www.vmpcrypt.pl

Instrukcja obsługi

Spis treści

1. Wstęp

Program VMPCrypt, przeznaczony dla systemów operacyjnych Microsoft Windows 98/ME/2000/XP/2003/Vista/7, został zaprojektowany do zapewnienia najwyższego poziomu bezpieczeństwa kryptograficznego szyfrowanych danych. W szczególności program służy do:

- Szyfrowania plików i folderów na dyskach lokalnych i sieciowych. Zaszyfrowane pliki/foldery zapisywane są w pliku archiwum lub dla każdego pliku tworzone mogą być osobne zaszyfrowane kopie źródłowych plików.

- Szyfrowania tekstów i poczty elektronicznej – edytowanych we wbudowanym edytorze tekstów. Wiadomości po zaszyfrowaniu można wysłać pocztą elektroniczną przy pomocy domyślnie stosowanego programu pocztowego, zapisać w pliku tekstowym lub w szyfrowanej książce, będącej zbiorem szyfrowanych dokumentów tekstowych.

- Generowania wysokiej jakości kluczy z losowych ruchów myszką – na podstawie chwilowej pozycji kursora myszki oraz odstępów czasu między zmianami pozycji kursora mierzonymi do jednej tysięcznej części sekundy.

- Bezpiecznego wymazywania plików z dysku – nadpisywania zawartości plików pseudolosowymi danymi od 1- do 99-krotnie. Wymazywanie pozwala uniknąć ryzyka odtworzenia plików nawet przy pomocy specjalistycznej aparatury.

2. Instalacja programu VMPCrypt

Po włożeniu płyty instalacyjnej do napędu otwiera się okno uruchamiania aplikacji (program start.exe). Z jego poziomu można uruchomić aplikację bezpośrednio z płyty lub zainstalować na komputerze.

Po wybraniu instalacji aplikacji uruchomiony zostanie instalator (setup.exe). Użytkownik będzie poproszony o potwierdzenie nazwy folderu, do jakiego program zostanie skopiowany i o potwierdzenie, czy instalator ma utworzyć folder w menu systemu Windows: Start → Programy oraz czy utworzyć skrót do programu na pulpicie i na pasku szybkiego uruchamiania systemu Windows.

Po wybraniu uruchomienia bezpośrednio z płyty aplikacja zostanie otwarta bez konieczności instalacji (plik vmpcrypt.exe). Plik ten można także skopiować na dowolny dysk, np. pamięć przenośną USB i uruchamiać aplikacje stamtąd, mając program zawsze przy sobie.

3. Ogólna idea kryptografii i krytyczna waga klucza

Kryptografia, stosowana prawidłowo, pozwala zapewnić bezwzględnie najwyższy poziom bezpieczeństwa (poufności) danych, w porównaniu np. z metodami ochrony danych na poziomie praw dostępu.

Szyfrowanie to nic innego jak jednokierunkowe przekształcenie danych – takie, aby możliwa była szybka zmiana postaci oryginalnych danych na szyfrogram – ciąg bajtów nieodróżnialny od ciągu losowego – ale aby wykonanie operacji odwrotnej było obliczalnie niewykonalne. Fundamentalnym składnikiem operacji szyfrowania jest KLUCZ KRYPTOGRAFICZNY. Dalej będziemy go nazywać po prostu kluczem lub hasłem. Klucz jest ciągiem bajtów, który jest parametrem szyfrowania. Dzięki znajomości klucza deszyfrowanie danych może być równie szybkie, jak ich szyfrowanie. Siła algorytmu tkwi w liczbie operacji, jakie trzeba wykonać, aby dane zdeszyfrować NIE ZNAJĄC KLUCZA lub po prostu, aby ten klucz złamać (znaleźć jego wartość).

Z matematycznego punktu widzenia złamanie szyfrogramu stworzonego z wykorzystaniem technologii VMPC wymaga wykonania średnio 2^{900} operacji. Gdyby każdy atom we wszechświecie wykonywał miliard operacji na sekundę przez miliard lat, to i tak wykonanie tak dużej liczby operacji byłoby nieosiągalne. Aplikacja posiada dodatkowe zabezpieczenie w postaci specjalnie skonstruowanego algorytmu inicjowania klucza (VMPC-KSA3). Nawet gdyby hipotetycznie szyfr VMPC został złamany, konstrukcja algorytmu VMPC-KSA3 sprawia, że nawet wtedy zdeszyfrowanie innych wiadomości (także zaszyfrowanych tym samym kluczem) nie jest możliwe. Tym samym, aby załamać algorytm szyfrowania wersji Pro, konieczne jest nie tylko złamanie szyfru strumieniowego VMPC, ale także odwrócenie (złamanie) funkcji VMPC-KSA3, co jest zadaniem o jeszcze wyższej złożoności.

Fundamentalnym warunkiem utrzymania bezpieczeństwa szyfrowania jest:

- Utrzymanie klucza w tajemnicy
- Stosowanie kluczy o odpowiednio dużej długości i odpowiednio wysokiej jakości

Stosowanie kluczy krótkich (np. w postaci kilkuliterowych haseł) tworzy tylko POZORNĄ ochronę. Mimo, że sam szyfr pozostaje niepokonany, atakujący może z łatwością pokonać tak krótki klucz. Dla przykładu – złamanie 6-literowego hasła złożonego tylko z małych (lub tylko z dużych) liter przez domowy komputer 3,2 GHz wymaga średnio PONIŻEJ PÓŁ GODZINY PRACY. Owszem, hasła typu „12345”, czy „asdfg”, „abcdef” są łatwe do zapamiętania. Tworzą one jednak jedynie pozorną ochronę danych. Jeśli szyfrujemy istotne dane takimi hasłami, nawet najlepszym algorytmem, musimy się liczyć, że każdy, kto będzie miał w tym choć minimalny interes, będzie w stanie bez wysiłku odnaleźć to hasło i odszyfrować dane (nawet najprostszą metodą przeszukiwania wszystkich możliwych haseł) Dla ilustracji – wszystkich możliwych haseł 6-literowych jest tylko około 300 milionów, a komputer 3,2 GHz wykonuje w ciągu sekundy ponad 3,2 miliarda elementarnych operacji na sekundę. Przeszukanie wszystkich możliwych haseł i trafienie na prawidłowe zabierze nawet kiepsko napisanemu programowi łamiącemu hasła tylko chwilę.

Co więc robić? Należy wykorzystać właściwości funkcji wykładniczych – a więc pozornie paradoksalne zjawisko, że zwiększając długość hasła tylko o kilka znaków zwiększamy złożoność jego złamania nieproporcjonalnie bardziej. Załóżmy, że dysponujemy szybkim komputerem, który hasło 6 znakowe jest w stanie złamać w ciągu 1 minuty. Gdy zastosujemy hasło 7 znakowe, czas złamania tego hasła wyniesie już 26 minut (liczba możliwych haseł zwiększy się 26-krotnie). Hasło 8-znakowe – już 26*26 minut, a więc 11 godzin. Hasło 9 znakowe – 26^3 minut = 12 dni. A hasło 10 znakowe – już prawie rok.

Oprócz długości hasła, która ma największy wpływ na złożoność jego złamania, ważne jest także z jakich znaków jest ono zbudowane. Lepiej jest, jeśli hasło składa się nie tylko z małych liter, ale np. z małych i dużych oraz z cyfr. Wówczas każdy znak hasła może mieć nie 26 różnych postaci, ale 26+26+10 = 62. Wtedy, gdyby ktoś umiał takie 6 znakowe hasło złamać w ciągu minuty, to przedłużenie takiego hasła do 10 znaków zmusiło by go do pracy już przez 62^4 minut, a więc 28 lat.

Jednakże CZŁOWIEK jest bardzo niedoskonałym źródłem dobrych, losowych haseł. Zastosowanie 10-znakowego hasła postaci „aB2aB2aB2a” owszem, z matematycznego punktu widzenia jest słuszne, ale niestety tylko pozornie. Hasło takie zawiera w sobie bardzo dużo REGULARNOŚCI, które przez łamiącego mogą być rozpatrywane ZANIM zajmie się on hasłami bardziej nieregularnymi. Haseł regularnych, wygodnych do zapamiętania dla człowieka jest naprawdę niewiele i zastosowanie regularnego hasła 10-znakowego może się wiązać z bardzo realnym ryzykiem złamania tego hasła w bardzo krótkim czasie.

Zatem widzimy, że dobry klucz (hasło):

- Musi być odpowiednio długi – odpowiednikiem szyfrowania z mocą 128 bitów jest 29 (!) znakowe hasło złożone z samych małych (lub samych dużych) liter lub 23-znakowe złożone z małych i dużych liter oraz cyfr.
- Musi być dobrej jakości – nie wykazywać żadnych regularności.

Dopiero stosowanie takich kluczy – odpowiednio długich i dobrej jakości – pozwala w pełni wykorzystać potencjał bezpieczeństwa oferowany przez technologię VMPC.

Program VMPCrypt posiada zaawansowany moduł do generowania kluczy o bardzo wysokiej jakości i wybranej przez użytkownika długości. Program wykorzystuje do tego celu losowe ruchy myszką, jakie użytkownik wykonuje oraz odstępy czasu między zmianami pozycji kursora myszki mierzone do jednej tysięcznej części sekundy. Odtworzenie serii przypadkowych ruchów myszką – co do dokładnej geometrii oraz z dokładnością czasową co do jednej tysięcznej sekundy jest w praktyce niemożliwe. Program przekształca parametry kursora myszki i generuje z nich chaotyczny (nieodróżnialny od losowego) ciąg znaków. Dzięki takiej metodzie wygenerowany zostaje klucz najwyższej jakości, który można bez obaw stosować do zabezpieczenie najbardziej wartościowych danych.

Oto przykład klucza o bardzo wysokiej jakości – 23 znakowego wygenerowanego z losowych ruchów myszką w programie VMPCrypt: QFZJw3UdecfTgHgnxxhphGr. Oczywiście zapamiętanie (lub utrwalenie) takiego klucza jest trudniejsze niż klucza typu „123”, ale jest to niewielki koszt w porównaniu z poziomem bezpieczeństwa, jaki dzięki niemu uzyskujemy.

Zastosowanie takiej jakości klucza daje gwarancję, że nasze dane są naprawdę bezpieczne i że nikt, nawet agencje rządowe dysponujące miliardami dolarów i potężnym sprzętem, nie będą w stanie złamać tego klucza i odczytać naszych danych.

Oczywiście siła szyfrowania jest niezależna od tego, czy sam algorytm szyfrowania jest jawny, czy nie. Siła szyfrowania tkwi bowiem tylko i wyłącznie w kluczu. Metody szyfrowania, które wymagają tajności algorytmu szyfrowania są bardzo niskiej jakości i należy ich unikać. Dlatego nawet odkrywca funkcji VMPC i autor szyfru VMPC nie będzie w stanie odszyfrować Twoich danych, jeśli utracisz klucz. Klucza należy zatem bardzo starannie pilnować. Utrata klucza oznacza jednoznacznie utratę wszystkich zaszyfrowanych nim danych. Jest to duża odpowiedzialność, ale także ogromna siła szyfrowania.

4. Szyfrowanie plików i folderów

Program VMPCrypt zapisuje zaszyfrowane pliki/foldery w jednym pliku archiwum (**szyfrowanie do archiwum**) lub dla każdego pliku tworzone mogą być osobne zaszyfrowane kopie źródłowych plików (**szyfrowanie osobno**).

Pliki archiwum są w pełni zaszyfrowane, nie zawierające żadnych jawnych danych, jak np. nagłówki. Zapewnia to najwyższy poziom bezpieczeństwa – po pliku archiwum nie można rozpoznać zawartości zaszyfrowanych tam plików, ich nazw, atrybutów, a nawet rozmiarów ani ilości plików w archiwum zapisanych. Co więcej, struktura pliku archiwum jest ze statystycznego punktu widzenia nieodróżnialna od struktury losowego ciągu danych. Dzięki temu możliwe jest ukrycie samego faktu użycia szyfrowania – zawsze możliwe jest bowiem twierdzenie, że dany plik wcale nie zawiera zaszyfrowanych danych, a jedynie serię pseudolosowych bajtów wygenerowanych w celach testów statystycznych.

Pliki archiwum można zapisywać w postaci archiwów samodeszyfrujących (w plikach typu EXE, a więc programach). Do zdeszyfrowania takiego archiwum wystarczy znajomość klucza, nie jest

natomiast potrzebny program VMPCrypt. Archiwum takie zawiera bowiem samo w sobie moduł deszyfrujący.

Pliki archiwum można automatycznie podzielić na dowolnej wielkości pliki składowe, np. na wypadek sytuacji, gdy duże archiwum chcemy nagrać na nośniki o małej pojemności (np. archiwum o rozmiarze 2 GB łatwo zmieści się na 3 płytach CD o pojemności 700 MB) .

Program zapewnia bardzo elastyczne możliwości wyboru – które pliki/foldery, czy całą zawartość folderów, czy tylko wybrane pliki/podfoldery chcemy zaszyfrować, zdeszyfrować lub zaktualizować w archiwum.

Przy szyfrowaniu plików osobno dla każdego pliku, np. "dane.txt", zostanie utworzona jego zaszyfrowana kopia, a do nazwy dodane rozszerzenie .vmpc (powstanie plik "dane.txt.vmpc"). Zaszyfrowane pliki pozostaną w tych samych folderach, co pliki źródłowe lub zostaną zapisane w nowym, wybranym przez użytkownika folderze.

4.1. Jak wybrać foldery / pliki do szyfrowania (lub wymazywania)

Aby zaszyfrować wybrany folder/foldery lub plik czy pliki, należy w lewej części głównego okna programu – widocznego bezpośrednio po uruchomieniu programu – wcisnąć przycisk „**Wybierz pliki**”.

4.1.1. Okno „Wybór Plików / Folderów”

Po wciśnięciu „**Wybierz pliki**” wyświetlone zostanie okno „**Wybór Plików / Folderów”** służące do przeglądania folderów i plików znajdujących się na dyskach lokalnych lub sieciowych. W oknie tym należy odszukać te foldery/pliki, które chcemy zaszyfrować. Aby wybrać dany folder/plik do szyfrowania, należy najechać na niego, a następnie wcisnąć przycisk „**Wybierz**”. Możliwe jest również – zamiast przycisku „Wybierz” – wciśnięcie Spacji na klawiaturze lub wciśnięcie prawego klawisza myszki i wybrania opcji „Wybierz”. Wszystkie te trzy drogi są równoważne i powodują wybranie podświetlonego folderu (folderów) lub pliku (plików) do głównego okna programu.

Aby zmienić lokalizację przeglądanych folderów możemy użyć przycisku „**Przeglądaj**” w górnej części okna lub wcisnąć Insert na klawiaturze. Lokalizację możemy także wpisać ręcznie w polu edycji znajdującym się w górnej części okna. Wybraną ostatnio lokalizację możemy zapamiętać wciskając przycisk „**Pamiętaj**”, a przy kolejnym uruchomieniu programu okno zostanie otwarte w tym folderze.

Aby zaznaczyć więcej niż jeden folder/plik za jednym razem, możemy klikać myszką na interesujące nas nazwy folderów/plików trzymając wciśnięty klawisz Ctrl lub Shift na klawiaturze.

Jeśli interesują nas tylko pliki określonego typu (np. tylko programy, a więc pliki z rozszerzeniem EXE (np. PROGRAM1.EXE), możemy skorzystać z filtra znajdującego się na dole okna. Wystarczy wpisać tam schemat, np. *.exe i wcisnąć Enter lub Tab, a w oknie znajdą się tylko pliki spełniające zadane kryterium (tu – tylko programy, a więc pliki z rozszerzeniem EXE). Wielkość liter w nazwach plików jest ignorowana (EXE = exe = ExE itp.). Jeśli pole obok wpisanego filtra nie jest zaznaczone, wówczas wyświetlone zostaną pliki, których nazwy nie spełniają kryterium filtra.

Przycisk **„vmpc”** ustawia filtr na pliki z rozszerzeniem „vmpc”, a więc zaszyfrowane osobno (patrz rozdz. 4.6). Użycie tego przycisku jest wygodne, jeśli chcemy wybrać te pliki do deszyfrowania. Po ich wybraniu możemy użyć przycisku „Deszyfruj osobno” (patrz rozdz. 6).

Przycisk **„nie vmpc”** ustawia filtr, aby wyświetlane były tylko pliki innego typu niż „vmpc”.

Przycisk **„brak”** ustawia filtr tak, aby wyświetlane były wszystkie pliki.

Jeśli chcemy wybrać wszystkie foldery/pliki znajdujące się w oknie, możemy użyć przycisku „**Wszystkie**” lub wcisnąć Ctrl + Spacja.

Przycisk „**Domyślny**” automatycznie dodaje domyślny folder deszyfrowania (patrz rozdz. 7.3.1), po czym jest on gotowy np. do wymazania. Można go zdefiniować podczas deszyfrowania archiwum.

Gdy wybraliśmy wszystkie foldery/pliki, które chcemy szyfrować – możemy wcisnąć „**Zamknij**” lub klawisz Esc lub prawy klawisz myszki → „Zamknij”.

4.1.2. Dalsze opcje wyboru plików / folderów

W chwili, gdy w głównym oknie programu mamy nazwy plików/folderów, które wybraliśmy przyciskiem „Wybierz pliki”, możemy dokładniej sprecyzować, które z tych plików/folderów czy też jaką część ich zawartości chcemy szyfrować. Do tego celu służą cztery przyciski znajdujące się poniżej listy plików/folderów (aby zaznaczyć więcej niż jeden plik/folder, możemy użyć klawiszy Ctrl lub Shift oraz lewego przycisku myszy).

Przycisk „**Odwołaj**” kwalifikuje podświetlone (wybrane) na liście foldery/pliki do zignorowania. Podczas szyfrowania (lub wymazywania) zostaną one pominięte.

Przycisk „**Wybierz**” kwalifikuje podświetlone (wybrane) na liście foldery/pliki do szyfrowania (lub wymazywania) – może być użyteczny po wcześniejszym użyciu przycisku „Odwołaj”.

Przycisk „**Odwołaj każdy**” kwalifikuje wszystkie widoczne na liście pliki/ foldery do zignorowania. Podczas szyfrowania czy usuwania zostaną one pominięte.

Przycisk „**Wybierz każdy**” kwalifikuje wszystkie widoczne na liście pliki/ foldery do szyfrowania.

Powyższe cztery przyciski dostępne są także w menu kontekstowym pod kursorem myszki po wciśnięciu prawego klawisza myszy na liście plików/folderów w głównym oknie programu.

Przycisk „**Wyczyść**”, znajdujący się po lewej stronie głównego okna programu czyści listę. Jeśli na liście znajdują się pliki/ foldery odwołane (zakwalifikowane do zignorowania przyciskiem „Odwołaj”), usuwa z listy tylko odwołane pliki/ foldery. W przeciwnym razie usuwa z listy wszystkie pliki/ foldery. Na plikach/folderach tych nie jest wykonywana żadna operacja dyskowa – ich nazwy jedynie usuwane są z listy.

4.2. Przygotowanie opcji szyfrowania plików / folderów do archiwum

Przed wciśnięciem przycisku „Szyfruj do archiwum” możemy ustawić, czy pliki przed szyfrowaniem mają zostać skompresowane oraz czy pliki po zaszyfrowaniu mają zostać wymazane z dysku.

4.2.1. Opcja „Kompresuj”

Opcję tę możemy zaznaczyć w dolnej części ekranu w głównym oknie programu. Jeśli opcja „**Kompresuj**” będzie zaznaczona, wówczas przed szyfrowaniem pliki zostaną skompresowane. Kompresja pozwala zmniejszyć objętość plików, ale jest operacją powolną i przy szyfrowaniu

dużych plików może to być uciążliwe. Zalecamy stosowanie kompresji tylko, jeśli uzyskanie jak najmniejszego pliku (plików) archiwum jest konieczne – np. gdy zaszyfrowane archiwum ma zostać przesłane przez Internet.

4.2.2. Opcja „Wymaż"

Opcję tę możemy zaznaczyć w dolnej części ekranu w głównym oknie programu. Jeśli opcja „**Wymaż**" będzie zaznaczona, wówczas po zaszyfrowaniu pliki zostaną wymazane z dysku. Samo usunięcie plików z Kosza z poziomu Windows jest tylko usunięciem logicznym i nie jest bezpieczne, ponieważ zawartości plików wciąż znajdują się na dysku i odpowiednim oprogramowaniem można te pliki odzyskać. Zamazanie plików jest realizowane poprzez zapisanie w miejsce ich oryginalnej zawartości nowych (pseudolosowych) danych. (Wymazanie pliku = fizyczne zamazanie zawartości pliku + logiczne usunięcie pliku). Po odkasowaniu wymazanego pliku atakujący odzyska jedynie pseudolosowe dane. Jeśli liczymy się z ryzykiem pracy z dyskiem w firmie wyspecjalizowanej w odzyskiwaniu danych, musimy uwzględnić fakt, że stopień namagnesowania powierzchni dysku jest – w pewnym stopniu – zależny od danych, które znajdowały się na dysku poprzednio. Dopiero wielokrotne zamazanie pliku rozmywa pierwotny stopień namagnesowania na tyle mocno, że odczytanie pierwotnych danych staje się niemożliwe. Do uzyskania maksymalnego poziomu bezpieczeństwa zalecamy stosowanie 10-krotnego zamazania (choć jest to operacja długotrwała, a w większości praktycznych zastosowań i scenariuszy zagrożeń wystarczy 1-krotne zamazanie). Wg niektórych źródeł (np. metoda Gutmanna) zaleca się stosowanie zamazywania nawet 35-krotnego. Liczbę rund wymazywania możemy ustawić w polu „**Liczba rund wymazywania**" w dolnej części głównego okna programu w zakresie od 0 do 99. 0 oznacza tylko logiczne usunięcie plików (bez wymazywania).

Generalną zasadą powinno być, że po zaszyfrowaniu oryginalne pliki powinny zostać wymazane z dysku. Trzymanie bowiem na dysku plików oryginalnych oraz ich kopii w postaci zaszyfrowanego archiwum z oczywistych względów mija się z celem (chyba że szyfrowaliśmy w celu przesłania danych). Stosując opcję wymazywania musimy być jednak ostrożni i upewnić się, że rzeczywiście posiadamy poprawny klucz, który po zaszyfrowaniu i wymazaniu plików/folderów pozwoli nam później te dane odszyfrować.

Algorytm szyfrowania plików/folderów programu VMPCrypt skonstruowany jest tak, że tylko pliki poprawnie zaszyfrowane zostają wymazane, jeśli opcja „Wymaż" jest zaznaczona. Jeśli w przypadku któregoś pliku nastąpi np. błąd odczytu, plik ten nie zostanie wymazany.

4.3. Rozpoczęcie szyfrowania – określenie klucza

Po wyborze plików/folderów do szyfrowania oraz określeniu, czy mają one zostać przed szyfrowaniem skompresowane, a po szyfrowaniu – wymazane – możemy przystąpić do szyfrowania wybranych plików/folderów. Możemy to zrobić wciskając przycisk „**Szyfruj do archiwum**" (który może zawierać dodatkowe napisy „Kompresuj" i/lub „Wymaż" – w zależności od naszego wyboru) lub „**Szyfruj osobno**".

Po jego wciśnięciu otwarte zostanie okno wprowadzenia klucza. Możemy wprowadzić tam klucz (hasło) z klawiatury i wcisnąć „**OK**". Poszczególne przyciski tego okna omówione są szczegółowo w rozdz. 7.1.1

Przycisk „**Utwórz losowy klucz**" w powyższym oknie pozwala wygenerować losowy klucz z przypadkowych ruchów muszką. Po jego wciśnięciu otwarty zostanie moduł generowania klucza, omówiony w rozdz. 11. Ogólne zasady generowania kluczy opisane są także w rozdz. 3.

Po wprowadzeniu klucza użytkownik zostanie poproszony o jego ponowne wprowadzenie w celu weryfikacji. Jeśli użytkownik jest całkowicie pewien, że wprowadził prawidłowy klucz, może zrezygnować z dodatkowej weryfikacji klucza i wcisnąć przycisk „**Nie weryfikuj**”.

Opcja „**Pamiętaj klucz**” określa, że raz wprowadzony klucz jest zapamiętywany, dzięki czemu można szyfrować i deszyfrować dane bez konieczności wprowadzania klucza za każdym razem. Klucz można później wymazać z pamięci przyciskiem "**Usuń klucz**".

4.4. Określenie parametrów tworzonego archiwum

Archiwum może się składać z jednego pliku lub z serii plików. Plik archiwum tworzony przez program VMPCrypt jest całkowicie nieodróżnialny od losowego ciągu danych – nie zawiera on żadnych niezaszyfrowanych danych, jak np. nagłówki. Wszystkie nagłówki archiwum także podlegają tu szyfrowaniu. Dzięki temu nie jest możliwe uzyskanie jakichkolwiek informacji o zawartości archiwum – nawet informacji o nazwach czy liczbie plików, jakie w archiwum zostały zapisane. Co więcej – ponieważ struktura pliku archiwum jest nieodróżnialna od losowego ciągu bajtów, można ukryć sam fakt użycia szyfrowania, zawsze można bowiem twierdzić np., że plik ten zawiera pseudolosowe dane wygenerowane dla celów badawczych.

Po zamknięciu okna weryfikacji klucza (rozdz. 4.3) pojawia się okno „**Zapis archiwum**”, w którym możemy określić nazwę archiwum, określić maksymalny rozmiar pojedynczego pliku archiwum, określić, czy ma powstać archiwum samodeszyfrujące oraz możemy wpisać tekst komentarza do archiwum. Po wyborze parametrów tworzonego archiwum możemy wcisnąć przycisk „**Szyfruj**”, po czym wybrane pliki/foldery zostaną zaszyfrowane (przed szyfrowaniem skompresowane, jeśli wybraliśmy taką opcję), po zaszyfrowaniu utworzone archiwum zostanie próbnie otwarte, aby ostatecznie upewnić się, czy operacja przebiegła poprawnie, wyświetlona zostanie szczegółowa informacja o utworzonym archiwum, a następnie – jeśli wybraliśmy taką opcję – te pliki/foldery, które zostały poprawnie zaszyfrowane i zapisane w archiwum, zostaną wymazane z dysku z wykorzystaniem wybranej wcześniej liczby rund wymazywania. W tym momencie operacja szyfrowania plików/folderów jest zakończona i wszystkie one znajdują się w postaci zaszyfrowanej w utworzonym pliku (plikach) archiwum.

4.4.1. Przyciski wyboru pliku

Przycisk „**Wybierz plik**” pozwala wybrać nazwę pliku dla tworzonego archiwum.

Przycisk „**Inny folder**” proponuje inny folder dla tworzonego archiwum. Foldery proponowane są z listy plików wybranych do szyfrowania.

Przycisk „**Nazwa + data**” dodaje do proponowanej nazwy pliku archiwum bieżącą datę i godzinę.

4.4.2. Opcja „Podziel archiwum na pliki wielkości”

Określa maksymalny rozmiar pojedynczego pliku tworzonego archiwum. Funkcja ta pozwala podzielić archiwum na pliki o określonym maksymalnym rozmiarze, np. takim, aby możliwe było ich nagranie na płyty CD/DVD czy dyskietki. Rozmiar możemy wpisać zarówno „ręcznie”, jak i wybrać z listy popularnych propozycji. Rozmiar podawany jest w megabajtach wg jednostek SI (1 MB to jeden milion bajtów). Jeśli powstanie więcej niż 1 plik danego archiwum (wybrany maksymalny rozmiar pojedynczego pliku archiwum (np. 700MB) będzie mniejszy niż rozmiar całego archiwum (np. 2 GB)), kolejne pliki archiwum tworzone będą wg schematu ARCH1.VMPAx, gdzie x=1,2,3,... (np. główny plik archiwum: ARCH1.VMPA, a pozostałe: ARCH1. VMPA1, ARCH1. VMPA2,...) Podczas otwierania archiwum (przycisk "Otwórz

archiwum" w głównym oknie programu) wszystkie pliki archiwum wieloplikowego muszą znajdować się w tym samym folderze, co wybrany główny plik archiwum.

4.4.3. Opcja „Archiwum samodeszyfrujące (exe)”

Określa, czy tworzone jest archiwum samodeszyfrujące. Archiwum takie ma postać programu (pliku typu EXE) i nie wymaga programu VMPCrypt do jego zdeszyfrowania. Po uruchomieniu, archiwum samodeszyfrujące (np. ARCH1.EXE) prosi o podanie klucza (kluczy), po czym możliwe jest deszyfrowanie wybranych folderów/plików. Archiwum samodeszyfrujące zapewnia taki sam poziom bezpieczeństwa kryptograficznego, jak zwykłe archiwum. Archiwum samodeszyfrujące może być wieloplikowe. Wszelkie operacje na archiwum samodeszyfrującym (jak deszyfrowanie, patrz rozdz. 7, czy aktualizacja zawartości, patrz rozdz. 8) jest możliwa tak samo, jak dla zwykłych archiwów.

Archiwa samodeszyfrujące są wygodne jeśli chcemy np. przesłać zaszyfrowane pliki/foldery pocztą elektroniczną, czy przekazać w inny sposób, osobie, która nie posiada programu VMPCrypt. Do zdeszyfrowania takiego archiwum wystarczy bowiem samo podanie prawidłowego klucza, a procedury deszyfrujące zapisane są w samym archiwum.

Jeśli opcja ta nie jest zaznaczona, program utworzy standardowe archiwum – plik typu VMPA.

4.4.4. Opcja „Pamiętaj oryginalne lokalizacje plików”

Określa, czy w archiwum zapamiętane zostaną oryginalne lokalizacje plików/folderów wybranych do szyfrowania. Po zaznaczeniu tej opcji będzie możliwe wybranie opcji automatycznego deszyfrowania plików do ich oryginalnej lokalizacji. Zaznaczenie tej opcji jest polecane przy tworzeniu szyfrowanych kopii zapasowych plików na jednym komputerze. Do przesyłania zaszyfrowanych plików na inne komputery zaleca się nie zaznaczanie tej opcji - pozwala to uzyskać wyższy poziom poufności - osoba deszyfrująca dane nie będzie widziała, z jakich folderów zostały pobrane zaszyfrowane pliki.

4.4.5. Okno „Komentarz”

Okno to umożliwia dodanie opcjonalnego tekstu komentarza do tworzonego archiwum. W komentarzu możemy zawrzeć dowolne dodatkowe informacje tekstowe dotyczące tworzonego archiwum, jak np. krótki opis jego zawartości. Treść komentarza jest szyfrowana. Komentarz może pozostać pusty. Komentarz będzie widoczny po otwarciu utworzonego archiwum (patrz rozdz. 7.1).

4.5. Wysyłanie utworzonego archiwum pocztą elektroniczną

Po utworzeniu archiwum możemy je w łatwy sposób wysłać pocztą elektroniczną. Wystarczy w tym celu wcisnąć przycisk „**Otwórz archiwum**” po lewej stronie głównego okna programu, na liście odnaleźć nazwę utworzonego archiwum i na nim wcisnąć prawy klawisz myszki. Pojawi się standardowe menu kontekstowe systemu Windows, na którym wystarczy wybrać Wyślij do → Adresat poczty. Utworzona zostanie wiadomość email z automatycznie załączonym plikiem archiwum.

Jeśli tworzyliśmy archiwum wieloplikowe, wówczas należy zmienić filtr w dolnej części okna przeglądania plików na „Wszystkie pliki” i dołączyć także pozostałe pliki archiwum (mające rozszerzenia VMPA1, VMPA2,....).

4.5.1. Blokowanie załączników email w systemie Windows

Niektóre programy pocztowe blokują przesyłanie załączników w postaci plików wykonywalnych (EXE), co może utrudnić przesyłanie emailem archiwów samodeszyfrujących. Prostym sposobem uniknięcia tej blokady jest ręczna zmiana nazwy pliku z np. arch.exe na arch.exe1 – pliki z rozszerzeniem innym niż „exe" nie powinny być blokowane. Po otrzymaniu pliku należy zmienić jego nazwę z powrotem na arch.exe i uruchomić.

4.6. Szyfrowanie plików osobno

Opcja ta tworzy dla każdego pliku jego zaszyfrowaną kopię.

Po wybraniu plików na listę plików (używając przycisku „**Wybierz pliki**", rozdz. 4.1) wciskamy przycisk „**Szyfruj osobno**". Pojawia się okno wprowadzenia klucza (rozdz. 4.3). Wszystkie pliki zostaną zaszyfrowane tym samym kluczem.

Dla każdego pliku, np. dane.txt, jego zaszyfrowana kopia zostanie zapisana w pliku z dodatkowym rozszerzeniem .vmpc (dane.txt.vmpc).

Jeśli zaznaczymy opcję „**do innego folderu**", będziemy mogli wybrać folder, w którym zaszyfrowane kopie plików zostaną zapisane.

4.7. Obliczanie sumy kontrolnej plików

Do obliczenia sumy kontrolnej plików znajdujących się na liście służy przycisk „**Suma kontrolna**". Kolejność plików nie ma znaczenia. Jeśli którykolwiek bit któregokolwiek pliku ulegnie zmianie, wartość sumy kontrolnej będzie całkowicie inna. Funkcja ta umożliwia sprawdzenie, czy pliki nie zostały uszkodzone. Suma kontrolna jest "odciskiem palca" (funkcją hashującą) wybranych plików obliczoną algorytmem VMPC-MAC.

5. Wymazywanie plików / folderów

Możliwe jest używanie programu VMPCrypt tylko do wymazywania plików/folderów z dysku. Gdy chcemy trwale i bezpiecznie pozbyć się jakichś plików/folderów lub gdy chcemy je ręcznie wymazać po ich zaszyfrowaniu, wówczas możemy skorzystać z przycisku „**Wymaż**", znajdującego się w dolnej części głównego okna programu.

Aby wybrać pliki/foldery, które chcemy wymazać, możemy użyć przycisku „**Wybierz pliki**" po lewej stronie głównego okna programu, a następnie wybrać te pliki/foldery, które chcemy wymazać. Bardziej szczegółowe instrukcje – jak wybierać pliki/foldery znajduje się w rozdz. 4.1.1 oraz rozdz. 4.1.2.

Po wybraniu plików/folderów do wymazania możemy określić ilokrotnie pierwotna zawartość plików zostanie zamazana – określić „**Liczbę rund wymazywania**", zgodnie z zaleceniami zawartymi w rozdz. 4.2.2.

Następnie wystarczy wcisnąć przycisk „Wymaż" i wybrane pliki/foldery zostaną wymazane z dysku. Należy pamiętać, że po operacji wymazania odzyskanie pierwotnych plików nie jest możliwe żadnymi metodami programowymi, a przy zastosowaniu odpowiednio większej liczby rund wymazywania (np. 3,5 czy 10 – w zależności od stopnia zaawansowania aparatury, jaką może dysponować atakujący, który chce odzyskać nasze dane) żadnymi metodami, nawet z wykorzystaniem specjalistycznej aparatury do fizycznej analizy powierzchni dysków.

6. Deszyfrowanie plików szyfrowanych osobno

W celu wybrania plików do deszyfrowania osobno należy użyć przycisku „**Wybierz pliki**”, (rozdz. 4.1). Następnie wciskamy przycisk „**Deszyfruj osobno**”. Pojawia się okno wprowadzenia klucza (rozdz. 4.3). Następnie pojawia się okno wyboru nowego folderu dla szyfrowanych plików (jeśli zaznaczyliśmy opcję „do innego folderu”). Możemy wybrać, w jakim folderze zapisane zostaną odszyfrowane pliki. Jeśli chcemy, żeby pliki odszyfrowane pozostały w tych samych folderach, w których znajdują się pliki zaszyfrowane, wciskamy „Anuluj” w oknie wyboru folderu lub odznaczamy opcję „do innego folderu”.

Dla każdego zaszyfrowanego pliku, np. dane.txt.vmpc, jego odszyfrowana kopia zostanie zapisana w pliku bez rozszerzenia .vmpc (dane.txt).

Dla każdego pliku obliczana jest suma kontrolna MAC. Jeśli w pliku zmianie uległ choć jeden bajt (np. w wyniku błędu transmisji danych lub celowego wrogiego działania), suma kontrolna MAC wykryje to i zostanie wyświetlony komunikat o błędzie. Jeśli zatem po odszyfrowaniu plików komunikat o błędzie nie został wyświetlony, możemy mieć pewność, że pliki po odszyfrowaniu mają dokładnie taką samą postać, jaką miały przed zaszyfrowaniem.

7. Deszyfrowanie plików / folderów zapisanych w archiwum

Aby zdeszyfrować wybrane pliki/foldery zapisane w pliku (lub plikach) archiwum musimy najpierw otworzyć archiwum – jest to możliwe tylko po podaniu prawidłowego klucza – a następnie wybrać, które pliki/foldery chcemy deszyfrować, po czym rozpocząć deszyfrowanie.

7.1. Otwarcie archiwum

Do otwarcia archiwum służy przycisk „**Otwórz archiwum**” znajdujący się po lewej stronie głównego okna programu. Po jego wciśnięciu pokazane zostaje systemowe okno przeglądania plików. Z listy możemy wybrać archiwum, które chcemy otworzyć. Po wybraniu archiwum wyświetlone zostanie okno „Wprowadzenie klucza”, w którym użytkownik zostanie poproszony o podanie klucza do otwieranego archiwum.

7.1.1. Okno „Wprowadzenie klucza”

W górnej części okna znajduje się pole edycji klucza, w którym możemy wpisać klucz „ręcznie”. Poniżej znajduje się przycisk „**Wczytaj klucz**”, który pozwala wybrać plik klucza (np. z Pen-Drive’a), zapisany wcześniej przyciskiem „Zapisz klucz” (patrz rozdz. 11.6).

Przycisk „**Zapisz klucz**” pozwala zapisać wprowadzony klucz do pliku. Szczegółowe omówienie zapisywania kluczy do plików znajduje się w rozdziale 11.6.

Po wprowadzeniu klucza – jeśli chcemy się upewnić, czy wpisaliśmy go poprawnie, możemy wcisnąć przycisk „**Zoom klucza**”, który wyświetli nam wprowadzony klucz w powiększeniu w formacie graficznym.

Przycisk „**Wyczyść**” wymazuje wpisywany aktualnie klucz w polu edycji klucza.

Opcja „**Pokaż klucz**”, znajdująca się w prawej części okna określa, czy wprowadzany klucz ma być pokazany na ekranie. Domyślnie klucz nie jest pokazywany, co po pierwsze pozwala na zachowanie większej poufności.

Przycisk „**Anuluj**” służy do rezygnacji z otwarcia archiwum – po jego wciśnięciu wszystkie dane zawierające wprowadzany klucz w pamięci RAM komputera są zamazywane i okno wprowadzenia klucza zostaje zamknięte.

Opcja „**Pamiętaj klucz**” określa, że raz wprowadzony klucz jest zapamiętywany, dzięki czemu można szyfrować i deszyfrować dane bez konieczności wprowadzania klucza za każdym razem. Klucz można później wymazać z pamięci przyciskiem "**Usuń klucz**".

Po wprowadzeniu klucza możemy wcisnąć przycisk „**Otwórz do deszyfrowania**”, który oznacza akceptację wprowadzonego klucza. Po jego wciśnięciu program spróbuje zdeszyfrować nagłówek archiwum oraz blok nazw plików. Jeśli ich sumy kontrolne MAC będą prawidłowe, wówczas archiwum zostanie otwarte. Jeśli suma kontrolna MAC nie będzie prawidłowa, wówczas użytkownik zostanie poproszony o ponowne wprowadzenie klucza (zwykle błąd MAC wynika z podania nieprawidłowego klucza).

Jeśli do szyfrowania archiwum użytych było wiele kluczy (wykorzystany został przycisk „Kolejny klucz”, wówczas po podaniu jednego z kluczy możemy wcisnąć przycisk „**Kolejny klucz**”, po czym wprowadzić kolejny klucz. Po wprowadzeniu ostatniego klucza należy wcisnąć przycisk „Otwórz do deszyfrowania”. Kolejność wprowadzania kluczy jest dowolna.

Archiwa tworzone przez program VMPCrypt posiadają **dwie kopie** zarówno nagłówka, jak i bloku nazw plików. Mechanizm ten ma na celu zabezpieczenie archiwum na bardzo rzadkie – hipotetyczne – sytuacje, gdy archiwum zostanie fizycznie uszkodzone (np. w wyniku ewentualnych błędów dyskowych). Jeśli błąd MAC pojawia się w jednej kopii, czy to nagłówka, czy bloku nazw plików, program spróbuje odczytać i zdeszyfrować jego drugą kopię. Mechanizm ten pozwolić może otworzyć archiwum nawet w sytuacji awarii dysku i powstania na nim lokalnych błędów.

Podczas otwierania archiwum **zawsze obie** kopie nagłówka oraz bloku nazw plików są odczytywane i deszyfrowane. Jeśli archiwum dało się otworzyć, ale jedna z kopii została uszkodzona, wówczas program także wyświetli odpowiednie ostrzeżenie i zaleci zaktualizowanie archiwum. Operacja aktualizacji, omówiona w rozdz. 8, odtwarza obie kopie nagłówka oraz obie kopie bloku nazw plików i zapisuje je na nowo w archiwum.

Obie kopie nagłówka oraz bloku nazw plików zaszyfrowane są innym wektorem inicjującym, dzięki czemu za każdym razem mają losowo („całkowicie”) inną postać w formie zaszyfrowanej.

7.1.2. Dwa sposoby otwierania archiwów samodeszyfrujących

Archiwa samodeszyfrujące (w plikach EXE), omówione w rozdz. 4.4.3 możemy otwierać do deszyfrowania w zwykły sposób, omawiany w rozdz. 7.1, oraz bezpośrednio – uruchamiając plik archiwum jak zwykłą aplikację w systemie Windows. Po uruchomieniu pliku archiwum automatycznie otwarte zostanie okno wprowadzenia klucza, omówione w rozdz. 7.1.1, a dalsza procedura deszyfrowania plików/folderów zarówno w archiwum zwykłym, jak i samodeszyfrującym jest taka sama i jest omówiona w rozdz. 7.2 i 7.3.

7.2. Wybór plików / folderów do deszyfrowania

Po otwarciu archiwum, omówionym w rozdz. 7.1, na liście w głównym oknie programu wyświetlone zostaną wszystkie pliki oraz foldery znajdujące się w zaszyfrowanym archiwum.

Przeglądać strukturę folderów możemy w standardowy sposób – klikając podwójnie lub wciskając Enter na folderze, do którego chcemy wejść. Jeśli chcemy wyjść o poziom wyżej w

strukturze folderów – kliknijmy na dwie kropki znajdujące się na samej górze listy lub strzałkę wstecz.

7.2.1. Dalsze opcje wyboru plików / folderów do deszyfrowania

W chwili, gdy w głównym oknie programu mamy wyświetlone nazwy plików/folderów, które znajdują się w zaszyfrowanym archiwum, możemy dokładniej sprecyzować, które z tych plików/folderów czy też jaką część ich zawartości chcemy zdeszyfrować. Do tego celu służą cztery przyciski znajdujące się poniżej listy plików/folderów (aby zaznaczyć więcej niż jeden folder/plik, możemy użyć klawiszy Ctrl lub Shift oraz lewego przycisku myszy).

Przycisk „**Wybierz**” kwalifikuje podświetlone (wybrane) na liście foldery/pliki do deszyfrowania.

Przycisk „**Odwołaj**” odwołuje zakwalifikowanie podświetlonych (wybranych) na liście folderów/plików do deszyfrowania.

Przycisk „**Wybierz każdy**” kwalifikuje wszystkie widoczne na liście pliki/foldery do deszyfrowania.

Przycisk „**Odwołaj każdy**” odwołuje zakwalifikowanie wszystkich widocznych na liście plików/folderów do deszyfrowania.

Powyższe cztery przyciski dostępne są także w menu kontekstowym pod kursorem myszki po wciśnięciu prawego klawisza myszy na liście plików/folderów w głównym oknie programu.

7.3. Rozpoczęcie deszyfrowania wybranych plików / folderów

Po wybraniu tych plików/folderów, które chcemy zdeszyfrować, możemy wcisnąć przycisk „**Deszyfruj**”, znajdujący się w dolnej części głównego okna programu. Po jego wciśnięciu wyświetlone zostanie okno wyboru lokalizacji dla deszyfrowanych plików/folderów.

7.3.1. Okno „Wybierz lokalizację dla deszyfrowanych plików”

W oknie tym określamy, gdzie (w jakich folderach i na jakich dyskach) mają zostać zapisane pliki/foldery po zdeszyfrowaniu.

Opcja „**Deszyfruj do oryginalnych lokalizacji**” dostępna jest, gdy podczas szyfrowania zaznaczona została opcja „Pamiętaj oryginalne lokalizacje plików” (rozdz. 4.4.4). Określa, że pliki/ foldery po zdeszyfrowaniu zapisane zostaną w dokładnie tych samych lokalizacjach (na tych samych dyskach i w tych samych folderach), z których zostały zaszyfrowane. Opcja ta może być użyteczna gdy pracujemy na jednym komputerze i w zaszyfrowanych archiwach trzymamy pewne pliki/foldery, które mają swoje „stałe” miejsce, np. C:\MOJE DOKUMENTY\POUFNE”. Po wybraniu opcji „Deszyfruj do oryginalnych lokalizacji” nie będziemy musieli podawać żadnych dodatkowych parametrów, a pliki/foldery z archiwum zostaną zapisane w ich oryginalnych lokalizacjach – a więc tam, gdzie znajdowały się przed szyfrowaniem.

Jaka jest oryginalna lokalizacja danego pliku/folderu w archiwum możemy w każdej chwili odczytać w prawej kolumnie „Lokalizacja” na liście plików/folderów w głównym oknie programu. Oczywiście interesuje nas nadrzędna lokalizacja, a więc ta wyświetlona bezpośrednio po otwarciu archiwum.

Opcja „**Deszyfruj do folderu:**” określa, że foldery/pliki po zdeszyfrowaniu zapisane zostaną w wybranej przez użytkownika lokalizacji (w wybranym folderze na wybranym dysku). Struktura podfolderów zostanie zachowana, a wybrana lokalizacja będzie folderem nadrzędnym dla deszyfrowanych folderów/plików. Innymi słowy oryginalna lokalizacja (wyświetlona w prawej

kolumnie listy plików/folderów bezpośrednio po otwarciu archiwum) zostanie zastąpiona lokalizacją wpisaną przez użytkownika. Domyślnie proponowaną lokalizacją jest podfolder „**Deszyfr**” folderu, w którym znajduje się plik archiwum.

Nową lokalizację możemy albo wpisać „ręcznie” w polu edycji znajdującym się w centralnej części okna, jak i wybrać z istniejącego w systemie drzewa folderów – po wciśnięciu przycisku „**Wybierz folder**”. Jeśli wpisaliśmy „ręcznie” nazwę nieistniejącego folderu, folder ten zostanie automatycznie utworzony. Może to być także folder zagnieżdżony. (wymagający utworzenia także folderów dla niego nadrzędnych).

Możemy skorzystać także z opcji „**Do domyślnego folderu**”. Określa ona, że pliki/foldery po zdeszyfrowaniu zapisane zostaną w domyślnym folderze deszyfrowania. Aby go zdefiniować, możemy użyć przycisku „**Zapamiętaj domyślny”**.

Jeśli zaznaczona będzie opcja „**Otwórz folder po deszyfrowaniu**”, automatycznie otwarty zostanie folder, w którym zapisano zdeszyfrowane pliki.

Po określeniu lokalizacji, wystarczy wcisnąć przycisk „**Deszyfruj**”, aby rozpocząć deszyfrowanie wybranych plików/folderów.

Jeśli po zdeszyfrowaniu wybranych plików/folderów pokazany zostanie komunikat „MAC: OK...”, wówczas możemy być pewni, że wybrane pliki/foldery zostały zdeszyfrowane całkowicie poprawnie. Jeśli podczas deszyfrowania wystąpią błędy (np. wskutek uszkodzenia archiwum), będą one komunikowane na bieżąco podczas deszyfrowania.

7.4. Wyświetlenie informacji o archiwum

W czasie, gdy archiwum jest otwarte w dolnej części ekranu w głównym oknie programu znajduje się przycisk „**Info archiwum**”, który służy do wyświetlenia szczegółowych informacji dotyczących otwartego archiwum.

7.5. Zamknięcie archiwum

Zamknąć otwarte archiwum możemy wciskając przycisk „**Zamknij**”, znajdujący się po lewej stronie głównego okna programu. Wszystkie dane zawierające klucz, nazwy plików, dane archiwum w pamięci komputera zostają zamazane i program wraca do stanu początkowego – gotowości do szyfrowania/wymazywania nowych plików/folderów lub otwarcia archiwum.

8. Aktualizacja zawartości archiwum i zmiana klucza

Program VMPCrypt oferuje elastyczne możliwości aktualizacji zwartości istniejących archiwów – dodawania nowych plików/folderów do archiwum, usuwania z archiwum wybranych plików/folderów, przepisywania wybranych plików/folderów (zastępowanie tych znajdujących się w archiwum nowymi o tych samych nazwach, odczytanymi z dysku) oraz zmiany klucza szyfrującego archiwum.

Aby rozpocząć aktualizację archiwum, należy najpierw archiwum otworzyć – przyciskiem „**Otwórz archiwum**” w głównym oknie programu, a następnie wprowadzić klucz i wcisnąć „**Otwórz do aktualizacji**”. Szczegółowo procedura otwierania archiwum została omówiona w rozdz. 7.1.

Po otwarciu archiwum w głównym oknie programu mamy wyświetlone nazwy plików/folderów, które znajdują się w zaszyfrowanym archiwum.

Jeśli chcemy **dodać do archiwum nowe pliki/foldery**, możemy użyć przycisku „**Wybierz pliki**” i wybrać te pliki/foldery, które chcemy dodać do archiwum. Dokładniej działanie tego przycisku zostało omówione w rozdz. 4.1.1.

Przy pomocy czterech przycisków znajdujących się poniżej listy plików/folderów możemy dokładniej sprecyzować, jakie operacje na wybranych plikach/folderach chcemy wykonać. (aby zaznaczyć więcej niż jeden folder/plik, możemy użyć klawiszy Ctrl lub Shift oraz lewego przycisku myszy).

Przycisk „**Przepisz**” kwalifikuje podświetlone (wybrane) na liście foldery/pliki do zastąpienia nowymi folderami/plikami o tych samych lokalizacjach i nazwach, odczytanymi z dysku. Funkcja ta dostępna jest, gdy podczas szyfrowania zaznaczona została opcja „Pamiętaj oryginalne lokalizacje plików” (rozdz. 4.4.4).

Funkcja ta jest użyteczna, gdy np. zdeszyfrowaliśmy pliki, zmieniliśmy ich zawartość i chcemy, aby pliki te ponownie trafiły do archiwum w już zmienionej formie i zastąpiły znajdujące się w archiwum „stare” wersje tych plików.

Funkcji „Przepisz” możemy także używać, jeśli tylko część plików z danego folderu w archiwum była zdeszyfrowana i uległa zmianie. Możemy, nie bacząc na to, które pliki z danego folderu deszyfrowaliśmy, zakwalifikować cały folder do przepisania. Program wprawdzie zaznaczy całą zawartość folderu do przepisania, ale algorytm aktualizacji działa tak, że jeśli plik/folder zakwalifikowany do przepisania nie znajduje się na dysku (nie można go odczytać z dysku), wówczas jest on kopiowany ze starego archiwum do nowego (do archiwum po aktualizacji).

Przycisk „**Usuń**” kwalifikuje podświetlone (wybrane) na liście pliki/foldery do usunięcia z archiwum. Jeśli pliki/ foldery te były dodane do archiwum przyciskiem „Wybierz pliki”, przycisk „Usuń” kwalifikuje je do zignorowania (nie zostaną dodane do archiwum po wciśnięciu przycisku „Aktualizuj”.

Przyciski „**Odwołaj**” i „**Odwołaj każdy**” odwołują zakwalifikowanie podświetlonych (wybranych) (przycisk „Odwołaj”) lub wszystkich widocznych (przycisk „Odwołaj każdy”) na liście plików/ folderów do zastąpienia, usunięcia lub zignorowania nowo dodanych.

Powyższe cztery przyciski dostępne są także w menu kontekstowym pod kursorem myszki po wciśnięciu prawego klawisza myszy na liście plików/folderów w głównym oknie programu.

W czasie, gdy archiwum jest otwarte w dolnej części ekranu w głównym oknie programu znajduje się przycisk „**Info archiwum**”, który służy do wyświetlenia szczegółowych informacji dotyczących otwartego archiwum.

Podobnie, jak w przypadku tworzenia archiwum, mamy możliwość wymazania oryginalnych plików odczytanych z dysku po ich poprawnym zapisaniu do archiwum i poprawnym zakończeniu całej procedury aktualizacji archiwum. Wystarczy w tym celu zaznaczyć opcję „**Wymaż**” znajdującą się w dolnej części głównego okna programu oraz określić liczbę rund wymazywania – w prawej dolnej części okna. Opcja wymazywania dotyczy plików/folderów dodawanych do archiwum (przyciskiem „Wybierz pliki”) oraz przepisywanych w archiwum (przycisk „Przepisz”). Dokładny opis funkcji wymazywania znajduje się w rozdz. 4.2.2.

Jeśli chcemy zmienić klucz szyfrujący archiwum, zaznaczamy opcję „**Zmień klucz**” znajdującą się obok przycisku „Aktualizuj”.

Po określeniu, jakie operacje na zawartości archiwum chcemy wykonać, możemy wcisnąć przycisk „**Aktualizuj**”, po czym wyświetlone zostanie okno „**Zapis archiwum**” służące do określenia parametrów archiwum. Okno to zostało omówione w rozdz. 4.4. Możemy w tym miejscu w oknie tym dokonać dodatkowych zmian archiwum – jak np. zmienić maksymalny

rozmiar pojedynczego pliku archiwum, zmienić nazwę pliku archiwum, określić, czy archiwum ma być samodeszyfrujące oraz możemy dodać/zmienić tekst komentarza.

Po określeniu parametrów archiwum w oknie „Zapis archiwum” (lub pozostawieniu ich bez zmian) możemy wcisnąć przycisk „**Aktualizuj**”. Wybrane zmiany zostaną wprowadzone do archiwum.

Zamknąć otwarte archiwum możemy wciskając przycisk „**Zamknij**”, znajdujący się po lewej stronie głównego okna programu, patrz rozdz. 7.5.

8.1. Sposób działania Aktualizacji archiwum

Opcja aktualizacji archiwum jest operacją wrażliwą. Jeśli podczas aktualizacji archiwum nastąpiłaby awaria, np. zanik napięcia w sieci elektrycznej, istniałoby ryzyko, że archiwum zostanie utracone – zapis jego zawartości zostanie zatrzymany w przypadkowym miejscu, przez co plik archiwum miałby nieprzewidywalną strukturę (awaria może nastąpić w każdej chwili) i otwarcie archiwum oraz zdeszyfrowanie plików mogłoby się okazać niemożliwe.

Mechanizm zastosowany w programie VMPCrypt zabezpiecza operację aktualizacji archiwum przed ewentualnymi awariami. Tym samym – jeśli podczas aktualizacji archiwum nastąpi np. zanik napięcia – zawsze będziemy mieli dostęp albo do archiwum „starego” – sprzed aktualizacji oraz do plików, które miały zostać do archiwum dodane lub w archiwum przepisane, albo do archiwum nowego, już w pełni zaktualizowanego.

Jeśli nazwa archiwum nie ulega zmianie, proces aktualizacji tworzy nowe tymczasowe archiwum o nazwie wg schematu ~~ARCH.VMPA, gdzie ARCH.VMPA jest nazwą pliku oryginalnego archiwum. Następnie kopiuje do tego tymczasowego archiwum zawartość oryginalnego archiwum wprowadzając żądane modyfikacje. Po zakończeniu aktualizacji powodzeniem nazwa oryginalnego archiwum jest zmieniana na nazwę wg schematu ~ARCH.VMPA i za zgodą użytkownika archiwum oryginalne jest usuwane z dysku. Nazwa archiwum tymczasowego (~~ARCH.VMPA) jest zmieniana na nazwę oryginalnego archiwum (ARCH.VMPA). Mechanizm ten zabezpiecza archiwum na wypadek awarii zasilania podczas aktualizacji. Jeśli awaria taka nastąpi, oryginalne archiwum będzie wciąż znajdowało się na dysku.

Jeśli zaznaczono opcję „Wymaż”, tylko te pliki, które udało się pomyślnie zapisać do archiwum zostaną wymazane.

8.2. Skasowanie całego archiwum

Jeśli chcemy skasować całe archiwum, możemy – po jego otwarciu – wcisnąć przycisk „**Skasuj**” znajdujący się w dolnej części głównego okna programu. Zostaniemy wówczas zapytani o potwierdzenie operacji, po czym archiwum może zostać skasowane. W przeciwieństwie do szyfrowanych plików, zawierających jawne informacje, wymazywanie archiwum z dysku nie jest konieczne, ponieważ zawiera ono tylko zaszyfrowane dane. Przycisk „**Skasuj**” powoduje zatem zwykłe logiczne usunięcie z dysku otwartego pliku archiwum (wraz z ewentualnymi pozostałymi plikami wchodzącymi w skład tego archiwum, jeśli archiwum jest wieloplikowe – patrz rozdz. 4.4.2). Jeśli jednak obawiamy się, że klucz szyfrujący archiwum mógł zostać ujawniony, archiwum lepiej będzie wymazać niż tylko skasować.

9. Szyfrowanie tekstów

Aby przejść w tryb szyfrowania/deszyfrowania tekstów możemy wcisnąć przycisk „**Teksty**”. Na ekranie pojawi się wówczas pole bezpiecznego edytora tekstów (nie tworzącego plików tymczasowych i trzymającego edytowaną treść tylko w pamięci RAM komputera) oraz zestaw przycisków służących do wysyłania tekstów pocztą elektroniczną, jak i przyciski do zapisywania lub wczytywania tekstów z plików tekstowych i szyfrowanych książek.

Do trybu pracy z plikami/folderami możemy powrócić w każdej chwili wciskając przycisk „**Pliki**”.

9.1. Wysyłanie zaszyfrowanej wiadomości

Aby wysłać zaszyfrowaną wiadomość pocztą elektroniczną wystarczy – po wpisaniu tekstu wiadomości w polu edytora tekstów – wcisnąć przycisk „**Email**”, a następnie „**Szyfruj**”. Po jego wciśnięciu program otwiera okno wprowadzenia klucza (zobacz rozdz. 4.3), a następnie szyfruje całą zawartość okna edycji tekstu przy użyciu wprowadzonego klucza. Zaszyfrowany tekst jest automatycznie zamieniany na standardowy system zapisu tekstowego Base64, który zastępuje znaki niezrozumiałe dla edytorów tekstowych znakami podstawowymi (A..Z, a..z, 0..9, +/=), co umożliwia bezpośrednie przesłanie zaszyfrowanego tekstu w wiadomości email. Zaszyfrowana wiadomość jest automatycznie kopiowana do schowka systemowego oraz uruchamiany jest domyślny program pocztowy. Podczas edycji wiadomości w programie pocztowym po użyciu klawiszy Ctrl + V lub prawego klawisza myszki i opcji „Wklej”, zaszyfrowany tekst znajdzie się automatycznie w wiadomości email.

9.2. Deszyfrowanie otrzymanej zaszyfrowanej wiadomości

Aby zdeszyfrować zaszyfrowaną wiadomość, musimy tekst wiadomości przenieść do programu VMPCrypt, np. przy pomocy schowka systemowego. W tym celu, np. w programie pocztowym, należy na tekście zaszyfrowanej wiadomości wcisnąć Ctrl + A (zaznacz wszystko), a następnie Ctrl + C (kopiuj) lub w menu kontekstowym, dostępnym po wciśnięciu prawego klawisza myszki na tekście wiadomości, wybrać najpierw „Zaznacz wszystko”, a następnie „Kopiuj”.

Po wykonaniu tej czynności tekst zaszyfrowanej wiadomości znajduje się w schowku systemowym i teraz w programie VMPCrypt wystarczy wcisnąć przycisk „Email”, a następnie „Deszyfruj”, aby wiadomość zdeszyfrować i wyświetlić w oknie edycji tekstu.

Oczywiście zanim wiadomość zostanie zdeszyfrowana, zostaniemy poproszeni o wprowadzenie klucza lub kluczy (wpisanie klucza z klawiatury lub, używając przycisku „Wczytaj klucz”, wczytać klucz z pliku), oraz wciśnięcie „OK”. Szczegółowy opis procedury wprowadzania klucza znajduje się w rozdz. 7.1.1.

Po wprowadzeniu klucza wiadomość zostanie zdeszyfrowana. Obliczona zostanie także suma kontrolna MAC deszyfrowanego tekstu. Jeśli suma kontrolna MAC jest nieprawidłowa, a tekst wygląda „chaotycznie”, najprawdopodobniej został użyty nieprawidłowy klucz. Jeśli suma MAC jest błędna, a tekst wygląda na prawidłowy, oznacza to, że w tekście zaszły niewielkie zmiany – został on np. zakłócony podczas transmisji. Jeśli treść tekstu jest bardzo precyzyjna (np. zawiera liczby) wówczas w takiej sytuacji powinniśmy poprosić nadawcę o ponowne przesłanie wiadomości. Nie wiemy bowiem, gdzie w wiadomości nastąpiło przekłamanie ani czy nie było celowym działaniem wrogiej strony.

Jeśli natomiast po zdeszyfrowaniu wiadomości wyświetlony zostanie komunikat „MAC: OK...”, możemy mieć pewność, że tekst został prawidłowo zdeszyfrowany co do jednego znaku.

9.3. Tryb szyfrowanego czata

Tryb szyfrowanego czata jest wygodny, jeśli chcemy przesyłać zaszyfrowane wiadomości na czacie lub przez komunikator jak np. gadu-gadu. Tryb ten można uruchomić przyciskiem „**Czat**". W trybie tym raz wprowadzony klucz jest zapamiętywany, dzięki czemu można szyfrować i deszyfrować teksty jednym przyciskiem (Szyfruj / Deszyfruj) bez konieczności wprowadzania klucza za każdym razem. Po zakończeniu sesji czata użyj przycisku "Usuń klucz" , aby wymazać zapamiętany klucz z pamięci.

9.4. Dodatkowe funkcje edycji i szyfrowania tekstów

9.4.1. Szyfrowanie tekstu

Możemy wykorzystać program VMPCrypt także do samego zaszyfrowania wiadomości tekstowej (bez jej wysyłania). Do tego celu służy przycisk „**Szyfruj**". Powoduje on wyświetlenie okna wprowadzenia klucza, a następnie szyfruje całą zawartość okna edycji tekstu przy użyciu wprowadzonego klucza oraz oblicza i dokleja na końcu sumę kontrolną MAC szyfrowanego tekstu, po czym zaszyfrowany tekst jest automatycznie zamieniany na standardowy system zapisu tekstowego Base64.

9.4.2. Deszyfrowanie tekstu

Aby zdeszyfrować tekst znajdujący się w oknie edycji możemy użyć przycisku „**Deszyfruj**". Po jego wciśnięciu zostaniemy poproszeni o podanie klucza (patrz rozdz. 7.1.1) , a następnie przy jego pomocy cała zawartość okna edycji tekstu zostanie zdeszyfrowana oraz zweryfikowana zostanie suma kontrolna MAC deszyfrowanego tekstu.

9.4.3. Przycisk „Wyślij"

Kopiuje zawartość całego okna edycji tekstu do schowka systemowego, a następnie uruchamia domyślny program pocztowy. Podczas edycji wiadomości w programie pocztowym po użyciu klawiszy Ctrl + V lub wciśnięciu prawego klawisza myszki i wybraniu opcji „Wklej" tekst znajdzie się automatycznie w wiadomości email.

9.4.4. Pozostałe funkcje dotyczące edycji tekstów

Przycisk „**Szukaj**" – szuka wpisanej frazy w tekście.

Przycisk „**Kopiuj**" – kopiuje zawartość całego okna edycji tekstu do schowka systemowego. Zawartość schowka można wkleić w dowolnej aplikacji służącej do pracy z tekstem (np. program pocztowy), używając klawiszy Ctrl + V lub używając opcji Edycja → Wklej.

Przycisk „**Wklej**" – czyści całą zawartość okna edycji tekstu, a następnie wkleja zawartość schowka systemowego.

Przycisk „**Wyczyść**" – czyści całą zawartość okna edycji tekstu.

Przycisk „**Zapisz do pliku**" – pozwala wybrać plik (tekstowy) i zapisać do niego zawartość okna edycji tekstu.

Przycisk „**Otwórz plik**” – pozwala wybrać plik (tekstowy), którego zawartość zostanie wczytana do okna edycji tekstu. Poprzednia zawartość okna zostanie wyczyszczona.

Opcja „**Rozmiar czcionki**” znajdująca się w lewej dolnej części głównego okna programu pozwala wybrać rozmiar czcionki użytej w oknie edycji tekstu.

Przycisk „**Plik**” włącza tryb szyfrowania plików tekstowych. W trybie tym po wciśnięciu "Szyfruj" tekst automatycznie będzie zapisany do wybranego pliku, a przed wciśnięciem "Deszyfruj" automatycznie wczytany z wybranego pliku. Po deszyfrowaniu klucz jest zapamiętywany, aby po wprowadzeniu zmian w tekście możliwe było jego szybkie zaszyfrowanie i zapisanie z powrotem do pliku jednym przyciskiem "Szyfruj". W każdej chwili można wymazać zapamiętany klucz z pamięci wciskając "Usuń klucz".

Przycisk „**Email**” włącza tryb szyfrowania emaili. W trybie tym zaszyfrowany tekst jest automatycznie kopiowany do schowka systemowego i uruchamiany jest domyślny program pocztowy. Tam po użyciu klawiszy Ctrl + V lub opcji Edycja → Wklej zaszyfrowany tekst zostanie wklejony do wiadomości email.

Przycisk „**Czat**” włącza tryb szyfrowanego czata. W trybie tym raz wprowadzony klucz jest zapamiętywany, dzięki czemu można szyfrować i deszyfrować teksty jednym przyciskiem (Szyfruj / Deszyfruj) bez konieczności wprowadzania klucza za każdym razem. Po zakończeniu sesji czata użyj przycisku "Usuń klucz" , aby wymazać zapamiętany klucz z pamięci.

Przycisk „**Tekst**” włącza podstawowy tryb szyfrowania tekstów.

Opcja „**Kopiuj**” określa, czy po zaszyfrowaniu tekst jest automatycznie kopiowany do schowka systemowego.

Opcja „**Wyślij**” określa, czy po zaszyfrowaniu tekst jest automatycznie kopiowany do schowka systemowego i uruchamiany jest domyślny program pocztowy. Tam po użyciu klawiszy Ctrl + V lub opcji Edycja → Wklej zaszyfrowany tekst zostanie wklejony do wiadomości email.

Opcja „**Zapisz**” określa, czy po zaszyfrowaniu tekst jest automatycznie zapisywany do pliku.

Opcja „**Wklej**” określa, że po wciśnięciu przycisku "Deszyfruj" zaszyfrowany tekst najpierw zostanie wklejony ze schowka systemowego, a następnie zdeszyfrowany.

Opcja „**Otwórz**” określa, czy po wciśnięciu przycisku "Deszyfruj" tekst jest automatycznie wczytywany z pliku przed deszyfrowaniem.

10. Szyfrowana książka

W trybie szyfrowania tekstów (po wciśnięciu przycisku „Teksty”) dostępna jest opcja szyfrowanej książki. Pełni ona funkcję szyfrowanej bazy danych dokumentów tekstowych. Jest wygodna do bezpiecznego przechowywania haseł, kontaktów, danych klientów czy też rozdziałów książki. Poszczególne wpisy do bazy danych nazywane są tu **dokumentami**. Każdy dokument ma postać dowolnego dokumentu tekstowego, który można edytować we wbudowanym edytorze.

Możliwe jest wygodne organizowanie dokumentów poprzez umieszczanie ich w folderach. Foldery mogą także zawierać podfoldery dla jeszcze większej elastyczności. Możliwe jest kopiowanie oraz przenoszenie dokumentów pomiędzy folderami.

Każda szyfrowana książka zapisywana jest w jednym pliku (nazwa pliku z rozszerzeniem .VMPB). Plik ten jest – podobnie jak plik archiwum – zaszyfrowany w 100%, tzn. każdy bajt

pliku jest zaszyfrowany i plik nie zawiera żadnych jawnych danych jak np. nagłówki. Plik jest nieodróżnialny od losowego ciągu danych.

Nagłówek książki oraz spis dokumentów, jako kluczowe dane niezbędne do prawidłowej pracy z książką, są zapisane w pliku na wszelki wypadek w **dwóch kopiach**, obie szyfrowane innym wektorem inicjującym, dzięki czemu obie kopie mają całkowicie inną postać po zaszyfrowaniu.

Wszelkie operacje na szyfrowanej książce są zabezpieczone przed ewentualną awarią systemu (np. awarią zasilania). Podczas wykonywania dowolnej operacji na książce (jak np. szyfrowanie dokumentu, usuwanie dokumentów) cała zawartość książki jest kopiowana do nowej książki tymczasowej z jednoczesnym wprowadzeniem pożądanych zmian (do nazwy pliku książki dodawany jest przedrostek „~") i dopiero po pomyślnym zakończeniu operacji stary plik książki jest usuwany, a nazwa książki tymczasowej zmieniana jest na nazwę właściwą.

Dzięki takiej konstrukcji algorytmu nawet w przypadku awarii np. zasilania podczas operacji na książce utracona zostanie książka tymczasowa (zapis do niej zostanie zatrzymany w nieokreślonym miejscu), ale książka sprzed zmian będzie zachowana na dysku w nienaruszonej postaci.

10.1. Utworzenie nowej książki

Aby utworzyć nową książkę, wciskamy przycisk „**Książka**". Otwiera się okno nawigacji po szyfrowanej książce. Możemy wpisać tytuł pierwszego dokumentu, wcisnąć „**Otwórz**" i w oknie edycji będziemy mogli wpisywać treść pierwszego dokumentu.

10.2. Szyfrowanie dokumentu

Po wpisaniu treści dokumentu wciskamy przycisk „**Szyfruj dokument**". Cała zawartość okna edycji tekstu zostanie zaszyfrowana i zapisana do pliku książki. Jeśli pracowaliśmy na świeżo utworzonej książce, program dodatkowo poprosi o wybranie pliku książki oraz wprowadzenie klucza szyfrującego książkę.

10.3. Otwarcie istniejącej książki

Otworzyć istniejącą książkę możemy przyciskiem „**Otwórz książkę**", po czym należy wprowadzić klucz szyfrujący książkę.

10.4. Zamknięcie książki

W każdej chwili możemy zamknąć książkę wciskając przycisk „**Zamknij**". Program wróci wówczas do standardowego trybu szyfrowania tekstów.

10.5. Nawigacja po książce

Po wciśnięciu przycisku „**Książka**", gdy książka jest otwarta, pojawia się okno nawigacji po szyfrowanej książce. Pozwala ono wykonywać szereg operacji na zawartości książki (na dokumentach i folderach).

Niektóre przyciski dostosowują swoje działanie w zależności od tego, czy znajdujemy się na liście dokumentów, czy też na liście folderów. **Rozmiary** list można zmieniać przeciągając myszką linię rozdzielającą obydwie listy. **Przechodzić** pomiędzy listą dokumentów i folderów można klikając myszką na wybranej liście lub używając **strzałek** lewo/prawo na klawiaturze.

Przycisk „**Otwórz**” otwiera wybrany dokument (lub dokumenty, jeśli zaznaczona jest opcja „**zaznaczone**” obok przycisku) albo folder.

Przycisk „**Zamknij**” zamyka szyfrowaną książkę.

Przycisk „**Nowy**” tworzy nowy dokument lub folder.

Przycisk „**Zmień**” zmienia tytuł dokumentu lub nazwę folderu.

Przycisk „**Usuń**” usuwa zaznaczone dokumenty.

Przyciski „**Zaznacz**” i „**Odznacz**” powodują zaznaczenie lub odznaczenie wybranych dokumentów. Po ich zaznaczeniu możliwe jest ich usunięcie lub eksport do okna edycji tekstów. Aby wyeksportować zaznaczone dokumenty, zaznaczamy opcję „**zaznaczone**” i wciskamy przycisk „**Otwórz**”.

Przyciski „Zaznacz” i „Odznacz” są także dostępne w menu kontekstowym, które można wywołać wciskając prawy klawisz myszki na liście dokumentów. Menu kontekstowe dostępne jest także na liście folderów.

Przycisk „**Wyczyść**” odznacza wszystkie dokumenty i foldery.

Przycisk „**Szukaj**” pozwala znaleźć dokumenty lub foldery, które zawierają wpisaną frazę w nazwie. Jeśli zaznaczono opcję „**wewnątrz dokumentów**”, wyszukane i zaznaczone zostaną wszystkie dokumenty zawierające wpisaną frazę w swojej treści. Jeśli opcja „wewnątrz dokumentów” nie jest zaznaczona, fraza będzie szukana w tytułach dokumentów.

Przycisk „**Sortuj**” zmienia sposób sortowania - zaznaczone dokumenty i foldery wyświetlane są na początku list. Aby wybrać sortowanie dokumentów wg nazwy lub numeru, możemy kliknąć odpowiedni tytuł kolumny na liście dokumentów.

10.6. Kopiowanie i przenoszenie dokumentów między folderami

Opcje kopiowania i przenoszenia dostępne są w menu kontekstowym na liście dokumentów (wywoływanym prawym przyciskiem myszki na liście dokumentów) oraz w menu głównym książki w opcji „**Edycja”**.

Opcja „**Kopiuj tu zaznaczone**” kopiuje wszystkie zaznaczone dokumenty do bieżącego folderu. Zaznaczone dokumenty są odszyfrowywane, szyfrowane na nowo i nowa zaszyfrowana kopia jest zapisywana w bieżącym folderze. Zaszyfrowany dokument oryginalny pozostaje na swoim starym miejscu. Do szyfrowania nowej kopii użyty jest nowy wektor inicjujący, dzięki czemu postać kopii po zaszyfrowaniu jest całkowicie inna niż postać oryginału po zaszyfrowaniu. W ten sposób nawet po wielokrotnym kopiowaniu tego samego dokumentu każda kopia, po zaszyfrowaniu, będzie miała całkowicie inną postać.

Opcja „**Przenieś tu zaznaczone**” przenosi zaznaczone dokumenty do bieżącego folderu. Dokumenty znikają z oryginalnych folderów i pojawiają się tylko w bieżącym folderze.

10.7. Opcje menu szyfrowanej książki

W menu w górnej części okna nawigacji po szyfrowanej książce znajdują się następujące opcje:

„**Plik**” – „**Szyfruj dokument**” – szyfruje zawartość okna edycji tekstu i zapisuje ją do pliku książki.

„**Plik**” – „**Zmień klucz**” – pozwala zmienić klucz szyfrujący książkę.

„**Plik**” – „**Zapisz jako**” – pozwala zapisać książkę do nowego pliku.

„**Plik**” – „**Nowa książka**” – tworzy nową książkę.

„**Zamknij dokument**” – zamyka bieżący dokument. Okno edycji tekstów przechodzi do standardowego trybu pracy, ale książka pozostaje otwarta.

„**Zamknij książkę**” – zamyka otwartą książkę.

„**Zamknij okno**” – zamyka okno nawigacji po szyfrowanej książce.

Funkcje znajdujące się w menu „**Edycja**” zostały omówione w rozdziale 10.6.

Funkcja „**Usuń folder**” w menu „Edycja” usuwa wybrany folder.

Po otwarciu dokumentu w oknie głównym programu pojawiają się przyciski „**Kopiuj wiersz 1, 2, 3**’ ułatwiające kopiowanie wybranych fragmentów tekstu. Funkcja ta może być przydatna, gdy w dokumentach na określonej pozycji (np. zawsze w pierwszym wierszu) trzymamy zapisane np. hasła. Przycisk „**Kopiuj kursor**” kopiuje do schowka systemowego wiersz, w którym aktualnie jest kursor.

11. Moduł Generowania Kluczy

Moduł Generowanie Kluczy można uruchomić po rozpoczęciu szyfrowania w oknie wprowadzenia klucza używając przycisku „Utwórz losowy klucz”. Moduł można uruchomić także przyciskiem „**Utwórz klucz**” lub wciskając Ctrl + K w głównym oknie programu (np. w celu wygenerowania klucza, którego użyjemy w przyszłości).

11.1. Wybór rozmiaru klucza

W lewej górnej części okna modułu generowania kluczy (w zakładce „Generowanie klucza”) znajduje się pole „**Rozmiar klucza w bajtach (1..64)**”. W polu tym możemy wybrać wielkość klucza, jaki będzie generowany z losowych ruchów myszką. Standardowo przyjętym rozmiarem jest 256 bitów (32 bajty), co odpowiada 45-znakowemu hasłu złożonemu z małych i dużych liter oraz cyfr.

Wybór rozmiaru klucza należy do użytkownika. Aby pomóc uniknąć stosowania zbyt krótkich kluczy, program automatycznie szacuje, ile czasu zajęłoby złamanie klucza o wybranej długości przez dwa rodzaje superkomputerów i wyświetla tę informację w prawej części okna modułu generowania kluczy. Ze względów bezpieczeństwa zalecamy stosowanie kluczy o rozmiarze 256 bitów (lub dłuższych).

11.2. Pole „Używaj" – wybór z jakich znaków zbudować klucz

W lewej górnej części okna modułu generowania kluczy (w zakładce „Generowanie klucza") znajduje się pole „**Używaj**", gdzie możemy zaznaczyć, aby generowany z losowych ruchów myszką klucz zbudowany był z małych liter, dużych liter lub cyfr. Oczywiście dowolna kombinacja jest możliwa (np. tylko małe litery lub małe, duże i cyfry, itp.) Im więcej znaków może wykorzystać klucz, tym będzie on mógł być krótszy. Dla przykładu klucz 128-bitowy złożony z samych cyfr wymaga aż 39 znaków (cyfr), natomiast ten sam 128-bitowy klucz zbudowany z małych i dużych liter oraz cyfr wymaga już tylko 23 znaków. Dla uniknięcia nieporozumień klucze generowane z losowych ruchów myszką nigdy nie zawierają w sobie następujących 6 liter: I oraz i (jak igła); L oraz l (jak lód); O oraz o (jak osa).

Klucz jest wyświetlony na ekranie, jeśli zaznaczona jest opcja „**Pokaż klucz**". Domyślnie klucz nie jest pokazywany, co pozwala zachować większe bezpieczeństwo.

11.3. Przycisk „Generuj klucz"

Powoduje rozpoczęcie procedury generowania klucza z przypadkowych ruchów myszką. Po jego wciśnięciu należy wykonać kursorem myszki serię możliwie najbardziej chaotycznych ruchów na znajdującym się po prawej stronie okna „**Obszarze odczytu pozycji myszy**". Klucz o zadanej długości jest generowany na podstawie bieżącej pozycji myszy w tym obszarze oraz na podstawie odstępów czasu między zmianami pozycji kursora myszy mierzonymi z dokładnością do jednej tysięcznej części sekundy. Im bardziej chaotyczne i nieregularne ruchy myszką, tym jakość klucza będzie wyższa. Zastosowany algorytm pozwala uzyskać klucze o strukturze w praktyce nieodróżnialnej od struktury kluczy idealnie losowych. Takie klucze są najtrudniejsze do złamania.

11.4. Przycisk „Wpisz klucz"

Powoduje rozpoczęcie procedury wpisania klucza z klawiatury (hasła). Zalecamy stosowanie kluczy wygenerowanych z losowych ruchów myszką. Jeśli jednak szyfrujemy dane o niższym stopniu poufności, możemy stosować także hasła wpisane z klawiatury. Zalecamy wówczas stosowanie zarówno małych, jak i dużych liter oraz cyfr, a także znaków specjalnych (jak @$#[*- itp.) oraz stosowanie haseł odpowiadającym długością minimum 128-bitowemu kluczowi losowemu. Stosowanie haseł krótszych niż 8-znakowych rodzi realne ryzyko, że hasło takie zostanie złamane nawet przy użyciu domowego komputera.

Gorąco zalecamy odczytywanie informacji wyświetlonej w prawej części okna – gdzie wyświetlany jest szacunkowy czas złamania wpisanego klucza .

11.5. Przycisk „Wczytaj klucz"

Powoduje wczytanie klucza z pliku. Klucz do pliku zapisany może być przyciskiem „Zapisz klucz", znajdującym się w zakładce „Zapis klucza" (rozdz. 11.6).

11.6. Przycisk „Zapisz klucz"

Znajduje się w lewej górnej części okna modułu generowania kluczy, w zakładce „Zapis klucza". Pozwala wybrać plik tekstowy, do którego ma być zapisany klucz. Klucz zapisany zostanie na samym początku pliku i zawsze kończy się dodatkowym znakiem "<" (znak mniejszości, kod ASCII 60 [hex:3C]). Klucze o długości poniżej 155 znaków są dodatkowo dopełniane znakami "-" (minus, kod ASCII 45 [hex:2D]) do długości 156 bajtów. Następnie klucz dodatkowo

dopełniany jest także znakami "-" do długości 1024 znaków, aby kopie klucza zapisane były w pewnej odległości od siebie na wypadek lokalnego uszkodzenia dysku.

Tak przygotowany klucz zapisywany jest w pliku w **trzech kopiach** następujących po sobie dla dodatkowego bezpieczeństwa przed ewentualnym uszkodzeniem dysku.

Na końcu pliku zapisywany jest stały charakterystyczny łańcuch znaków, który może pomóc odnaleźć klucz na uszkodzonym dysku. Łańcuch ten ma postać:

uvdrakbcrhytckbsvsqeysnzzvampahwkhnmxkeawapswjdbtexwnaswe

Po zapisaniu klucza do pliku możliwe jest jego wczytanie (przy deszyfrowaniu lub ponownym szyfrowaniu tym samym kluczem) przyciskiem „Wczytaj klucz" w zakładce „Generowanie klucza" (patrz rozdz. 11.5) lub bezpośrednio w oknie wprowadzenia klucza (rozdz. 4.3).

Zapisywanie kluczy w plikach jest wygodne, ponieważ nie wymaga zapamiętywania kluczy o wysokiej jakości, które z istoty rzeczy mają skomplikowaną postać. Jednakże klucze należy zapisywać na innych nośnikach niż te, gdzie znajdują się zaszyfrowane dane. Jeśli zaszyfrowane archiwum trzymamy na komputerze na dysku, to trzymanie klucza na tym samym komputerze, nawet na innym dysku, jest bardzo ryzykowne, bo wystarczy, że atakujący przeszuka nasze dyski (wystarczy mu na to parę minut), znajdzie klucz i będzie w stanie zdeszyfrować dane. Klucz zatem nie tylko musi być dobrej jakości i odpowiednio długi, ale musi być dobrze strzeżony i trzymany w tajnym/zaufanym miejscu.

Zalecamy dlatego zapisywanie kluczy nie na dyskach, ale na nośnikach przenośnych, takich jak płyty CD, czy urządzenia typu Pen-Drive lub dowolnych innych urządzeniach, które nie są stałymi częściami komputera. Możliwe jest także zrobienie fotografii monitora po wciśnięciu przycisku „**Zoom klucza**".

Reguła ta ma mniejsze zastosowanie, jeśli uważamy nasz komputer za bezpieczny, a szyfrujemy dane tylko w celu przesłania ich np. przez Internet.

11.7. Przycisk „Kolejny klucz"

Znajduje się w dolnej części okna modułu generowania kluczy, w zakładce „Zapis klucza". Powoduje przejście do generowania kolejnego klucza. Generowanie wielu kluczy do jednego szyfrowania może być użyteczne w sytuacji, gdy prawo deszyfrowania może mieć tylko **pełna grupa osób**. W takiej sytuacji każda z osób ma swój własny klucz i deszyfrowanie możliwe jest tylko, jeśli podane zostaną wszystkie klucze. Funkcja ta umożliwia także dodatkowe zwiększenie bezpieczeństwa poprzez stosowanie wielu kluczy przez jednego użytkownika. Wtedy np. główny klucz o długości 256 bitów, wygenerowany z ruchów myszą, zapisujemy np. na CD, USB, czy kartce papieru, a drugi klucz, np. w postaci hasła wpisanego z klawiatury, używamy jako dodatkowego klucza. Liczba możliwych do podania kluczy jest nieograniczona. Kolejność podawania kluczy jest dowolna. Jeśli brakuje choć jednego klucza, złamanie szyfrogramu na podstawie pozostałych kluczy jest tak samo złożone, jak złamanie całego brakującego klucza.

11.8. Przycisk „Połącz klucze"

Znajduje się w dolnej części okna modułu generowania kluczy, w zakładce „Zapis klucza". Łączy wprowadzone klucze w jeden nowy klucz. Podczas deszyfrowania należy podać tylko klucz wynikowy (podanie kluczy składowych nie pozwoli zdeszyfrować danych). Funkcja ta może być użyteczna w sytuacji wielopoziomowego protokołu uzgadniania klucza, który polega na tym, że strony uzgadniają wiele kluczy różnymi kanałami (np. przez telefon, SMS, fax, Internet, PKI, osobiście, listem tradycyjnym, czy innymi metodami), a następnie łączą te klucze w jeden klucz wynikowy. Istotą takiego rozwiązania jest minimalizowanie ryzyka przechwycenia

wszystkich kluczy przez niepowołaną stronę. Kolejność podawania kluczy jest dowolna. Te same klucze zawsze dają ten sam wynik połączenia. Jeśli brakuje choć jednego klucza, odnalezienie klucza wynikowego na podstawie pozostałych kluczy jest tak samo złożone, jak złamanie całego brakującego klucza.

11.9. Ogólne funkcje modułu generowania kluczy

Przycisk „**Anuluj**” i „**OK**” czyści w pamięci operacyjnej komputera wszystkie dane zawierające klucz i zamyka moduł generowania klucza.

Przycisk „**Resetuj**” czyści w pamięci operacyjnej komputera wszystkie dane zawierające klucz i przywraca moduł generowania klucza do stanu początkowego – takiego, w jakim był zaraz po jego uruchomieniu.

11.10. Zarządzanie kluczami

Sposób zarządzania kluczami zależy od upodobań i wymagań użytkownika – czy woli on zapisywać klucze na płycie CD, urządzeniu Pen-Drive, czy innym nośniku, czy też preferuje on zapis klucza na kartce papieru lub w jeszcze inny sposób lub tylko zapamiętanie. Wszystkie te sposoby mają na celu utrwalenie klucza – powinny zapewnić kluczowi tajność, ale i bezpieczeństwo – gdy utracimy klucz, zdeszyfrowanie danych nie będzie możliwe żadnym sposobem. Dlatego dla bardzo istotnych danych można trzymać kopię zapasową klucza – np. kopię „dyżurną” trzymać na Pen-Drive, a kopię zapasową, zapisaną na kartce papieru lub sfotografowaną – trzymać ukrytą np. w sejfie. Sposobów na zarządzanie kluczami jest znacznie więcej i od inwencji i upodobań użytkownika zależy, które z nich najwygodniej i najbezpieczniej będzie mu stosować.

12. Funkcje dodatkowe oraz ułatwiające pracę

12.1. Pamiętanie klucza

Raz wprowadzony klucz można zapamiętać, aby możliwe było wygodne szyfrowanie / deszyfrowanie większej ilości danych bez konieczności wprowadzania klucza za każdym razem. Służy do tego opcja „**Pamiętaj klucz**” w oknie wprowadzania klucza (rozdz. 7.1.1) oraz przycisk „**Usuń klucz**” w głównym oknie programu.

12.2. Szyfrowanie w trybie prywatnym

Opcja ta dostępna jest tylko dla klientów posiadających licencję na aplikację (wersja darmowa z licencją testową dostępna w Internecie jej nie posiada). Dane zaszyfrowane w trybie prywatnym mogą być odszyfrowane tylko w **licencjonowanej** kopii aplikacji (po podaniu prawidłowego klucza). Podanie prawidłowego klucza w wersji darmowej nie pozwoli odszyfrować danych.

Uruchomienie trybu prywatnego odbywa się poprzez specjalną procedurę wprowadzania klucza: jako pierwszy klucz należy wprowadzić znak ‘**.**’ (**kropka**). Po jego wprowadzeniu nastąpi automatyczne przełączenie w tryb prywatny i wtedy należy wprowadzić właściwy klucz (lub klucze) do szyfrowania.

Technologia i poziom bezpieczeństwa szyfrowania w trybie prywatnym są **identyczne** jak w trybie standardowym. Technicznie: jedyną różnicą między trybami jest inna wartość początkowa wewnętrznej permutacji w algorytmie inicjowania klucza (Key Initialization Algorithm). Używanie

trybu prywatnego zamiast standardowego do zwiększenia poziomu bezpieczeństwa jest bezcelowe.

Tryb prywatny może być wykorzystywany np. przez naszą firmę do publikowania informacji przeznaczonych **tylko** dla naszych klientów.

12.3. Szyfrowanie kluczem stałym

Jeśli podczas szyfrowania nie wprowadzono klucza, dane zostaną zaszyfrowane **kluczem stałym**. Szyfrowanie kluczem stałym nie daje żadnego bezpieczeństwa kryptograficznego, ale może być użyteczne, gdy chcemy np. skorzystać z samej kompresji plików lub umieszczenia wielu plików/folderów w jednym pliku archiwum, także samodeszyfrującym, czy np. wielu dokumentów tekstowych w jednym pliku książki.

12.4. Wyszukiwanie plików i folderów

Podczas pracy z plikami do szyfrowania lub otwartym archiwum możliwe jest wyszukiwanie plików i folderów znajdujących się na liście. Przycisk „**Szukaj**” pozwala wyszukać pliki i foldery, które zawierają wpisaną frazę w swojej nazwie.

12.5. Ustawienia

Po wciśnięciu przycisku „**Ustawienia**” (lub klawisza F1) pojawia się okno, w którym możemy na stałe skonfigurować wiele parametrów działania programu.

12.6. Przeciąganie plików

W celu ułatwienia znajdowania potrzebnych plików możliwe jest przeciąganie plików z eksploratora systemu Windows (wciśnięcie lewego przycisku myszki na pliku, przesunięcie kursora myszki na okno programu i puszczenie przycisku myszki) – program rozpoznaje przeciągane pliki archiwum (VMPA), pliki szyfrowane osobno (VMPC), pliki szyfrowanych książek (VMPB) oraz pliki tekstowe – jeśli jesteśmy w trybie szyfrowania tekstów.

12.7. System bieżącej pomocy

Program posiada system bieżącej pomocy – wciśnięcie prawego klawisza myszki nad dowolnym przyciskiem w programie powoduje wyświetlenie szczegółowej informacji na temat funkcji tego przycisku. Aby zamknąć okno pomocy wystarczy najechać kursorem myszki na obszar „Zamknij”, wewnątrz ramki w dolnej części okna. Aby zamykać okno klikając przycisk „Zamknij”, można w oknie pomocy odznaczyć opcję „Automatyczne zamknięcie”.

12.8. System skrótów klawiszowych

Program posiada system skrótów klawiszowych. Każdy przycisk można wywołać z klawiatury wciskając najczęściej kombinacje podstawowych klawiszy – Enter, Spacja, Ctrl, Shift. Skrót klawiszowy jest wyświetlony na większości przycisków w formie skróconej. Po najechaniu kursorem myszki na przycisk, po chwili pojawi się pełna informacja, jaki klawisz lub kombinacja klawiszy wywołuje dany przycisk. Korzystanie ze skrótów klawiszowych zależy od indywidualnych upodobań użytkownika, ale w praktyce może przyspieszyć pracę z programem.

12.9. System autokontroli

Program posiada system autokontroli – przy każdym uruchomieniu obliczana jest specjalna suma kontrolna pliku .exe zawierającego program. W przypadku, gdyby choć jeden bajt pliku uległ zmianie (np. wskutek działania wirusa lub uszkodzenia dysku) program wyświetli komunikat zalecający ponowną instalację programu. Praca programu będzie kontynuowana.

12.10. Uruchamianie z wiersza poleceń

Program może być uruchamiany także z **wiersza poleceń** (tryb wygodny np. przy automatycznym archiwizowaniu danych przy pomocy plików typu BAT). Dostępna jest wówczas funkcja szyfrowania i deszyfrowania pojedynczego pliku lub całego folderu w trybie szyfrowania plików osobno (patrz rozdz. 4.6), wymazywania pliku (także wymazywania bez wcześniejszego szyfrowania) oraz wczytania klucza z wiersza poleceń lub z pliku. Program rozróżnia następujące parametry:

/k=... Klucz. Np. "/k=abc"
/kf=... Plik klucza. Np. "/kf=c:\vmpck1.txt"
Jeśli parametr /k lub /kf nie zostanie podany,
pliki zostaną zaszyfrowane/odszyfrowane KLUCZEM STAŁYM

/src=... Plik lub folder źródłowy. Np. "/src=c:\plik.txt" "/src=c:\mój prywatny folder"

/dst=... Folder docelowy. Np. "/dst=c:\mój folder"
Parametr /dst jest opcjonalny. Jeśli nie zostanie podany,
pliki wynikowe zostaną zapisane w tych samych folderach, co pliki wejściowe

/e Szyfruj
/d Deszyfruj
/x Tylko wymaż podany plik lub zawartość podanego folderu

/w... Określ liczbę rund wymazywania. Np. "/w0" "/w1" "/w25"
/w0 oznacza samo logiczne usunięcie plików (0 rund wymazywania)

Parametru /w używamy wraz z parametrami /e, /d, /x.
Np. parametry /e /w2 spowodują, że pliki po zaszyfrowaniu
zostaną wymazane z użyciem 2 rund.
Np. /d /w0 oznacza, że pliki po odszyfrowaniu
zostaną tylko logicznie usunięte (0 rund wymazywania)

/i Automatycznie zastępuj istniejące pliki

/v Automatycznie dodaj rozszerzenie "vmpc" do nazwy deszyfrowanego pliku
Np. parametry "/src=c:\plik.txt" /d /v
spowodują odszyfrowanie pliku c:\plik.txt.vmpc

------ WARTOŚCI DOMYŚLNE: ------

Jeśli przy samym wymazywaniu (/x) nie podano parametru /w,
przyjmowana jest domyślnie 1 runda wymazywania (tożsame z podaniem /x /w1).

Jeśli przy szyfrowaniu (/e) lub deszyfrowaniu (/d) nie podano parametru /w,
wejściowe pliki NIE ZOSTANĄ WYMAZANE ANI USUNIĘTE.

Jeśli przy szyfrowaniu (/e) lub wymazywaniu (/x) podano sam parametr "/w" (a nie np. "/w3"), przyjmowana jest domyślnie 1 runda wymazywania.

Jeśli przy deszyfrowaniu (/d) podano sam parametr "/w" (a nie np. "/w3"),
przyjmowane jest domyślnie samo logiczne usunięcie plików (0 rund wymazywania).

------ UWAGI DODATKOWE: ------

Dla parametrów /kf /src /dst:
Jeśli nazwa pliku zawiera spacje, należy cały parametr podać w CUDZYSŁOWACH "...",
np. "/src=mój plik.txt".
Dla uniknięcia ryzyka pomyłki zalecamy zawsze podawać parametry
"/kf=..." "/src=..." "/dst=..." w cudzysłowach.

Kolejność podawania parametrów nie jest istotna, ale ze względów bezpieczeństwa
KLUCZ (/k lub /kf) musi być podany jako PIERWSZY parametr.

12.11. Możliwość pracy bez instalacji

Program może pracować także bez instalacji. Plik programu – vmpcrypt.exe – można skopiować w dowolne miejsce (np. na płytę CD czy na pamięć USB) i stamtąd uruchamiać. Pozwala to mieć program **zawsze przy sobie**.

Plik vmpcrypt.exe znajduje się na płycie instalacyjnej programu. Jeśli program był dostarczony tylko w wersji elektronicznej, wówczas należy najpierw zainstalować program na komputerze, a następnie odnaleźć plik vmpcrypt.exe w folderze, w którym program został zainstalowany i stamtąd skopiować go.