Dane

Marcin Szeliga
marcin@wss.pl

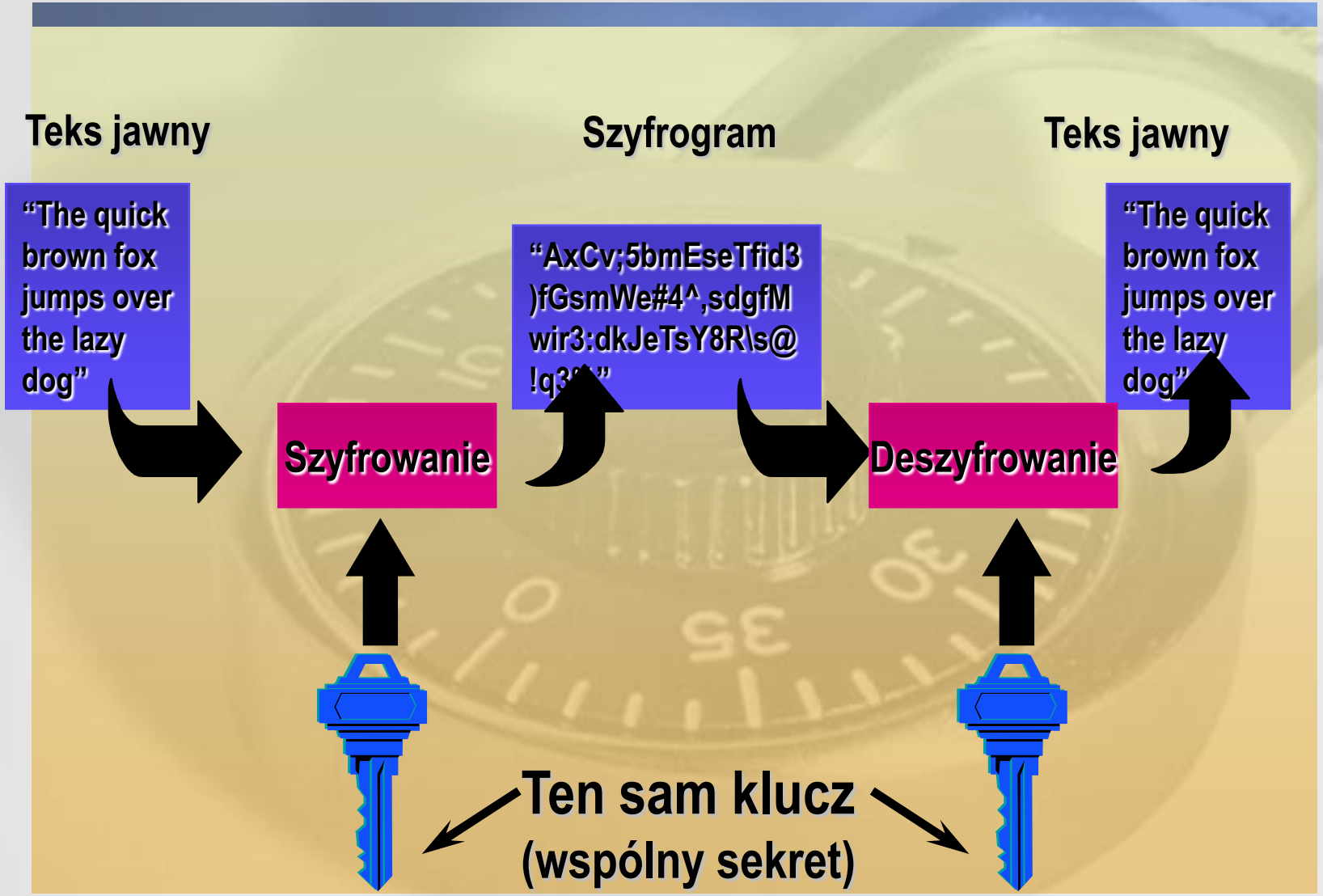
Agenda

- **Kryptologia**
  - Szyfrowanie symetryczne
    - Tryby szyfrów blokowych
  - Szyfrowanie asymetryczne
  - Systemy hybrydowe
  - Podpis cyfrowy
- **Kontrola dostępu do danych**

Kryptologia

- **Model dogłębnej obrony**
  - Kryptografia w roli ostatniej linii obrony
- **Zasada najsłabszego ogniwa**
  - Szyfrogram jest co najwyżej tak bezpieczny jak klucz deszyfrujący
  - Udany atak kryptoanalityczny pozostanie niewykryty
- **Zasada Kerckhoffsa:**
  - Bezpieczeństwo szyfrogramu powinno zależeć wyłącznie od ukrycia klucza, a nie ukrycia użytego do szyfrowania i deszyfrowania algorytmu

Kryptologia - Algorytmy symetryczne



Kryptologia - Algorytmy symetryczne

- **Zalety:**
  - Szybkość (od 1 000 do 10 000 razy większa niż algorytmów asymetrycznych
  - Łatwa i tania implementacja sprzętowa
- **Wady:**
  - Konieczność uzgodnienia klucza
  - Ogromna liczba kluczy - $n(n–1)/2$, gdzie n jest liczbą użytkowników systemu (1225 dla n=50)

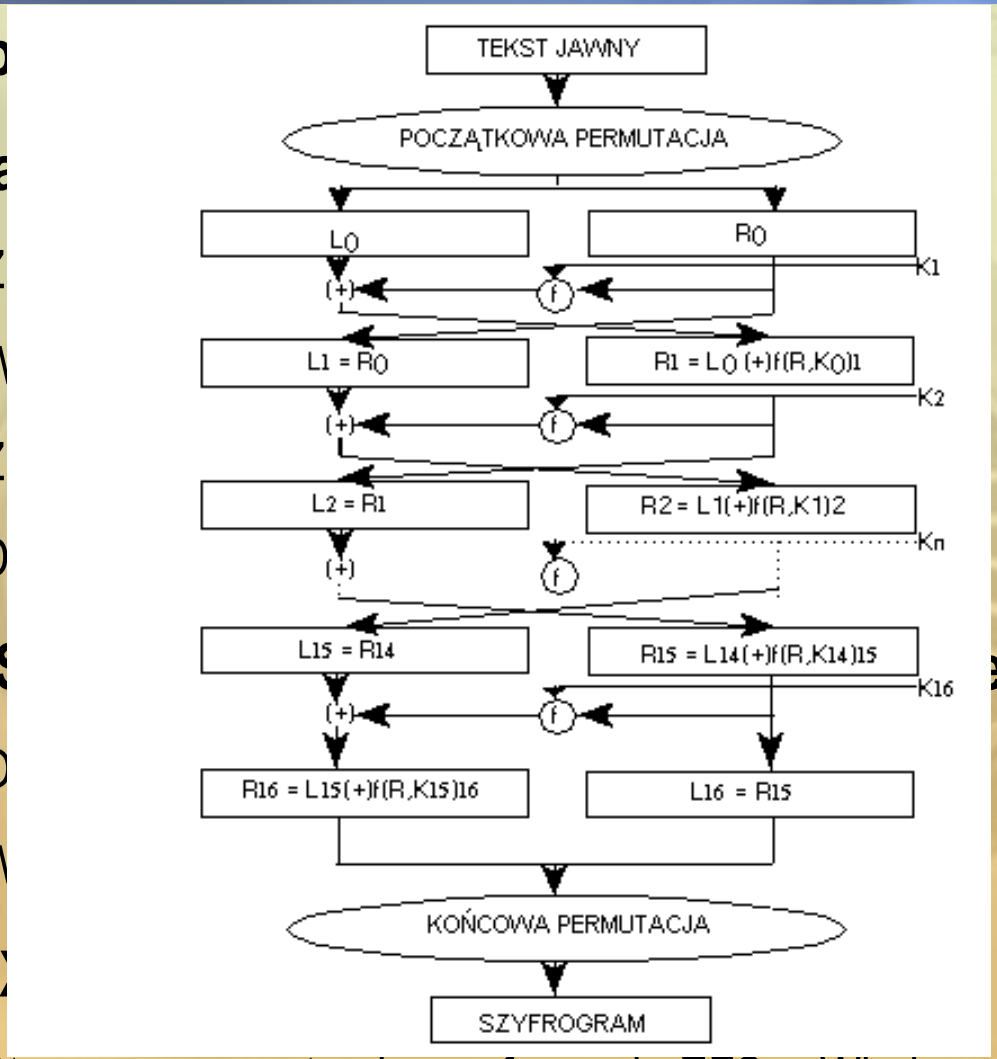
Kryptologia - Algorytmy symetryczne

- **AES (Advanced Encryption Standard)**
  - Od nazwisk twórców nazwany Rijndael
  - Zwycięzca konkursu 1997-2000 NIST na następcę protokołu DES
  - Bezpieczny
  - Szybki (wydajność zależy od dł. klucza)
  - Używa128, 196 lub 256 bitowych kluczy

  Ze względu na kolizje klucze o długości n bitów gwarantują bezpieczeństwo na poziomie n/2 bitów

Kryptologia - Algorytmy symetryczne

- DES - op
  - Poda
    - Z
    - W
    - Z
    - D
  - 3DES
    - O
    - W
  - DES
    - Stworzony na potrzeby szyfrowania EFS w Windows 2000



Kryptologia - Algorytmy symetryczne

- **RC2 (RC - Ron's Code) :**
  - Został zamówiony w 1987 przez firmę Lotus
  - Ujawniony w 1996
  - Blok o długości
  - Faktyczne b mie 34 bitów
- **RC4 :**
  - Opracowany w 994
  - Klucze o długości 4 w
  - Kłopoty z implementacją
  - Szyfrogram ujawnia informacje o kluczu

Kryptologia – Tryby szyfrów blokowych

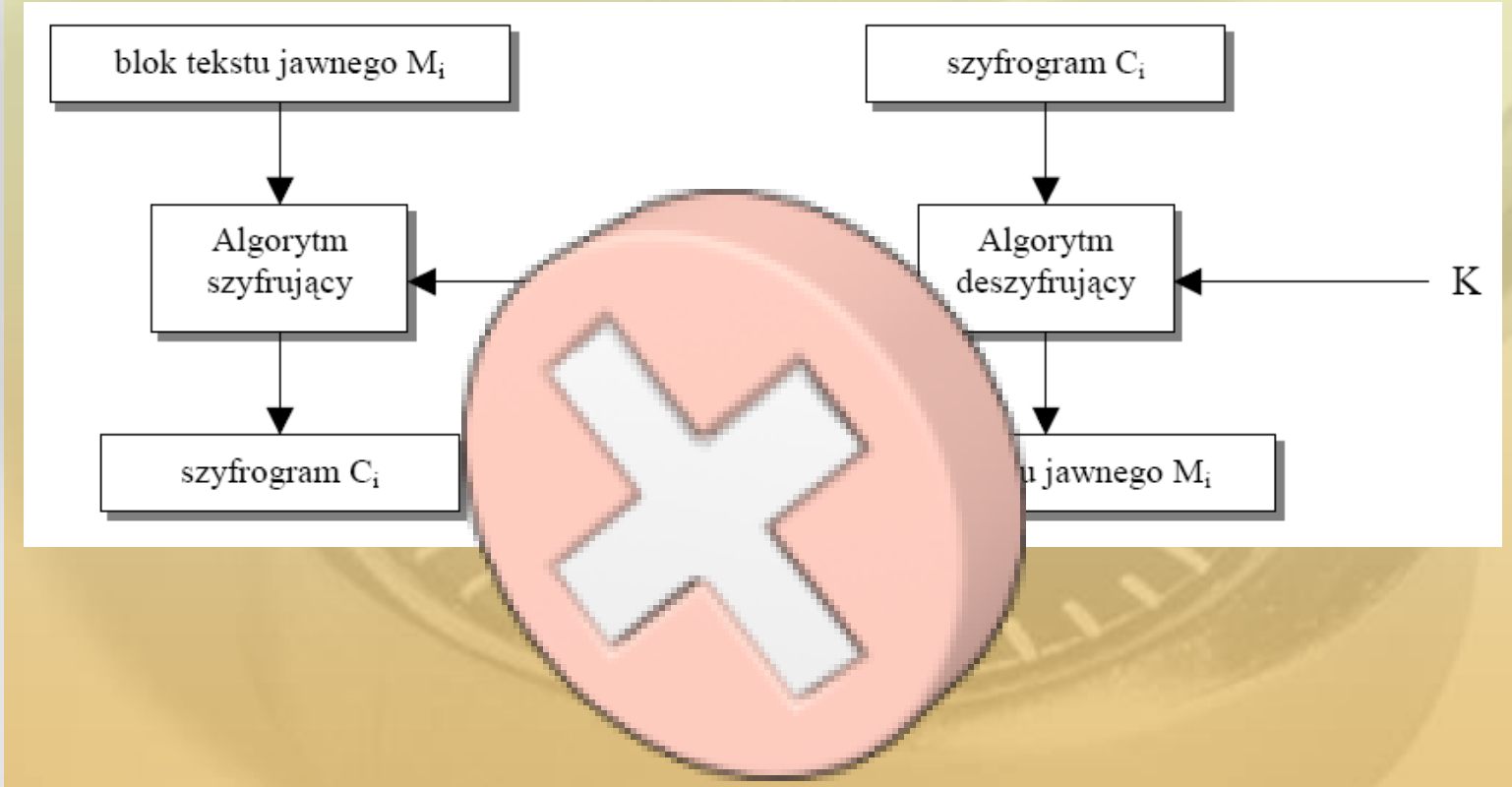
- **Szyfry blokowe umożliwiają jedynie szyfrowanie bloku tekstu jawnego o ściśle określonej długości, podczas gdy my chcemy zaszyfrować strumień danych…**
- **Tryby przekształcania strumieni w bloki o określonej długości:**
  - Tryb elektronicznej książki kodowej ECB
  - Tryb łańcuchowego szyfru blokowego CBC
  - Tryb sprzężenia zwrotnego OFB
  - Tryb licznika CTR

Kryptologia – Tryby szyfrów blokowych

- **Tryb elektronicznej książki kodowej ECB**
  - Dane są dzielone na bloki o określonej długości
  - Kolejne bloki są szyfrowane tym samym kluczem
- **Wada - identycznym blokom tekstu jawnego będą odpowiadały identyczne bloki szyfrogramu**

Kryptologia – Tryby szyfrów blokowych

- **ECB – Zasada działania**

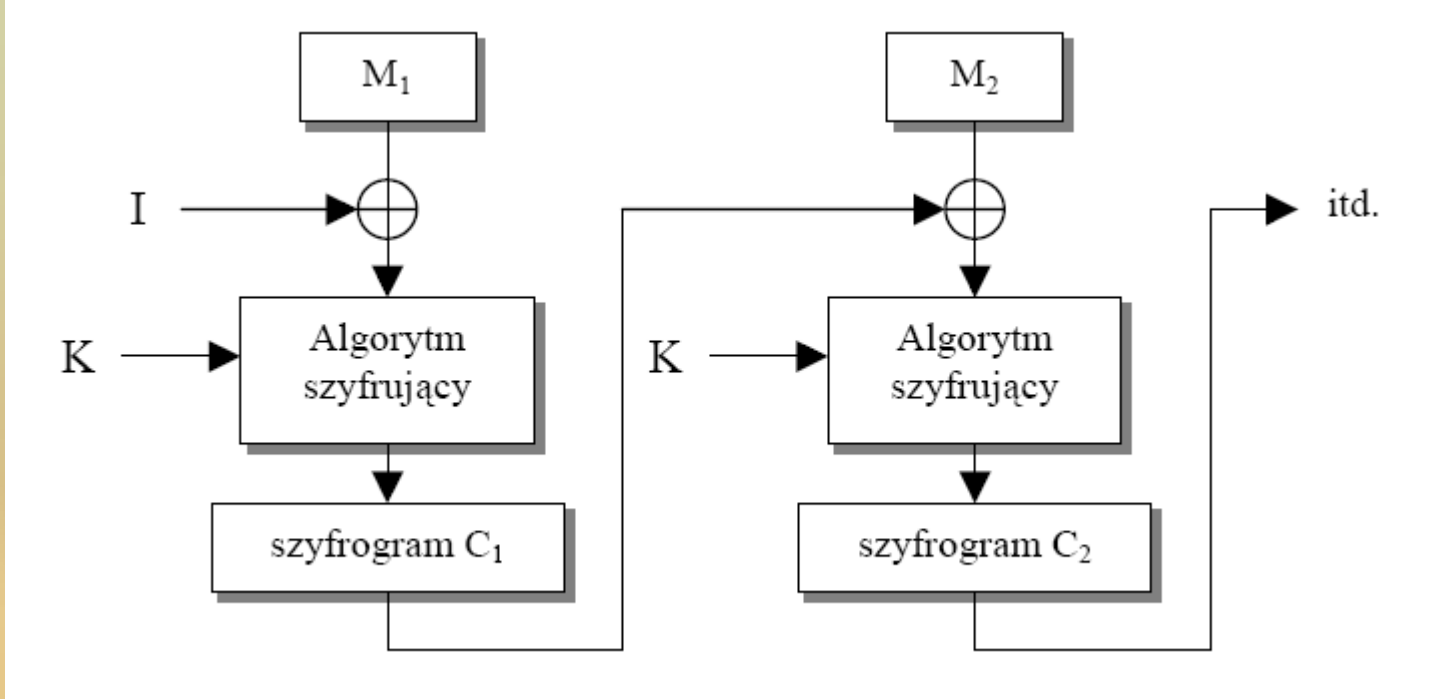


Kryptologia – Tryby szyfrów blokowych

- **Tryb łańcuchowego szyfru blokowego CBC**
  - każdy blok tekstu jawnego przed zaszyfrowaniem jest przekształcany funkcją XOR z szyfrogramem uzyskanym poprzez zaszyfrowanie poprzedniego bloku wiadomości
  - pierwszy blok wiadomości jest szyfrowany przy użyciu wektora inicjującego IV

Kryptologia – Tryby szyfrów blokowych

- **CCB – Zasada działania**

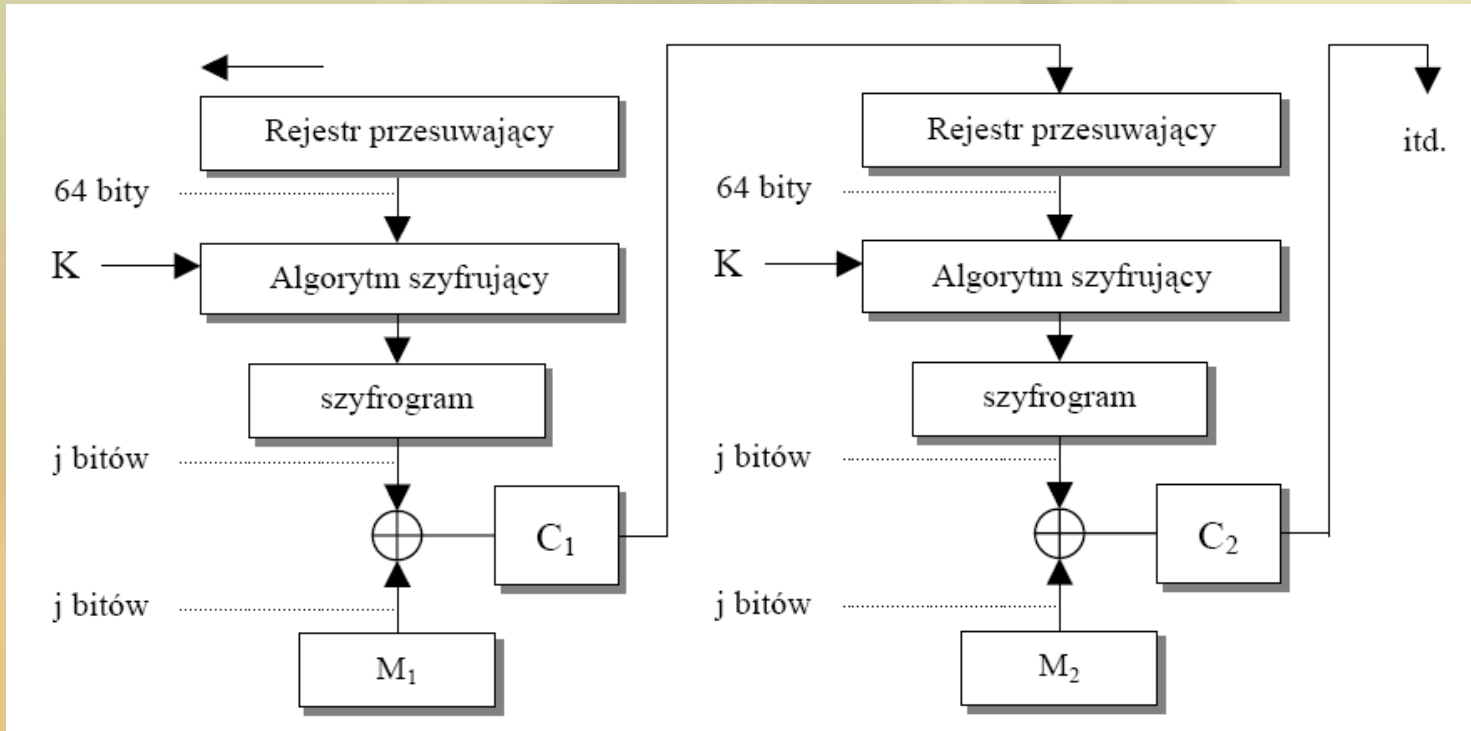


Kryptologia – Tryby szyfrów blokowych

- **Tryby sprzężenia zwrotnego OFB i CFB:**
  - Wybierany jest wektor inicjujący
  - Wektor inicjujący jest szyfrowany
  - Uzyskany szyfrogram jest wykorzystywany jako:
    - początek strumienia szyfrującego dla funkcji XOR,
    - Tekst jawny, którego zaszyfrowanie dostarczy kolejny fragment strumienia szyfrującego

Kryptologia – Tryby szyfrów blokowych

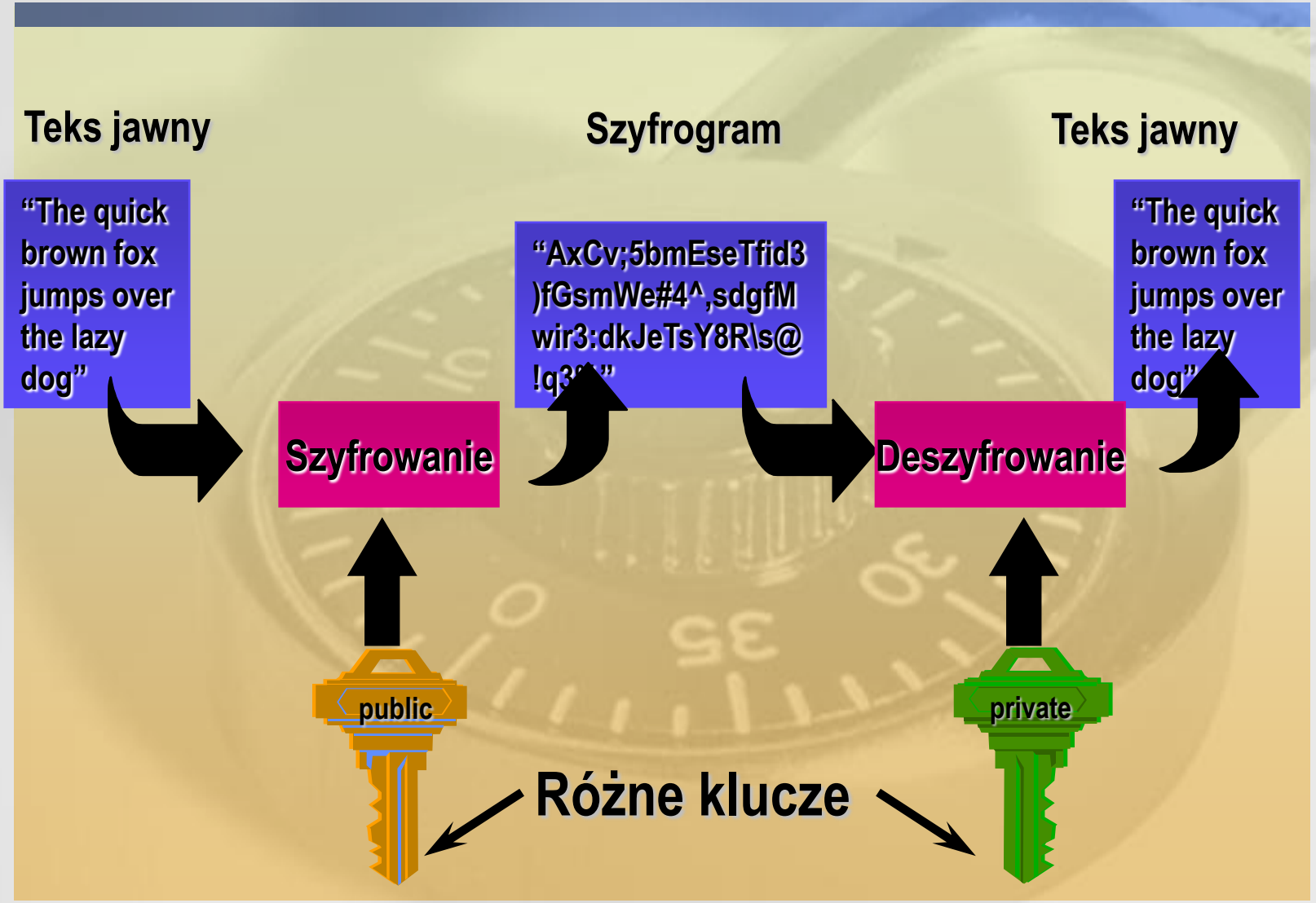
- **CFB – Zasada działania**



Kryptologia – Tryby szyfrów blokowych

- **Tryb licznika CTR:**
  - Popularny tryb szyfrów blokowych
  - Umożliwia odszyfrowanie wybranego bloku bez konieczności deszyfrowania całego szyfrogramu
  - Przypomina tryb OFB:
    - Wybierany jest wektor inicjujący
    - Wektor inicjujący jest szyfrowany
    - Otrzymany szyfrogram jest mieszany funkcją XOR z wiadomością

Kryptologia – Algorytmy asymetryczne



Kryptologia - Algorytmy asymetryczne

- **Zalety:**
  - Rozwiązuje problem bezpiecznej wymiany kluczy
  - Redukuje liczbę kluczy
  - Pozwala na zbudowanie relacji zaufania
- **Wady:**
  - Bardzo mała wydajność
  - Problem rozszerzenia zaufania z komputera na ludzi (organizacje)

Kryptologia - RSA

- **Opracowany przez Rivesta, Shamira, Adlemana w 1968**
- **Podstawą jest „funkcja zapadkowa”:**
  - Wybierz dwie wielkie liczby pierwsze p i q: p = 7, q = 11
  - Oblicz iloczyn n = p*q: n = 77

512 bitowy klucz odpowiada sile 60 bitowych kluczy algorytmów symetrycznych

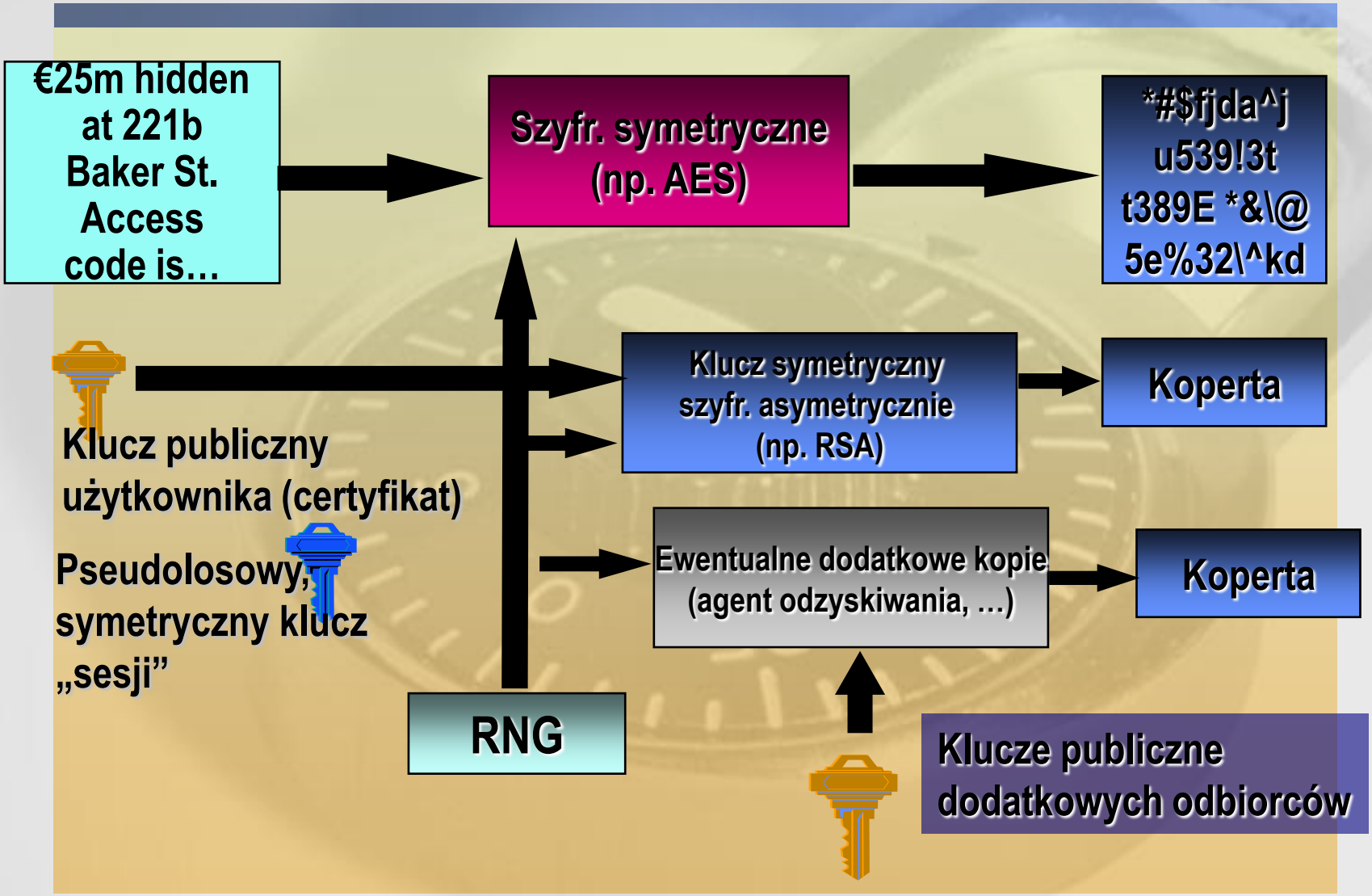
NWD

31 =

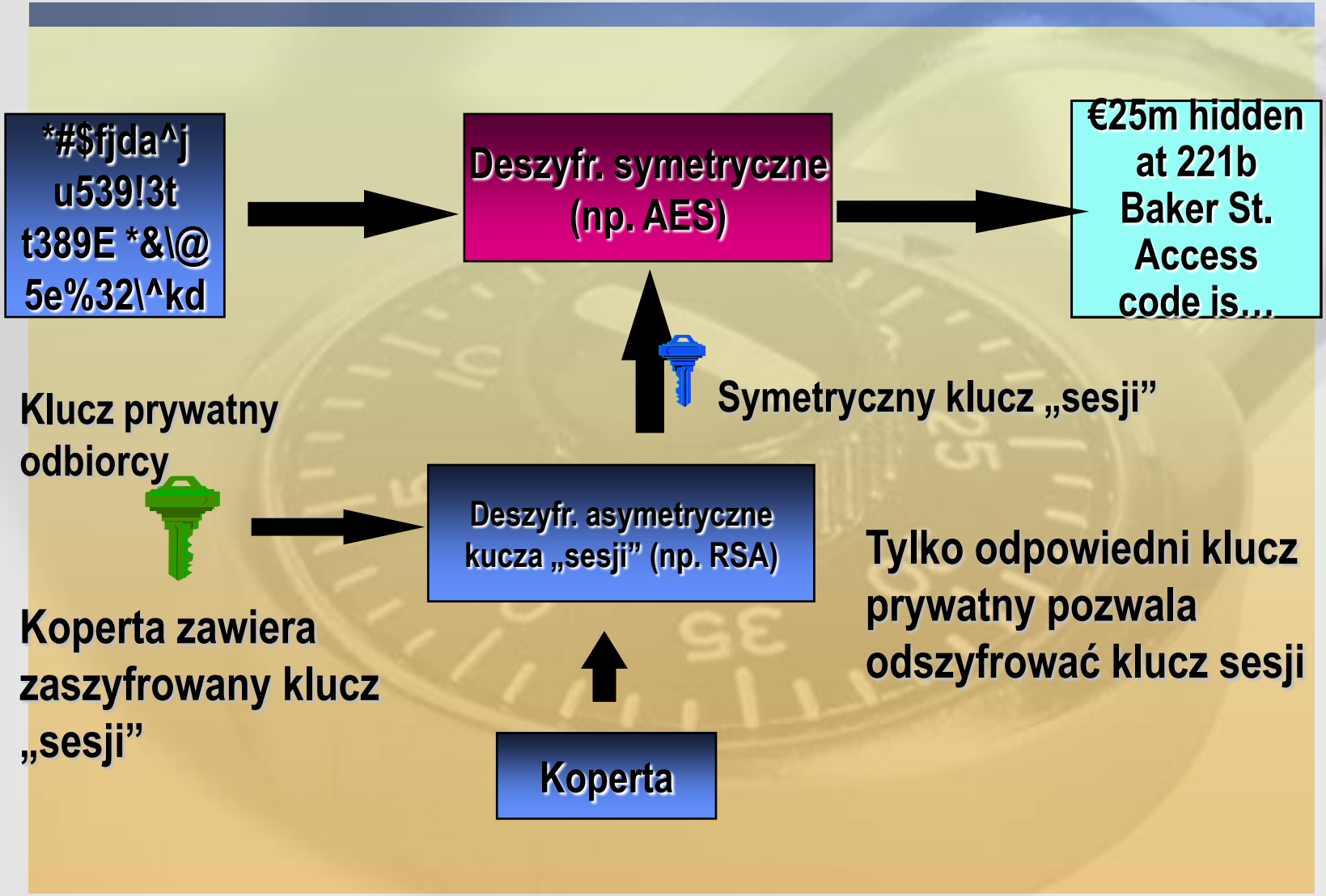
1(mod 60) (d nie może być małe)

  - Liczby n i d to klucz prywatny: 77, 13
  - Zaszyfruj dane $s = m^e \pmod n$: m = 2, $s = 2^{37} \bmod 77 = 51$
  - Odszyfruj dane $m = c^d \pmod n$: $m = 51^{13} \bmod 77 = 2$

Kryptologia - Systemy hybrydowe: Szyfrowanie



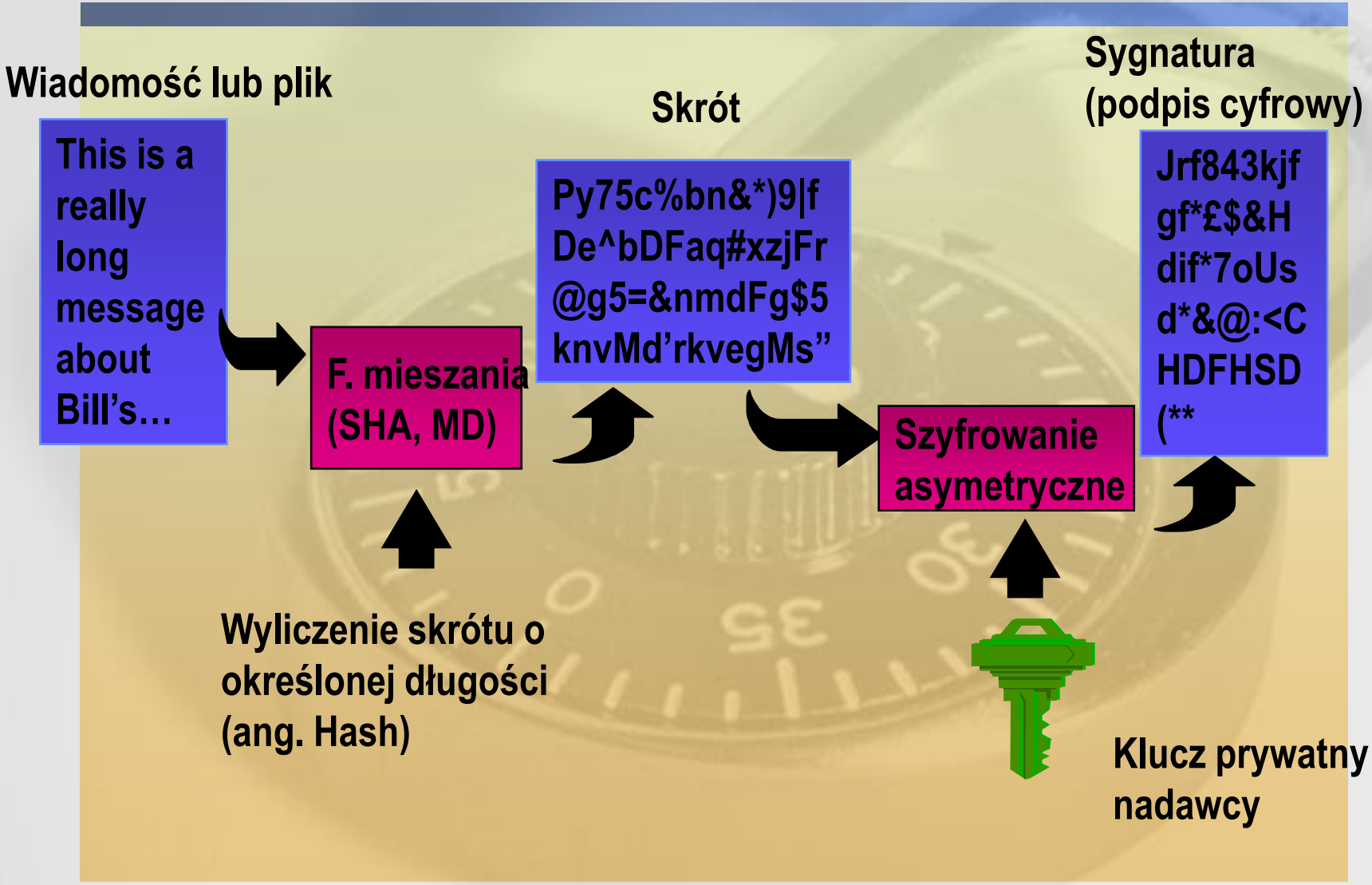
Kryptologia - Systemy hybrydowe: Deszyfrowanie



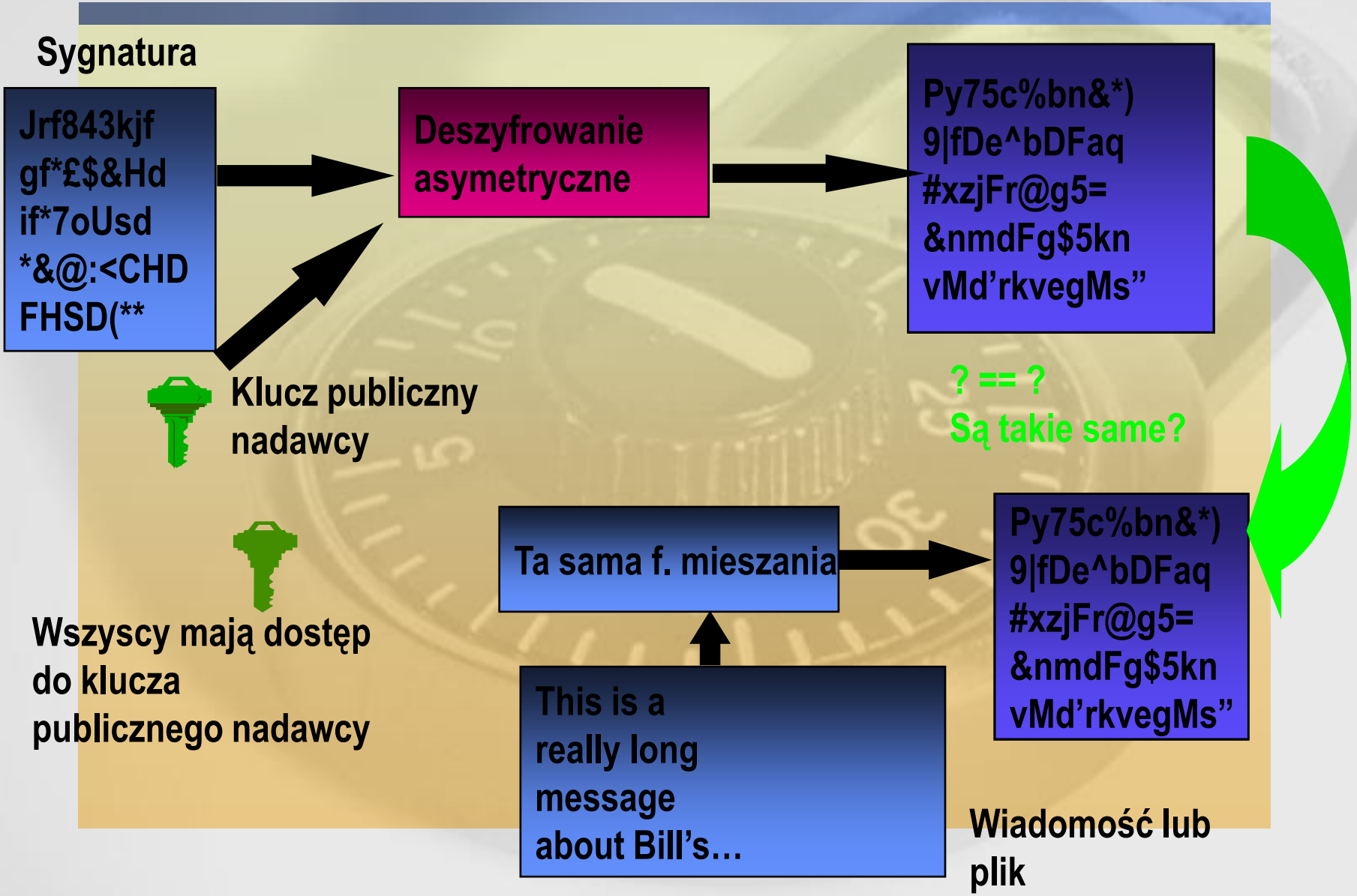
Kryptologia – Funkcje mieszania

- **Zwracają sygnaturę o ściśle określonej długości**
- **Kolizje i atak urodzinowy**
- **MD 2,4,5:**
  - Opracowane przez Ronalda Rivesta w latach 1989 - 91
  - Zwracają wyniki o długości 128 bitów
  - Od 2004 znane są skuteczne techniki ataku
- **SHA-0, SHA-1:**
  - Opracowana w 1993 (SHA-0), poprawiona w 1995 (SHA-1)
  - Zwracają wyniki o długości 160 bitów
  - Bezpieczeństwo na poziomie: SHA-0 29 bitów; SHA-1 63 bitów

Kryptologia – Podpisywanie cyfrowo wiadomości



Kryptologia – Sprawdzanie podpisu cyfrowego

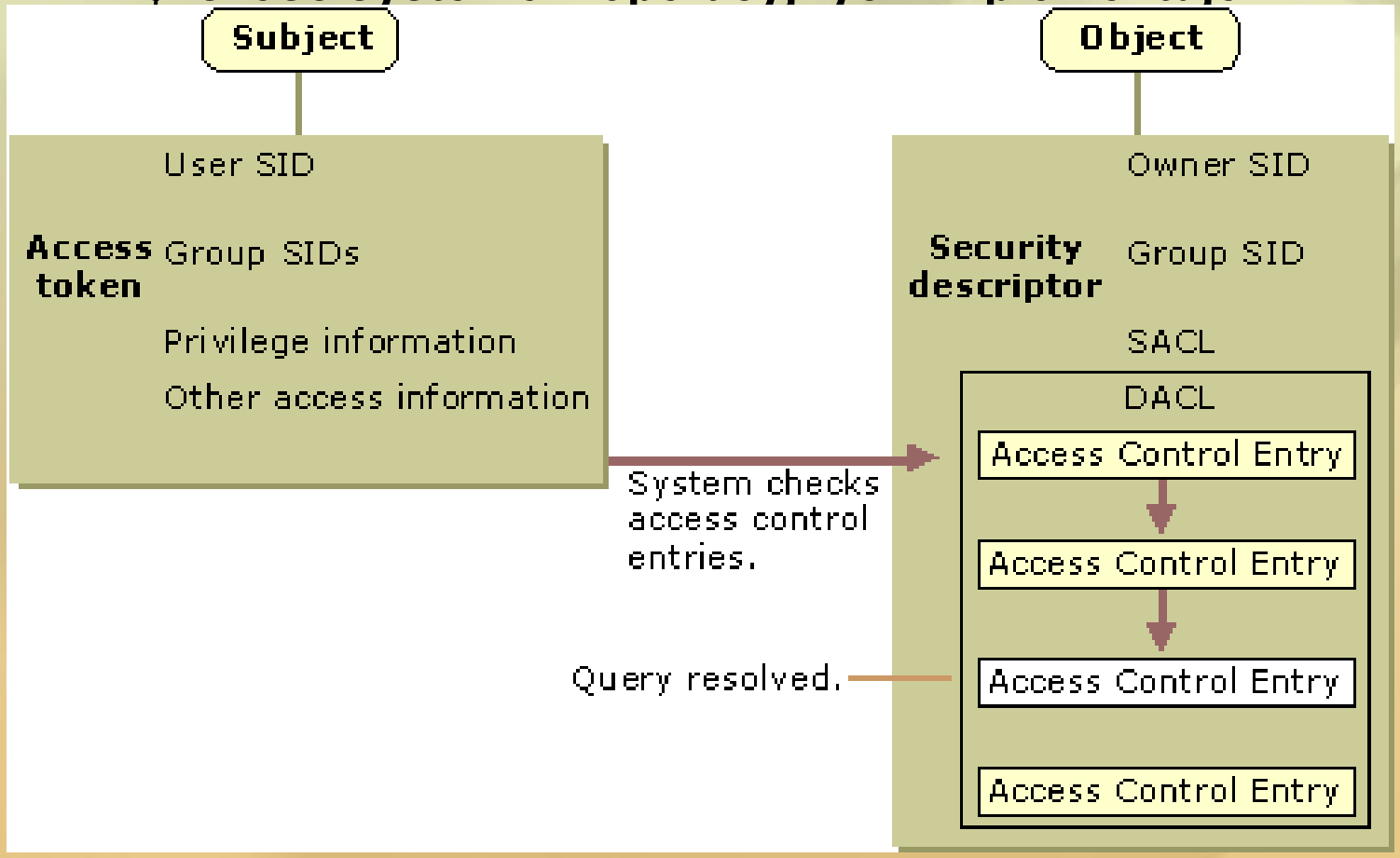


Kryptologia

- **Zbudowanie bezpiecznego systemu kryptograficznego jest wyjątkowo trudne:**
  - Nie implementuj samodzielnie algorytmów
  - Nie używaj tajnych algorytmów
  - Zamiast algorytmów, używaj gotowych kryptosystemów
    - „Znalazłem tą bibliotekę w Sieci…”
    - CAPI, CAPICOM, CNG, …
  - Dobry system poprawia bezpieczeństwo użytych algorytmów
  - Łatwiej jest zabezpieczyć (mały) klucz niż (duże) dane
- **Szyfrowanie gwarantuje poufność i autentyczność danych, nic więcej …**

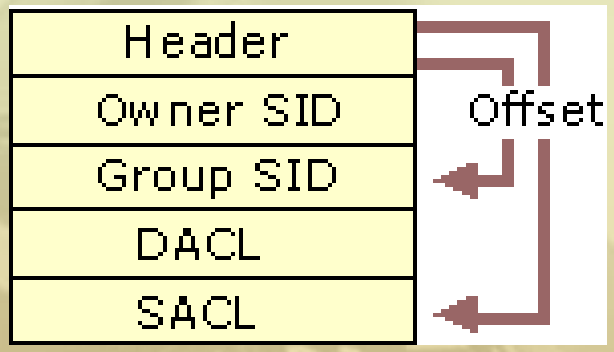
Kontrola dostępu do danych

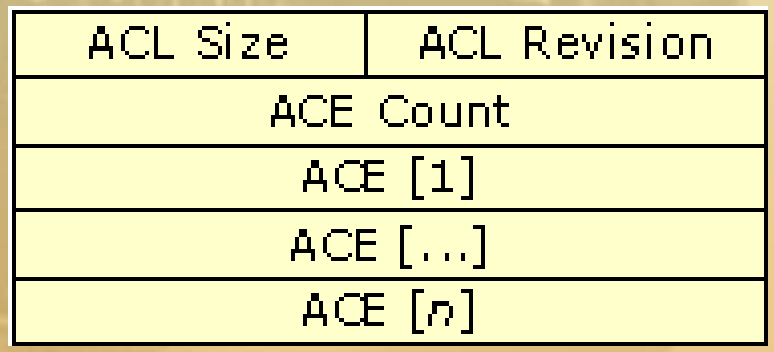
- Większość systemów operacyjnych implementuje



Kontrola dostępu do danych

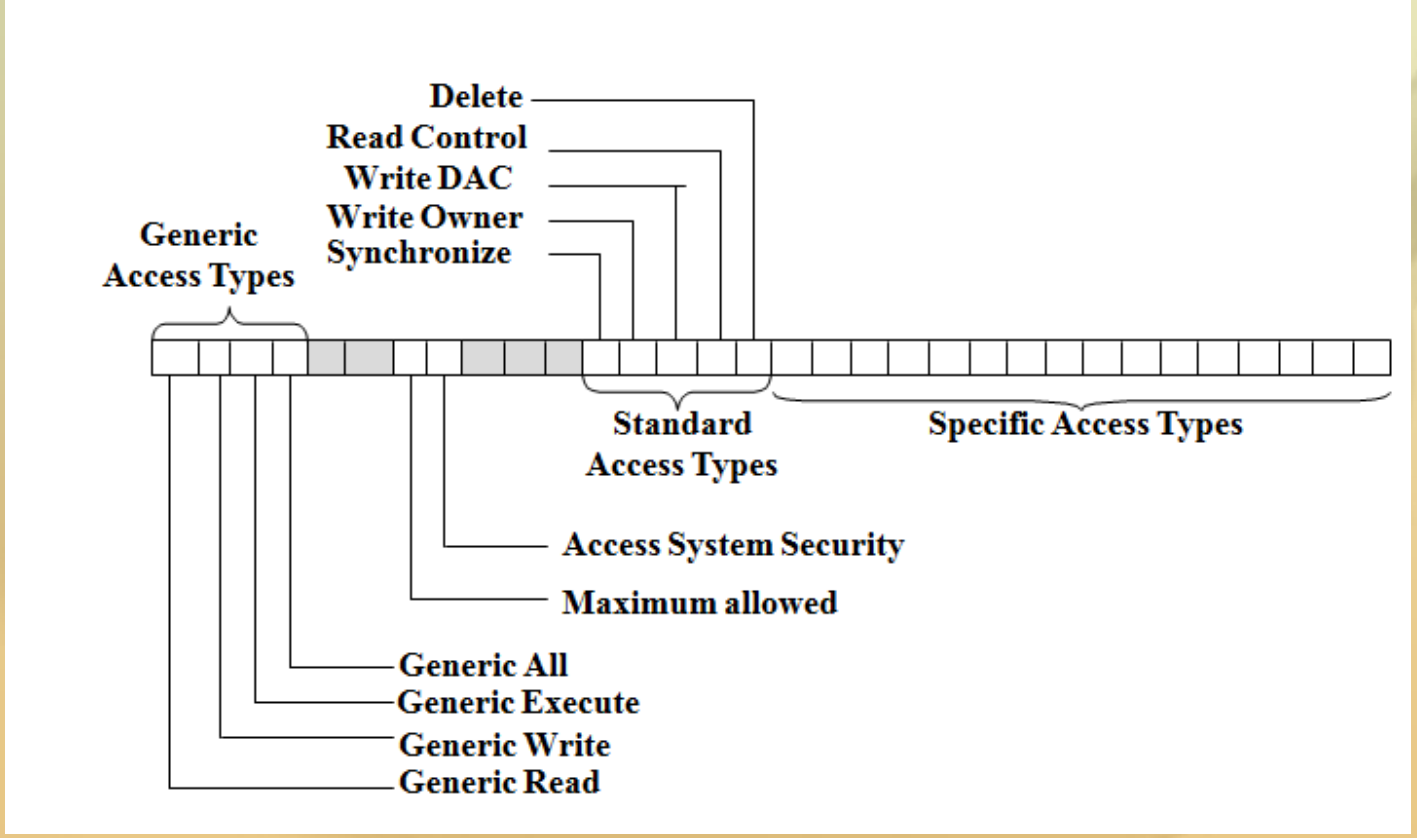
- **Lista ACL zawiera:**
  - Nagłówek ACL
  - Wpisy ACE:
    - Nagłówek ACE
    - Uprawnienia
    - SID
    - Nagłówek ACE
    - Uprawnienia
    - SID
    - …





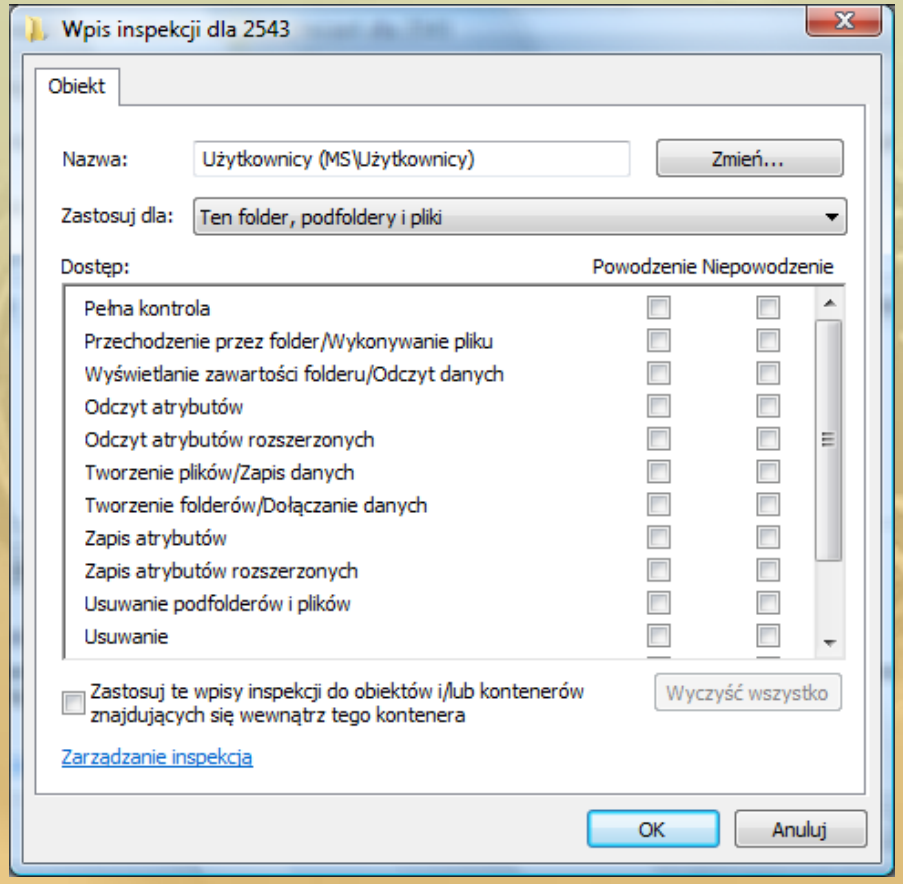
Kontrola dostępu do danych

- **Uprawnienia (ACE) mogą być:**
  - Nadane, odebrane lub nieustalone



Kontrola dostępu do danych

- Lista SACL pozwala monitorować udane i nieudane próby użytkowników uzyskania dostępu do obiektu



Kontrola dostępu do danych

- **Inspekcja jest domyślnie wyłączona**