

Szyfrowanie danych

Czym jest kryptografia?

Kryptografia to nauka zajmująca się układaniem szyfrów. Nazwa pochodzi z greckiego słowa: kryptos - "ukryty", gráphein "pisać,,.

Wyróżniane są dwa główne nurty kryptografii:

- **Kryptografia symetryczna**
- **Kryptografia asymetryczna**

Kryptografia symetryczna (symmetric cryptography)

Algorytmy z kluczem tajnym

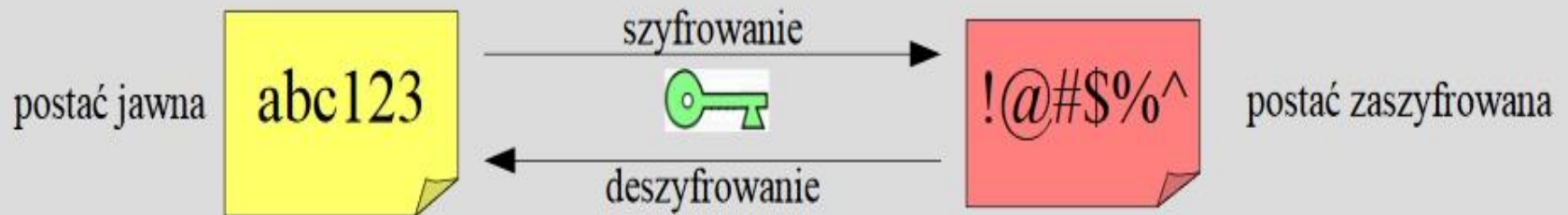
- ▶ Szyfrowanie z użyciem jednego klucza, wspólnego dla obu stron.
- ▶ Nadawca jak odbiorca wiadomości posługują się tym samym kluczem.
nadawcy - szyfrowania komunikatów,
adresatowi - do odszyfrowywania zakodowanej treści.
- ▶ konieczność uzgodnienia wspólnego klucza przed rozpoczęciem wymiany komunikatów.
- ▶ Musi istnieć sposób bezpiecznego przekazania tajnego klucza..
- ▶ Komunikacji za pomocą kanałów nie zapewniających należytego bezpieczeństwa.

Kryptografia asymetryczna

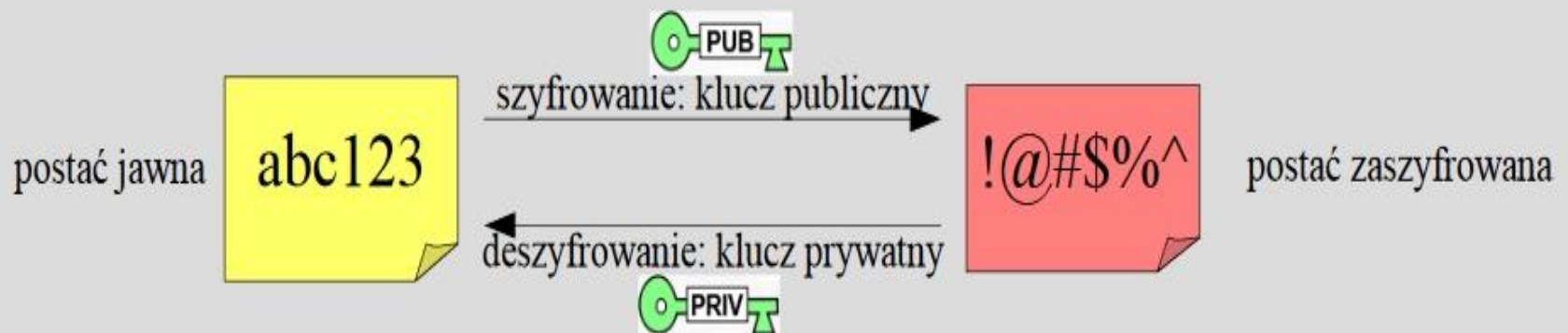
Algorytmy z kluczem publicznym

- ▶ Algorytmy z kluczem publicznym używają różnego klucza do szyfrowania i deszyfrowania, oraz klucz deszyfrującego.
- ▶ klucz deszyfrujący nie może (praktycznie) być wyprowadzony z klucza szyfrującego.
- ▶ Algorytmy te są ważne ponieważ mogą być używane do transmisji kluczy kodujących.

SZYFROWANIE SYMETRYCZNE



SZYFROWANIE ASYMETRYCZNE



klucze są matematycznie powiązane – prywatny: 2 liczby pierwsze (rzędu 100 cyfr) ,
publiczny: ich iloczyn
uzyskanie klucza prywatnego z publicznego praktycznie nierealne⁵. rozkład na czynniki
zajmuje kilka milionów lat

Przykładowe algorytmy szyfrujące

- ▶ RSA
- ▶ DES
- ▶ IDEA

RSA

- ▶ **RSA** to pierwszy i obecnie jeden z dwóch najpopularniejszych algorytmów kryptografii asymetrycznej.
- ▶ RSA opiera się na trudności faktoryzacji dużych liczb – znalezienie szybkiej metody faktoryzacji doprowadziłoby do złamania RSA.
- ▶ Najpowszechniej używanym algorytmem z kluczem publicznym.
- ▶ Może być używany zarówno do szyfrowania jak i do podpisywania.
- ▶ Jest uważany za bezpieczny gdy używa się odpowiednio długich kluczy (768 – stosunkowo mało bezpieczne, 4096 – dobre bezpieczeństwo).
- ▶ .RSA jest obecnie najważniejszym algorytmem z kluczem publicznym.
- ▶ Od 2000 roku jest produktem opensource.

DES

- ▶ DES jest oparty na kluczu prywatnym.
- ▶ DES jest blokowym algorytmem z 64 bitowym blokiem.
- ▶ DES używa kluczy 56 bitowych (podatny na złamanie)
- ▶ DES jest wystarczająco silny by zatrzymać większość przypadkowych hackerów i osób trzecich.
- ▶ DES staje się zbyt słaby i nie powinien być używany w nowych projektach kryptograficznych.
- ▶ Odmiana DESa - potrójny DES bazuje na używaniu DESa trzy razy (zazwyczaj sekwencji szyfruj-deszyfruj-szyfruj z trzema różnymi niepowiązanymi z sobą kluczami).

IDEA

(International Data Encryption Algorithm)

- ▶ IDEA używa 128 bitowego klucza i jest generalnie uważany za bardzo bezpieczny.
- ▶ Jest obecnie jednym z najbardziej znanych publicznie algorytmów.
- ▶ Jest stosunkowo nowym algorytmem.
- ▶ Nie udało się dotychczas przeprowadzić na niego udanego ataku.
- ▶ IDEA jest opatentowany w USA i w większości krajów europejskich.
- ▶ Nie komercyjne użycie IDEA jest darmowe.
- ▶ Poleca się używanie tego algorytmu.

Zadanie

- ▶ Odszukaj w dostępnych źródłach informacji przykłady innych algorytmów szyfrujących. W kilku zdaniach opisz ich cechy, sposób działania.

Szyfrowanie w WINDOWS

od Windows 7

Windows wyposażony jest w dwa narzędzia:

1. oparte na systemie plików EFS,
2. **BitLocker**

EFS

- ▶ System szyfrowania plików EFS dostępny jest od Windows 7 Professional wzwyż i wymaga dysku sformatowanego w systemie NTFS.
- ▶ Opiera się na kontach użytkowników i jest przezroczysty dla wszystkich operacji na danych. Oznacza to, że uprawniony użytkownik nie musi rozszyfrowywać pliku, by go otworzyć i zabezpieczać po zakończeniu pracy - operacje te są przeprowadzane automatycznie w tle.
- ▶ Zaszifrować można pojedynczy obiekt (na przykład plik) czy ich grupę (pliki i katalogi), a operacja szyfrowania polega na zaznaczeniu jednej opcji w jego właściwościach.
- ▶ Do szyfrowania wykorzystywany jest mechanizm hybrydowy. Plik szyfruje się kluczem symetrycznym, a dopiero ten klucz szyfrowany jest asymetrycznie. Podstawą tego zabezpieczenia jest hasło konta użytkownika. **Jeżeli ono będzie łatwe do uzyskania, szyfrowanie danych niewiele pomoże.**

BitLocker

- ▶ **BitLocker** szyfruje cały dysk. To zabezpieczenie jest przezroczyste dla operacji przeprowadzanych przez użytkownika.
- ▶ Ma ono za zadanie chronić **dane** przed niepowołanym dostępem w przypadku utraty całego komputera czy nośnika.
- ▶ Wbudowane zostało w **Windows 7 Ultimate i Enterprise**, wymaga dodatkowej, niewielkiej partycji startowej NTFS.
- ▶ Mechanizm **BitLocker** wykorzystuje do działania moduły TPM, użytkownik zmuszony jest podać PIN, umieścić w złączu USB nośnik zawierający klucz bądź użyć obydwu tych mechanizmów.
- ▶ Jeżeli pecet nie został wyposażony w TPM, można go uruchomić jedynie za pomocą nośnika USB z kluczem szyfrującym.
- ▶ Istnieje także wersja do zabezpieczania zewnętrznych nośników danych - BitLocker ToGo.

Szyfrowanie danych Windows 7

- ▶ 1. Aby zaszyfrować *dane* za pomocą mechanizmów EFS, kliknij obiekt (katalog, plik) prawym przyciskiem myszy i wybierz *Właściwości*. Na zakładce *Ogólne* użyj przycisku *Zaawansowane* w sekcji *Atrybuty*.

Atrybuty:



Tylko do odczytu (dotyczy tylko plików w folderze)



Ukryty

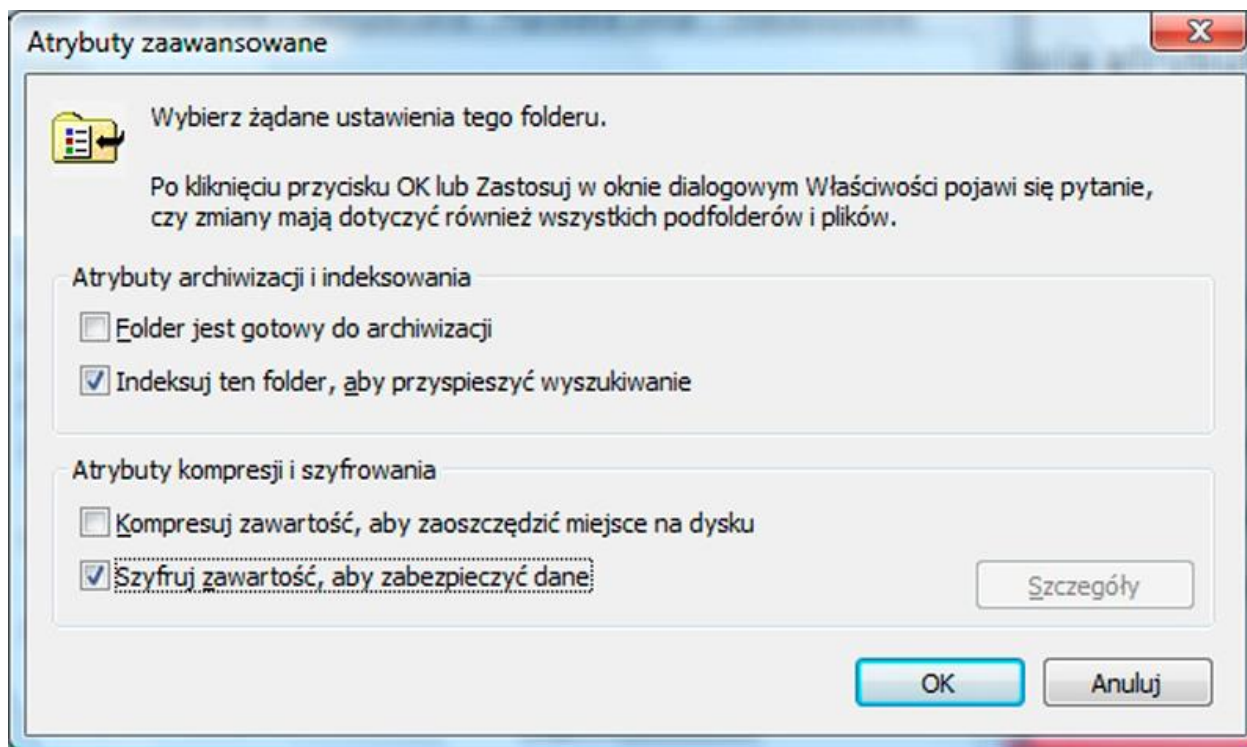
Zaawansowane...

- ▶ Szyfrowanie EFS włącza się tak samo, jak ustawia atrybuty pliku

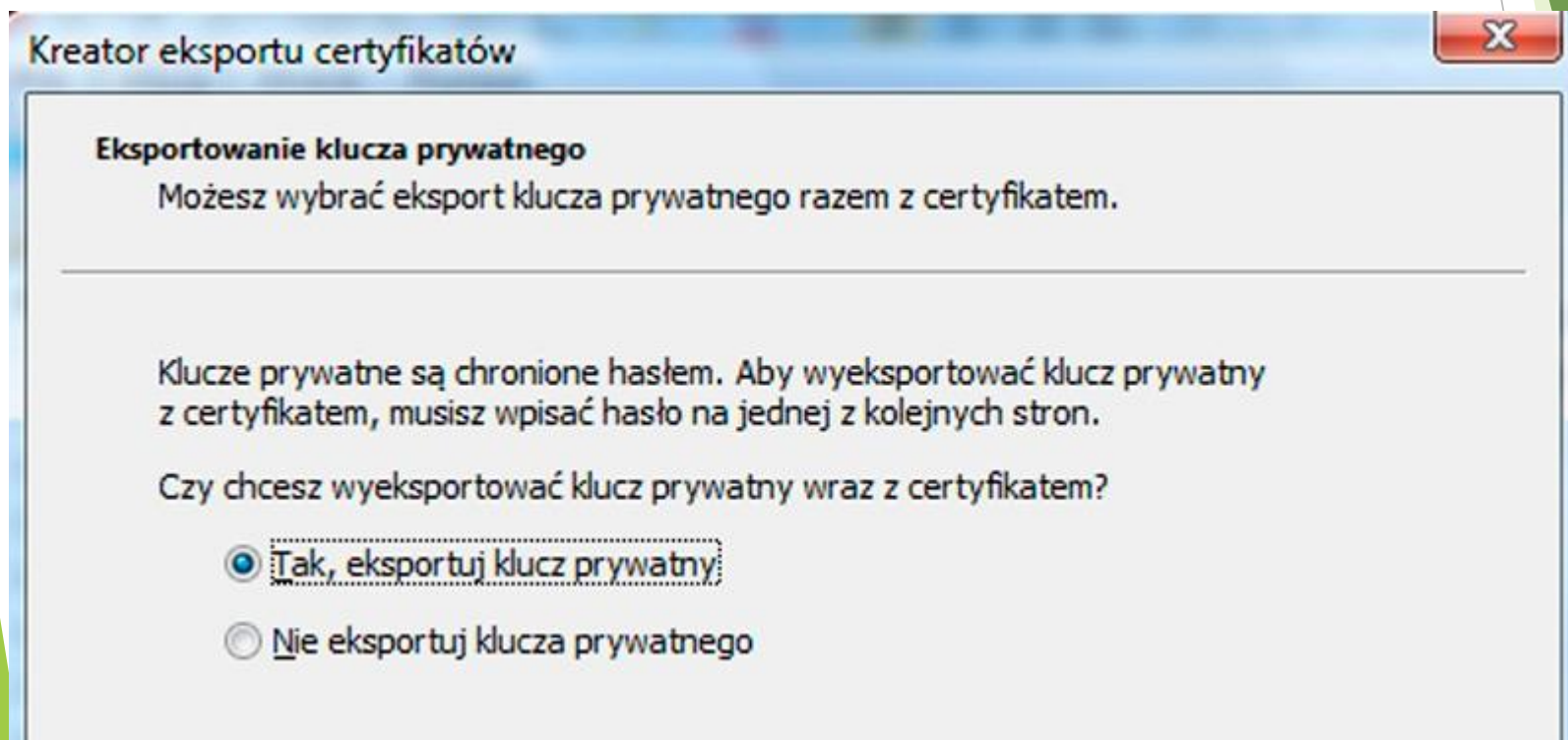
- ▶ 2. Zaznacz opcję *Szyfruj zawartość, aby zabezpieczyć dane* w sekcji *Atrybuty kompresji i szyfrowania*.

Uwaga: szyfrowanie i kompresja są opcjami rozłącznymi, nie można ich użyć jednocześnie. Kliknij OK w dwóch kolejnych oknach.

- ▶ Wybierz opcję *Zastosuj zmiany do tego folderu, podfolderów i plików*, co zagwarantuje, że wszystkie dane w katalogu również zostaną zaszyfrowane, i zaakceptuj wybór. Zabezpieczony katalog zostanie oznaczony zielonym kolorem



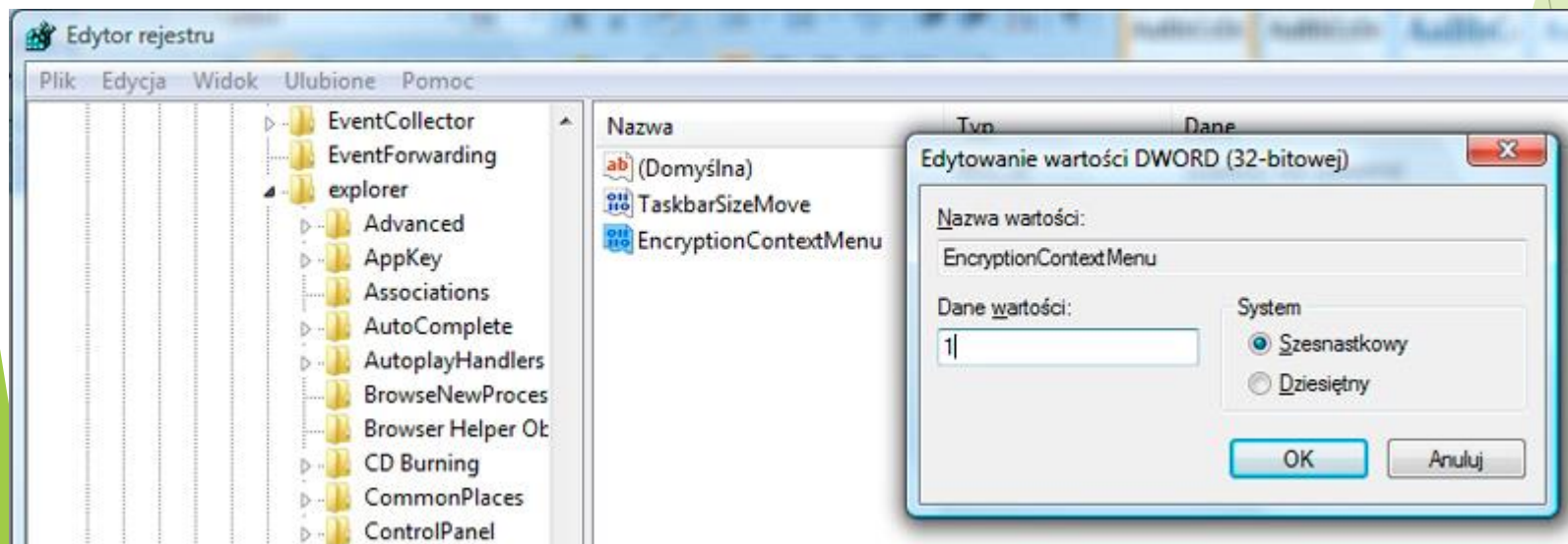
- ▶ 3. Reinstalacja systemu czy wykasowanie konta użytkownika może uniemożliwić dostęp do zaszyfrowanych danych. Dlatego należy wyeksportować certyfikat użytkownika oraz klucz, który w razie kłopotów pozwoli odczytać pliki. W tym celu rozwiń menu startowe, wpisz polecenie *certmgr.msc* i wciśnij [ENTER]. Rozwiń folder Osobisty i kliknij Certyfikaty. Zaznacz w prawej części okna certyfikat, który w kolumnie *Zamierzone cele* ma opis *System szyfrowania plików*.



- ▶ 4. Rozwiń menu *Akcja*, wybierz *Wszystkie zadania i Eksportuj*. W kolejnych krokach kreatora, w oknie Eksportowanie klucza prywatnego zaznacz opcję *Tak, eksportuj klucz prywatny*. Przejdź dalej. Zaznacz *Wymiana informacji osobistych* i ponownie kliknij *Dalej*.
- ▶ 5. Klucz prywatny musi być chroniony za pomocą dodatkowego hasła. Wpisz je dwukrotnie. Określ nazwę i wskaż miejsce, gdzie ma zostać zapisany plik z certyfikatem, i zakończ pracę kreatora przyciskiem *Zakończ*. Zabezpiecz plik certyfikatu, wgrywając go najlepiej na dysk przenośny i umieszczając w niedostępnym dla osób nieupoważnionych miejscu. Odzyskiwanie **dostępu do danych** przeprowadza się za pomocą tego samego menedżera. Wystarczy zaimportować zapisany plik.

Szyfrowanie w menu kontekstowym

- ▶ Aby zaszyfrować plik bądź katalog za pomocą funkcji dostępnej w systemie, trzeba najpierw otworzyć właściwości danego obiektu, a następnie wybrać odpowiednią zakładkę i przycisk. Jeżeli często szyfrujesz różne dane, na pewno skorzystasz z możliwości umieszczenia odpowiedniego polecenia w menu kontekstowym Eksploratora Windows. Uruchom w tym celu edytor rejestru i otwórz kolejno następujące klucze: *HKEY_LOCAL_MACHINE | SOFTWARE | Microsoft | Windows | CurrentVersion i Explorer*. Zaznacz klucz *Advanced*.



Szyfrowanie w menu kontekstowym

- ▶ Kliknij prawym przyciskiem myszy w prawej części okna, wybierz polecenie *Nowy i Wartość DWORD*. Nadaj wartości nazwę *EncryptionContextMenu*, wciśnij dwukrotnie [ENTER] i jako daną wartości wpisz 1. Zaakceptuj zmiany i zamknij edytor. Polecenie szyfrowania zostanie dodane do menu.

