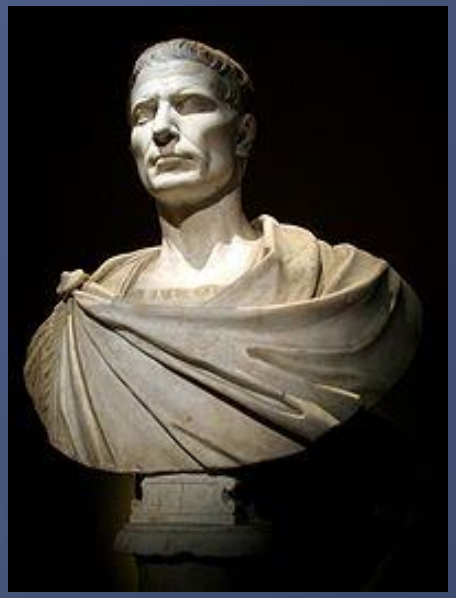
BEZPIECZEŃSTWO DANYCH

Szyfr Cezara



- Ludzie od dawien dawna próbowali utajniać wysyłane do siebie wiadomości. Robili to za pomocą szyfrowania przekazywanych sobie tekstów przy użyciu wymyślanych przez siebie mechanizmów (szyfrów).
- Jeszcze przed naszą erą datują się pierwsze takie próby…
- Przykładem może być szyfr Cezara – nazwa pochodzi od rzymskiego władcy (100 r. p.n.e. – 44 r. p.n.e.) Juliusza Cezara, który szyfrował swoją korespondencję z Cyceronem (mówca, filozof i polityk rzymski).

Szyfr Cezara

Login – uczen
Hasło - qwerty

- Zamiast każdej litery pisano literę występującą w alfabecie trzy miejsca dalej. Tak więc, jeśli użyjemy dzisiejszego alfabetu łacińskiego

  abcdefghijklmnopqrstuvwxyz

  to zamiast c będziemy pisać f, zamiast *g* piszemy *j*, zamiast *y* piszemy *b*. Alfabet traktujemy cyklicznie, tzn. po ostatniej literze *z* następuje ponownie litera *a* itd.
- Aby zobaczyć jak działało szyfrowanie według starożytnych zajrzyj na tę stronę:

http://www.math.edu.pl/szyfr-cezara

Inne szyfry klasyczne

- Szachownica Polibiusza
- Szyfr afiniczny
- Szyfr Bacona
- Szyfr Beauforta
- Szyfr cmentarny
- Dysk Jeffersona – urządzenie szyfrujące
- Szyfr Vernama
- Szyfr Vigenère'a
- Szyfr Ottendorfa

Szachownica Polibiusza

Rodzaj szyfru monoalfabetycznego wymyślony w starożytności przez greckiego historyka Polibiusza. Szyfr ten przypisuje każdej literze liczbę, według następującej tabeli:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Cyfry oznaczają położenie danej litery w tabeli – pierwszą cyfrą jest numer wiersza, a drugą – kolumny. Tak na przykład tekst:

ŚCIŚLE TAJNE

kryptografia

po zaszyfrowaniu (nie uwzględniając polskich znaków) przyjmuje postać:

43 13 24 43 31 15 44 11 24 33 15

Bezpieczeństwo danych

Wspomniane sposoby zabezpieczania przekazywanych informacji to już historia i to nawet zamierzchła.

Dzisiaj w dobie tak szybkiego rozwoju technologii informacyjnej i komputeryzacji kiedy wiele ważnych danych przekazujemy właśnie w formie elektronicznej potrzebne są bardziej skomplikowane metody zabezpieczające dane przesyłane przez sieć.

Mam na myśli:

- szyfrowanie listów elektronicznych,
- szyfrowanie stron WWW oraz
- podpis elektroniczny.

Dba o to nauka zwana kryptografią.

Czym jest kryptografia?

Kryptografia zajmuje się praktycznym zastosowaniem wiedzy matematycznej w celu ochrony danych przechowywanych w komputerach, podczas przesyłu informacji przez sieć komputerową, w której występują dane w postaci cyfrowej.

Ma ona ogromne znaczenie w ochronie danych komputerowych.

Nie jest to oczywiście pełny opis, ponieważ kryptografia zajmowała się ochroną danych ogólnie, nie tylko komputerowych, jednak w dzisiejszych czasach ma to już raczej tylko znaczenie historyczne.

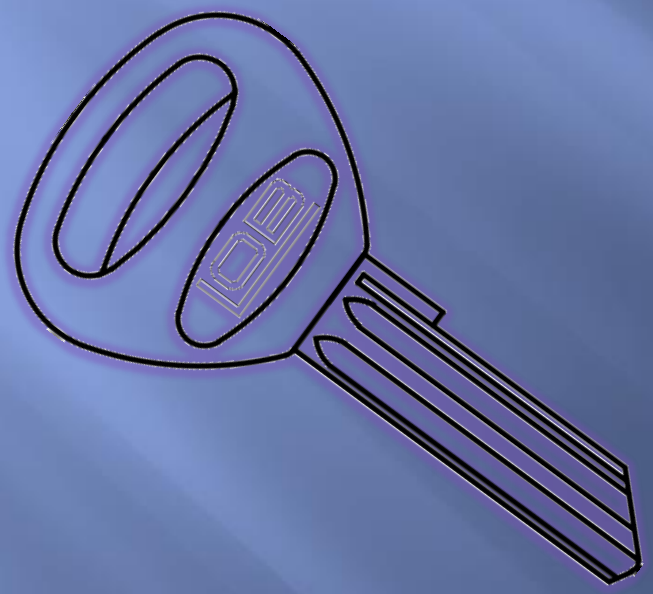
Podstawowe pojęcia

- Szyfrowanie (kodowanie) - proces przekształcania tekstu jawnego w szyfrogram tak, że zostaje ukryta jego zawartość przed osobami postronnymi. Do przekształcenia używa się algorytmu szyfrującego.

Podstawowe pojęcia

- Tekst jawny - tekst w postaci pierwotnej, zrozumiałej dla nadawcy i odbiorcy, który zostanie poddany procesowi szyfrowania. Taki tekst może być również odczytany przez osobę trzecią, nieupoważnioną do tego.
- Szyfrogram - tekst zakodowany, w postaci niezrozumiałej dla nadawcy i odbiorcy, który wymaga odszyfrowania.
- Deszyfrowanie (dekodowanie) - proces przekształcania szyfrogramu w tekst jawny tak, że jego zawartość zostaje ponownie odkryta. Do przekształcenia używa się algorytmu deszyfrującego.

Podstawowe pojęcia



Klucz – w kryptografii informacja umożliwiająca wykonywanie pewnej czynności kryptograficznej – szyfrowania, deszyfrowania, podpisywania, weryfikacji podpisu itp.

Podstawowe pojęcia

Kryptografia symetryczna

- W algorytmach symetrycznych **klucz** służy do szyfrowania i deszyfrowania wiadomości. Do obu tych czynności używa się tego samego klucza, dlatego powinien być znany tylko uczestnikom.

Kryptografia asymetryczna

W kryptosystemach asymetrycznych wyróżniamy klucz **publiczny** oraz **prywatny**. Ten pierwszy może być zupełnie jawny, drugi powinien znać tylko właściciel.

Dwie najważniejsze funkcje kryptografii asymetrycznej to:

- **szyfrowanie** – wtedy klucz publiczny służy do szyfrowania, a prywatny do deszyfrowania
- **podpisy cyfrowe** – klucz prywatny służy do generacji podpisów, klucz publiczny do ich weryfikacji

Podpis cyfrowy

- Podpis cyfrowy jest blokiem danych, który został wygenerowany za pomocą określonego tajnego klucza oraz istnieje klucz publiczny, który może być użyty do weryfikacji czy podpis został naprawdę wygenerowany za pomocą odpowiadającego mu klucza prywatnego.
- Podpisy cyfrowe są używane do weryfikacji czy wiadomość naprawdę pochodzi od właściwego nadawcy (zakładając, że tylko nadawca zna klucz prywatny odpowiadający jego kluczowi publicznemu).

Funkcje podpisu

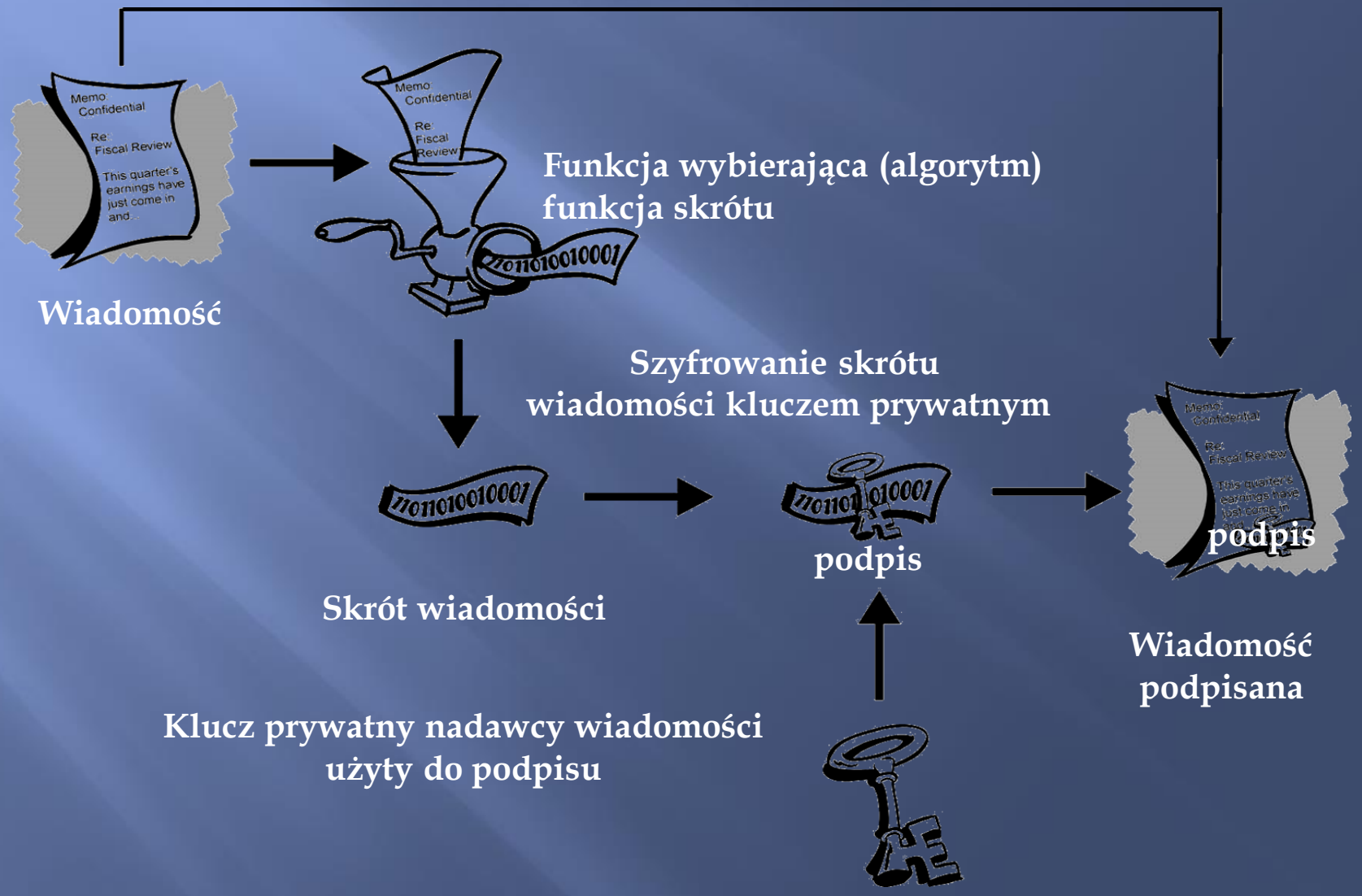
Podpis tradycyjny (odręczny)

Podpis elektroniczny

1001101001011001011010101110000100101111100001111000100110100000010101011101010011000010111010 01...

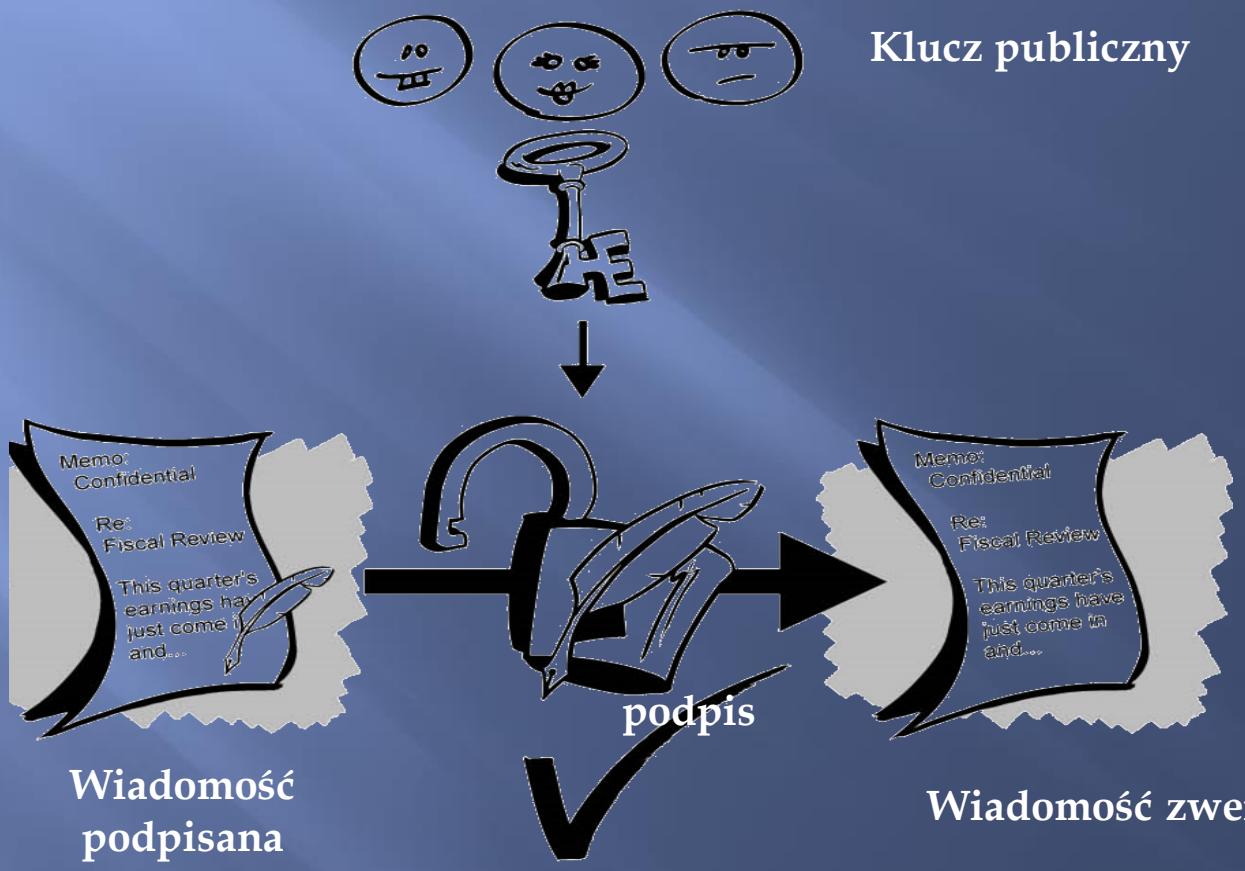
- Związany z określoną osobą
- Związany z określonym dokumentem
- Istnieje możliwość weryfikacji podpisu

Proces podpisywania wiadomości

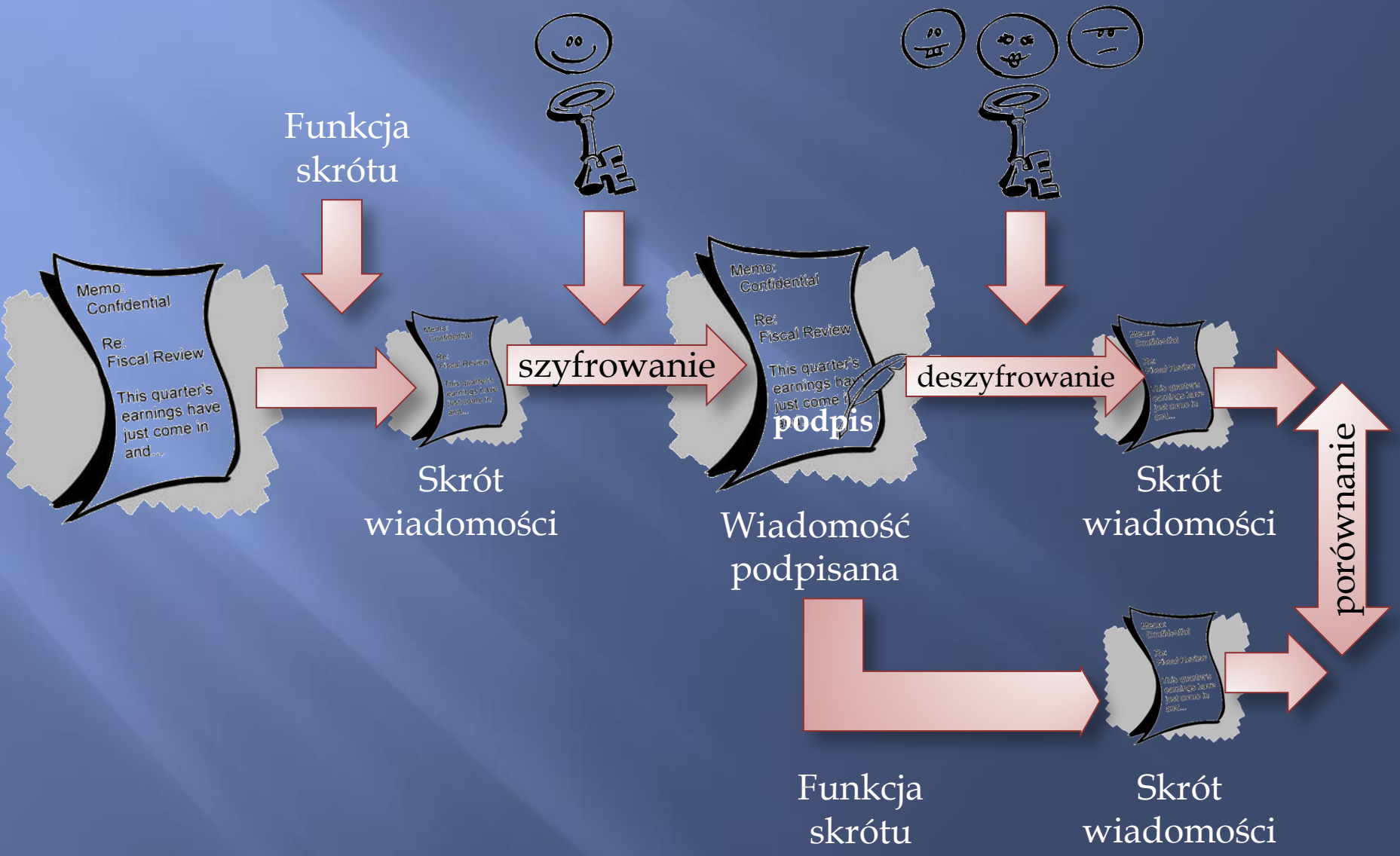


Weryfikacja podpisu

Weryfikacja przebiega automatycznie i wykorzystuje klucz publiczny autora podpisu



Podpisywanie i weryfikacja



Podpis cyfrowy a prawo

Polska:

Ustawa z dnia 18 września 2001r. o podpisie elektronicznym zrównuje go w oczach prawa z ręcznym

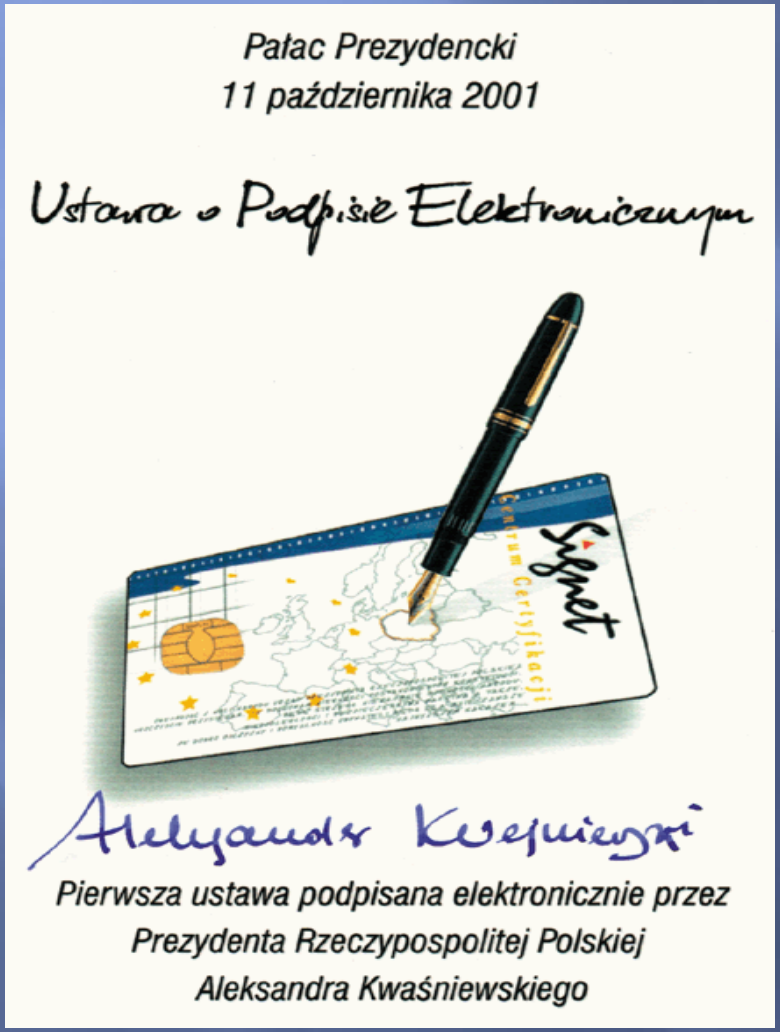
Unia Europejska:

Dyrektywa z 13 grudnia 1999r. Parlamentu Europejskiego i Rady, dotycząca podpisów elektronicznych (*UE 99/93*)

Stany Zjednoczone:

Ustawa o podpisach elektronicznych w obrocie krajowym i globalnym z 24 stycznia 2000r. (*E-SIGN*)

Oficjalny pierwszy podpis elektroniczny



Prezydent RP Aleksander Kwaśniewski podpisał ustawę na dwa sposoby: tradycyjnie (piórem) oraz elektronicznie - z wykorzystaniem specjalnej karty z mikroprocesorem.

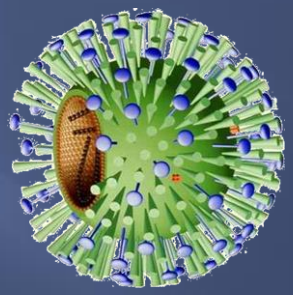
Notatka

1. Szyfrowanie - proces przekształcania tekstu jawnego w szyfrogram tak, że zostaje ukryta jego zawartość przed osobami postronnymi.
2. Deszyfrowanie - proces przekształcania szyfrogramu w tekst jawny tak, że jego zawartość zostaje ponownie odkryta.
3. Klucz – w kryptografii informacja umożliwiająca wykonywanie pewnej czynności kryptograficznej – szyfrowania, deszyfrowania, podpisywania, weryfikacji podpisu itp.
4. Kryptografia symetryczna – ten sam klucz służy do szyfrowania i deszyfrowania wiadomości.
5. Kryptografia asymetryczna – wymaga używania dwóch kluczy publicznego i prywatnego (tajnego).
6. Podpis cyfrowy jest blokiem danych, który został wygenerowany za pomocą określonego tajnego klucza oraz istnieje klucz publiczny, który może być użyty do jego weryfikacji.
7. Tworzenie podpisu – podpisywany dokument jest traktowany funkcją skrótu, w wyniku czego powstaje skrót wiadomości, który jest szyfrowany kluczem prywatnym. W efekcie powstaje podpis cyfrowy, który jest dołączany do dokumentu. Odbiorca deszyfruje podpis za pomocą klucza publicznego i otrzymuje skrót dokumentu. Jednocześnie dokument traktowany jest funkcją skrótu – powstaje drugi skrót. Jeśli oba skróty są identyczne, to podpis zostaje zweryfikowany.

Wirusy, robaki, trojany

Wirus komputerowy to krótki program komputerowy, zwykle szkodzący systemowi operacyjnemu lub utrudniający pracę użytkownikowi komputera. Każdy wirus ma zdolność samopowielania.

wirus komputerowy



wirus grypy

- Potrzebuje organizmu, w którym będzie żył (plik)
- Namnaża się gdy dostanie się do organizmu
- Samoreplikacja odbywa się bez udziału organizmu

Wirusy, robaki, trojany

Robak komputerowy to samoreplikujący się program komputerowy, podobny do wirusa komputerowego.

Główną różnicą jest to, że podczas gdy wirus potrzebuje nosiciela - jakiegoś pliku wykonywalnego, który modyfikuje doczepiając do niego swój kod wykonywalny, to robak jest pod tym względem samodzielny a rozprzestrzenia się poprzez:

- wykorzystanie luk w systemie,
- naiwność użytkownika .

Oprócz replikacji, robak może mieć wbudowane procedury dodatkowe, takie jak niszczenie systemu plików lub wysyłanie poczty.

Wirusy, robaki, trojany

Koń trojański, trojan to określenie oprogramowania, które podszywając się pod przydatne lub ciekawe dla użytkownika aplikacje dodatkowo implementuje niepożądane, ukryte przed użytkownikiem funkcje (programy szpiegujące, bomby logiczne, furtki umożliwiające przejęcie kontroli nad systemem przez nieuprawnione osoby itp.). Nazwa pochodzi od mitologicznego konia trojańskiego.

Najpopularniejszymi szkodliwymi działaniami są:

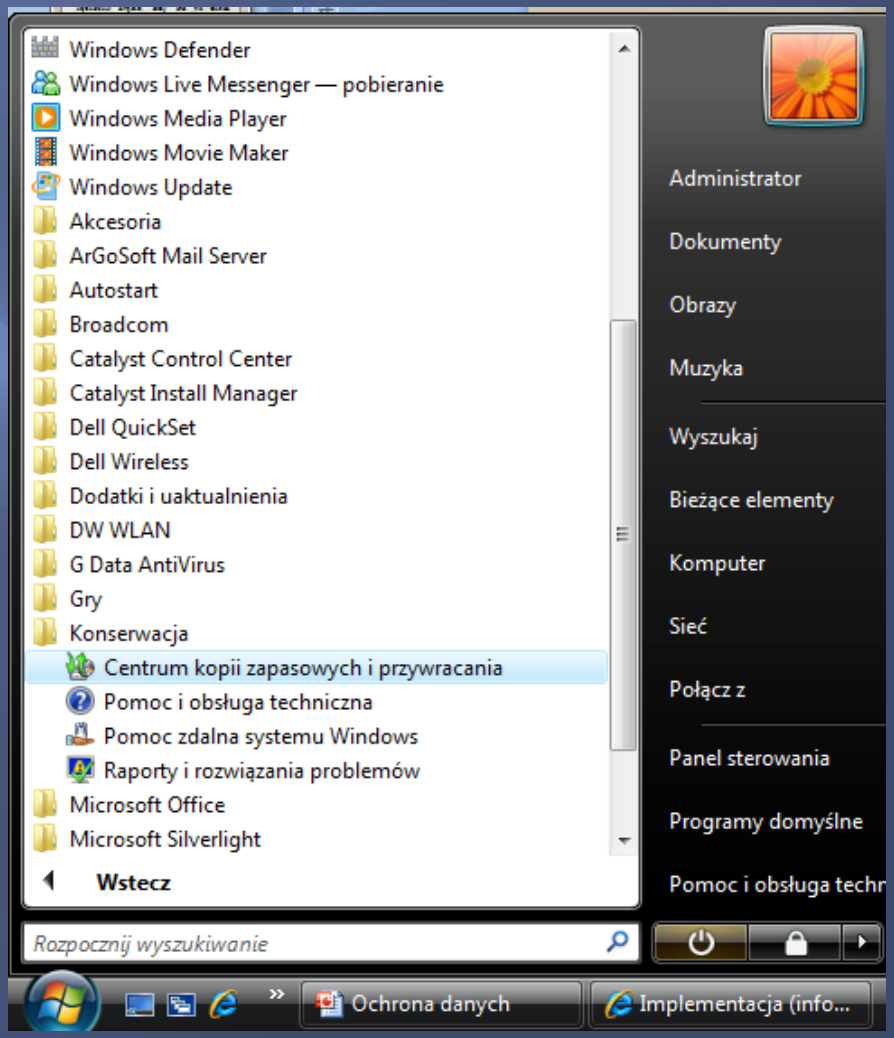
- instalowanie w systemie back doora i udostępnianie kontroli nad systemem nieuprawnionym osobom w celu rozsyłania spamu,
- szpiegowanie i wykradanie poufnych danych użytkownika (spyware),
- utrudnianie pracy programom antywirusowym,
- zmienianie strony startowej przeglądarki WWW i prezentowanie reklam,
- działania destruktywne (kasowanie plików, uniemożliwianie korzystania z komputera).

Profilaktyka

- Nie uruchamiaj nieznanych programów
- Nośniki pamięci wkładane do komputera sprawdzaj programem antywirusowym
- Nie wyrażaj zgody na instalowanie programów dostępowych do stron internetowych
- Zainstaluj oprogramowanie antywirusowe i uaktualniaj bazę danych z informacjami o wirusach
- Instaluj poprawki do sytemu operacyjnego – ataki następują po wykryciu błędów w systemie
- Aby utrudnić uruchamianie programów bez twojej wiedzy zainstaluj zaporę sieciową np. ZoneAlarm darmowy program
- Zainstaluj tez program wykrywający trojany i programy szpiegowskie np. Ad-aware

Kopie zapasowe

Kopia, która umożliwia odzyskanie danych po awarii komputera powinna:

- Zawierać wszystkie istotne pliki
- Być aktualna
- Znajdować się na nośniku innym niż ten, który uległ awarii

W najprostszym przypadku można archiwizować dane za pomocą programu do archiwizacji np. WinZip, WinRAR, EasyZip