

## IDŹ DO

PRZYKŁADOWY ROZDZIAŁ



SPIS TREŚCI

## KATALOG KSIĄŻEK

KATALOG ONLINE

ZAMÓW DRUKOWANY KATALOG

## TWÓJ KOSZYK

DODAJ DO KOSZYKA

## CENNIK I INFORMACJE

ZAMÓW INFORMACJE  
O NOWOŚCIACH

ZAMÓW CENNIK

## CZYTELNIA

FRAGMENTY KSIĄŻEK ONLINE

# Szyfrowanie informacji za pomocą PGP. Ćwiczenia praktyczne

Autor: Piotr Czarny  
ISBN: 83-7197-744-1  
Format: B5, stron: 112



W czasach, gdy dostęp do komputerów jest powszechny a łatwość zdobycia informacji krążących w Internecie jest tak wielka jak otwarcie słoika z konfiturą, przesyłanie ważnych informacji o firmie, danych osobowych, projektów czy publikacji – jest niewskazane i niebezpieczne. Jak zatem chronić prywatność plików i informacji? Czy istnieje metoda na tyle skuteczna, by jej zawierzyć?

Oczywiście, że każdy kod, szyfr można złamać. Jednak zastosowanie najnowszych metod kryptograficznych daje nam minimalną pewność, że nikomu nie będzie się chciało używać komputerów wartości setek milionów dolarów do rozszyfrowania elektronicznego listu zawierającego chroniony dokument. Warto zauważyć, że użycie klasycznego domowego komputera nic nie da, ponieważ czas rozszyfrowania to lata.

Dlaczego warto zainteresować się programem PGP?

Ponieważ aplikacja ta może być uzupełnieniem systemu zabezpieczeń. Jest ona równie ważna jak zamki w drzwiach pomieszczeń, systemy identyfikacji pracowników mających dostęp do różnych obszarów firmy, alarmy antywłamaniowe.

Oprócz zapewnienia poufności przesyłanych danych PGP można wykorzystać do:

- szyfrowania poszczególnych plików lub całych folderów. Chronić można nie tylko pliki utworzone w Wordzie lub Excelu, ale również skanowane zdjęcia i rysunki,
- potwierdzania autentyczności informacji. PGP umożliwia dopisanie na końcu wiadomości sekwencji znaków. Odbiorca, używając klucza publicznego nadawcy może sprawdzić, czy wiadomość została napisana przez osobę, która ją podpisała kluczem prywatnym i czy nic w jej treści nie zostało zmienione.

„Ćwiczenia praktyczne” nauczą cię, jak:

- pozyskać program PGP,
- zainstalować go w systemie,
- używać, by właściwie chronić swoją prywatność i informacje. kluczem prywatnym i czy nic w jej treści nie zostało zmienione.



# Spis treści

<b>Wstęp</b> .....	<b>5</b>
<b>Rozdział 1. Pozyskiwanie oprogramowania z Internetu</b> .....	<b>11</b>
<b>Rozdział 2. Instalacja programu WinZip</b> .....	<b>15</b>
<b>Rozdział 3. Rozpakowywanie wersji instalacyjnej programu PGP</b> .....	<b>19</b>
<b>Rozdział 4. Instalacja PGP</b> .....	<b>21</b>
Generowanie kluczy.....	24
<b>Rozdział 5. Eksportowanie i importowanie kluczy</b> .....	<b>31</b>
Eksportowanie klucza publicznego do pliku.....	31
Eksportowanie klucza prywatnego do pliku.....	33
Przesyłanie klucza publicznego pocztą elektroniczną.....	36
Importowanie kluczy.....	39
<b>Rozdział 6. Okno PGPkeys</b> .....	<b>41</b>
Keys.....	43
Validity.....	44
Trust.....	45
Size.....	45
Description.....	45
Key ID.....	46
Creation.....	46
Expiration.....	46
ADK.....	47
<b>Rozdział 7. Hasło</b> .....	<b>49</b>
Wybór i zapamiętanie hasła.....	49
Zmiana hasła.....	50

---

<b>Rozdział 8. Zarządzanie kluczami .....</b>	<b>53</b>
Wykonywanie kopii bezpieczeństwa .....	53
Dodawanie nowej nazwy użytkownika lub adresu do pary kluczy .....	55
Dodawanie identyfikatora fotograficznego do klucza .....	56
<b>Rozdział 9. Szyfrowanie korespondencji .....</b>	<b>59</b>
Kodowanie i podpisywanie listów w aplikacjach, które nie obsługują wtyczek PGP .....	70
<b>Rozdział 10. Pobieranie klucza publicznego z serwera .....</b>	<b>73</b>
Weryfikacja autentyczności kluczy .....	74
<b>Rozdział 11. Dzielenie i łączenie kluczy .....</b>	<b>79</b>
Łączenie kluczy .....	82
<b>Rozdział 12. Szyfrowanie i podpisywanie plików .....</b>	<b>87</b>
<b>Rozdział 13. Nieodwracalne usuwanie plików .....</b>	<b>97</b>
PGP Wipe .....	102
<b>Zakończenie .....</b>	<b>111</b>

# Wstęp

Powszechne zastosowanie komputerów w wielu dziedzinach życia oprócz dobrodziejstw przyniosło również zagrożenia. Łatwiej jest chronić informacje zapisane tylko na papierze niż te, które istnieją w postaci plików. Dokument drukowany ma postać fizyczną. Można ponumerować jego kopie czy ewidencjonować osoby korzystające z nich.

Aby ściśle kontrolować każdy etap przetwarzania informacji elektronicznych, konieczna jest wiedza o działaniu programów i funkcjonowaniu komputera. Może się zdarzyć, że chociaż chronić będziemy plik z danymi, to osoba postronna uzyska dostęp do poufnych informacji, odczytując kopię zapasową, którą utworzył program użyty do edycji dokumentu.

Kolejnym zagrożeniem poufności jest przesyłanie danych. Nie zawsze można powierzyć je zaufanemu kurierowi. Czasami trzeba dane przekazać siecią komputerową lub Internetem. Korzystając z błyskawicznego przesyłu musimy liczyć się z tym, że ktoś może przechwycić informacje. Jest to tym bardziej prawdopodobne, że może być wykonane umyślnie. W dobie permanentnego wyścigu z czasem przewagę nad konkurencją, a więc sukces na rynku, może zapewnić nowa technologia, ciekawy produkt, niestandardowy pomysł. Wszyscy starają się chronić swoje zasoby informatyczne oraz pozyskiwać dane o przeciwnikach.

Najczęściej występują 2 rodzaje przestępstw komputerowych:

- ❖ Kradzież zasobów. Zagrożenie występuje wtedy, gdy złodziej jest w stanie poprawnie zinterpretować dane lub działa na zlecenie. Przestępstwo nie zawsze wiąże się z utratą danych. Dane mogą one być po prostu skopiowane. Poszkodowany często o tym fakcie nie ma pojęcia.
- ❖ Przekłamanie zasobów. Dane zwykle bywają zmieniane w minimalnym zakresie. Jeżeli modyfikacji dokonano w dyskretny sposób, jest to trudne do wykrycia. Przestępstwo może polegać na przechwyceniu oryginalnego listu, przesyłanego siecią Internet, i zastąpieniu go listem o zmienionej treści.

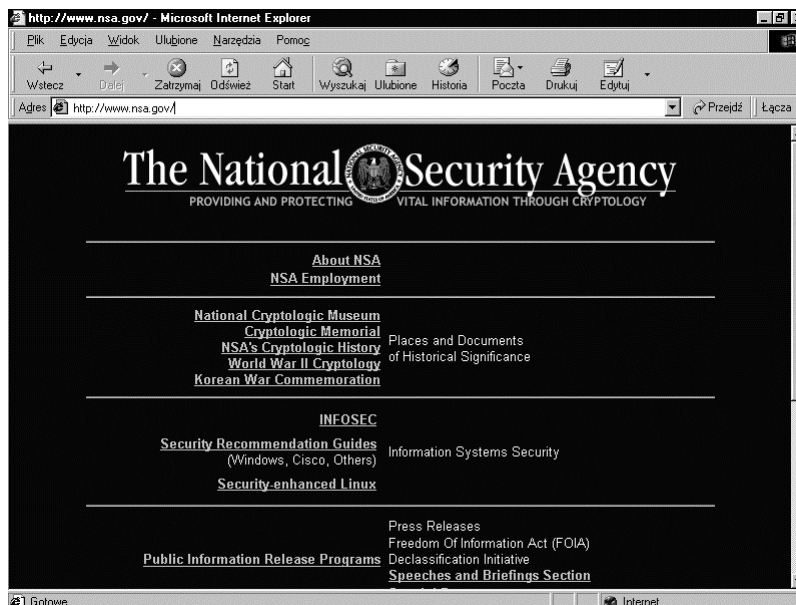
## NSA

Kto jeszcze, oprócz konkurencji, może być zainteresowany naszymi danymi? Informacje o tym kto, z kim i czym handluje są przydatne dla rządów państw. Służby specjalne nastawiają elektroniczne uszy w poszukiwaniu np. terrorystów.

Do publicznej wiadomości podano informację o istnieniu National Security Agency (rysunek W.1). Czym się zajmuje NSA? Do jej zadań należy między innymi:

- ❖ nagrywanie informacji przesyłanych drogą radiową z każdego centymetra kwadratowego kuli ziemskiej i ponad 120 satelitów (w tym również rozmów telefonicznych);
- ❖ dekodowanie zaszyfrowanych wiadomości;
- ❖ rozpoznawanie luk w zabezpieczeniach oprogramowania komputerowego;
- ❖ analizowanie pozyskanych informacji.

**Rysunek W.1.**  
Strona Web NSA  
<http://www.nsa.gov/>



Oczywiście wszystkiego nie są w stanie zrobić ludzie. Nad opracowywaniem wyników pracują nieprzerwanie baterie superkomputerów.

Pracochłonność obróbki danych można w znacznym zakresie zmniejszyć. Wymaga to przygotowania odpowiedniego oprogramowania, które sprzedawane jest nic nie podejrzewającym nabywcom. Firma występująca o koncesję na eksport oprogramowania, zawierającego moduły szyfrujące, może otrzymać kilka sugestii. Ich spełnienie jest warunkiem uzyskania zezwolenia. Zalecenia mogą dotyczyć np. wprowadzenia stałego nagłówka do każdego bloku szyfrowanej wiadomości. Można również zmodyfikować procedurę generowania kluczy, tak aby miały one wspólną sekwencję znaków. Poprawki nie zmieniają w znaczący sposób działania algorytmu klucza, natomiast umożliwią wydzielenie szyfrowanych wiadomości z szumu informacyjnego. Stałe elementy pliku ułatwią złamanie kodu osobom wiedzącym o ich istnieniu.

W czasie zimnej wojny znaczenie Agencji było dużo większe, a jej istnienie tajne. Skrót nazwy tłumaczono żartobliwie jako *No Such Agency* albo *Never Say Anything*. Można sądzić, że po wydarzeniach 11.IX.2001 r. aktywność Agencji nasiliła się.

# Echelon

Jednym z produktów NSA jest system szpiegowski o kryptonimie „Echelon”. Służy on do nieustannego monitorowania łączy komunikacyjnych: naziemnych, podmorskich oraz satelitarnych. Może on przechwytywać zarówno sygnały analogowe (rozmowy telefoniczne), jak i cyfrowe (transmisja w sieci Internet).

Głównymi celami „Echelonu” są obiekty cywilne (rządy, organizacje, firmy) w krajach całego świata.

System oficjalnie powstał, aby służyć obronności USA oraz zwalczaniu przestępczości. Nic nie stoi jednak na przeszkodzie, aby używać go do zbierania informacji mających charakter handlowy lub naukowy (szpiegostwo przemysłowe).

Współpracując z rządem USA firmy amerykańskie odnoszą praktycznie nieograniczone korzyści, otrzymując zebrane w ten sposób informacje. Handlowcy znają treść negocjacji europejskiej konkurencji i mają ułatwione zadanie przy przejmowaniu klientów. Konstruktorzy mają możliwość zapoznania się z najnowszymi konkurencyjnymi technologiami, które mogą patentować na terenie USA.

Powyższe informacje nie nastrajają optymistycznie. Gdy komuś bardzo zależy na poznaniu tajemnicy i gdy ma tak olbrzymią przewagę środków technicznych, jaką ma wielkie państwo nad obywatelem lub firmą — nie ma szans na zachowanie poufności. Można jednak próbować bronić się przed naruszeniem prywatności czy kradzieżą pomysłów. Najlepiej wszystkie informacje przekazywać drugiej stronie na ucho. To ideał. W praktyce naszymi sprzymierzeńcami są... czas i pieniąż. Bezpieczeństwo danych jest pojęciem względnym. Jeżeli rozkodowywaniem informacji zajmuje się osoba dysponująca komputerem PC, to prawdopodobnie zanim upora się z zadaniem... informacja przestanie być aktualna. Gdy poznanie treści listu ma wielkie znaczenie, można do tego celu użyć superkomputera. Godzina jego pracy jest tak droga, że tylko nieliczne pliki są analizowane w ten sposób.

Zagadnienia związane ze skuteczną i bezpieczną wymianą informacji są na tyle ważne, że powstała oddzielna gałąź nauki. Jest nią kryptografia.

# Kryptografia

Kryptografia obejmuje bardzo wiele zagadnień. Najważniejsze z nich to:

- ❖ kamuflowanie wiadomości i maskowanie działania programów (steganografia);
- ❖ zasady doboru haseł;
- ❖ skuteczne niszczenie dokumentów i kasowanie plików;
- ❖ wykrywanie ukrytych kanałów w aplikacjach;
- ❖ eliminowanie ulotu elektromagnetycznego, podsłuchu i przechwytywania danych;
- ❖ kontrola dostępu i identyfikacja (bezbłędne sprawdzenie, kto chce wejść do systemu lub pomieszczenia);

- ❖ autentyzacja i certyfikacja (zagwarantowanie, że dana osoba jest autorem dokumentu);
- ❖ podpisy cyfrowe (sposób przekonania osoby trzeciej o autentyczności dokumentu);
- ❖ dobór parametrów kryptosystemu, aby był bezpieczny przez jak najdłuższy okres czasu mimo postępów kryptoanalizy;
- ❖ integralność danych (uniemożliwienie niewykrywalnej modyfikacji pliku);
- ❖ zabezpieczenie przed kopiowaniem („znak wodny”).

Jak widać, problemów wymagających rozwiązania jest bardzo wiele. W ćwiczeniach zajmiemy się głównie poufnością danych — przesyłaniem wiadomości pomimo podsłuchu. Zagadnienie jest niemal tak stare jak ludzkość. Od dawna trudzono się nad tym, jak przekazać wiadomość z zamku A do zamku B mimo grasujących na gościńcu zbójców.

Żeby przechwycenie wiadomości przez osobę trzecią nie spowodowało poznania treści przesyłki, należy ją zaszyfrować. Prawowity adresat musi umieć rozkodować przekaz. Zatem zagadnienie sprowadza się do bezpiecznego przekazania odbiorcy informacji o sposobie odtajnienia przeznaczonej dla niego przesyłki.

Istnieją dwa rozwiązania tego problemu. Pierwsze to *kryptografia symetryczna* (kryptografia klucza tajnego). Sprowadza się ona do szyfrowania za pomocą klucza, który obie strony muszą uprzednio uzgodnić. Ten rodzaj kryptografii zakłada istnienie bezpiecznego kanału komunikacyjnego (np. spotkania bez świadków).

Drugim rozwiązaniem jest *kryptografia asymetryczna* (kryptografia klucza publicznego). Polega ona na stosowaniu dwóch kluczy: prywatnego i publicznego. Klucz publiczny może być podany do ogólnej wiadomości. Służy on wyłącznie do szyfrowania informacji, które można rozszyfrować tylko za pomocą odpowiedniego klucza prywatnego. Znajomość klucza publicznego nie pozwala na rozkodowanie przesyłki. Dlatego klucze publiczne można swobodnie przekazywać dowolną metodą innym użytkownikom, którzy będą chcieli zaszyfrować informacje przeznaczone dla odbiorcy. Natomiast własny klucz prywatny należy dokładnie zabezpieczyć, aby być pewnym, że tylko my będziemy w stanie rozszyfrować otrzymane informacje.

Aby komunikacja była dwustronna, każda strona musi posiadać własny klucz prywatny (do rozkodowywania otrzymanych wiadomości) oraz klucz publiczny (do kodowania wysyłanych wiadomości).

Komunikacja z wykorzystaniem klucza publicznego wymaga zastosowania odpowiedniego narzędzia. Narzędziem tym, powszechnie stosowanym na całym świecie, jest aplikacja o nazwie PGP.

## PGP

Program PGP może być uzupełnieniem systemu zabezpieczeń. Jest on równie ważny jak zamki w drzwiach pomieszczeń, systemy identyfikacji pracowników, mających dostęp do różnych obszarów firmy, czy alarmy antywłamaniowe. Oprócz zapewnienia poufności przesyłanych danych program PGP można wykorzystać do:

- ❖ Szyfrowania poszczególnych plików lub całych folderów. W ten sposób chronić można nie tylko pliki utworzone w Wordzie lub Excelu, ale również skanowane zdjęcia i rysunki.
- ❖ Potwierdzania autentyczności informacji. PGP umożliwia dopisanie na końcu wiadomości sekwencji znaków. Odbiorca, używając klucza publicznego nadawcy, może sprawdzić, czy wiadomość została napisana przez osobę, która ją podpisała kluczem prywatnym i czy nic w treści wiadomości nie zostało zmienione.

## Dlaczego PGP

W PGP używane są pary kluczy: jeden służy do zaszyfrowania listu (klucz publiczny), drugi do odszyfrowania (klucz prywatny). Klucz publiczny musi być udostępniony nadawcy. Można go bezpiecznie przesłać Internetem. Zastosowanie odpowiedniego algorytmu powoduje, że znajomość klucza szyfrowania nie wystarczy do deszyfracji listu ani do utworzenia klucza prywatnego.

Klucz deszyfrowania jest generowany na podstawie pary dużych liczb pierwszych. Klucz szyfrowania jest wyliczany na podstawie iloczynu dużych liczb pierwszych. Znajomość iloczynu dwóch liczb pierwszych wystarcza do złamania kodu. Jak zwykle diabeł tkwi w szczegółach. Dla odpowiednio dużych liczb (rzędu 10 do potęgi 100) istnieje bardzo dużo kombinacji liczb pierwszych.

Zastosowany w PGP algorytm szyfrowania kluczem publicznym nosi nazwę *RSA*.

Nazwa algorytmu jest skrótem pochodzącym od pierwszych liter nazwisk jego twórców: Rivest, Shamir, Adleman. *RSA* jest uważany za bezpieczny, gdy używa się odpowiednio długich kluczy. W chwili obecnej uważa się, że stosunkowo bezpieczne są klucze o długości nie mniejszej niż 768 znaków. Bardziej bezpiecznymi są jednak klucze o długości nie mniejszej niż 1024 znaki.

Bezpieczeństwo danych jest pojęciem względnym. Rozwój dotyczy wszystkich nauk. Postępy w faktoryzacji dużych liczb lub upowszechnienie komputerów o wielkich mocach obliczeniowych mogą spowodować, że dane, które uważano za dobrze zabezpieczone, staną się łatwo dostępne.

## Koniec mitu

W numerze 167. „Rzeczpospolitej” z dnia 19 lipca 1997 roku zamieszczony został artykuł autorstwa Piotra Kościelniaka, zatytułowany „Złamany szyfr”. Oto jego fragment:

„Do złamania 52-bitowego kodu DES nie był potrzebny nawet wyjątkowo wyrafinowany program. Rocke Verser — programista z Loveland w Kolorado, który nadzorował prace nad łamaniem szyfru w grupie nazwanej DESCHALL — użył najprostszego z możliwych metod: przetestował każdy możliwy klucz — dokładnie było ich 72 057 594 037 927 936 — nieco ponad 72 kwadryliony. Do sprawdzenia kluczy grupa DESCHALL używała sieci tysięcy komputerów połączonych ze sobą Internetem.

Metodyczne poszukiwanie klucza rozpoczęło się w lutym tego roku. Verser i jego grupa mieli sporo szczęścia, na właściwe rozwiązanie bowiem udało im się natrafić po pokonaniu ok. 25 procent wszystkich kombinacji. Na rozwiązanie natrafił Michael Sanders z Salt Lake City — posiadacz komputera z procesorem Pentium 90 MHz.”

Artykuł został napisany przed pięciu laty. Dziś już nie można kupić komputera z procesorem Pentium 90, wiele programów nie będzie na nim działało. Za pięć lat z uśmiechem będziemy się odnosić do dzisiejszych nowinek technicznych. Może się jednak zdarzyć, że dane, które dziś zakodujemy, za kilka lat staną się publiczną tajemnicą, dlatego trzeba używać najskuteczniejszych z dostępnych zabezpieczeń.

## Zrób to sam

W rozdziale o NSA znalazła się wzmianka o ingerencji administracji w sprzedawane programy. Żadna władza świadomie nie pozbawi siebie kontroli nad jakimś obszarem gospodarki. Prowadziłoby to do jej samounicestwienia. Należy przyjąć za pewnik, że każdy program szyfrujący jest dopuszczony do obrotu publicznego wtedy, gdy „Wielki Brat” może odczytywać zabezpieczone w tym programie wiadomości. Jeżeli chcemy mieć całkowitą pewność, że dysponujemy najlepszym możliwym zabezpieczeniem, nie należy korzystać z gotowych programów, ponieważ wówczas nie jesteśmy w stanie sprawdzić ich kodu źródłowego. Trzeba znaleźć algorytm znany od kilku lat i... napisać program szyfrujący we własnym zakresie. Używać go należy tylko w niezbędnych przypadkach. W przeciwnym razie dostarczymy przeciwnikowi... odpowiednio dużo materiałów do analizy.

Do bieżącej korespondencji można używać programów w rodzaju PGP z jak najdłuższymi kluczami. W ten sposób należy przysyłać tylko te wiadomości, które przestaną być aktualne po czasie, który będzie potrzebny na ewentualne złamanie zabezpieczeń.