

BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH

cz. I

Zagadnienia

1. Podstawowe wiadomości i terminologia

- polityka bezpieczeństwa
- uwierzytelnianie, autoryzacja, kontrola dostępu, ...

2. Poufność, integralność, dostępność

Bezpieczeństwo

Co to jest bezpieczeństwo?

Def.: **System informatyczny jest bezpieczny**, jeśli jego użytkownik może na nim polegać, a zainstalowane oprogramowanie działa zgodnie ze swoją specyfikacją.

Simson Garfinkel, Gene Spafford
Practical Unix and Internet Security

Możemy mówić, że system jest bezpieczny, jeśli np. zawsze można od niego oczekiwać, że wprowadzone dziś na stałe dane będą w nim jeszcze za tydzień, nie ulegną zniekształceniu i nie zostaną odczytane przez nikogo nieuprawnionego – ufamy, że system będzie przechowywał i chronił dane.

Szerszy kontekst

WIARYGODNOŚĆ

System wiarygodny =

- dyspozycyjny (*available*) = dostępny na bieżąco
- niezawodny (*reliable*) = odporny na awarie
- bezpieczny (*safe*) = przyjazny dla środowiska
- bezpieczny (*secure*) = zapewniający ochronę danych

Ochrona



1. Określenie zasobów = „Co chronić?”
2. Identyfikacja zagrożeń = „Przed czym chronić?”
3. Oszacowanie ryzyka = „Ile czasu, wysiłku i pieniędzy można poświęcić na należna ochronę” (analiza kosztów i zysku)



Strategia bezpieczeństwa

Normy i zalecenia zarządzania bezpieczeństwem

- PN-ISO/IEC 27000:2012 „Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia”
- PN-ISO/IEC 27001:2014-12 „Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania”
- PN-ISO/IEC 27005 „Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji”
- Ustawa o ochronie danych osobowych z 29-08-1997 (z poprawkami ☺ 2015, ...)
- Rozporządzenie MSWiA z 29-04-2004 w sprawie warunków technicznych i organizacyjnych ... przetwarzania danych osobowych
- Ustawa o ochronie informacji niejawnych z 5-08-2010
- ...

Określenie zasobów = „Co chronić?”

- sprzęt komputerowy
- infrastruktura sieciowa
- wydruki
- strategiczne dane
- kopie zapasowe
- wersje instalacyjne oprogramowania
- dane osobowe
- dane audytu
- zdrowie pracowników
- prywatność pracowników
- zdolności produkcyjne
- wizerunek publiczny i reputacja



Identyfikacja zagrożeń = „Przed czym chronić?”

- włamywacze komputerowi
- infekcje wirusami
- destruktywność pracowników / personelu zewnętrznego
- błędy w programach
- kradzież dysków / laptopów (również w podróży służbowej)
- utrata możliwości korzystania z łączy telekomunikacyjnych
- bankructwo firmy serwisowej / producenta sprzętu
- choroba administratora / kierownika (jednoczesna choroba wielu osób)
- powódź

Przestępstwa komputerowe

Praktycznie wszystkie przypadki naruszające bezpieczeństwo w sieci Internet wyczerpują znamiona przestępstw określonych w obowiązującym prawie RP.

W szczególności mają tu zastosowanie:

- artykuły 267-269 KK
- artykuł 287 Kodeksu Karnego



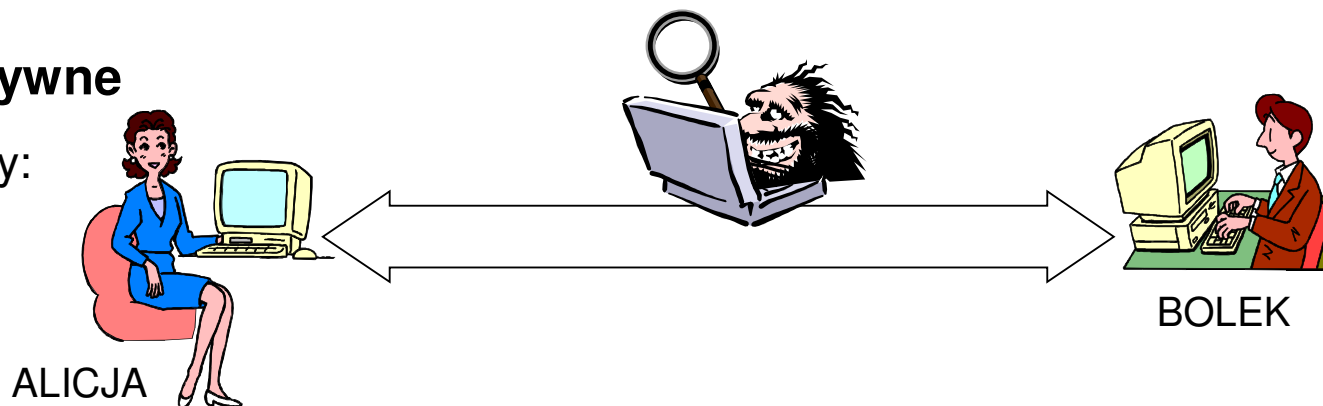
Zazwyczaj przestępstwa te nie są ścigane z oskarżenia publicznego, lecz na wniosek pokrzywdzonego.

Atak na system informatyczny

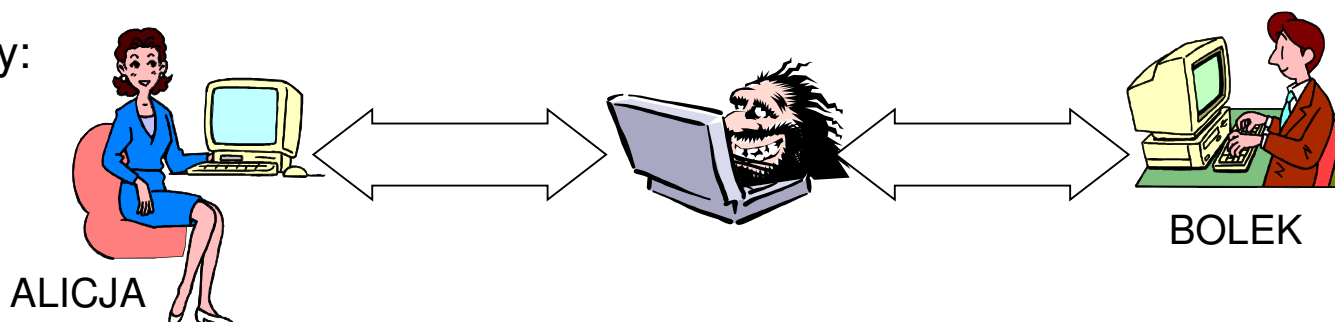
Klasy ataków

pasywne / aktywne

- pasywny:



- aktywny:




lokalne/zdalne

- lokalny: atakujący już ma dostęp do systemu (konto) i próbuje zwiększyć swe uprawnienia

Atak na system informatyczny

Przykłady ataków

- podszywanie (ang. *masquerading*)
 - podsłuch (ang. *eavesdropping*)
 - powtórzenie (ang. *replaying*)
 - manipulacja (ang. *tampering*), przechwytywanie sesji (ang. *hijacking*)
 - wykorzystanie luk w systemie (ang. *exploiting*)
 - zablokowanie usług (ang. DoS = *Denial of Service*)
 - spam, scam, spim, spit, blog spam, search spam
 - phishing (*personal data fishing*), spear-phishing
 - ...
- 
- "Layer 8" attacks

Atak na system informatyczny

Podstawowe fazy ataku

1. skanowanie (wyszukanie słabości, np. sondowanie usług)
2. wyznaczenie celu (np. niezabezpieczona usługa, znany exploit)
3. atak na system
4. modyfikacje systemu umożliwiające późniejszy powrót
5. usuwanie śladów
6. propagacja ataku

Zabezpieczenia

Złożoność problemu stosowania zabezpieczeń

1. Zasada naturalnego styku z użytkownikiem
2. Zasada spójności poziomej i pionowej
3. Zasada minimalnego przywileju
4. Zasada domyślnej odmowy dostępu

Zabezpieczenia

Elementarne pojęcia:

1. Identyfikacja (ang. *identification*)

- użytkownicy są identyfikowani w systemie za pomocą UID (*user identifier*)

2. Uwierzytelnianie (ang. *authentication*)

- jest to proces weryfikacji tożsamości użytkownika; najczęściej opiera się na tym:
 - co użytkownik wie (*proof by knowledge*), np. hasło
 - co użytkownik ma (*proof by possession*), np. elektroniczną kartę identyfikacyjną

Zabezpieczenia

Elementarne pojęcia:

3. Autoryzacja (ang. *authorization*)

- jest to proces przydzielania praw (dostępu do zasobów) użytkownikowi

4. Kontrola dostępu (ang. *access control*)

- jest to procedura nadzorowania przestrzegania praw (dostępu do zasobów)

Zabezpieczenia

Elementarne pojęcia:

5. Poufność (ang. *confidentiality*)

- ochrona informacji przed nieautoryzowanym jej ujawnieniem

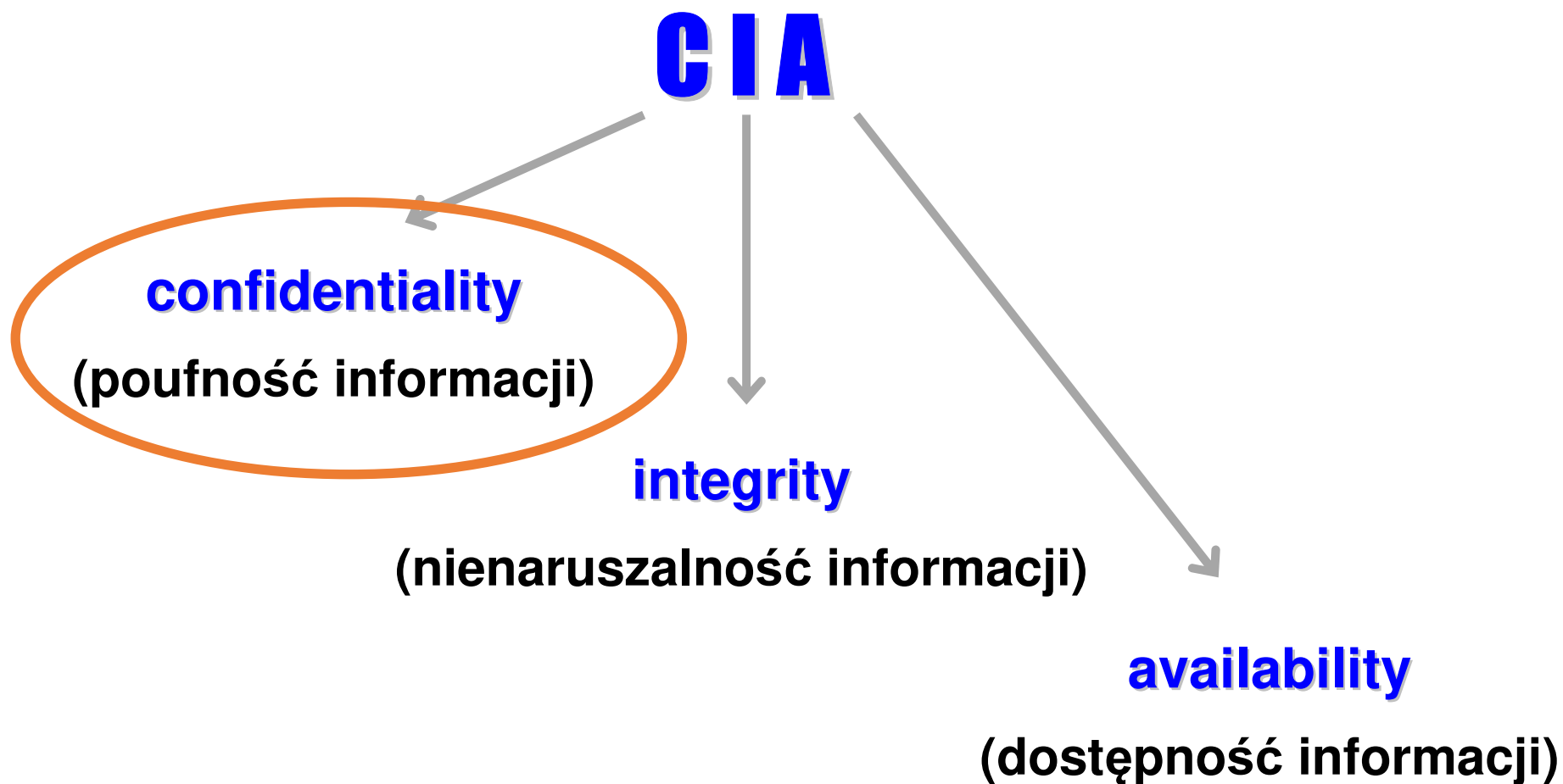
6. Nienaruszalność (integralność; ang. *data integrity*)

- ochrona informacji przed nieautoryzowanym jej zmodyfikowaniem (ew. detekcja takiej modyfikacji)

7. Niezaprzeczalność (ang. *nonrepudiation*)

- ochrona przed fałszywym zaprzeczeniem
 - przez nadawcę – faktu wysłania danych
 - przez odbiorcę – faktu otrzymania danych

Ogólne własności bezpieczeństwa



Poufność informacji

Zagrożenia:



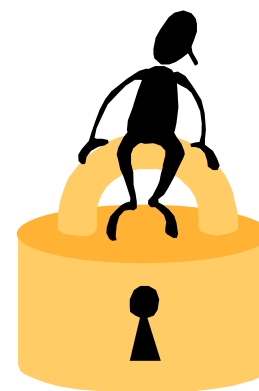
1. nieuprawniony dostęp do danych w miejscu składowania
2. nieuprawniony dostęp do danych w miejscu przetwarzania
3. podsłuchanie danych przesyłanych w sieci

podśluch zdalny – ad 2. i 3.

Poufność informacji

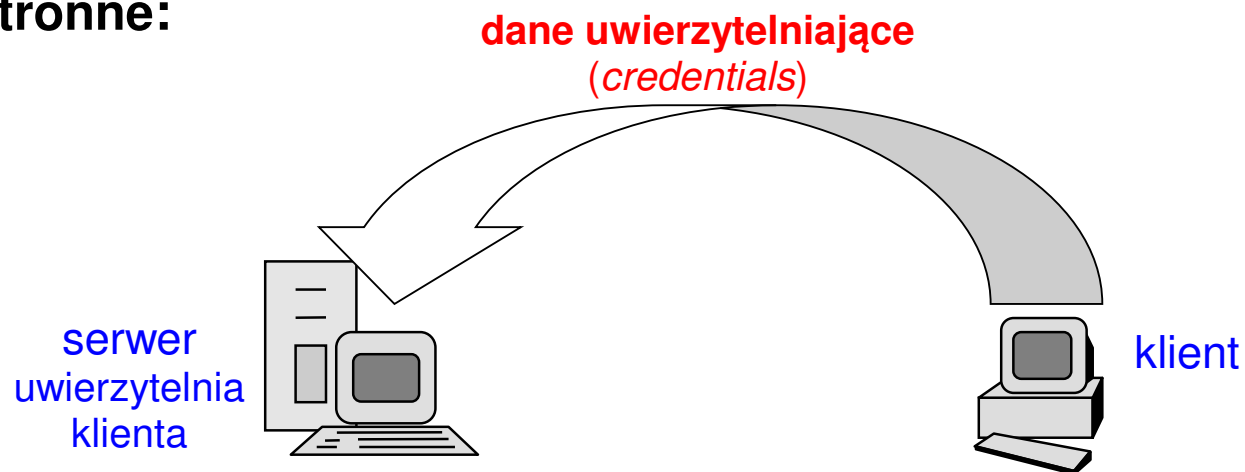
Mechanizmy obrony:

- uwierzytelnianie użytkowników
- autoryzacja i kontrola dostępu do zasobów
- utrudnianie podsłuchu



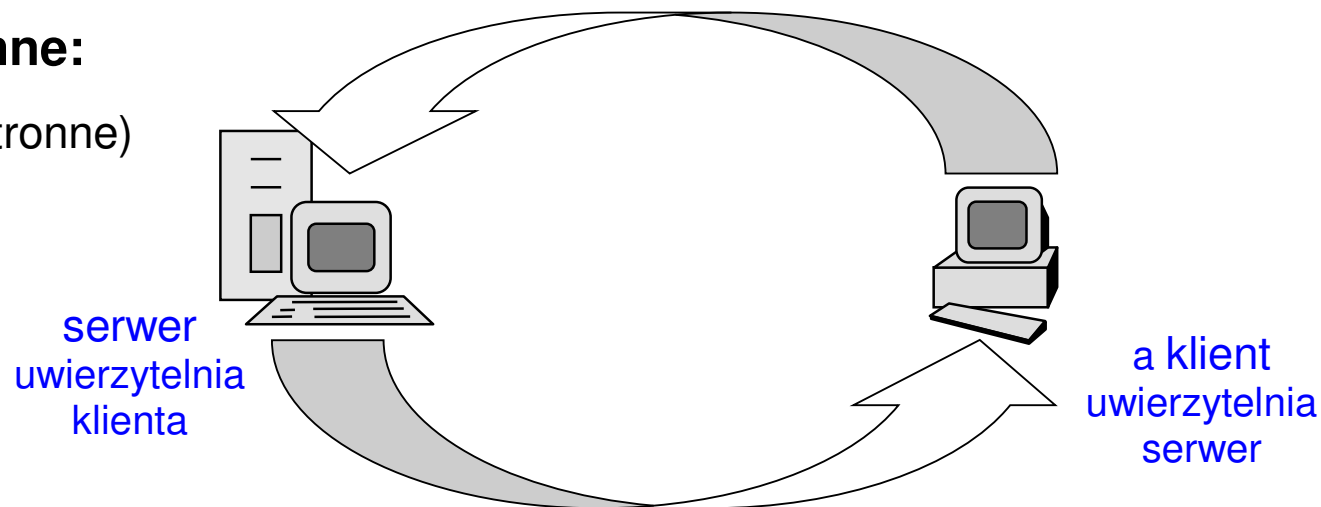
Uwierzytelnianie

Uwierzytelnianie jednostronne:



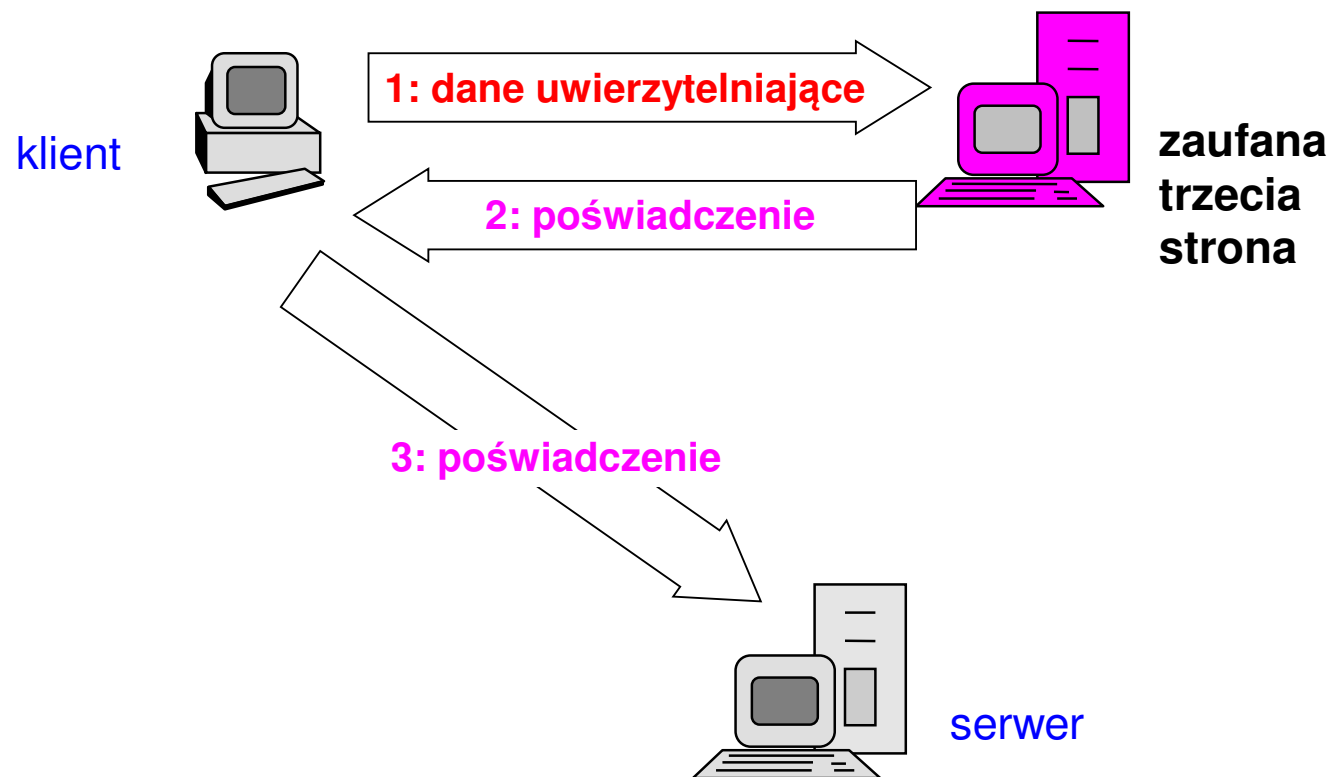
Uwierzytelnianie obustronne:

- dwuetapowe (2 x jednostronne)
- jednoetapowe



Uwierzytelnianie

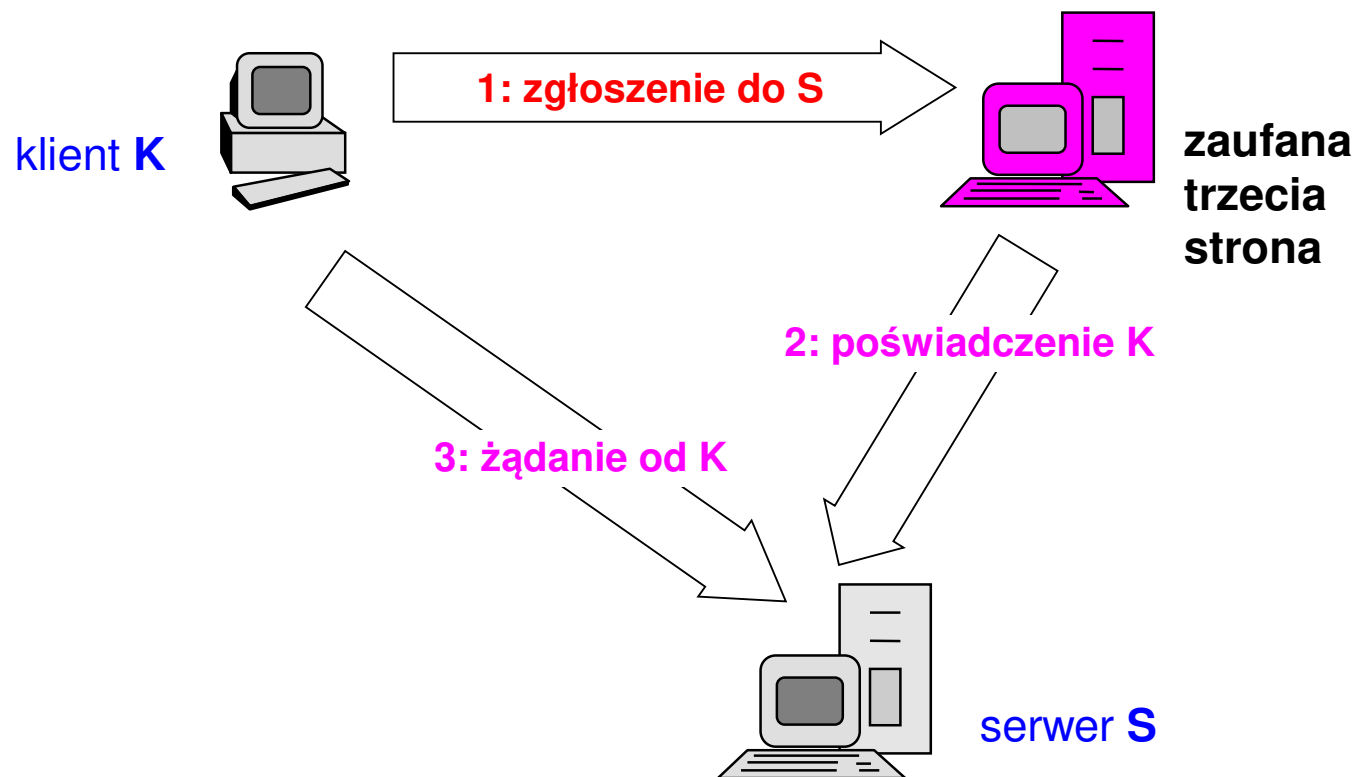
Uwierzytelnianie z udziałem zaufanej trzeciej strony:



Uwierzytelnianie

Uwierzytelnianie z udziałem zaufanej trzeciej strony:

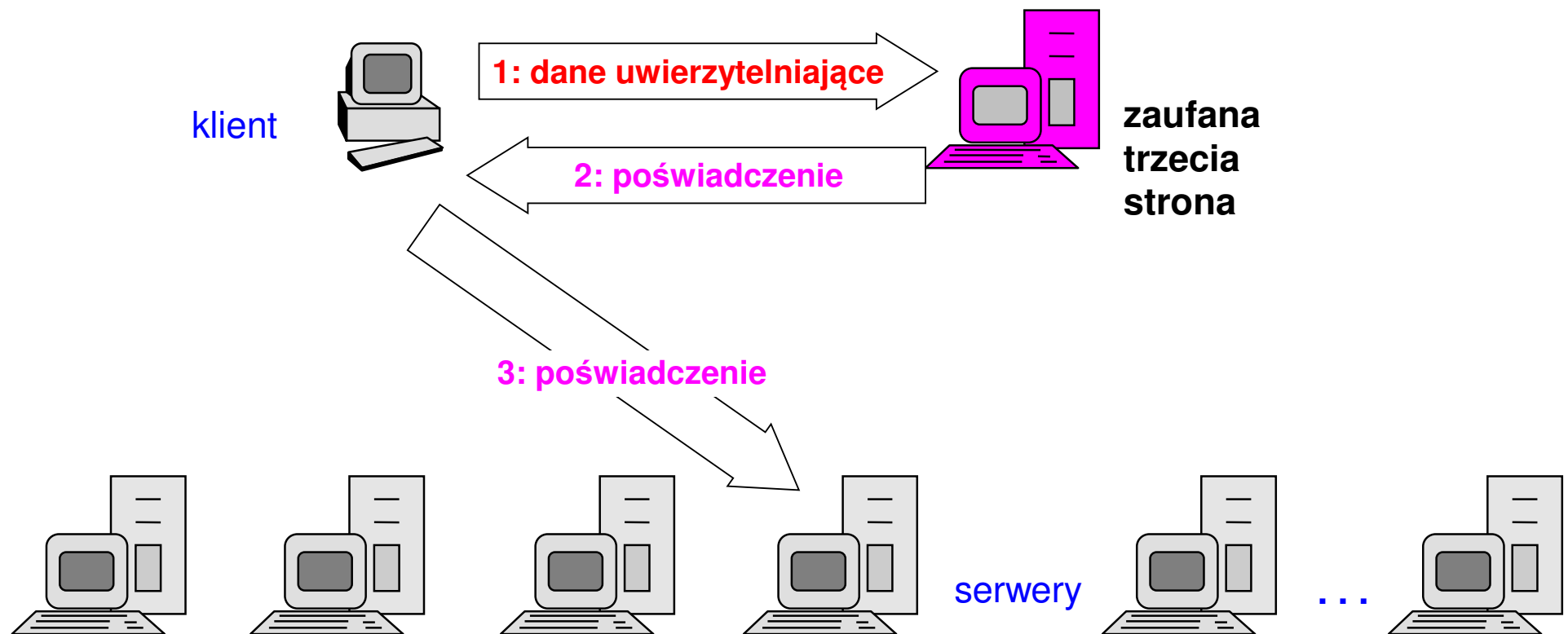
- dlaczego nie tak?



Uwierzytelnianie

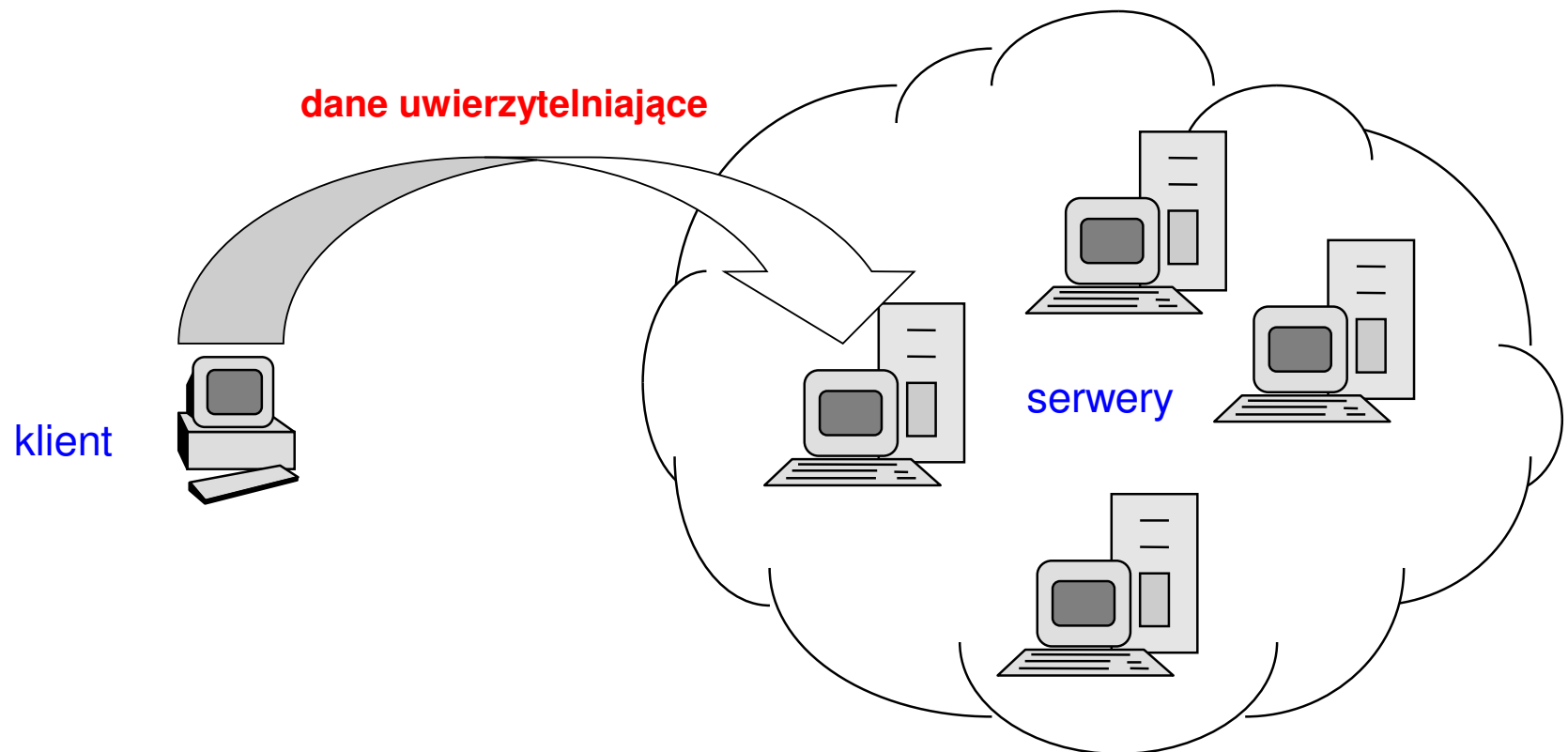
Uwierzytelnianie z udziałem zaufanej trzeciej strony:

- wiele serwerów (np. cała domena)



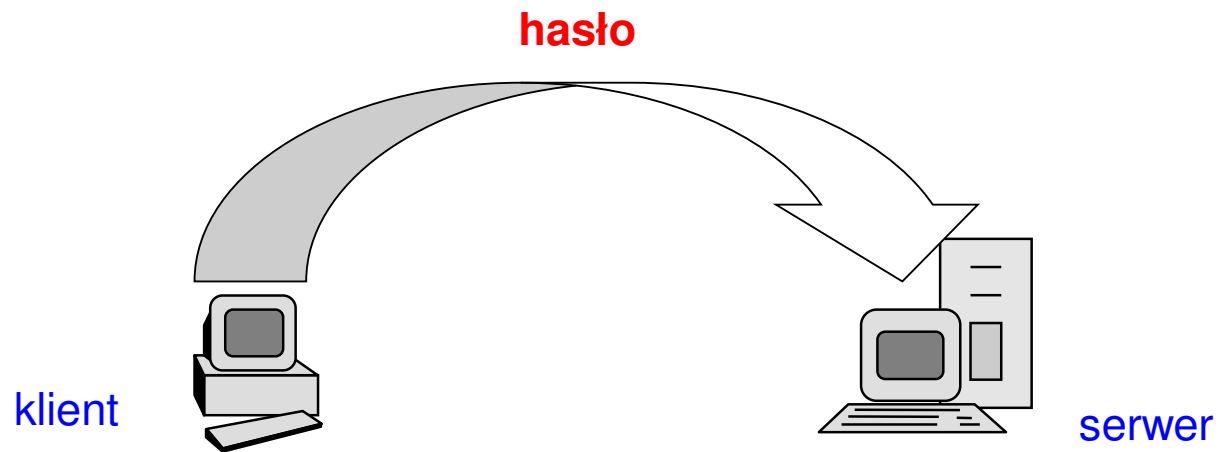
Uwierzytelnianie

Uwierzytelnianie jednokrotne (SSO – *single sign-on*):



Uwierzytelnianie

Dane uwierzytelniające



Uwierzytelnianie

Hasła

- hasło można złamać:
 - odgadnąć, np. metodą przeszukiwania wyczerpującego (*brute-force attack*) lub słownikową (*dictionary attack*)
 - podsłuchać w trakcie niezabezpieczonej transmisji
 - wykraść z systemowej bazy haseł użytkowników
 - pozyskać inną metodą (np. kupić)
- hasła domyślne (instalacyjne) !

Uwierzytelnianie

Hasła – złamanie hasła

Metoda przeszukiwania wyczerpującego (*brut-force attack*):

- 8 znaków z 64-znakowego alfabetu: 64^8 czyli ok. 280 bilionów wartości
- założmy moc obliczeniową o wydajności 64 milionów iteracji DES na sekundę
- 25 iteracji dla każdego hasła – 2,5 miliona haseł na sekundę
- dowolne hasło zostanie złamane (280 bilionów wartości) w 3,5 roku

Uwierzytelnianie

Hasła – podstawowe reguły

czego nie wolno:

- wybierać hasła o małej długości
- wybierać jako hasło znanego słowa, imienia, nazwiska, daty urodzenia, numeru telefonu, numeru rejestracyjnego
- zmieniać hasła tak, by nowe było zależne od starego
(np. z 012345 na 123456)
- zapisywać hasła w widocznych lub łatwo dostępnych miejscach
(jak np. fragment biurka zakryty klawiaturą, wewnątrz szuflady czy dyskietka / płyta z danymi)
- informować nikogo o swoim haśle



Uwierzytelnianie

Hasła – podstawowe reguły

co należy:

- wybierać długie i mało znane słowo lub frazę (kombinacja różnych znaków)
- wybrać hasło w sposób na tyle losowy na ile tylko możliwe
- zmieniać hasło możliwie często, lecz w nieprzewidywalny sposób
- zmienić hasło natychmiast, jak tylko rodzi się podejrzenie, że ktoś mógł je poznać

co można:

- zlecić systemowi wygenerowanie trudnego hasła

Przykładem trudnego do złamania hasła może być SzNsndJsAsz, które powstało z fragmentu fraszki Jana Kochanowskiego pod tytułem „Na zdrowie”:

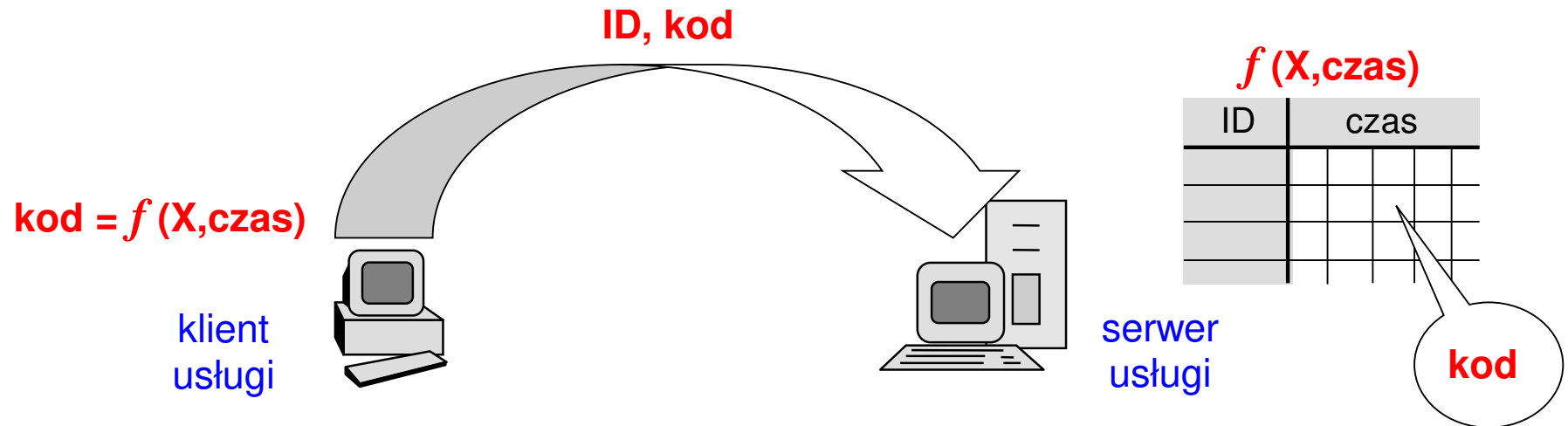
„Ślachetne zdrowie, Nikt się nie dowie, Jako smakujesz, Aż się zepsujesz”

Uwierzytelnianie

Hasła jednorazowe (OTP – *one-time passwords*)

Metoda z synchronizacją czasu (*time synchronization*):

- klient generuje **unikalny kod** w funkcji pewnego parametru **X** użytkownika (identyfikatora, kodu PIN, hasła, numeru seryjnego karty identyfikacyjnej) oraz bieżącego **czasu**
- serwer weryfikuje otrzymany kod korzystając z identycznej funkcji (z odpowiednią tolerancją czasu)



Uwierzytelnianie

Hasła jednorazowe – produkty

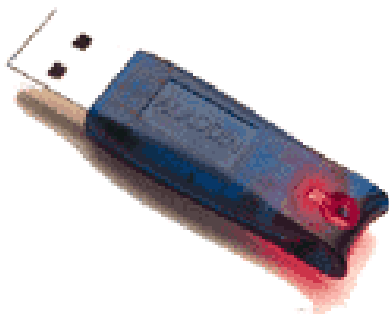
- SecureID (Security Dynamics / RSA Security Inc.)
- S/Key (Fill Carn, Bellcore – Bell Communication Research)
- OPIE (NRL – US Naval Research Laboratory)
- ...



Uwierzytelnianie

Karty identyfikacyjne (*security tokens*):

- smart cards
- smart keys
- i-buttons
- USB tokens



Contact Smart Card



Contactless Chip

Antenna

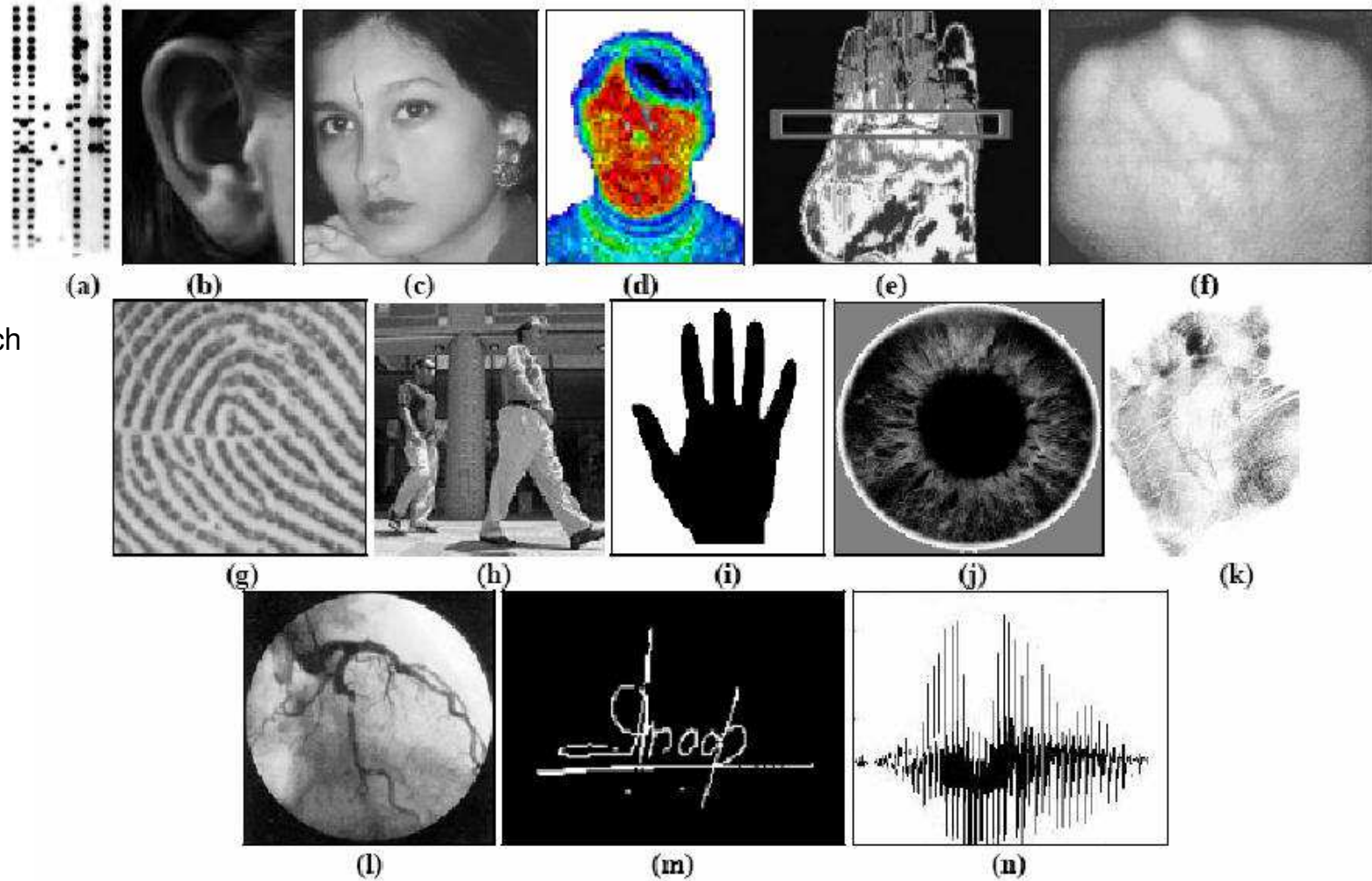
Contactless
Smart Card



Uwierzytelnianie

Uwierzytelnianie biometryczne

- (a) klucz DNA
- (b) małżowina uszna
- (c) geometria twarzy
- (d) termogram twarzy
- (e) termogram dłoni
- (f) obraz żył krwionośnych na zaciśniętej pięści
- (g) odcisk palca (dermatoglify)
- (h) chód
- (i) geometria dłoni
- (j) tęczówka oka
- (k) odcisk dłoni
- (l) obraz siatkówki
- (m) podpis odręczny
- (n) głos



Poufność informacji

Utrudnianie podsłuchu

- topologia gwiazdy (okablowanie strukturalne)
- sztuczne generowanie ruchu (*traffic padding*)
- zdefiniowanie listy stanowisk, z których dany użytkownik może uzyskać dostęp do systemu (adresy MAC lub IP) – zamknięte grupy użytkowników
- fizyczna ochrona pomieszczeń z węzłami sieci i serwerami
- szyfrowanie

Poufność informacji

Ograniczanie emisji elektromagnetycznej

- atak przez przechwycenie promieniowania jest nadal tańszy od innego typu ataków (np. ataku kryptoanalitycznego)
- ... mimo że wymaga bardzo specjalistycznego sprzętu
- TEMPEST (*Transient Electromagnetic Pulse Emanation Standard*)
 - ekranujące materiały konstrukcyjne:
 - obudowy
 - przewody
 - ekranujące materiały elastyczne:
 - tapety
 - wykładziny

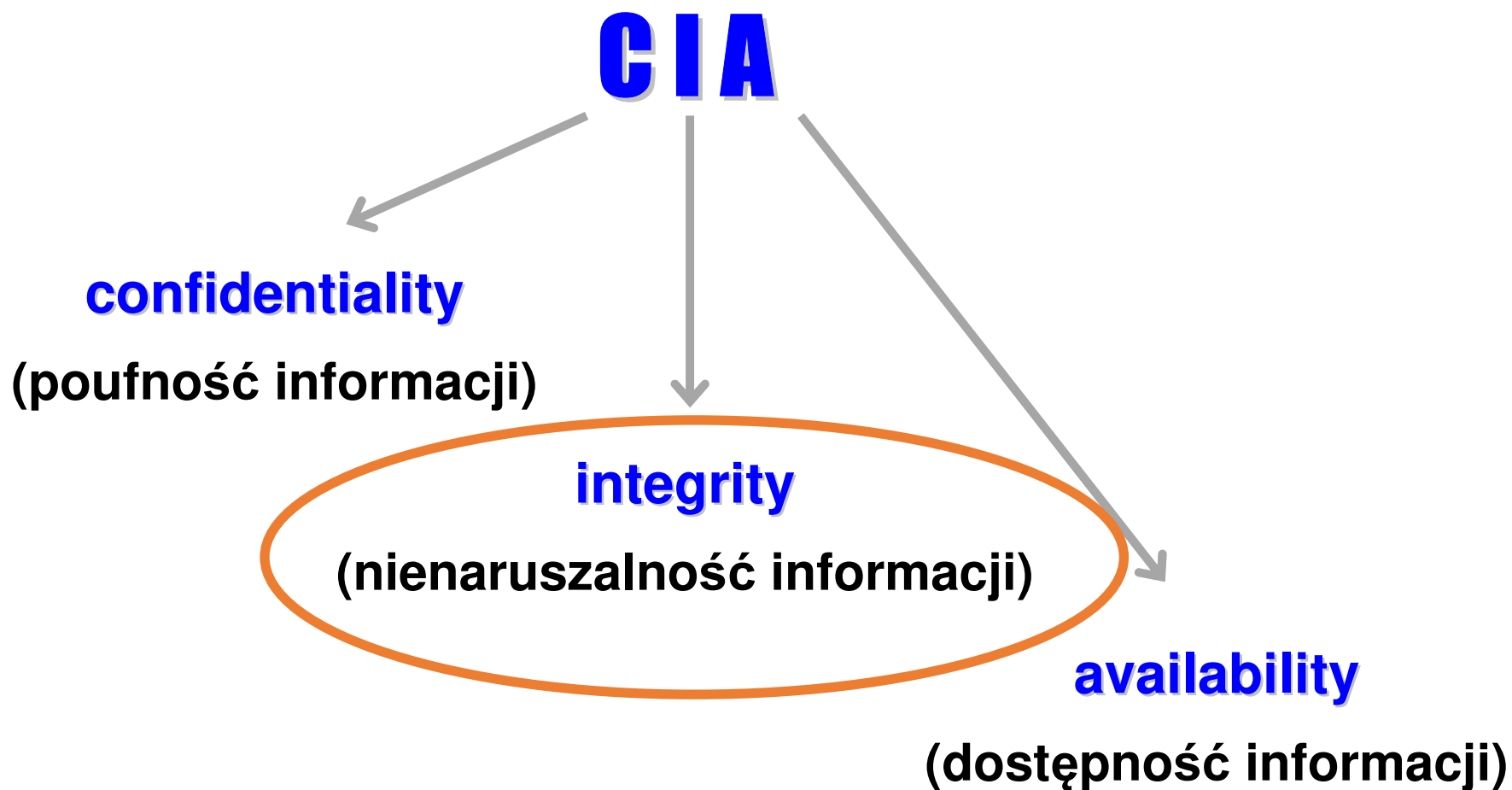
Poufność informacji

Zagrożenia

Uwaga: przypadkowy dostęp do pozostawionej aplikacji !



Ogólne własności bezpieczeństwa



Integralność informacji

Zagrożenia:

- nieuprawniona lub przypadkowa modyfikacja danych

Mechanizmy obrony:

- kontrola dostępu do danych
- sumy kontrolne
- kryptograficzne sumy kontrolne = podpis elektroniczny
- rejestracja operacji na danych (*auditing*)
- kontrola antywirusowa

Autoryzacja

Pojęcia podstawowe:

Zasób (obiekt)

- jest jednostką, do której dostęp podlega kontroli
- przykłady: programy, pliki, relacje bazy danych, czy całe bazy danych
- obiekty o wysokiej granulacji: poszczególne krotki bazy danych

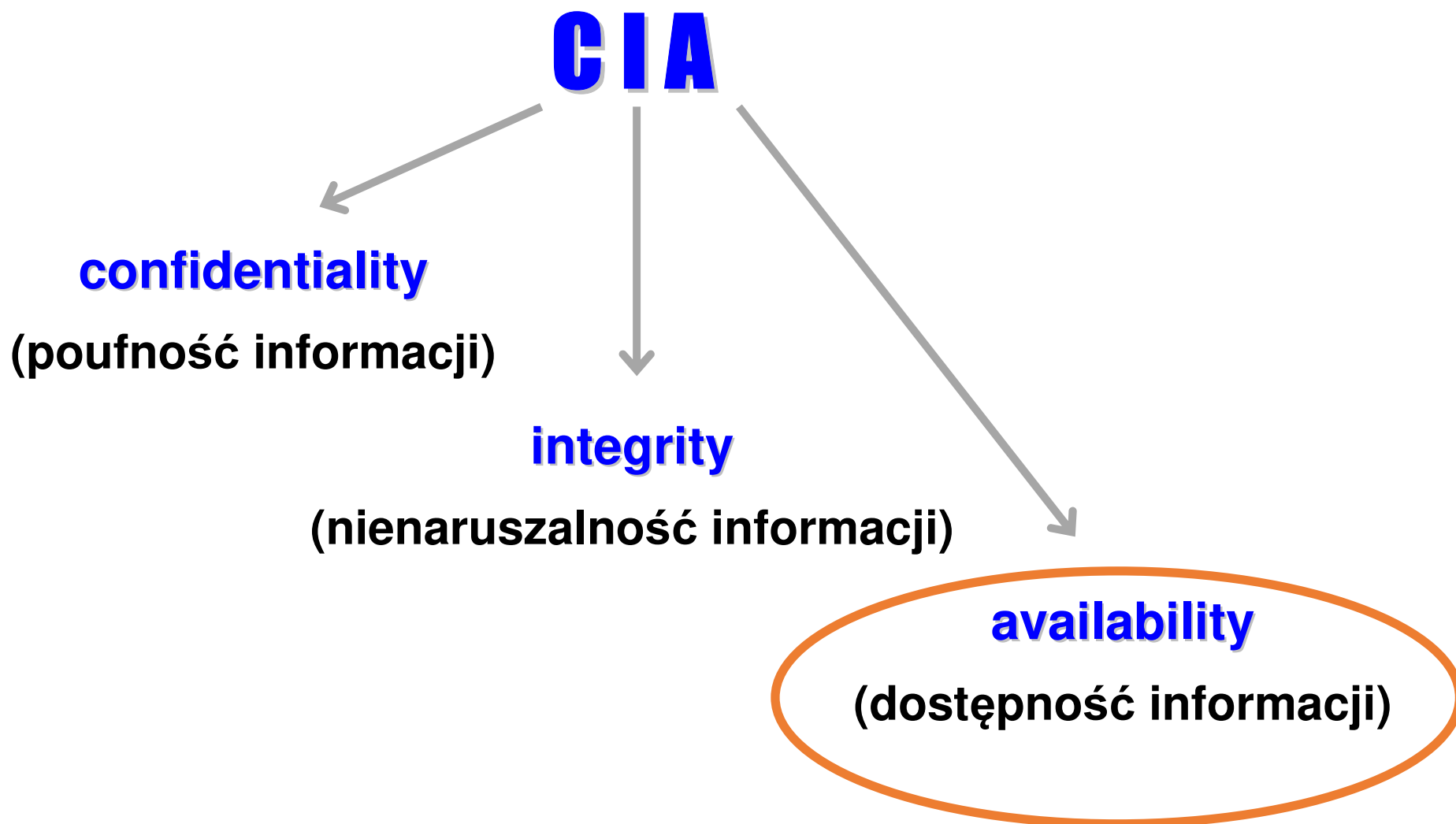
Podmiot

- ma dostęp do zasobu
- przykłady: użytkownik, grupa użytkowników, terminal, komputer, aplikacja, proces

Prawa dostępu

- określają dopuszczalne sposoby wykorzystania zasobu przez podmiot

Ogólne własności bezpieczeństwa



Dostępność informacji

Zagrożenia:

- awaria sprzętu i błędy oprogramowania, klęska żywiołu, celowy sabotaż

Mechanizmy obrony:

- ciągłość zasilania urządzeń sieciowych
- systemy redundantnych usług:
 - macierze dyskowe RAID
 - serwery lustrzane
 - grona serwerów (*clusters*)
- archiwizacja (*backup*) danych
- kontrola antywirusowa

BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH

cz. II

Zagadnienia

Elementy kryptografii

1. Terminologia
2. Szyfry symetryczne i asymetryczne
3. Funkcje skrótu i podpis cyfrowy
4. Zarządzanie kluczami (PKI)

```
  \
  .001.^
  u$0N=1
  z00BAI
  |..=~.
  ;s<'
  NRX~=-\
  z0c^<X^
  ~B0s~^
  @0$H~'
  n$0=XN;.\
  iBBB0vU1=~'\
  ` $000cRr`vul
  FAHZuqr-'
  ZZUFA@FI.\
  ;BRHv n$U^~
  `ARN1    ^0si
  'Onv~    01.'
  c0qr     rs.\
  aUU~     ul\
  `R0-     :.\
  nn~\     -=.~|-
  =1^'.. \
           ..
```

Podstawowe pojęcia

Kryptologia – wiedza dotycząca bezpiecznej komunikacji, obejmująca **kryptografię** i **kryptoanalizę**.

Kryptografia – dziedzina wiedzy obejmująca zagadnienia związane z utajnieniem danych (przesyłanie wiadomości i zabezpieczenia dostępu do informacji) przed niepożądanymi osobami.

Utajnienie oznacza tu, że wiadomość jest trudna do odczytania (rozszyfrowania) przez osobę nie znającą tzw. klucza rozszyfrowującego – dla niej wiadomość będzie wyłącznie niezrozumiałym ciągiem znaków.

Kryptoanaliza – dziedzina wiedzy zajmująca się łamaniem szyfrów, czyli odczytywaniem zaszyfrowanych wiadomości bez znajomości kluczy rozszyfrowujących.

Podstawowe pojęcia

Kryptogram (szyfrogram) – zaszyfrowana postać wiadomości czytelnej.

Klucz szyfrowania – ciąg danych służących do szyfrowania wiadomości czytelnej w kryptogram za pomocą algorytmu szyfrowania. Klucz ten jest odpowiednio ustalany (uzgadniany) przez nadawcę w fazie szyfrowania.

Klucz rozszyfrowujący – ciąg danych służących do rozszyfrowania kryptogramu do postaci wiadomości czytelnej za pomocą algorytmu deszyfrowania. Klucz ten odpowiada kluczowi szyfrowania wykorzystanemu w fazie szyfrowania.

Przemienność kluczy oznacza, że role dwóch kluczy z pary mogą ulec przestawieniu. W takiej parze kluczy informację zaszyfrowaną jednym kluczem można rozszyfrować tylko przy pomocy odpowiadającego mu drugiego klucza z pary, i odwrotnie, informację zaszyfrowaną drugim kluczem można rozszyfrować wyłącznie przy pomocy klucza pierwszego.

Proste szyfry

Szyfrowanie metodą podstawiania

Monogram, przekształcenie szyfrujące $f(x) = x + \Delta$

szyfr Cezara "A" \Rightarrow ("A" + 3) = "D"

kod Captain Midnight "A" \Rightarrow ("A" + Δ); $\Delta = 1, \dots, 26$

$\Delta = 3$ x $f(x)$

A		D
B		E
C		F
	...	
W		Z
X		A
Y		B
Z		C

S		U		S
E		G		E
K	\rightarrow	M	\rightarrow	K
R		T		R
E		G		E
T		W		T

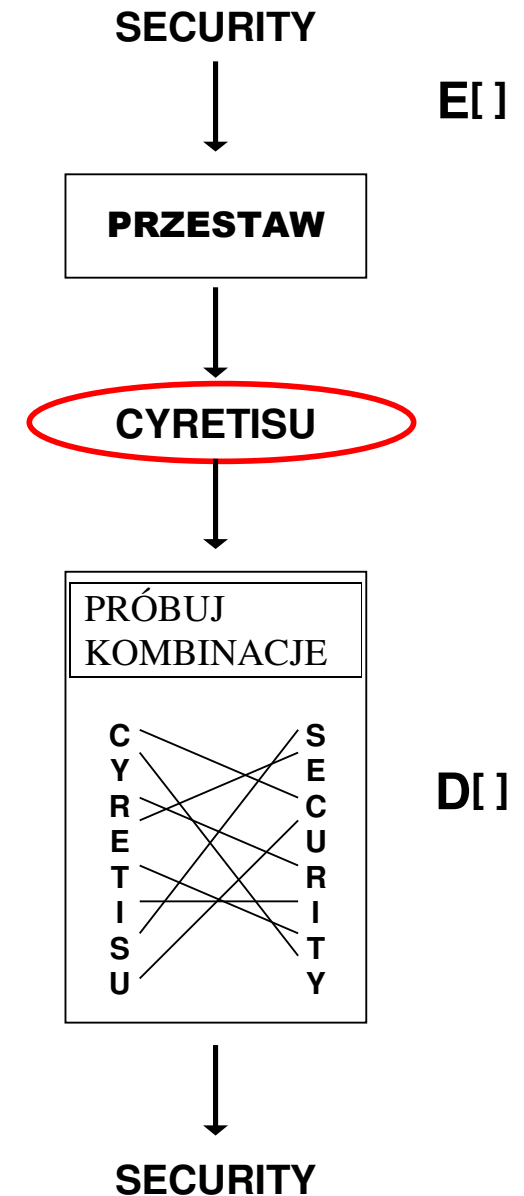
Proste szyfry

Szyfrowanie metodą przestawiania

Przestawianie losowe:

Przestawianie z figurą geometryczną

- o figura geometryczna definiuje transpozycję wiadomości czytelnej

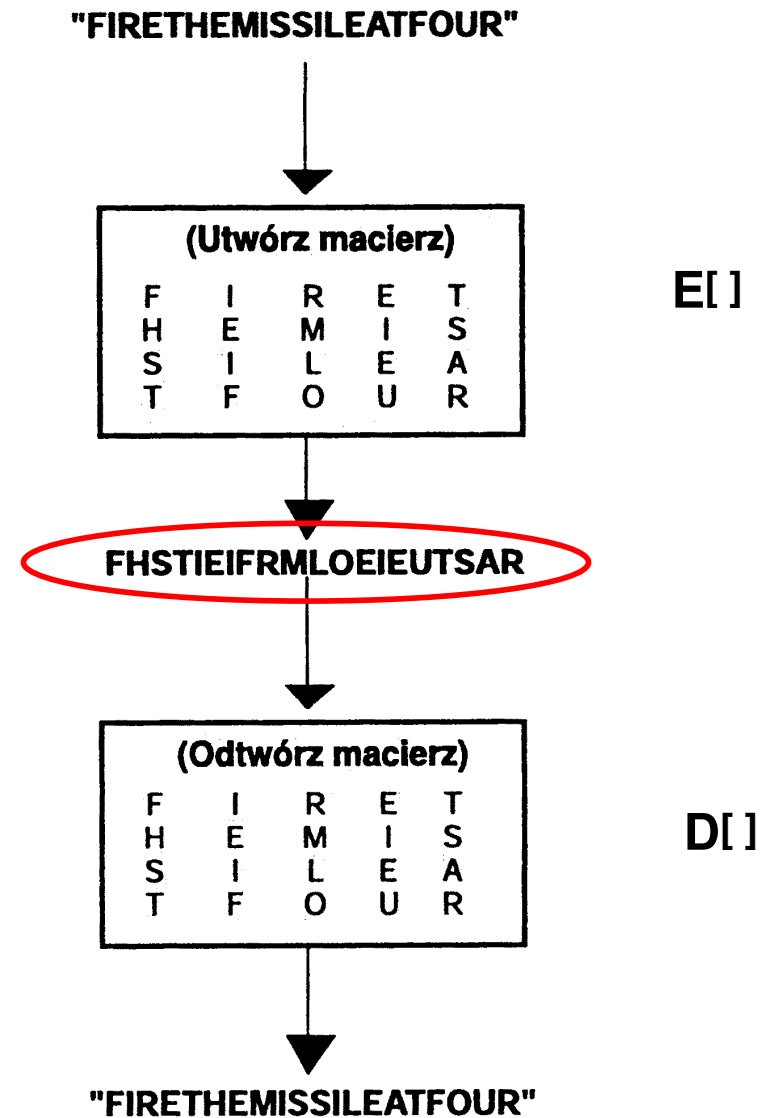


Proste szyfry

Szyfrowanie metodą przestawiania

Przestawianie z macierzą przekształceń:

- rolę figury transpozycji pełni macierz
- kluczem jest rozmiar macierzy,
np. $k = (5,4)$



Współczesna kryptografia

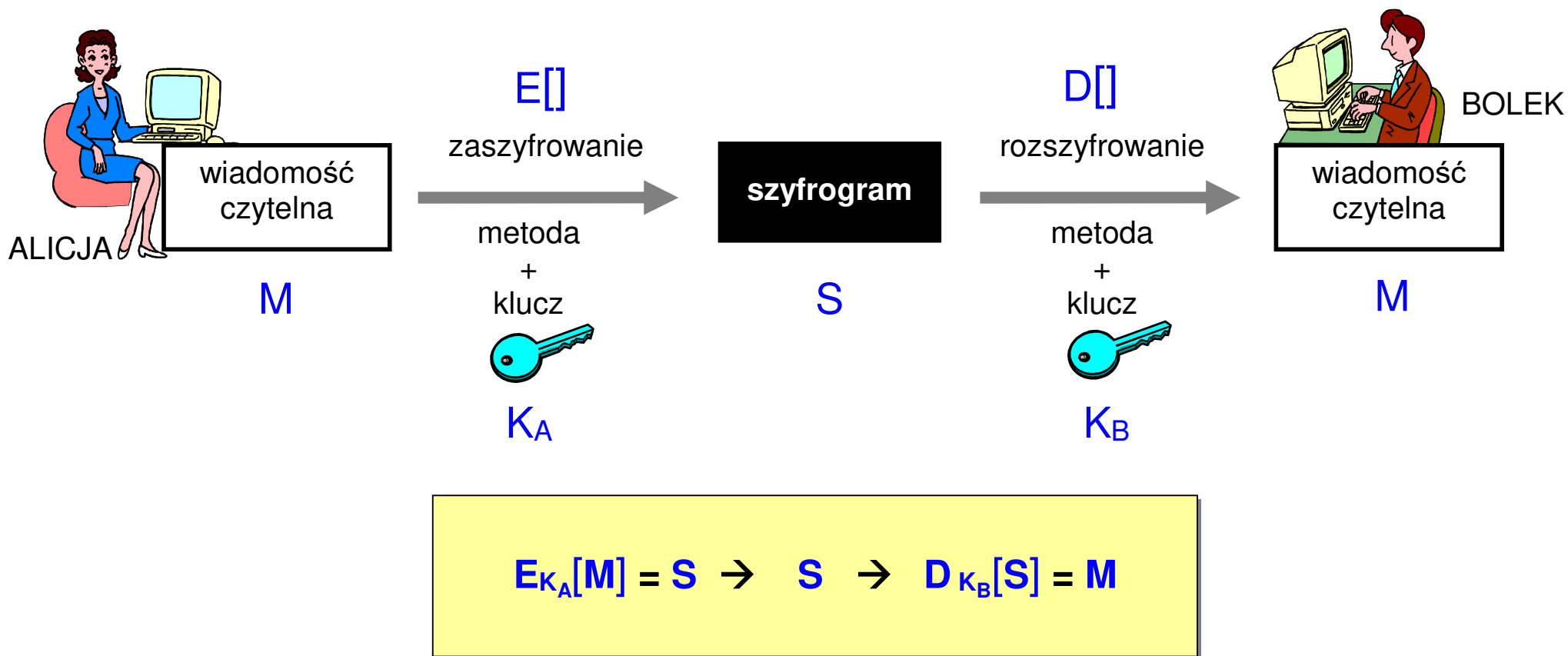
Zasada Kerckhoffsza

Algorytm szyfrowania i deszyfrowania jest jawny

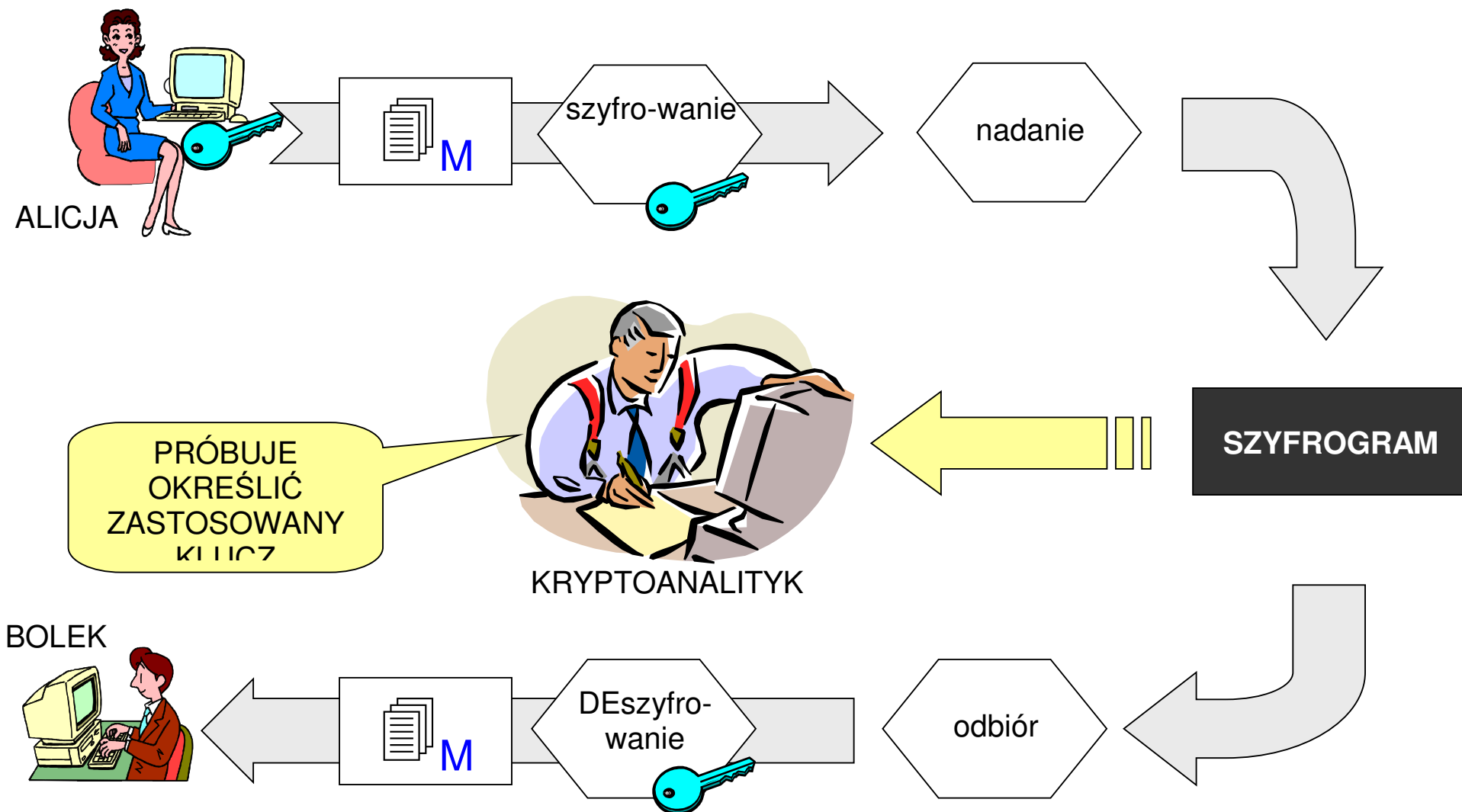
- siła metody kryptograficznej nie polega na tajności algorytmu
- lecz na tajności pewnego zmiennego parametru tego algorytmu (klucza)

Szyfrowanie z kluczem

Schemat ogólny

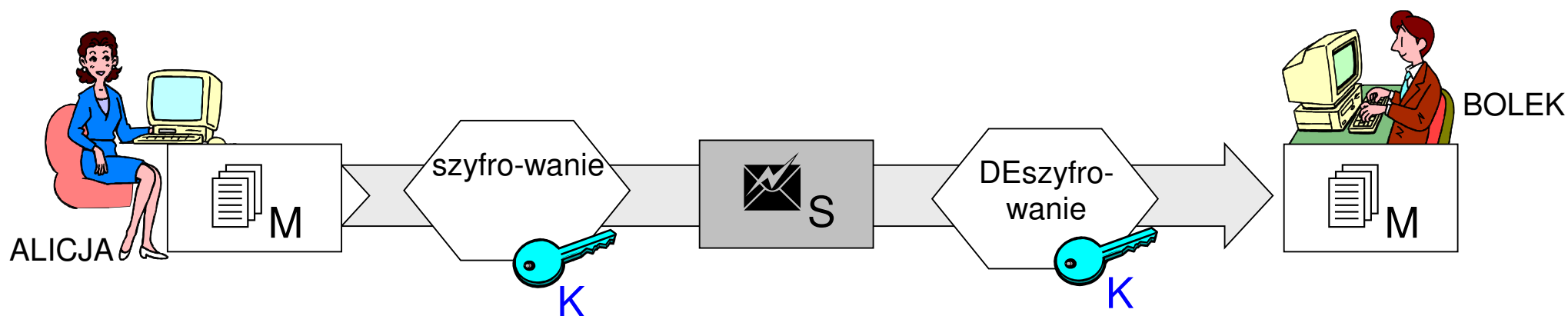


Kryptoanaliza



Szyfrowanie symetryczne

- wspólny tajny klucz K_{A-B} (dalej oznaczany K)
- $E_K[M] = S \rightarrow S \rightarrow D_K[S] = M$



Cecha:

- $D_K [E_K [M]] = M$

Szyfrowanie symetryczne

Podstawowe problemy:

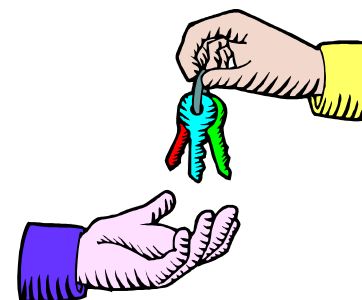
problem tajności klucza

- wiadomość jest bezpieczna dopóki osoba trzecia nie pozna tajnego klucza **K**



problem dystrybucji klucza

- jak uzgodnić wspólny klucz bez osób trzecich, będąc oddalonym o setki, a nawet tysiące kilometrów



problem skalowalności

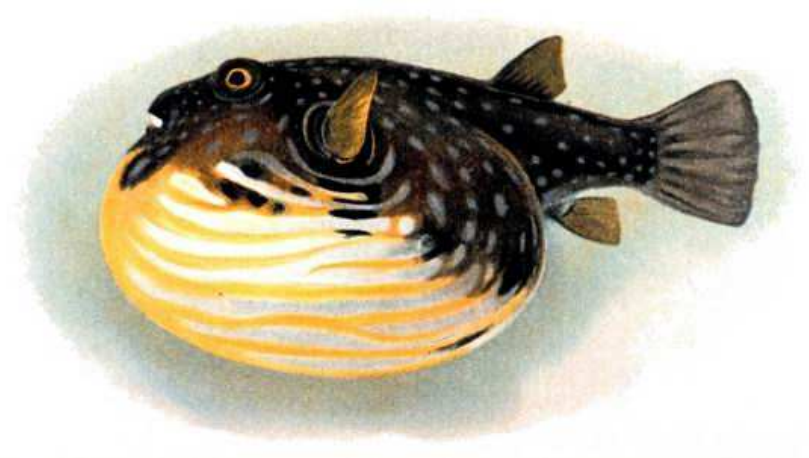
- 2 os. = 1 kl.; 3 os. = 3 kl.; 4 os. = 6 kl.; 10 os. = 45 kl.; 100 os. = 4950 kl.; ...

autentyczność

- czy tajność klucza zapewnia autentyczność?

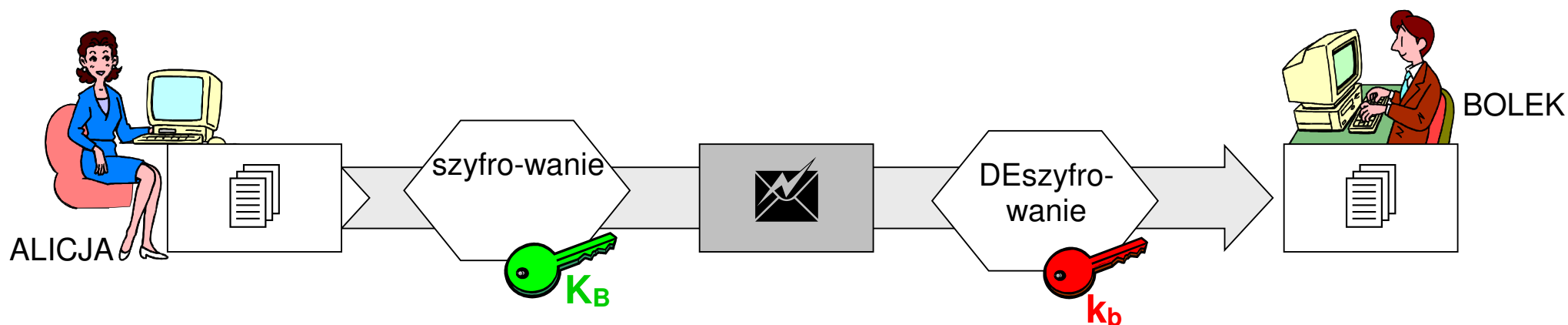
Przykładowe algorytmy

- **DES** (Data Encryption Standard) i 3DES
- **RC** – bardzo wydajne algorytmy symetryczne o zmiennej długości klucza (prawnie zastrzeżone – RSA Data Security, Ron Rivest)
 - RC2, RC5, RC6 – blokowe
 - RC4 – strumieniowy
- **Blowfish**
- **IDEA** (*International Data Encryption Algorithm*)
opracowany w 1991r. przez Swiss Federal Institute of Technology
(James L. Massey i Xuejia Lai)



Szyfrowanie asymetryczne

- odbiorca **B** posiada parę kluczy: prywatny klucz k_b oraz publiczny klucz K_B
- $E_{K_B}[M] = S \rightarrow S \rightarrow D_{k_b}[S] = M$
- znajomość klucza publicznego K_B nie wystarcza do naruszenia poufności szyfrogramu uzyskanego przy zastosowaniu tego klucza



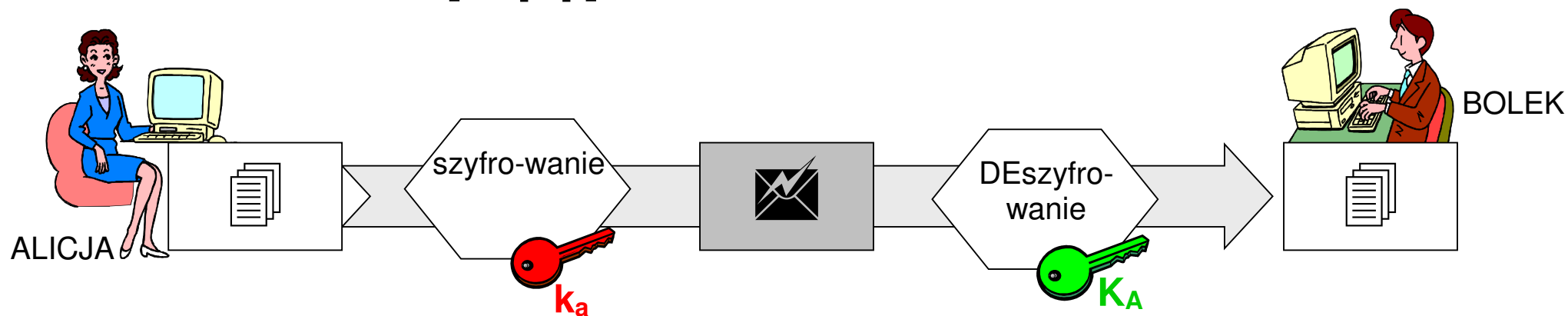
Szyfrowanie asymetryczne

Cechy:

- o przemienność kluczy:

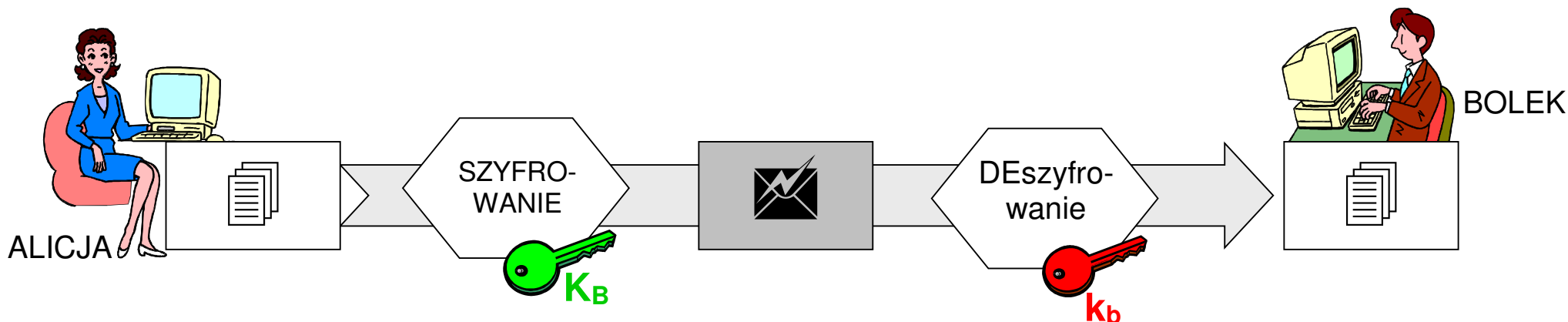
- $D_k [E_K [M]] = M$

- $D_K [E_k [M]] = M$

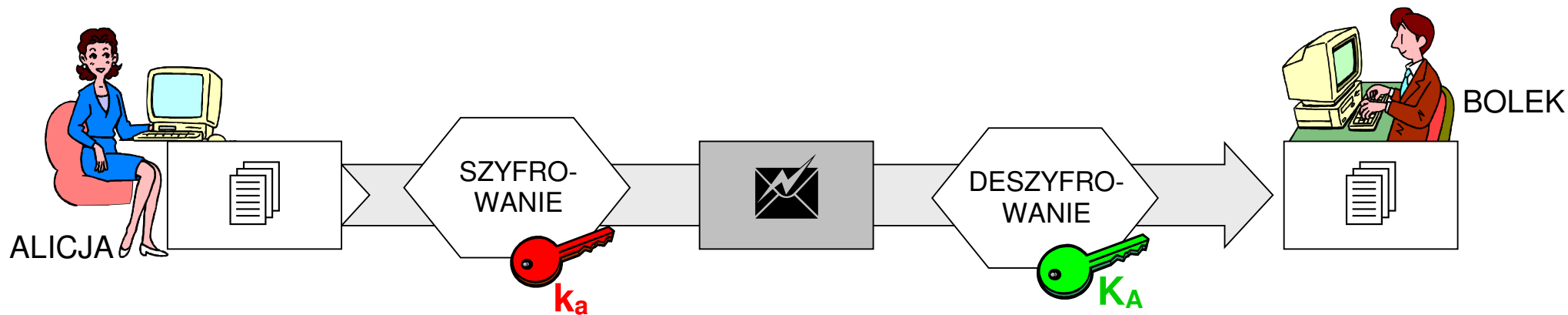


Szyfrowanie asymetryczne

zapewnienie poufności:



zapewnienie autentyczności:



Autentyczność

Metoda 1:

- szyfrujemy całą wiadomość kluczem prywatnym nadawcy
- kosztowne obliczeniowo – koszt rośnie z wielkością wiadomości

Metoda 2:

- tworzymy skrót wiadomości o ustalonym z góry rozmiarze n
- szyfrujemy kluczem prywatnym nadawcy tylko skrót
- koszt mały – n małe
- koszt stały – nie rośnie z wielkością wiadomości i zależy tylko od n

Skrót

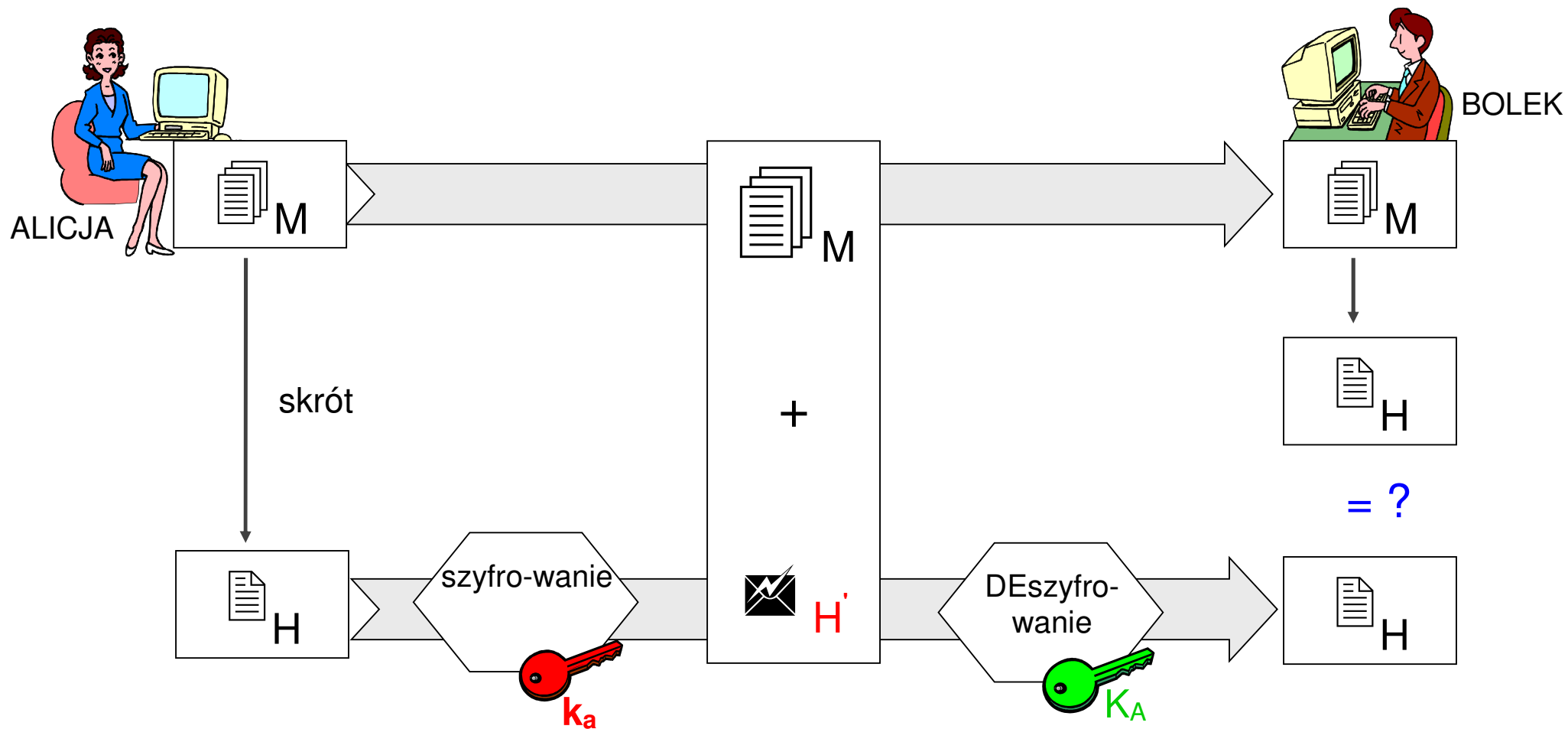
Funkcja skrótu

- jednokierunkowa funkcja, najczęściej mieszająca (*hash function*) $h[M]$
- $H=h[M]$ – **skrót** o stałym rozmiarze

Wymagane własności:

- kompresja: $|H| < |M|$
- łatwość obliczeń: czas wielomianowy wyznaczenia $h[M]$ dla dowolnego M
- odporność na **podmianę** argumentu: dla danego $h[M]$ obliczeniowo trudne znalezienie $M' :: h[M] = h[M']$
- odporności na **kolizje**: obliczeniowo trudne znalezienie dwóch dowolnych argumentów $M \neq M' :: h[M] = h[M']$

Podpis cyfrowy



All in one



k_a

K_A

M

H

$$E_{k_a}[H] = H'$$

$$E_{K_B}[M + H'] = S$$

M H'



S



$$D_{k_b}[S] = M + H'$$

M H'



H

=

H

$$D_{K_A}[H'] = H$$

poufność
integralność
autentyczność
niezaprzeczalność



BOLEK

k_b

K_B

Popularne algorytmy skrótów i podpisu

HAVAL – skrót o zmiennej długości: 128b, 160b, 192b, 224b lub 256b

Whirlpool – ISO/IEC 10118-3 (2004), skrót 512b

ElGamal – algorytm asymetrycznego szyfrowania i podpisywania

DSA – odmiana algorytmu ElGamala opracowana przez NSA

HMAC (RFC 2104) – podpis cyfrowy z szyfrowaniem symetrycznym

AES-CCM (AES-CMAC) / **AES-GCM** (AES-GMAC)

Dystrybucja kluczy publicznych

Warianty

1. pobranie klucza bezpośrednio od właściciela B
 2. pobranie klucza z centralnej bazy danych
 3. pobranie z własnej prywatnej bazy danych zapamiętanego wcześniej klucza pozyskanego sposobem 1 lub 2
- w ogólności istnieje ryzyko podstawienia przez nieuczciwą osobę własnego klucza pod klucz użytkownika B

Certyfikaty kluczy publicznych

Certyfikacja

- w celu uniknięcia podstawienia klucza publicznego stosuje się certyfikację
- certyfikat jest podpisany przez osobę (instytucję) godną zaufania
- jest nią urząd poświadczający CA (*Certification Authority*)
- urząd poświadczający CA potwierdza, iż informacja opisująca użytkownika B jest prawdziwa a klucz publiczny faktycznie do niego należy
- certyfikat zawiera podstawowe dane identyfikujące właściciela
- posiada też okres ważności
- niezależnie od okresu ważności klucze mogą zostać uznane za niepoprawne – urząd poświadczający CA musi przechowywać listę niepoprawnych i nieaktualnych certyfikatów

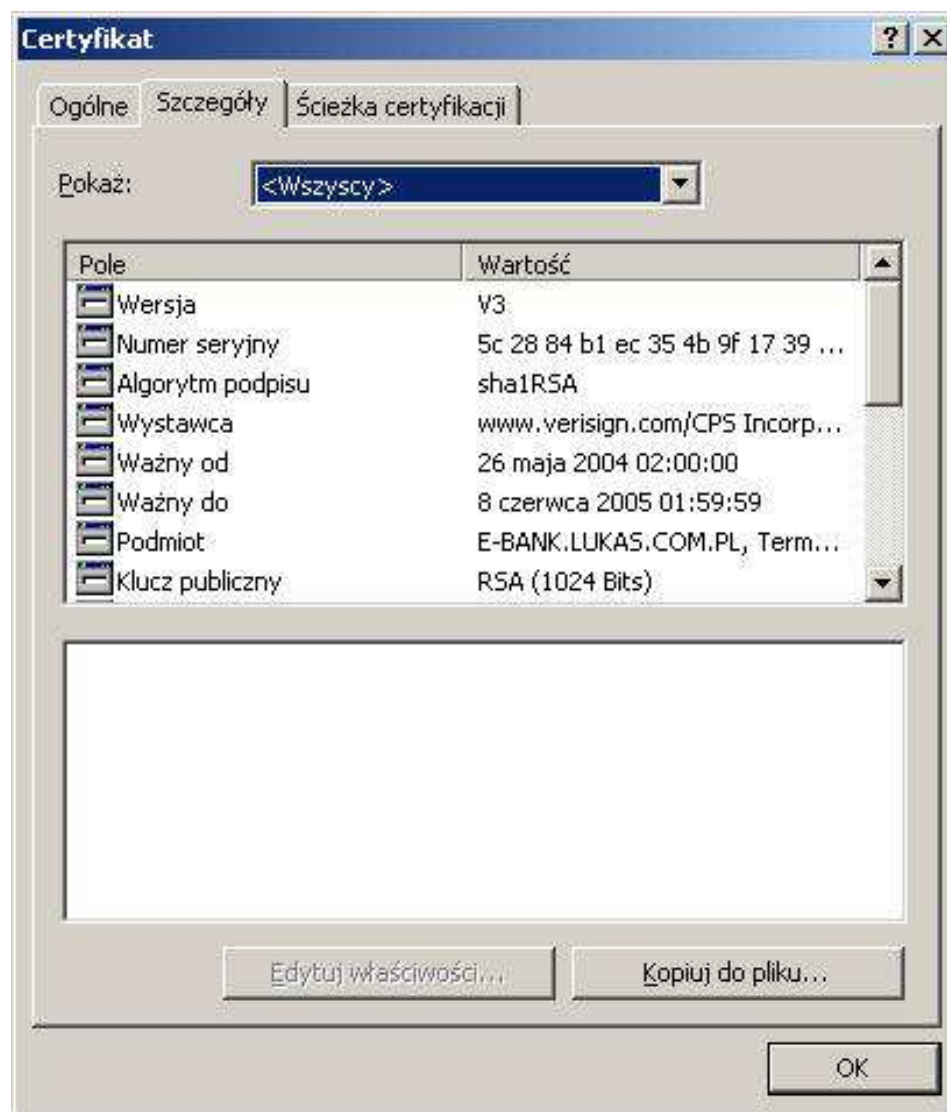
Certyfikaty kluczy publicznych

Struktura podstawowa typowego certyfikatu

Wersja	informuje o kolejnych wersjach certyfikatu
Numer seryjny	wartość niepowtarzalna, związana z certyfikatem
Identyfikator algorytmu (algorytm, parametry)	algorytm stosowany do podpisania certyfikatu
Wystawca	urząd certyfikujący CA, który wystawił certyfikat
Okres ważności	początkowa i końcowa data ważności certyfikatu
Podmiot	nazwa podmiotu, dla którego stworzono certyfikat
Klucz publiczny podmiotu (algorytm, parametry, klucz)	klucz publiczny podmiotu z identyfikatorem algorytmu
Podpis	podpis urzędu certyfikującego CA

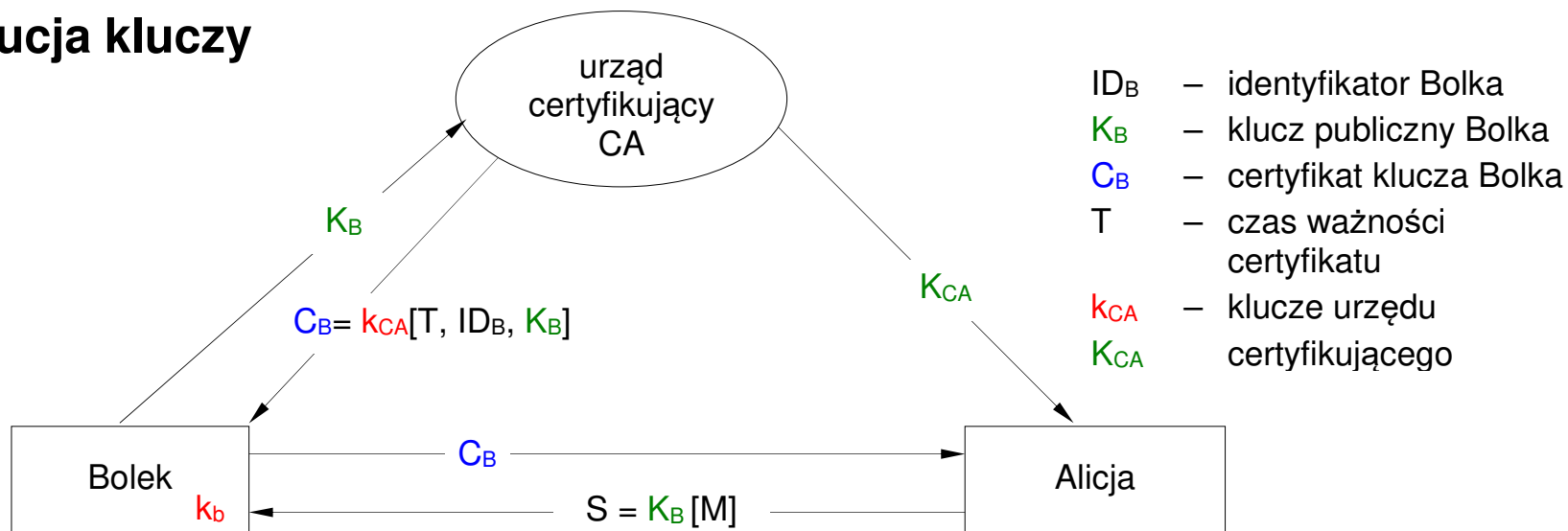
Certyfikaty kluczy publicznych

Przykład certyfikatu



Certyfikaty kluczy publicznych

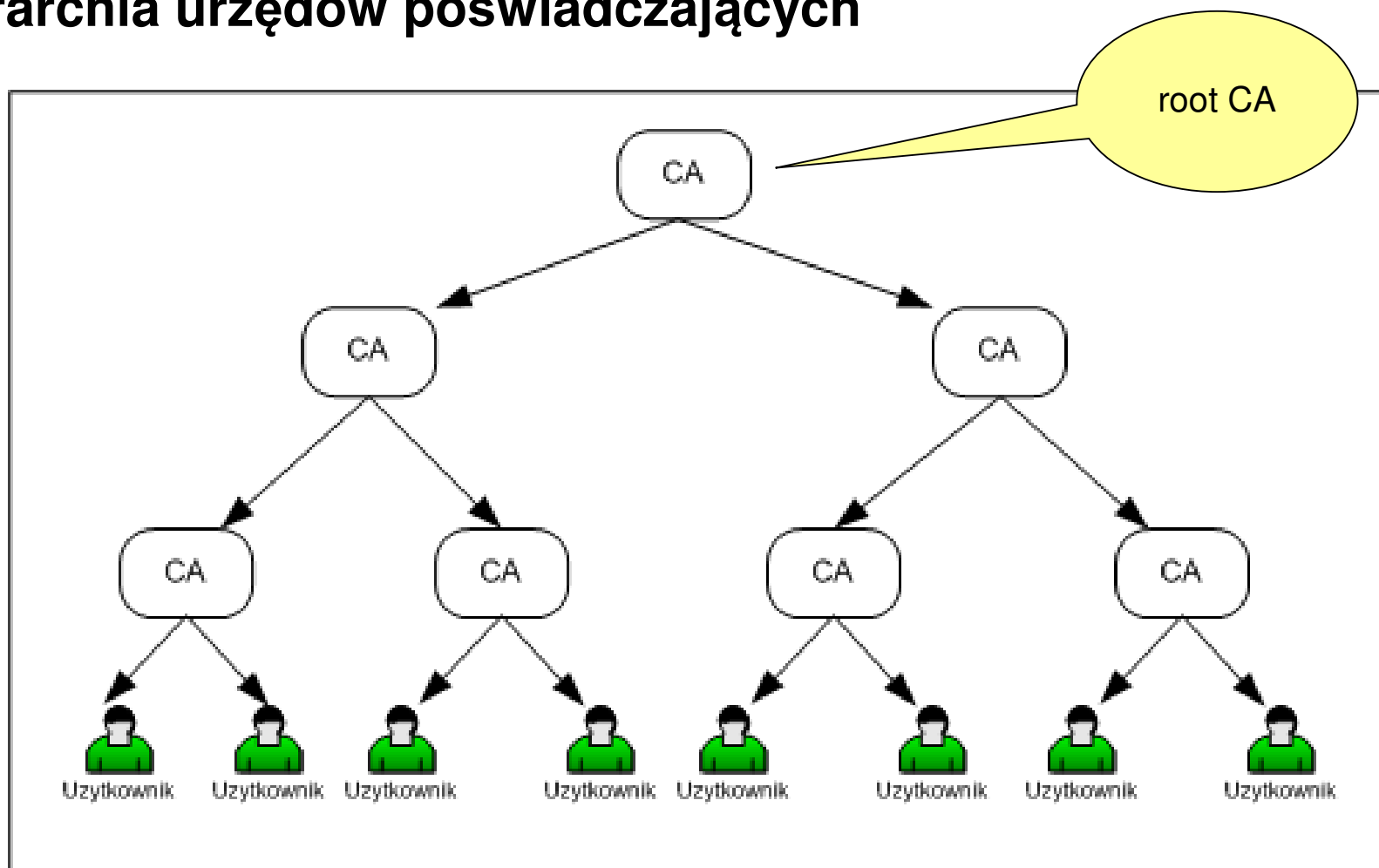
Dystrybucja kluczy



- w celu uzyskania certyfikatu użytkownik zwraca się do urzędu certyfikującego CA dostarczając mu swój klucz jawny
- do odczytania certyfikatu niezbędny jest tylko i wyłącznie klucz jawny urzędu certyfikującego
- użytkownik może przesłać swój certyfikat do innych użytkowników w celu zweryfikowania jego autentyczności (Web of Trust)

Certyfikaty kluczy publicznych

Hierarchia urzędów poświadczających



Infrastruktura kluczy publicznych

PKI (*Public Key Infrastructure*) - komponenty

- urzędy CA
- punkty rejestrujące, poręczające zgodność kluczy z identyfikatorami (lub innymi atrybutami) posiadaczy certyfikatów
- użytkownicy certyfikatów podpisujący cyfrowo dokumenty
- klienci weryfikujący podpisy cyfrowe i ścieżki certyfikacji do zaufanego CA
- repozytoria przechowujące i udostępniające certyfikaty i listy unieważnień CRL (*Certificate Revocation List*)

Infrastruktura kluczy publicznych

Polska

Ustawa o podpisie elektronicznym z dn. 18 września 2001

Podpis elektroniczny

- zostaje złożony przy *użyciu bezpiecznego urządzenia* (SSCD – *Security Signature Creation Device*, norma CWA 14169 Europejskiego Komitetu Standaryzacji)
- i certyfikatu kwalifikowanego
- wywołuje skutki prawne równoważne podpisowi własnoręcznemu

Infrastruktura kluczy publicznych

Polska

Certyfikat kwalifikowany

- wydawany na podstawie umowy i po weryfikacji tożsamości w *kwalifikowanym CA*
- znajduje zastosowanie w każdym przypadku składania oświadczenia woli
- ważny nie dłużej niż 2 lata

Certyfikaty niekwalifikowane (tzw. powszechne)

- szyfrowanie danych, poczta, www, urządzenia sieciowe, oprogramowanie

Znacznik czasu

- kwalifikowany (jak data poświadczona notarialnie, art. 81 KC)
- i niekwalifikowany

Infrastruktura kluczy publicznych

**Kwalifikowane CA wpisane do rejestru
Narodowego Centrum Certyfikacji (www.nccert.pl)**

- Krajowa Izba Rozliczeniowa www.kir.pl
- Sigillum www.sigillum.pl
- Certum www.certum.pl
- TP Internet
- MobiCert
- ...



Infrastruktura kluczy publicznych

Ceny

	<i>Cena</i>	<i>Okres ważności</i>
Private Email	0 zł	(3 miesiące)
Certum Silver	50 zł	(rok)
Certum Silver - odnowienie	25 zł	(rok)
Certum Gold	200 zł	(rok)
Certum Gold - odnowienie	100 zł	(rok)
Certum Platinum (karta+czytnik)	700 zł	(2 lata)
Certum Platinum - odnowienie	200 zł	(2 lata)

	<i>Cena</i>	<i>Okres ważności</i>
Private Web Server	0 zł	(min. 3 miesiące)
Enterprise Web Server	500 zł	(rok)
Enterprise Web Server - odnowienie	250 zł	(rok)
Wildcard Domain	1000 zł	(rok)
Wildcard Domain - odnowienie	500 zł	(rok)
Trusted Web Server	1000 zł	(2 lata)
Trusted Web Server - odnowienie	500 zł	(2 lata)

