzymania ciągu pseudolosowego. Szyfrogram jest otrzymywany jako wynik funkcji XOR tego ciągu z tekstem jawnym. Metoda użyteczna przy szyfrowaniu długich informacji.

1.3.7.4 Output Feedback Mode - OFB

(Tryb ze sprzężeniem zwrotnym z wyjścia)

Podobny do CFB. Danymi wejściowymi dla algorytmu szyfrującego jest poprzedzający blok wyjściowy IDEA. Użyteczna przy zorientowanej strumieniowo transmisji poprzez zaszumiony kanał.

1.3.7.5 Interleave - Przeplot

Parametr wykorzystywany przy pracy szyfru IDEA w trybie CBC, CFB i OFB. Definiuje głębokość sprzężenia zwrotnego.

Przyjmując oznaczenia:

N	-	współczynnik przeplotu
Z	-	128. bitowy klucz
x[i]	-	64-bitowy blok danych
y[i]	-	64-bitowy blok szyfrogramu
IDEAe(Z, ...)	-	funkcja szyfrująca
IDEAd(Z, ...)	-	funkcja odszyfrowująca
^	-	działanie XOR

można poszczególne tryby pracy algorytmu przedstawić w postaci następujących równań:

i) ECB

y[i]=IDEAe(Z, x[i])
x[i]=IDEAd(Z, y[i])

ii) CBC

y[i]=IDEAe(Z, x[i] ^ y[i-N])
x[i]=IDEAd(Z, y[i] ^ y[i-N])

iii) CFB

y[i]=x[i] ^ IDEAe(Z, y[i-N])
x[i]=y[i] ^ IDEAd(Z, y[i-N])

iv) OFB

h[i]=IDEA(Z, h[i-N])
y[i]=x[i] ^ h[i]
x[i]=y[i] ^ h[i]

1.3.8 Podstawowe informacje dotyczące algorytmu MD5

Funkcja skrótu (message-digest function) MD5 została opracowana przez Rona Rivesta z MIT. Algorytm skraca tekst wejściowy o dowolnej długości do postaci unikalnego 128-bitowego ciągu. W funkcji MD5 każdy bit wynikowy zależy od każdego bitu wejściowego. Cecha ta, w połączeniu ze skomplikowanym systemem przekształceń wewnętrznych algorytmu, minimalizuje prawdopodobieństwo, że dwie różne wiadomości zostaną skrócone do tej samej postaci.

Poniżej przedstawiono skróty czterech wyrazów:

```
MD5 ("krawat")    = df85bc0a1a695bb34f29d0327d6b0ad7
MD5 ("Marta")     = 83f9c4eb242966cdcada1d01be5d9b15
MD5 ("marta")     = a763a66f984948ca463b081bf0f0e6d0
MD5 ("plomba")    = b29795ff70be9e892bb7bf82744abdfa
```

Więcej informacji o funkcji skróru MD5, można znaleźć w [RIVEST92], [SCHNEI94].

2. OPIS DZIAŁANIA systemu Vivaldi

2.1 Generacja klucza

2.1.1 Generatory: losowy i pseudolosowy

Przygotowanie do generacji kluczy w systemie Vivaldi rozpoczyna się wraz z uruchomieniem programu (rysunek 2.1.1).

Rysunek 2.1.1

Użytkownik proszony jest wówczas o wpisanie z klawiatury losowego ciągu znaków. Czasy odstępu pomiędzy poszczególnymi uderzeniami w klawiaturę, mające rozkład losowy, tworzą wartość początkową dla generatora pseudolosowego (skramblera). Skrambler generuje pseudolosowy ciąg bitów (ziarno) inicjujący strukturę losową modułu RSA. Warto podkreślić, iż **proces zliczający odstępy** pomiędzy kolejnymi naciśnięciami klawiszy (np. przy wyborze opcji menu) **jest aktywny przez cały czas** - jest uruchomiony w tle (jako program rezydentny).

Skrambler jest zbudowany na bazie Rejestru Przesuwnego z Liniowym Sprzężeniem (Linear Feedback Shift Register).

2.1.2 Tworzenie pary kluczy: publicznego i prywatnego [2]

Proces generacji rozpoczyna się od żądania użytkownika utworzenia nowej pary kluczy i składa się z następujących kroków:

i) Program prosi użytkownika o wybranie żądanej długości klucza,

[2] porównaj dodatek B - składowe kluczy RSA

ii) i nazwy pliku do którego mają zostać zapisane jego części składowe (domyślnie przyjmowane są rozszerzenia .PUB dla klucza publicznego i .PRI dla klucza prywatnego).

2.1.3 Tworzenie klucza sesyjnego dla algorytmu IDEA

Klucz sesyjny o długości 128 bitów jest generowany poprzez podanie zawartości bufora losowego[3] funkcji skrótu MD5 ([RIVEST92], [SCHNEI94]. Zapewnia to jego wysoką entropię.

2.2 Tworzenie sum kontrolnych CRC

Zastosowanie algorytmu CRC (Cyclic Redundancy Code - Cykliczny Kod Nadmiarowy) umożliwia kontrolę integralności danych transmitowanych przez zaszumiony kanał komunikacyjny.

2.3 Polskie znaki

System Vivaldi obsługuje polskie znaki zgodne ze stroną kodową 852. Obsługa została zaimplementowana dla kart VGA. W przypadku wykrycia w pliku CONFIG.SYS ustawienia kraju "Polska" (kod 48 dla COUNTRY.SYS), program informuje użytkownika o możliwości wystąpienia konfliktu ze sterownikiem do strony kodowej 852 dostarczanym wraz z systemem MS-DOS przez firmę Microsoft. Zalecane jest użycie strony kodowej 437 (domyślnej).

Moduł ten jest naszym drobnym wkładem w obronę języka polskiego przed makabreskami z rodzaju "**Wystapil blad ogolny**".

2.4 Zamazywanie plików

System Vivaldi posiada opcję bezpiecznego kasowania plików - zamazywania. Opcja ta niszczy zawartość wybranego pliku - chroni przed odzyskaniem zawartości pliku przez narzędzia typu UNDELETE (MS DOS), UNERASE (Norton Utilities), SALVAGE (Novell).

Także wszystkie pliki tymczasowe tworzone przez system Vivaldi są zamazywane.

[3] jeśli bufor jest pusty użytkownik jest proszony o podanie losowego ciągu (rys 2.1.1)

3. OBSŁUGA systemu Vivaldi

3.1 Wymagania i zalecenia dla pracy systemu Vivaldi

3.1.1 Wymagania

- komputer z procesorem 386[4] lub wyższym,
- system operacyjny MS-DOS 5.0 lub wyższy,
- 250 kB wolnej pamięci podstawowej RAM + pamięć niezbędna do uruchomienia programu do przekazywania plików.

3.1.2 Zalecenia

- twardy dysk,
- karta VGA,
- zainstalowany program typu cache (smartdrv.exe, ncache.exe, ncache2.exe).

3.2 Instalacja systemu Vivaldi

System jest dostarczany w postaci samorozpakowującego się archiwum o nazwie VIVAxxxx.EXE, gdzie xxxx jest numerem aktualnej wersji.

Aby zainstalować program należy:
1. Wybrać napęd w komputerze.
2. Stworzyć katalog (np. o nazwie VIVALDI).
3. Przekopiować plik VIVAxxxx.EXE do utworzonego katalogu.
4. Uruchomić plik VIVAxxxx.EXE.

Zmienna środowiskowa COMSPEC[5] powinna być ustawiona.

3.3 Konfiguracja. Opis zmiennych systemowych

Parametry - zmienne systemowe dla programu Vivaldi są przechowywane w pliku VIVALDI.INI. Plik ten powinien być dostosowany indywidualnie do potrzeb użytkownika. Nie ma znaczenia, czy zmienne definiowane w tym pliku są zapisane małymi czy też wielkimi literami. Znak ; (średnik) poprzedza

---

[4] typ procesora jest sprawdzany przed uruchomieniem systemu Vivaldi przy pomocy programu CPU Check. Gdy nie zostanie wykryty procesor zgodny z 386 - na ekranie pojawia się informacja "**Program potrzebuje co najmniej procesora 386 !**". Autorem narzędzia CPU Check jest Tomasz Kawecki (email: tkawecki@tele.pw.edu.pl).

[5] np. jeśli używanym interpreterem jest COMMAND.COM, znajdujący się na w podkatalogu C:\DOS należy w pliku AUTOEXEC.BAT umieścić komendę

```
SET COMSPEC=C:\DOS\COMMAND.COM
```

komentarz. Oczywiście nie wszystkie zmienne muszą być określone w pliku konfiguracyjnym - część zmiennych przyjmuje wartości domyślne.

3.3.1 Opis procedury konfiguracji programu:

1. Czy plik VIVALDI.INI jest w aktualnym katalogu?
2. Jeśli jest: wczytaj ustawienia z pliku VIVALDI.INI i skocz do 6.
3. Jeśli nie ma: czy VIVALDI.INI jest w katalogu, gdzie umieszczony jest program VIVALDI.EXE.
4. Jeśli jest: wczytaj ustawienia z pliku VIVALDI.INI i skocz do 6.
5. Jeśli nie ma: przyjmij domyślne ustawienia.
6. (Jeśli podano) wczytaj ustawienia z linii komend.

Jak widać ustawienia z linii komend mają większy priorytet niż ustawienia z pliku VIVALDI.INI.

3.3.2 Opis poszczególnych zmiennych

Typy danych:

logiczny - przyjmowane wartości: Tak lub Nie,
numeryczny - liczby,
znakowy - ciągi znakowe.

Tabela 3.3.2

Nazwa zmiennej[6]	Typ	Wartość domyślna	Znaczenie
Bez_winiety	logiczny	Nie	wyłączenie wyświetlenia informacji o autorach (po uruchomieniu systemu)
Czekaj_na_klawisz	logiczny	Nie	po operacjach kompresji, szyfrowania, kopiowania, system będzie czekał na wciśnięcie klawisza
Demo	logiczny	Nie	włączenie pokazywania: 1. formatu nagłówków przy wczytywaniu kluczy i opcji Odszyfrowanie + dekompresja 2. składowych poszczególnych kluczy (opcja ta pociąga za sobą ustawienie: Czekaj_na_klawisz=Tak) opis: dodatek A i B

[6] nazwy zmiennych zostały tak dobrane, aby istniała, możliwość poprawnego skonfigurowania programu na komputerze bez polskich znaków

Edytor	znakowy	brak	pełna ścieżka do edytora zewnętrznego
Informacja_o_dysku	logiczny	Tak	włączenie wyświetlania informacji o zasobach dysku przy zmianie napędu
Interfejs_aktywny	logiczny	Nie	interfejs zostanie uruchomiony po procesie kompresja/szyfrowanie i odszyfrowanie/dekompresja
Kasuj_przekazywany_plik	logiczny	Nie	przy aktywnym interfejsie (Interfejs_aktywny=Tak) plik przekazywany do/przez warstwę niższą zostanie skasowany
Klucz_prywatny	znakowy	brak	pełna ścieżka do domyślnego klucza prywatnego (wczytywanego przy inicjacji systemu)
Klucz_publiczny	znakowy	brak	pełna ścieżka do domyślnego klucza publicznego (wczytywanego przy inicjacji systemu)
Kompresja	logiczny	Tak	włączenie modułu kompresji
Koniec_bez_zapowiedzi	logiczny	Nie	wyłączenie żądania potwierdzenia przy wyjściu
Nazwa_interfejsu	znakowy	brak	pełna ścieżka do interfejsu
Podpis	logiczny	Tak	włączenie generacji podpisu cyfrowego
Przeplot	numeryczny	1	parametr dla szyfru IDEA 0<Przeplot<1024
Raport	logiczny	Tak	będzie drukowany raport zrealizowanych usług po procesie kompresja/szyfrowanie i odszyfrowanie/dekompresja
Szyfrowanie	logiczny	Tak	włączenie modułu szyfrującego
Tryb_szyfrowania	znakowy	CBC	tryb pracy szyfru IDEA: ECB, CBC, CFB, OFB
Typ_kompresji	znakowy	LZHUF	algorytm kompresji: LZARI, LZHUF, LZSS
WE_klucz	znakowy	brak	ciąg inicjujący dla warstwy niższej oznaczający żądanie ODBIERANIA
WE_kod_OK	numeryczny	0	wartość zwracana przez warstwę niższą oznaczająca, że ODBIERANIE zakończyło się sukcesem
WE_parametr	znakowy	brak	dodatkowy parametr dla warstwy niższej przy wywołaniu procesu ODBIERANIE
WY_klucz	znakowy	brak	ciąg inicjujący dla warstwy niższej oznaczający żądanie WYSYŁANIE

WY_kod_OK	numeryczny	0	wartość zwracana przez warstwę niższą oznaczająca, że WYSYŁANIE zakończyło się sukcesem
WY_parametr	znakowy	brak	dodatkowy parametr dla warstwy niższej przy wywołaniu procesu WYSYŁANIE
Zainstaluj_polskie_znaki	logiczny	Tak	instalacja polskich znaków na komputerach wyposażonych w kartę graficzną VGA

3.3.3 Konfiguracja systemu z linii komend

Zmienne mogą być też definiowane przy wywołaniu VIVALDI.EXE (jako parametry):

```
VIVALDI.EXE +opcja_1=wartość  +opcja_2=wartość   ...
```

Np.

```
VIVALDI.EXE +demo=tak  +kompresja=nie  +przeplot=666
```

3.3.4 Przykład pliku konfiguracyjnego VIVALDI.INI

```
;początek pliku VIVALDI.INI
;to jest przykład
     Bez_winiety = Tak
     Czekaj_na_klawisz = Nie
     Demo=Nie
     Edytor = C:\TOOLS\NC\NCEDIT
     Informacja_o_dysku = Nie
     Interfejs_aktywny=Tak
     Kasuj_przekazywany_plik = Tak
     Klucz_prywatny   = vivaldi.pri
     Klucz_publiczny  = antonio.pub
     Kompresja = Nie
     Koniec_bez_zapowiedzi = Tak
     Nazwa_interfejsu=C:\HDLC\HDLC.EXE
     Przeplot = 8
     Szyfrowanie = Tak
     Popdis = Nie
     Tryb_szyfrowania = OFB
     Typ_kompresji = LZARI
     WE_klucz=RECEIVE
     WE_kod_OK =2
     WE_parametr = C:\HDLC\HDLCREC.INI
```

```
      WY_klucz=SEND
      WY_kod_OK =1
      WY_parametr = C:\HDLC\HDLCSEND.INI
      Zainstaluj_polskie_znaki=Nie
;Koniec pliku VIVALDI.INI
```

3.4 Format wywołania warstwy niższej (format interfejsu)

```
Nazwa_interfejsu XX_klucz Nazwa_pliku_przekazywanego XX_parametr
```

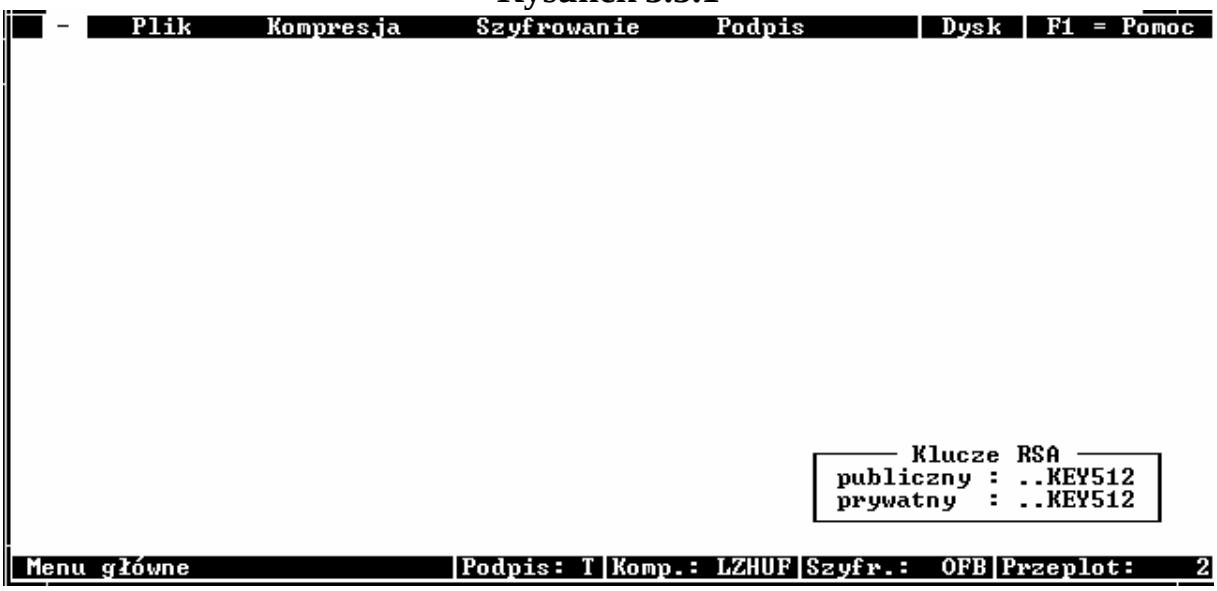
Wartość zwracana przez warstwę niższą (ERRORLEVEL, kod wyjścia) jest porównywana przez system Vivaldi z XX_kod_OK. Oznaczenia: XX - WY (WYsyłanie) lub WE (odbieranie). Nazwa_pliku_przekazywanego - ustalona przez system Vivaldi nazwa (stała).

3.5 Obsługa systemu Vivaldi

3.5.1 Schemat ekranu

Rysunek 3.5.1 przedstawia schemat ekranu.

Rysunek 3.5.1



3.5.1.1 Wskaźnik aktywności interfejsu

przyjmuje dwie wartości:

- Dysk - [Interfejs_aktywny=Nie]- skompresowane/zaszyfrowane pliki są kierowane na dysk/pobierane z dysku,

- Interfejs - [Interfejs_aktywny=Tak]- skompresowane/zaszyfrowane pliki są przekazywane warstwie niższej/odbierane od warstwy niższej.

3.5.1.2 Wskaźnik operacji

aktualnie wykonywana czynność.

3.5.1.3 Wskaźnik podpisu

jeśli przekazywany plik będzie podpisany pojawia się napis PODPIS; w przeciwnym przypadku zanika.

3.5.1.4 Wskaźnik kompresji

aktualny algorytm kompresji (LZARI, LZHUF, LZSS) lub BRAK jeśli kompresja jest wyłączona.

3.5.1.5 Wskaźnik szyfrowania

aktualny tryb pracy szyfru IDEA (ECB, CBC, CFB, OFB) lub BRAK jeśli szyfrowanie jest wyłączone.

3.5.1.6 Wskaźnik przeplotu

aktualna wartość przeplotu.

3.5.1.7 Wskaźnik kluczy

nazwy aktywnych kluczy: publicznego i prywatnego.

3.5.2 Hierarchia okien. Opis dostępnych funkcji

Poniższa lista przedstawia hierarchię okien (rozwijanych menu) dostępnych w programie i krótki opis reprezentowanych przez nie funkcji:

≡

O autorach ...
informacje o autorach
O programie ...
informacje o programie

Plik

Zmień napęd
zmiana aktywnego napędu
Pokaż aktywne usługi
pokazuje aktualnie dostępne usługi kryptograficzne
Zabezpiecz
proces zabezpieczania (archiwizacji)
Odbezpiecz

proces odbezpieczania (dearchiwizacji)

Obejrzyj plik

podgląd wybranego pliku

Zamaż plik

zamazanie (bezpieczne skasowanie) wybranego pliku

Edytuj plik

edycja wybranego pliku przy użyciu edytora zewnętrznego

Zajrzyj do DOS-a

wywołanie interpretera DOS

Koniec

powrót do DOS-a

Kompresja

LZARI

wybór algorytmu LZARI

LZHUF

wybór algorytmu LZHUF

LZSS

wybór algorytmu LZSS

Włącz/Wyłącz

włączenie/wyłączenie kompresji

Szyfrowanie

RSA

opcje dla RSA

Generuj parę kluczy

generacja pary kluczy dla RSA (o podanych poniżej wielkościach)

512-bitów - niższy stopień komercyjny ...

768-bitów - wyższy stopień komercyjny ...

1024-bity - stopień militarny, wolny ...

Może innym razem...

Wczytaj klucz publiczny

wczytanie klucza publicznego

Wczytaj klucz prywatny

wczytanie klucza prywatnego

Zmień hasło

zmiana hasła chroniącego klucz prywatny

IDEA

opcje dla IDEA

ECB

wybór trybu pracy szyfru ECB

CBC

wybór trybu pracy szyfru CBC

CFB

wybór trybu pracy szyfru CFB

OFB

wybór trybu pracy szyfru OFB

Przeplot

określenie przeplotu

Włącz/Wyłącz

włączenie/wyłączenie szyfrowania

Podpis

Włącz/Wyłącz

włączenie/wyłączenie generacji podpisu

Pomoc jest dostępna po naciśnięciu klawisza **F1.**

Do wyboru okna należy używać klawiszy **kursora** i klawisza **Enter**.

3.6 Błędy - spis komunikatów

Spis jest ułożony problemowo. W obrębie zagadnienia - alfabetycznie.
Wyodrębniono następujące grupy błędów:

- błędy globalne,
- błędy przy określaniu opcji,
- błędy obsługi plików z wiadomościami,
- błędy modułu kompresji,
- błędy szyfru RSA,
    - błędy obsługi odczytu kluczy,
    - błędy obsługi zapisu kluczy,
- błędy szyfru IDEA,
- błędy weryfikacji podpisów cyfrowych,
- błędy krytyczne DOS.

Wszystkie błędy za wyjątkiem błędów krytycznych DOS mają charakter informacyjny. Błędy DOS wymagają decyzji użytkownika:

P - powtórz (RETRY) lub Z - zignoruj (IGNORE).

3.6.1 Błędy globalne

"Brak pamięci"

niewystarczająca ilość pamięci (podczas rezerwacji).

"Nazwy plików: WEjściowego i WYjściowego są takie same"

podana nazwy: pliku WEjściowego i WYjściowego są takie same. Zignorowanie tego ostrzeżenie spowodowało by błędną pracę systemu.

"Nie jest wczytany"

informacja, że dany typ klucz nie został wczytany.

"Nie można odczytać"

nie można odczytać pliku.

"Nie można otworzyć pliku"

nie można otworzyć pliku.

"Nie można uruchomić"

nie można uruchomić programu (przyczyny - brak pamięci, brak programu, niewłaściwy format pliku typu EXE lub COM, itp.). W przypadku pojawienia się tego błędu podczas uruchomiania edytora zewnętrznego - sprawdzić ustawienie zmiennej Edytor w pliku VIVALDI.INI.

"Nie można usunąć z pamięci generatora liczb losowych"

generator liczb losowych jest programem działającym w tle, pojawienie się tego błędu jest równoznaczne z zawieszeniem się komputera po wyjściu z systemu. Błąd ten może pojawić się tylko w przypadku uruchomienia innego programu rezydentnego po wywołaniu interpretera (funkcja Plik/Zajrzyj do DOS-a).

"Nie można zainicjować interfejsu"

nie można uruchomić interfejsu (przyczyny - brak pamięci, brak programu, niewłaściwy format pliku typu EXE lub COM, itp.). Sprawdzić ustawienie zmiennej Nazwa_interfejsu w pliku VIVALDI.INI.

"Nie można zainstalować generatora liczb losowych"

patrz uwagi do "Nie można usunąć z pamięci generatora liczb losowych**".**

"Nie można zapisać"

nie można zapisać pliku.

"Nie wykryto karty graficznej zgodnej z VGA"

ostrzeżenie może pojawić się przy inicjacji polskich znaków - są one dostępne tylko dla kart graficznych zgodnych z VGA.

"Nie znaleziono żadnego pliku"

oznacza, że aktualny napęd nie zawiera żadnego pliku.

"Nieoczekiwany błąd programu"

błąd wewnętrzny.

"Niepoprawna ścieżka, brak pliku lub długość pliku równa 0"

informacja pochodząca od funkcji Plik/Obejrzyj plik.

"Niewłaściwe wywołanie funkcji"

błąd wewnętrzny.

"Niewłaściwy napęd"

wskazany napęd nie jest dostępny w systemie.

"Plik nie został odebrany"

warstwa niższa nie odebrała poprawnie pliku.

"Plik nie został wysłany"

warstwa niższa nie przesłała poprawnie pliku.

"Plik wymiany zmieniony"

plik VIVALDI.SWP został zmodyfikowany (rozmiar, atrybuty lub data).

"Program wykrył, że kraj: Polska (kod 48) jest ustawiony w CONFIG.SYS"

ostrzeżenie - nie jest zalecane użycie systemu Vivaldi i sterownika Microsoft do strony kodowej 852.

"Wewnętrzna zmienna programu nie zdefiniowana"

podana zmienna nie została zdefiniowana w VIVALDI.INI.

"Zła suma kontrolna pliku"

plik został uszkodzony - zła suma kontrolna (CRC).

"Zmienna środowiskowa COMSPEC nie jest ustawiona"

patrz instalacja systemu Vivaldi.

3.6.2 Błędy przy określaniu opcji

""Przeplot" nie jest parametrem trybu ECB"

próbowano definiować przeplot dla ECB.

"Szyfrowanie powinno być włączone"

próbowano definiować przeplot przy wyłączonym szyfrowaniu.

"Wartość parametru "przeplot" powinna należeć do przedziału <1; 1024)"

podana wartość parametru Przeplot nie należy do przedziału <1; 1024)

3.6.3 Błędy obsługi plików z wiadomościami

"Niewłaściwa wersja programu"

wiadomość stworzona przez inną (najprawdopodobniej nowszą) wersję systemu Vivaldi.

"Niewłaściwy nagłówek pliku z wiadomością"

wskazany plik nie jest plikiem systemu Vivaldi.

"Nieznany algorytm kompresji"

wykryty algorytm kompresji nie jest znany.

"Nieznany algorytm szyfrowania"

wykryty algorytm szyfrowania nie jest znany.

"Plik nie zawiera wiadomości"

wskazany plik nie zawiera wiadomości.

"Uszkodzony nagłówek pliku z wiadomością"

niewłaściwa suma kontrolna części sterującej.

3.6.4 Błędy modułu kompresji

"Błąd wewnętrzny modułu kompresji"

błąd wewnętrzny.

"Nie można odczytać pliku WEjściowego"

nie można odczytać pliku WEjściowego.

"Nie można zapisać pliku WYjściowego"

nie można odczytać pliku WYjściowego.

"Nieprawidłowy rozmiar pliku"

nieprawidłowy rozmiar dekompresowanego pliku - plik uszkodzony.

"Plik jest pusty"

długość wskazanego pliku wynosi 0.

3.6.5 Błędy szyfru RSA

"Niewłaściwy klucz".

nie można aktualnym kluczem prywatnym odszyfrować klucza sesyjnego.

"Struktura losowa niezainicjowana"

błąd wewnętrzny.

3.6.5.1 Błędy obsługi czytania kluczy

"Niewłaściwa wersja programu"

klucz wygenerowany przez inną (najprawdopodobniej nowszą) wersję systemu Vivaldi.

"Niewłaściwy nagłówek pliku z kluczem"

wskazany plik nie jest plikiem systemu Vivaldi.

"Oczekiwano końca pliku"

nie wykryto znaku końca pliku (EOF) przy czytaniu pliku z kluczem.

"Plik nie zawiera klucza prywatnego"

wskazany plik nie zawiera klucza prywatnego.

"Plik nie zawiera klucza publicznego"

wskazany plik nie zawiera klucza publicznego.

"Plik nie zawiera klucza"

wskazany plik nie zawiera klucza.

"Uszkodzony klucz"

niewłaściwa suma kontrolna klucza.

"Uszkodzony nagłówek pliku z kluczem"

niewłaściwa suma kontrolna części sterującej.

3.6.5.2 Błędy obsługi zapisu kluczy

"Nie można zapisać pliku z kluczem prywatnym"

błąd zapisu pliku z kluczem prywatnym.

"Nie można zapisać pliku z kluczem publicznym"
błąd zapisu pliku z kluczem publicznym.

3.6.6 Błędy szyfru IDEA

"Brak danych do odszyfrowania"
długość wskazanego pliku wynosi 0.

"Nie można otworzyć pliku WEjściowego"
nie można otworzyć pliku WEjściowego.

"Nie można otworzyć pliku WYjściowego"
nie można otworzyć pliku WYjściowego.

"Nieprawidłowy tryb",
błąd wewnętrzny.

"Niewłaściwy znak w kluczu"
błąd wewnętrzny.

"Plik WEjściowy nie jest właściwym kryptogramem"
plik WEjściowy został uszkodzony.

"Wartość parametru 'przeplot' jest ujemna lub równa 0"
błąd wewnętrzny.

"Wartość parametru 'przeplot' przekracza 1023"
błąd wewnętrzny.

"Wprowadzono zbyt wiele wartości inicjujących"
błąd wewnętrzny.

"Zbyt duża wartość inicjująca"
błąd wewnętrzny.

"Zbyt duża wartość klucza"
błąd wewnętrzny.

3.6.7 Błędy przy weryfikacji podpisu

"Niewłaściwy klucz".
nie można aktualnym kluczem publiczny odszyfrować podpisu.

"Niewłaściwy podpis"
podpis nie został zweryfikowany

3.6.8 Błędy krytyczne DOS

"Błąd danych - zła suma kontrolna"
zła suma kontrolna na poziomie sprzętu.

"Błąd odczytu"
błąd odczytu DOS.

"Błąd ogólny"

ogólny błąd DOS.

"Błąd wyszukiwania"

błąd wyszukania DOS.

"Błąd zapisu"

błąd zapisu DOS.

"Dysk zabezpieczony przed zapisem"

dyskietka zabezpieczona przed zapisem. Odblokować i ponowić próbę.

"Napęd niegotowy"

brak dyskietki w napędzie

"Nie znaleziono sektora"

uszkodzony nośnik.

"Niewłaściwe wywołanie"

błąd wywołania DOS.

"Nieznana komenda"

DOS nie rozpoznał komendy.

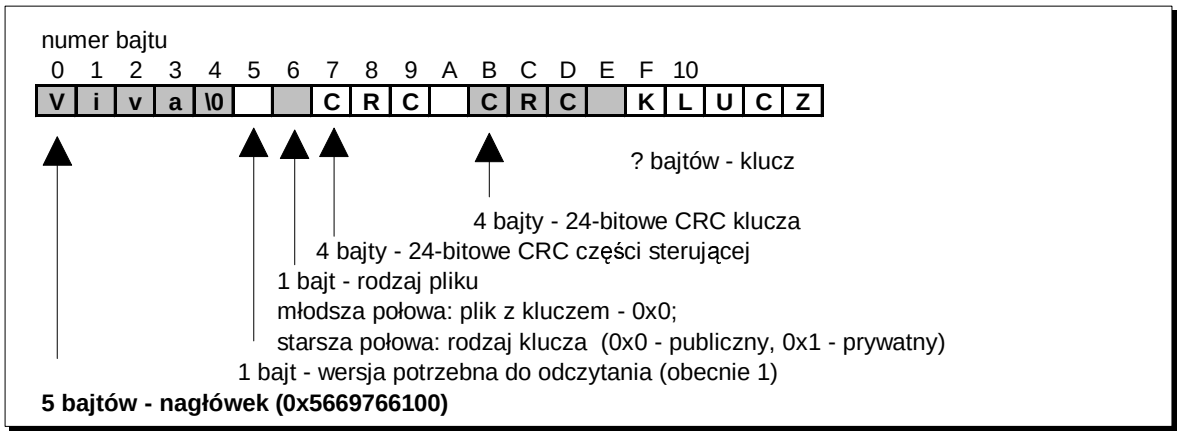
"Nieznany typ nośnika"

DOS nie rozpoznał nośnika.

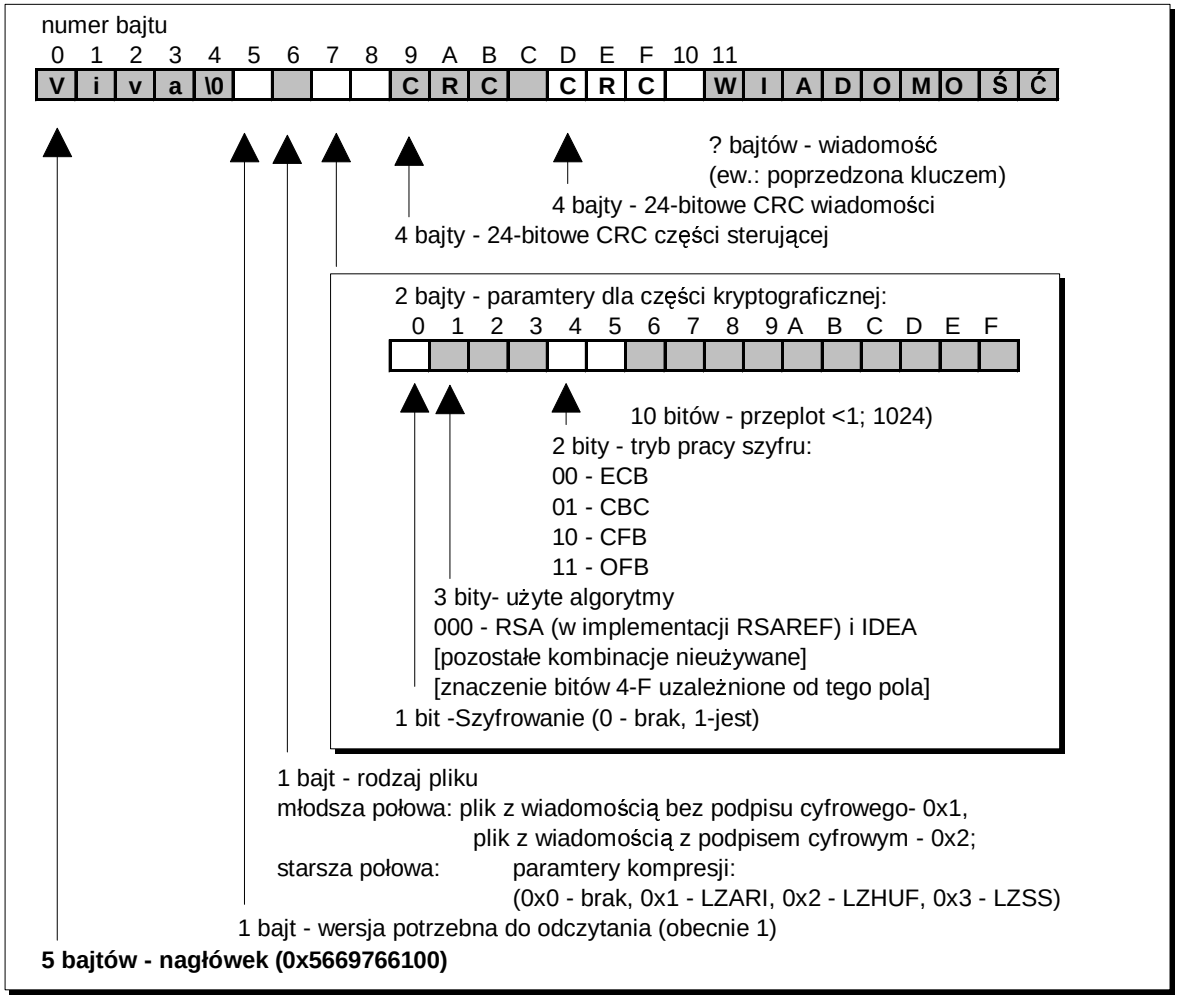
DODATEK A - Format nagłówków

Format nagłówków plików generowanych przez aplikację Vivaldi:

Klucze:



Wiadomości:



Nagłówki są widoczne przy ustawieniu zmiennej Demo=Tak.

DODATEK B - Składowe kluczy RSA

Pogrubioną kursywą zaznaczono wartości identyczne dla pary kluczy:

Składowe klucza publicznego:

długość - długość klucza w bitach,
modulo - n,
publiczny wykładnik - e [7]**.**

Przykład:

```
długość   : 1024

modulo    :
0xE14FABC767A815B5423212C9594A36EE4D0F6E24E542ED1F59761C400113E56AD5DE92A24
1F8639851A61B1B5F962228AC47FB05024FECEFAFC5F06D0817789ED1E636F3D2704B401DBC
CBF9E04489F1EF1AE424DD4637827307404BC55B8CD7D0397CFB4E0B7DA9CD38BC55CAA981E
63B4501DFB8AC78FFD5A2D611EDEB8A13

wykładnik : 0x010001
```

Składowe klucza prywatnego:

długość - długość klucza w bitach,
modulo - n,
publiczny wykładnik - e ,
wykładnik - d,
1. liczba pierwsza - p (p>q),
2. liczba pierwsza - q,
wykładnik 1 - d mod (p-1)
wykładnik 2 - d mod (q-1)
współczynnik - q^{-1} mod p

Przykład:

```
długość             : 1024

modulo              :
0xE14FABC767A815B5423212C9594A36EE4D0F6E24E542ED1F59761C400113E56AD5DE92A24
1F8639851A61B1B5F962228AC47FB05024FECEFAFC5F06D0817789ED1E636F3D2704B401DBC
CBF9E04489F1EF1AE424DD4637827307404BC55B8CD7D0397CFB4E0B7DA9CD38BC55CAA981E
63B4501DFB8AC78FFD5A2D611EDEB8A13

publiczny wykładnik : 0x010001

wykładnik           :
0x881E22D0382E52D70BA3C6B7BFEAD71EC68D60E4876114725110CAE65C005224660AAE19B
AB33E30227BB07AAC17BE9145EBC299F718A432F5C5268828504DBCBB07013E3F1413CC56B8
3951E08FE6BEF517A16672E58E5EB0280A634D1F69EB742BA844BD10773105FD1A437C4DE54
B62958ABF3EADE0D97C2FC380EB605D51

1. liczba pierwsza  :
0xF84A77F409ADAD6225A478D4FE20C189D84ED762B744F92B35C4C249BA51EFB0BF62A1474
02100C42048E11E6111F6CABF4E75CB57894B849EA099CBA1DE3189
```

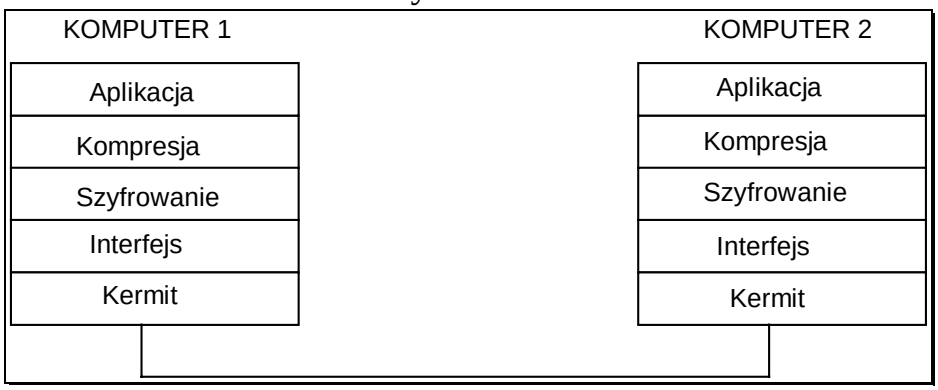
[7] zawsze 0x010001=65537.

```
2. liczba pierwsza  :
0xE84E8C9DB8D39075F6AB3D7D4F6D0D199D64405789E1C2869AB13081BEE0FD32404238458
0092C40AFD38A7E658E0A90CE881BFF1C5732AF154D0BF03B52C3BB

wykładnik 1         :
0xADE040A6A6CC789A3DF0332A3D9924CFEAAA33CD8EB87FA1D1F2AB78C4413310DCC62E595
E407E6FDA880F169E35DD5558A992764723FFBDACF49D1F6C88D4B9

wykładnik 2         :
0x6277A10CDDA1F792B8DABEB695EB106972186359779D54F9FF29E9F8A4F2F2FFD0D300CD1
CC74695A8B18EFBA28A419A3DA0DDD515AB3455983ECF37A5BDA02F

współczynnik        :
0x79902D02D728EE9B0F2139934655A7A81FB6D80C6103126869B850A39209369B99E6AD733
59074650A6597EE922A6359AD9B601C88E060A4724F7DB4F6B825E1
```

Składowe są widoczne przy ustawieniu zmiennej Demo=Tak.

DODATEK C - Przykład współpracy systemu Vivaldi z warstwami niższymi

Rysunek C



Kermit jest popularnym programem komunikacyjnym opracowanym na Uniwersytecie Columbia w Nowym Jorku. Oto skrypt dla Kermita (VIVA2KER.INI) umożliwiający połączenie dwóch komputerów przez łącze szeregowe RS-232 C (rysunek C):

```
if < \v(version) 314 -
  stop 1 -
  Ta wersja VIVA2KER.INI wymaga wersji MS-DOS Kermit 3.14 lub
wyższej
set block 3
set window 8
set receive packet-length 2000
set control prefix all
test COM1
if fail   end 0
set port COM1
set speed 38400
```

Oto niezbędne ustawienia dla systemu Vivaldi [8]:

```
Interfejs_aktywny=Tak
Kasuj_przekazywany_plik=Tak
Nazwa_interfejsu=C:\KERMIT\KERMIT.EXE
WY_klucz=SEND
WY_parametr = , -f C:\KERMIT\VIVA2KER.INI
WY_kod_OK =0
WE_klucz=RECEIVE
WE_parametr = , -f C:\KERMIT\VIVA2KER.INI
WE_kod_OK =0
```

[8] założono, że Kermit i plik VIVA2KER.INI są umieszczone w podkatalogu `C:\KERMIT\`

Literatura

[DAEMAN] - J.Daeman, R. Govaerts, J.Vandewalle - Weak Keys for IDEA

[DUDEK94] - A.Dudek - Jak pisać wirusy - Read Me, Wydanie 2, Warszawa 1994

[DUNCAN88] - R.Duncan - Advenced MS-DOS Programming - Microsoft Press, Washington 1988

[EASTLA94] - D. Eastlake, S. Crocker, J. Schiller - Randomness Recommendations for Security - RFC 1750, December 29, 1994

[GAJ] - K.Gaj - Selection of Algorithms for the Software Implemantation of the RSA Cryptosystem

[GALLAG78] - R.G.Gallager - Variations on a Theme by Huffman - IEEE Transactions On Information Theory, vol. IT-24, no. 6, November 1978

[HOLZNE93] - S.Holzner - Programowanie w Borland C++ - Intersoftland, Warszawa 1993

[HOWARD91] - P.G.Howard, J.S.Vitter - Practical Implementations of Arithmetic Coding, Proceedings of Data Compression Conference, 1991

[LAI91] - X.Lai - Datailed Description and a Software Implemantation of the IPES Cipher, November 8, 1991

[MEIER] - W.Meier - On the Security of the IDEA Block Cipher

[PEM93] - RFC[9]1421 - 1424:

- RFC 1421 - J. Linn - Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures, October 2,1993

- RFC 1422 - S. Kent - Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management, October 2,1993

[9]Dokumenty RFC są dostępne na wielu serwerach FTP m.in. **ftp.pwr.edu.pl**

- RFC 1423 - D. Balenson - Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers, October 2, 1993

- RFC 1424 - B. Kaliski - Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services, October 2,1993

[RIVEST92] - R.Rivest - The MD5 Message-Digest Algorithm, RFC 1321, April 1992

[RSAREF92] - RSAREF: A Cryptografic Toolkit for Privacy-Enhanced Mail Library Reference Manual, RSA Laboratories, March 2, 1992

[RSAREF94] - RSAREF: A Cryptografic Toolkit Library Reference Manual, Version 2.0, RSA Laboratories, March 21, 1994

[SCANLO92] - L.Scanlon - Assembler 8086/8088/80286 - Intersoftland, Warszawa 1992

[SCHNEI94] - B.Schneier - Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, 1994

[STORER88] - J.A.Storer - Data Compression: Methods and Theory - Computer Science Press, 1988

[SZCZYP95] - K.Szczypiorski, K.Wrona - Pretty Good Privacy - Ogólnodostępna metoda ochrony informacji - IT PW (CITCOM), Warszawa 1995

[TANENB81] - A.S.Tanenbaum - Computer Networks - Prentice Hall, 1981

[WILLIA93] - R.N.Williams - A Painless Guide to CRC Detection Algorithms - ftp.adelaide.edu.au/pub/rocksoft/crc_v3.txt, 19 August 1993

[ZENG91] - K.Zeng, C. Yang, D. Wei, T.R.N Rao - Pseudorandom Bit Generators in Stream-Cipher Cryptography - IEEE Computer, vol. 24, no. 2, February 1991

[ZIMMER93] - P.Zimmermann - PGP 2.3a User's Guide - June, 14 1993 (także późniejsze edycje)

[ZIV77] - J.Ziv, A.Lempel - A Universal Algorithm for Sequential Data Compression - IEEE Transactions On Information Theory, vol. IT-23, no. 3, May 1977

[ZIV78] - J.Ziv, A.Lempel - Compression of Individual Sequences via Variable-Rate Coding - IEEE Transactions on Information Theory, vol. IT-24, no. 5, September 1978

Kontakt z autorami

Wszelkie pytania i uwagi prosimy kierować pod poniższe adresy poczty elektronicznej:

Krzysztof Szczypiorski

e-mail:kszczypi@tele.pw.edu.pl
http://www.tele.pw.edu.pl/~kszczypi

PGP key fingerprint = 17 3B CB 12 79 C9 5E C8 A6 56 67 CB 6B 8A 6E 24

Konrad Wrona

e-mail:kwrona@tele.pw.edu.pl
http://www.tele.pw.edu.pl/~kwrona

PGP key fingerprint = 67 E4 E2 C4 0B 4E 9A FB C3 2F 9E E8 5C 21 70 03