

Bezpieczeństwo informacji



dr inż. Jacek Czerniak
jczerniak@ukw.edu.pl

Bydgoszcz, 2013



Zakres tematyczny

- Wprowadzenie do kryptologii
- Podpis elektroniczny
- Typy algorytmów i tryby ich pracy
- Metody uwierzytelniania podpisów
- Sprzętowe moduły kryptograficzne
- Matematyczne podstawy kryptologii



Literatura

- Bruce Schneier, „Kryptografia dla praktyków”, WNT 2002
- Dorothy Elisabeth Robling Denning, „Kryptografia i ochrona danych”, WNT 1993
- William Stallings, „Ochrona danych w sieci i intersieci”, WNT 1997
- Mirosław Kutylowski, Willy-B. Strothmann, „Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych”, LUPUS 1998
- Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, „Handbook of Applied Cryptography”, CRC Press 1997



Warunki zaliczenia ZO

- Zaliczenie laboratorium + Test „20”:
 - 20 pytań w 20 min.
 - Cztery odpowiedzi, jedna dobra
 - Tylko punkty dodatnie
 - Pułap zaliczenia 60% czyli 12 z 20 pkt.

Wprowadzenie do **Szyfrowania i podpisu cyfrowego**



dr inż. Jacek Czerniak

www.jczerniak.ukw.edu.pl

Kierunek studiów: IB

Bydgoszcz, 2013



Kryptologia, kryptografia, kryptoanaliza

- *Kryptografia* - metody matematyczne realizacji usług poufności, integralności, uwierzytelniania (autentyczności i niezaprzeczalności)
- *Kryptoanaliza* - metody matematyczne przełamывania, osłabiania, pokonywania usług realizowanych metodami kryptograficznymi



Pojęcia podstawowe

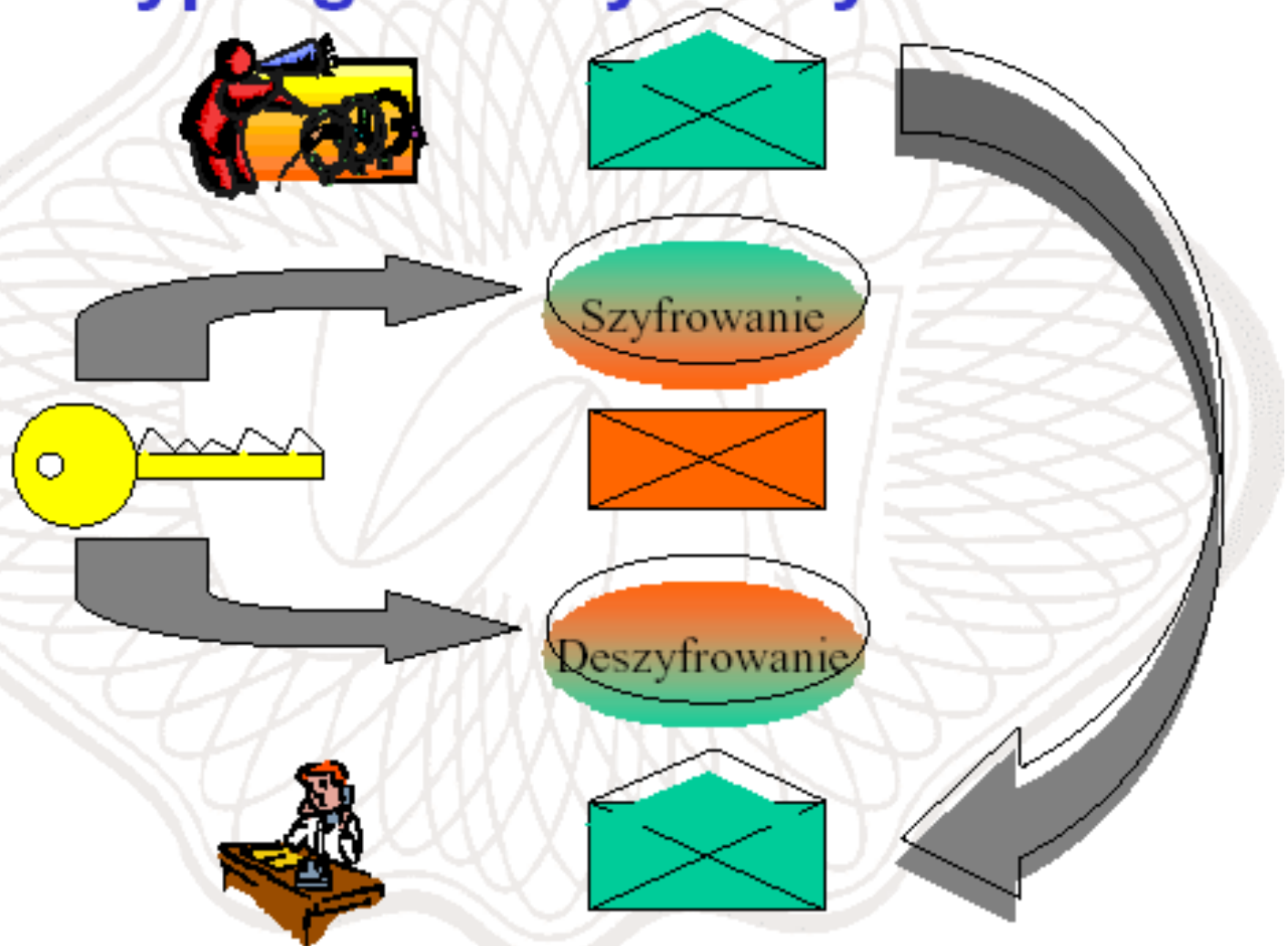
- Prywatność, poufność (*ang.privacy, confidentiality*)
- Integralność danych (*ang.data integrity*)
- Uwierzytelnianie podmiotów, identyfikacja (*ang.entity authentication, identification*)
- Uwierzytelnianie wiadomości, uwierzytelnianie pochodzenia danych (*ang.message authentication*)
- Podpis cyfrowy (*ang.digital signature*)
- Certyfikacja (*ang.certification*)



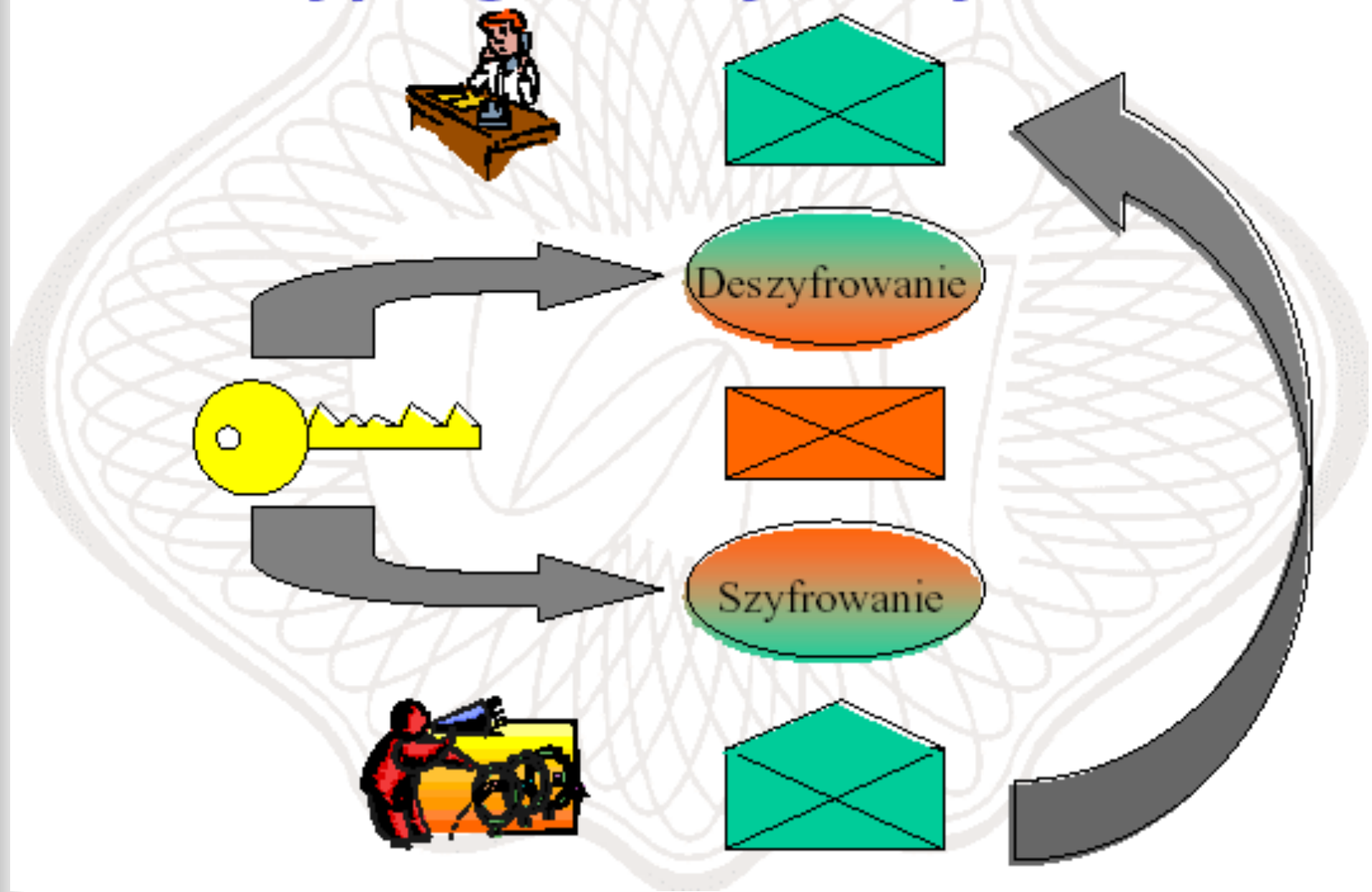
Pojęcia podstawowe

- Unieważnienie (*ang.revocation*)
- Znakowanie czasu (*ang.time stamping*)
- Poświadczenie (*ang.witnessing*)
- Niezaprzeczalność (*ang.non-repudiation*)
- Szyfrowanie (*ang.encryption, ciphering*)
- Deszyfrowanie (*ang.decryption, deciphering*)
- Klucz kryptograficzny (*ang.cryptographic key*)

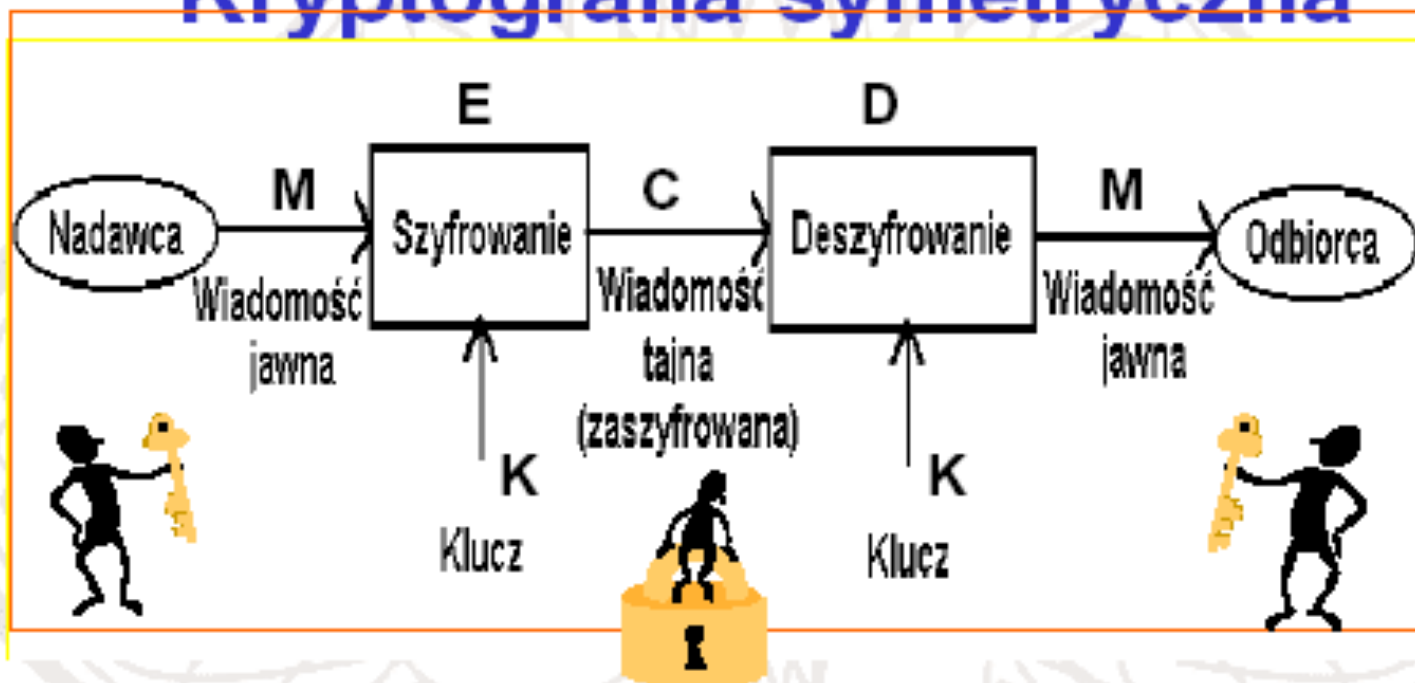
Kryptografia symetryczna



Kryptografia symetryczna



Kryptografia symetryczna



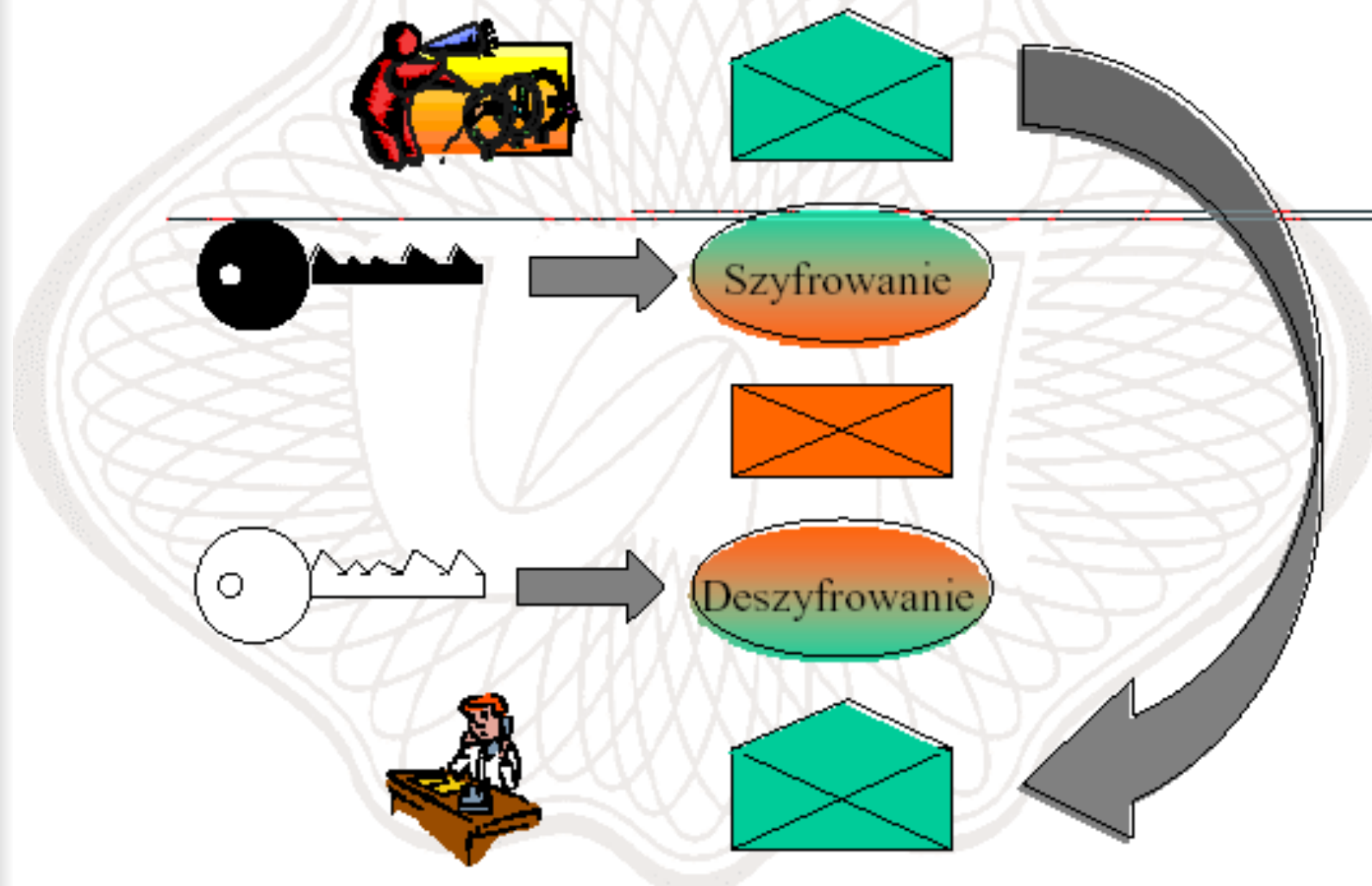
$$E_K(M) = C$$

$$D_K(C) = M$$

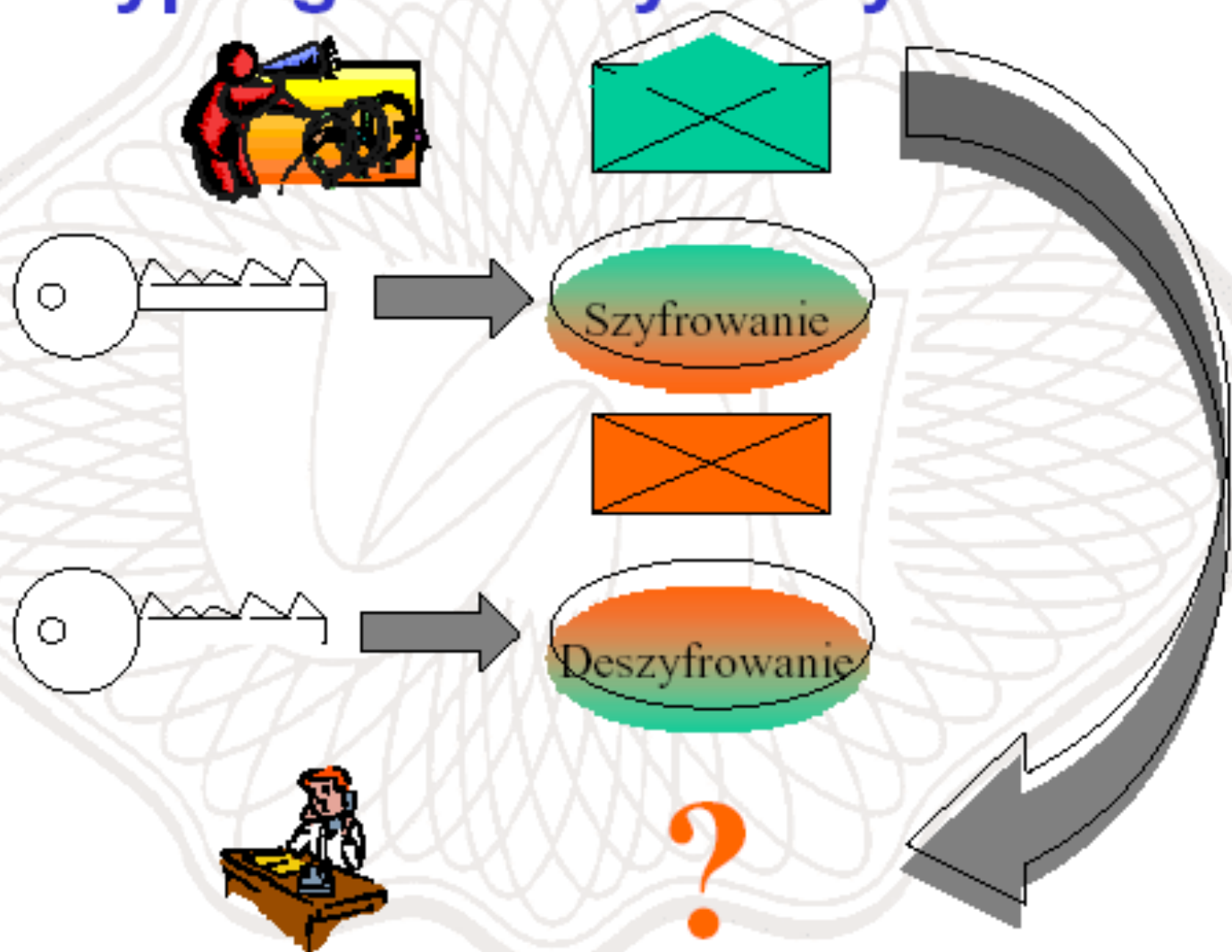
dla wszystkich dopuszczalnych M :

$$D_K(E_K(M)) = M$$

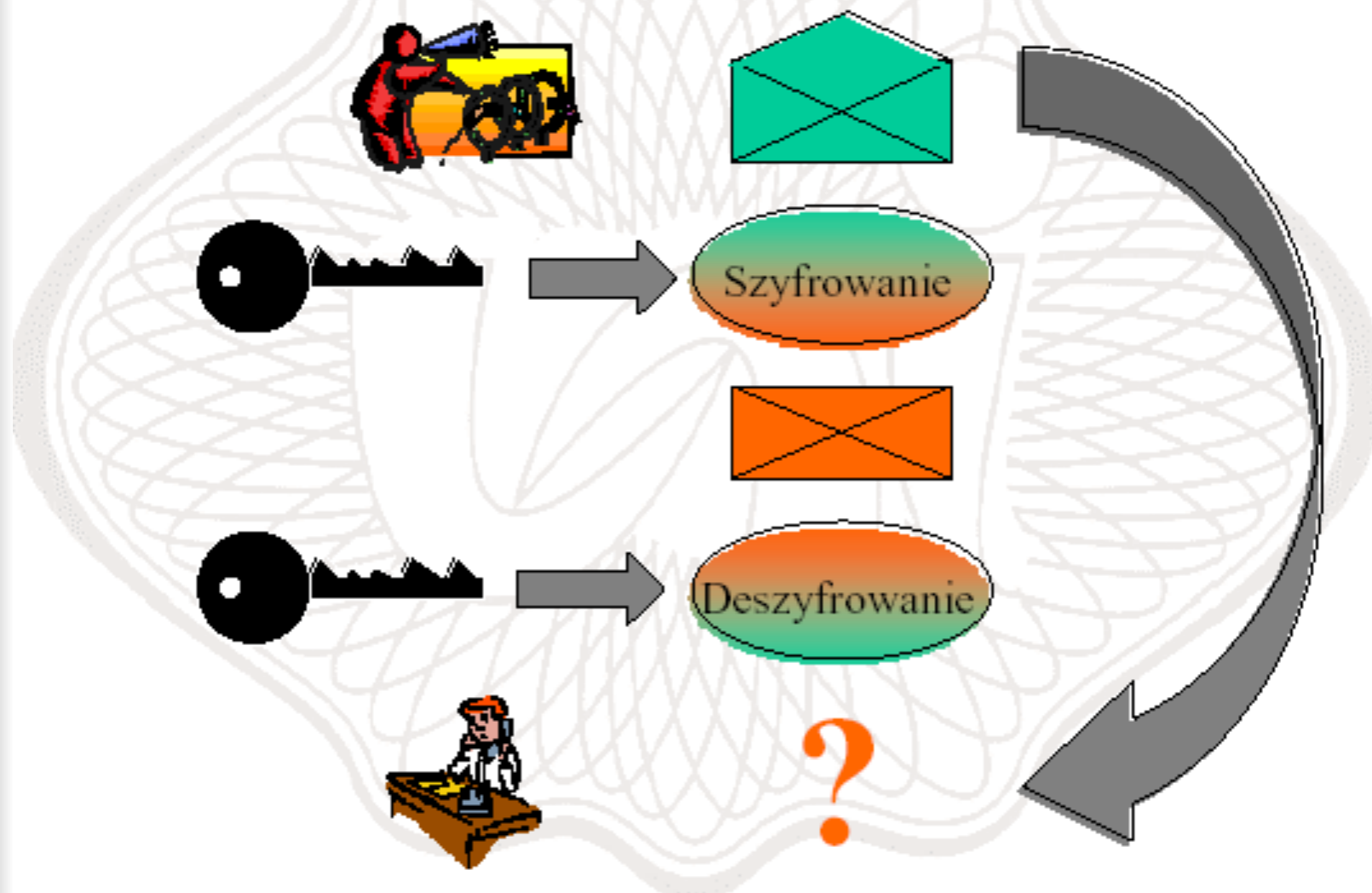
Kryptografia asymetryczna



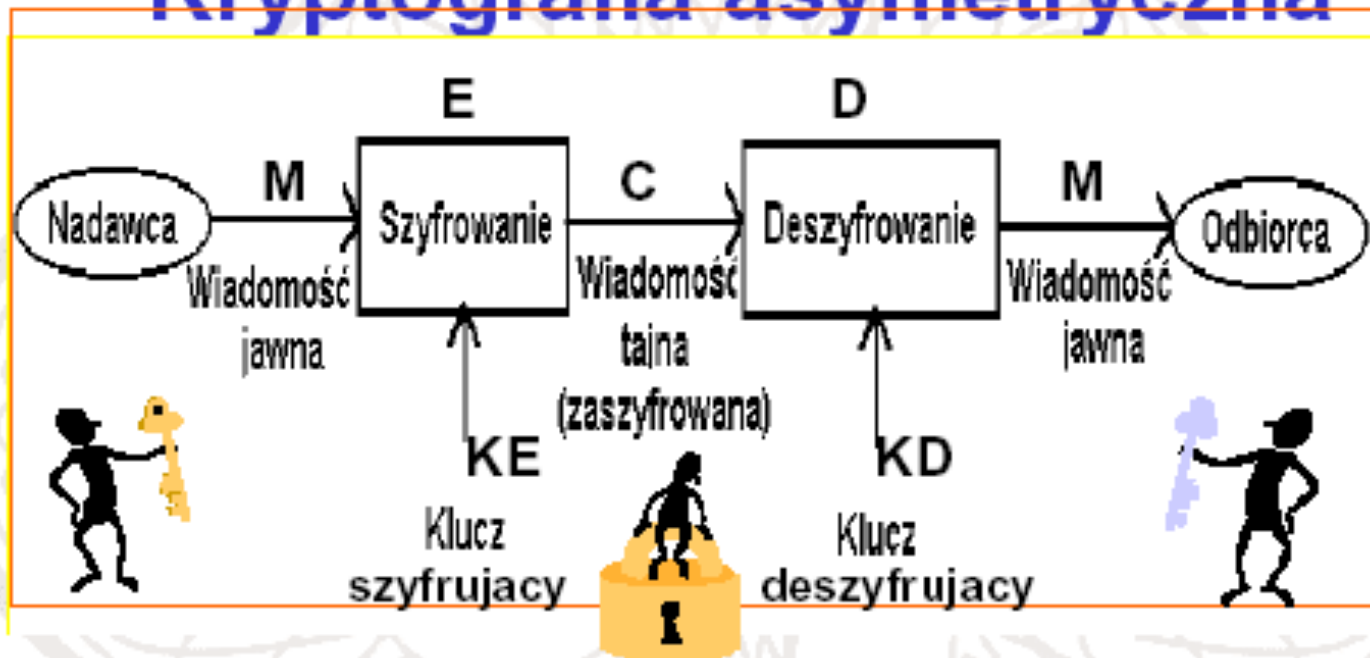
Kryptografia asymetryczna



Kryptografia asymetryczna



Kryptografia asymetryczna



$$E_{KE}(M) = C$$

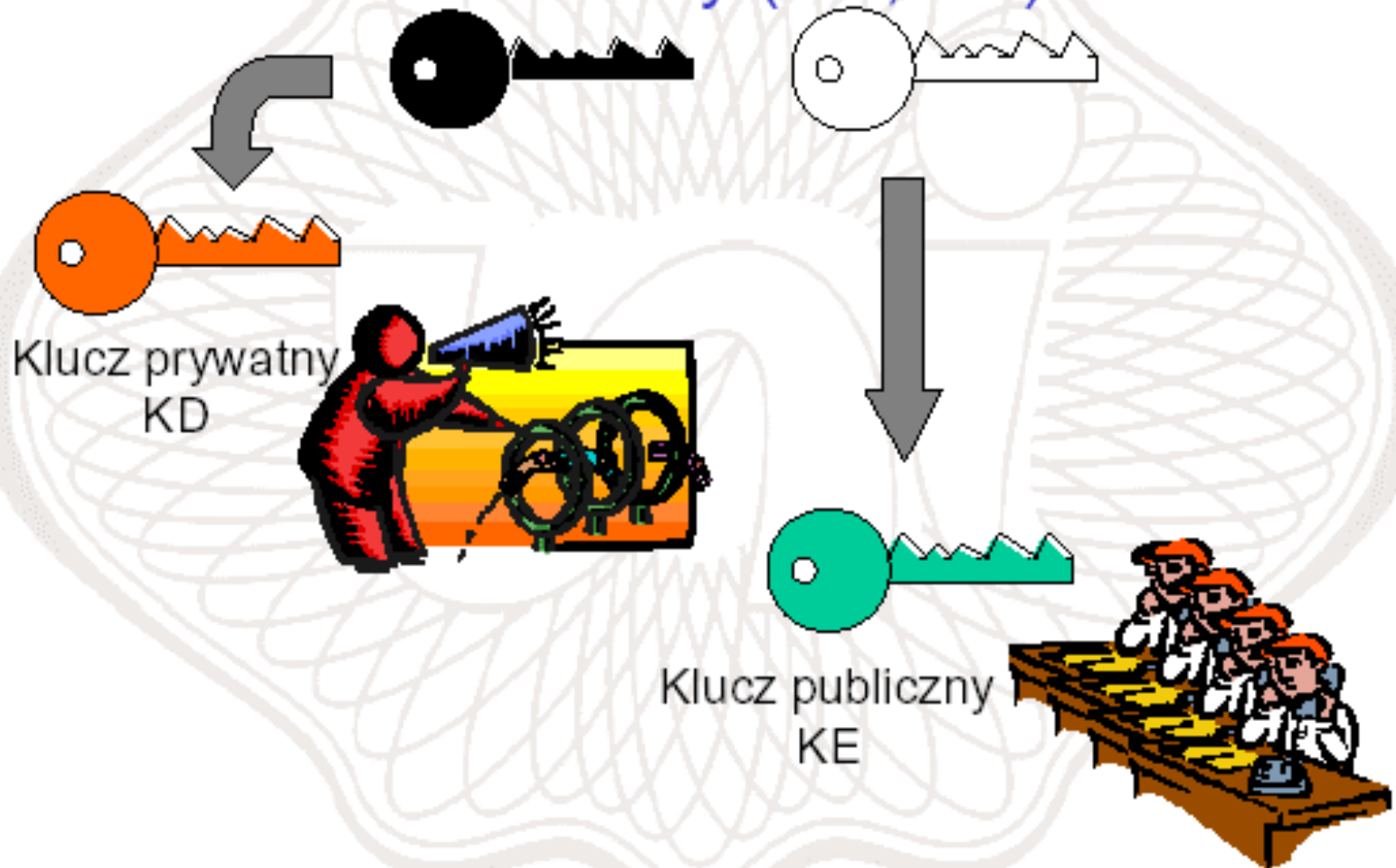
$$D_{KD}(C) = M$$

dla wszystkich dopuszczalnych M:

$$D_{KD}(E_{KE}(M)) = M$$

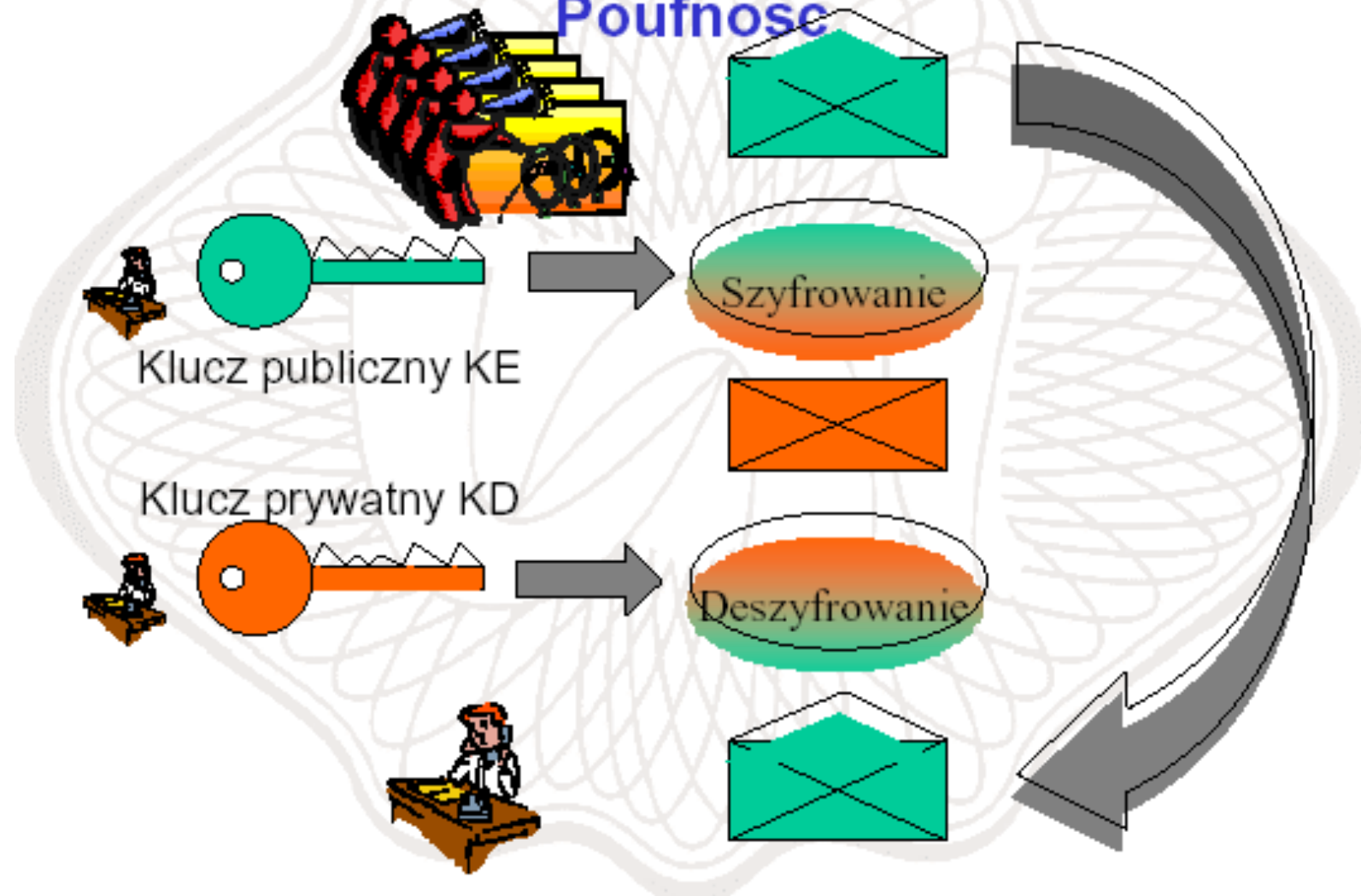
Kryptografia asymetryczna

Para kluczy (KD, KE)



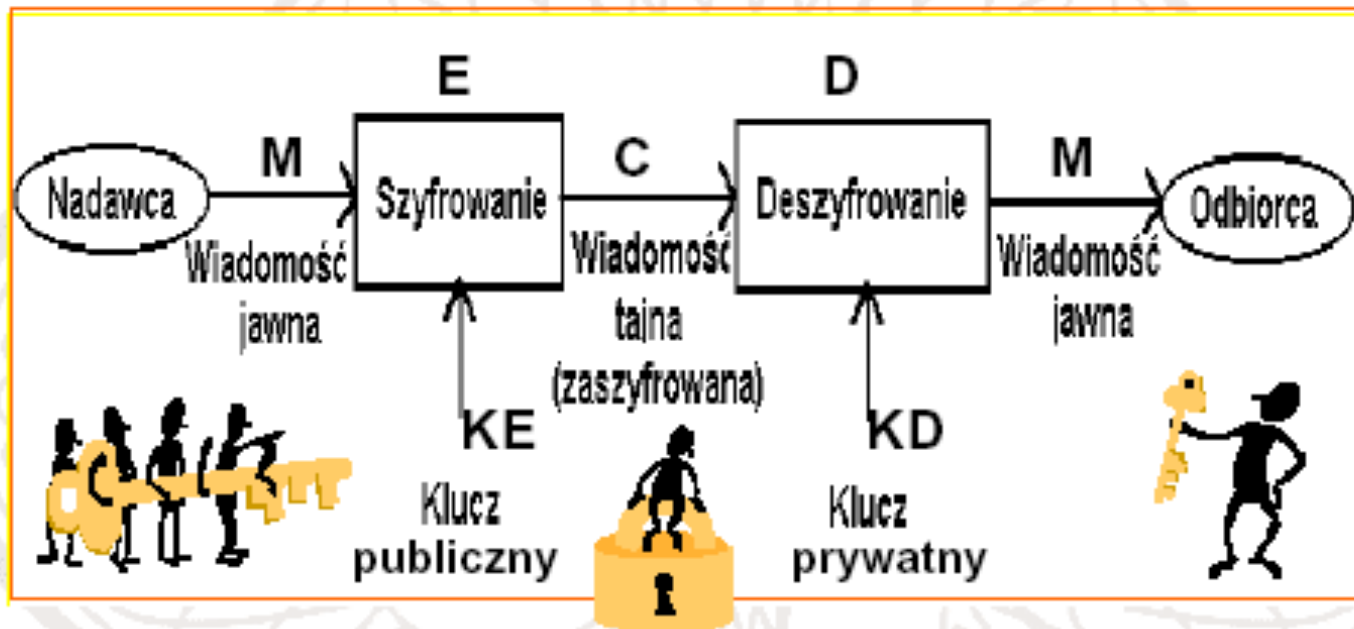
Kryptografia asymetryczna

Poufność



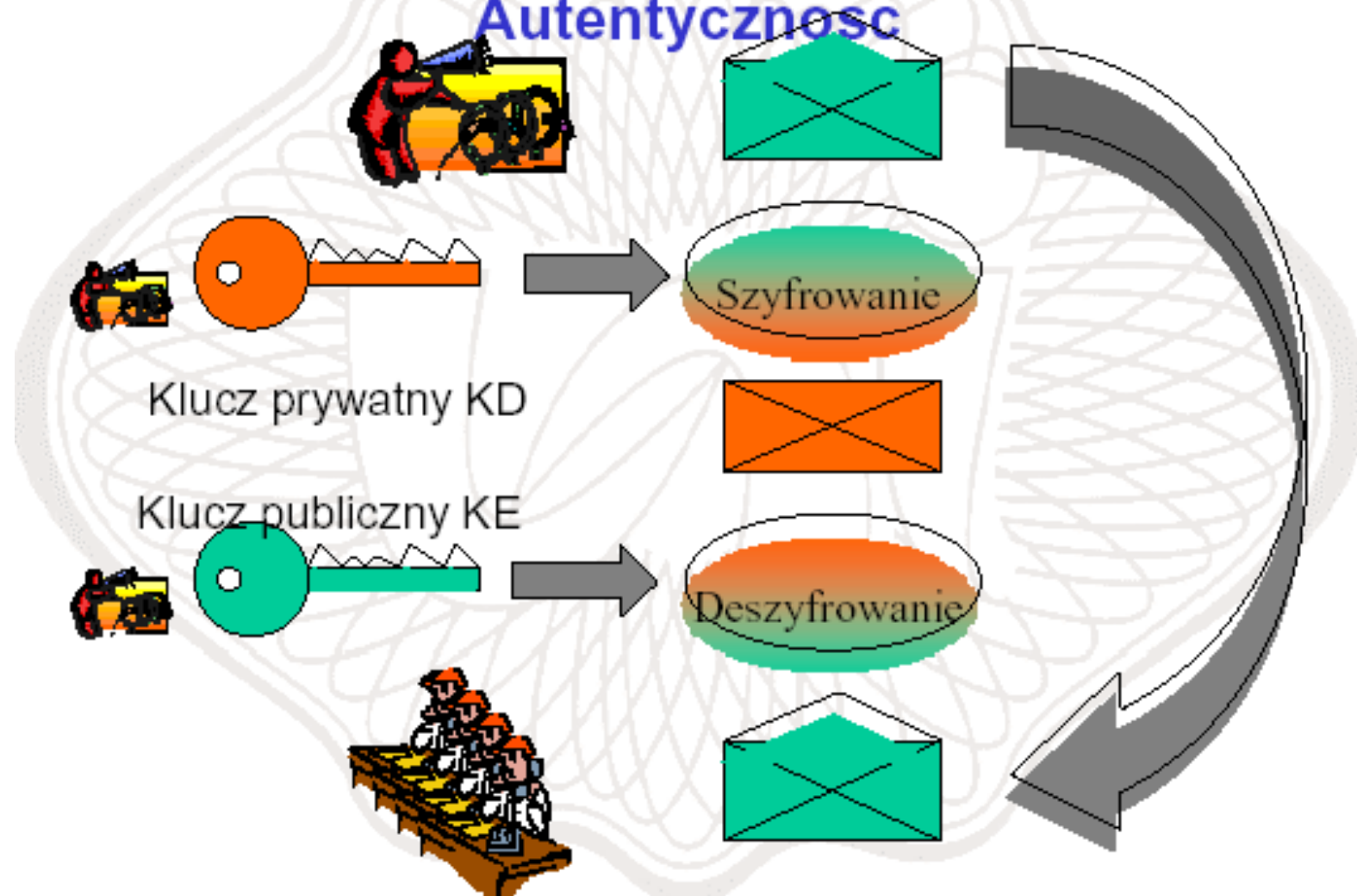
Kryptografia asymetryczna

Poufnosc



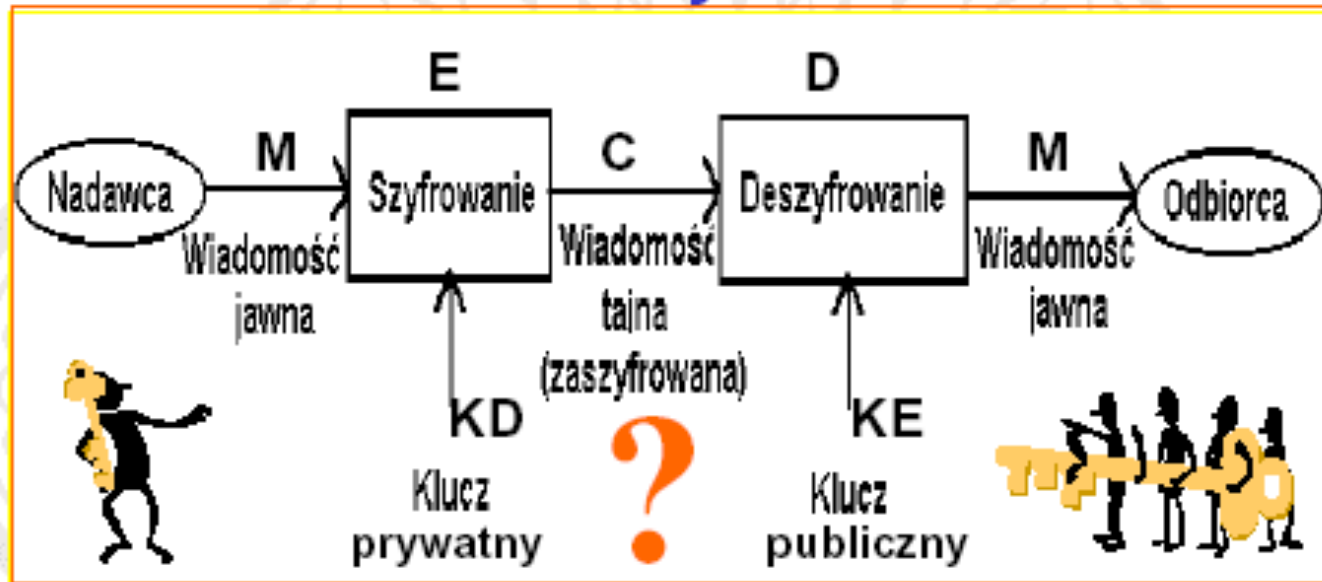
Kryptografia asymetryczna

Autentyczność

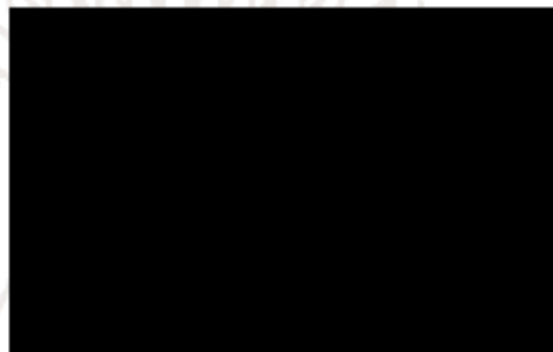


Kryptografia asymetryczna

Autentyczność



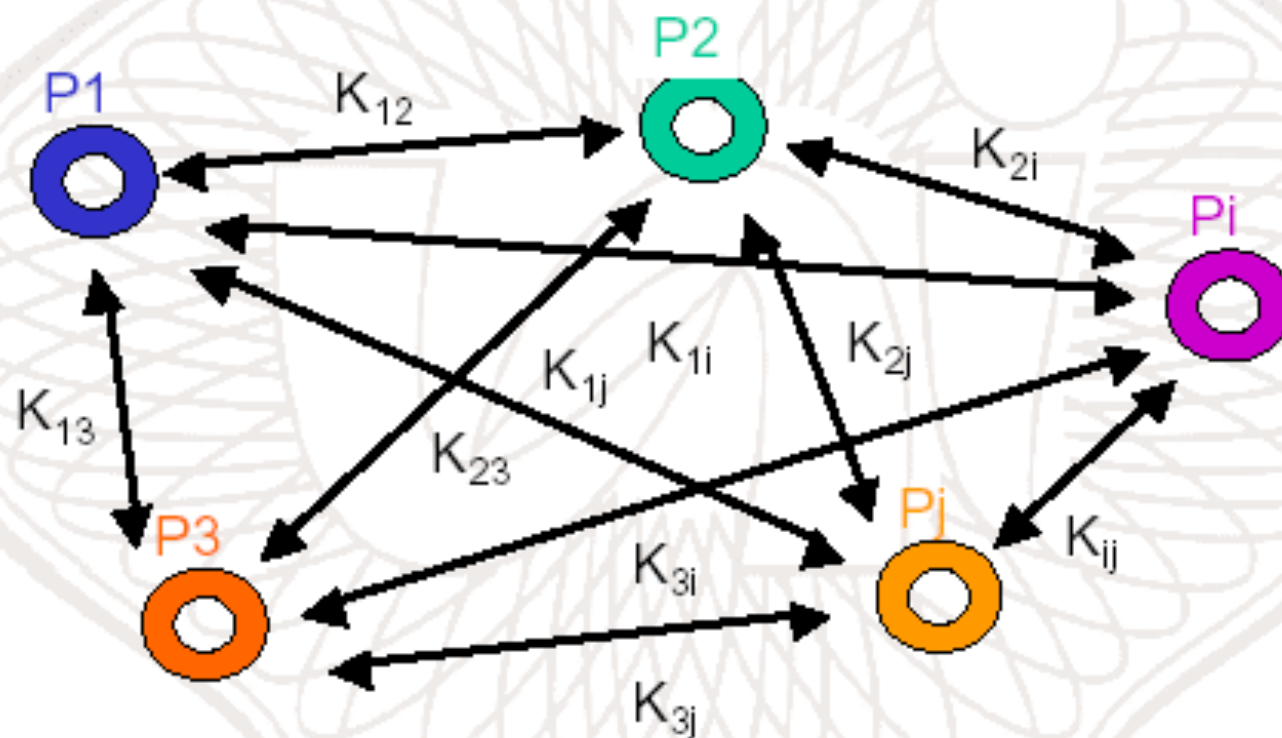
Czy algorytm szyfrujący powinien być tajny ?



August Kerckoffs (1835- 1903)

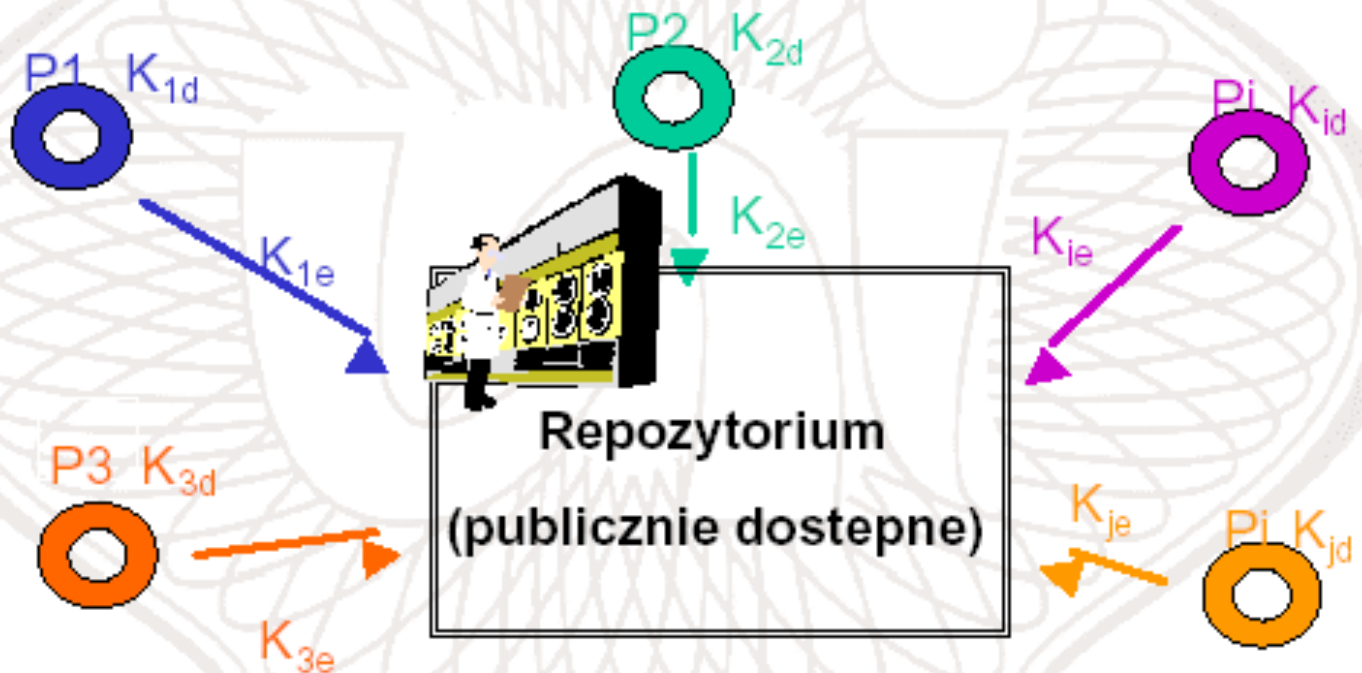
"Bezpieczeństwo szyfru musi zależeć
całkowicie od (bezpieczeństwa)
klucza kryptograficznego" !!!!

Liczba kluczy w systemie kryptografii symetrycznej



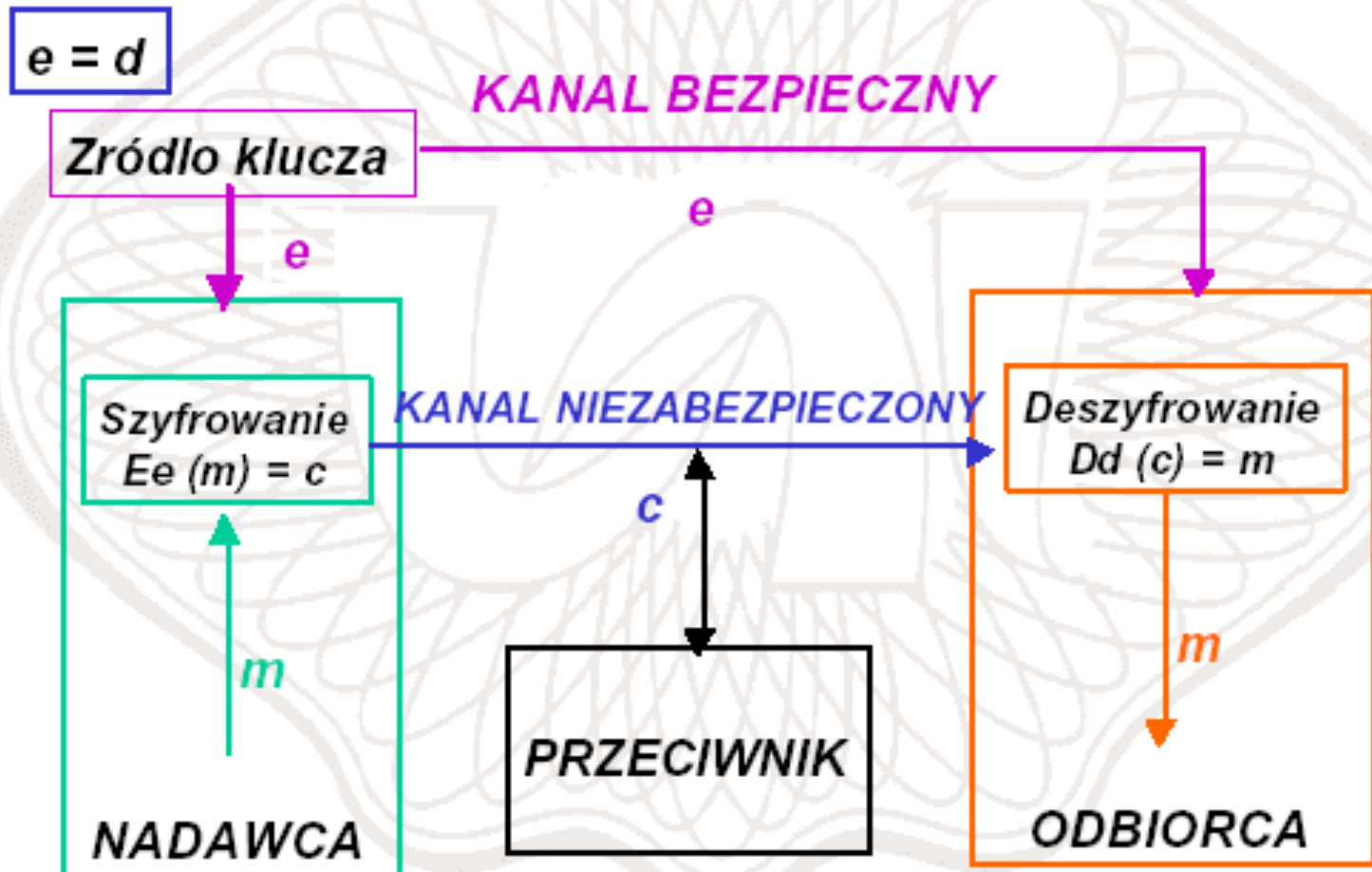
Liczba kluczy dla N podmiotów = $N \times (N-1) / 2 = 0.5 N^2 - 0.5 N$

Liczba kluczy w systemie kryptografii asymetrycznej



Liczba par kluczy dla N podmiotów = N

Symetryczny system kryptograficzny



Techniki szyfrowania

Szyfry blokowe



Szyfry strumieniowe





SZYFRY BLOKOWE- definicja

Szyfry blokowe to procedury, które szyfrują niewielkie bloki danych (znacznie mniejsze od typowej wiadomości), współcześnie jest to najczęściej 128 bitów (AES), choć do niedawna przeważały 64-bitowe bloki (DES, 3DES, Blowfish (kryptografia), IDEA). Klucze są znacznie mniejsze, mają zwykle od 128 do 256 bitów, przy czym wartości mniejsze od 80 (DES – 56) są uważane za niewystarczające. Typowy szyfr blokowy składa się z kilkunastu dość prostych rund przekształcających blok. Operacje używane w tych szyfrach są zwykle proste, ale pochodzą z "różnych światów", np. używa się dodawania, XOR, przesunięć cyklicznych, różnego typu S-BOXów, mnożenia modulo liczb pierwszych itd. Już kilka rund takich operacji zupełnie zaburza jakikolwiek porządek i jest bardzo trudne do analizowania.



SZYFRY STRUMIENIOWE – def.

Szyfry strumieniowe szyfrują każdy znak tekstu jawnego osobno, generując znak strumienia szyfrującego i przekształcając go na przykład z użyciem funkcji XOR go ze znakiem danych, w związku z czym nie jest konieczne oczekiwanie na cały blok danych, jak w przypadku szyfrów blokowych. Najpopularniejszym współczesnym szyfrem strumieniowym jest RC4, którego stosowanie jest ograniczone ze względu na warunki licencyjne. Inne popularne szyfry strumieniowe to A5/1 i A5/2 stosowane w telefonii komórkowej. Do szyfrów strumieniowych należą też historyczne szyfry polialfabetyczne i monoalfabetyczne.



Bezpieczeństwo klucza publicznego

Bezpieczeństwo kryptosystemów klucza publicznego oparte jest na aktualnej wiedzy teoretycznej i możliwościach technologicznych dotyczących rozwiązania danego problemu obliczeniowego.

Rodzaje ataków na systemy kryptograficzne:

- **Aatak bierny**
- **Aatak czynny**

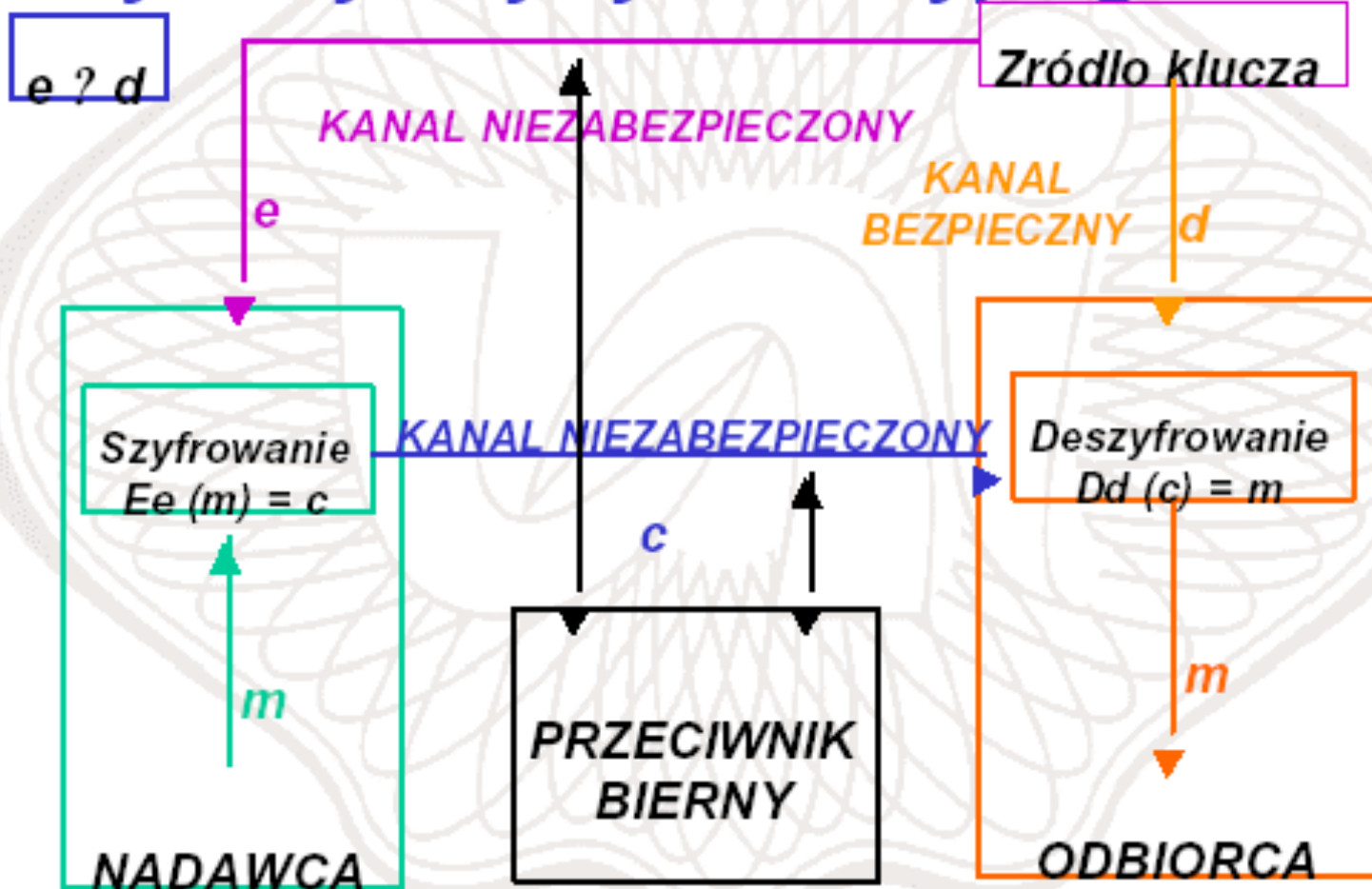


Atak bierny

Przeciwnik nie będący stroną w protokole podsłuchuje wiadomości przekazywane w czasie realizacji protokołu i na tej podstawie próbuje wydobyć informacje jawne. Odpowiada to łamaniu szyfru ze znanym tylko szyfrogramem.

Bierni oszuści realizują protokół, ale jednocześnie próbują wydobyć z niego więcej wiadomości niż potrzebują do swego działania.

Asymetryczny system kryptograficzny



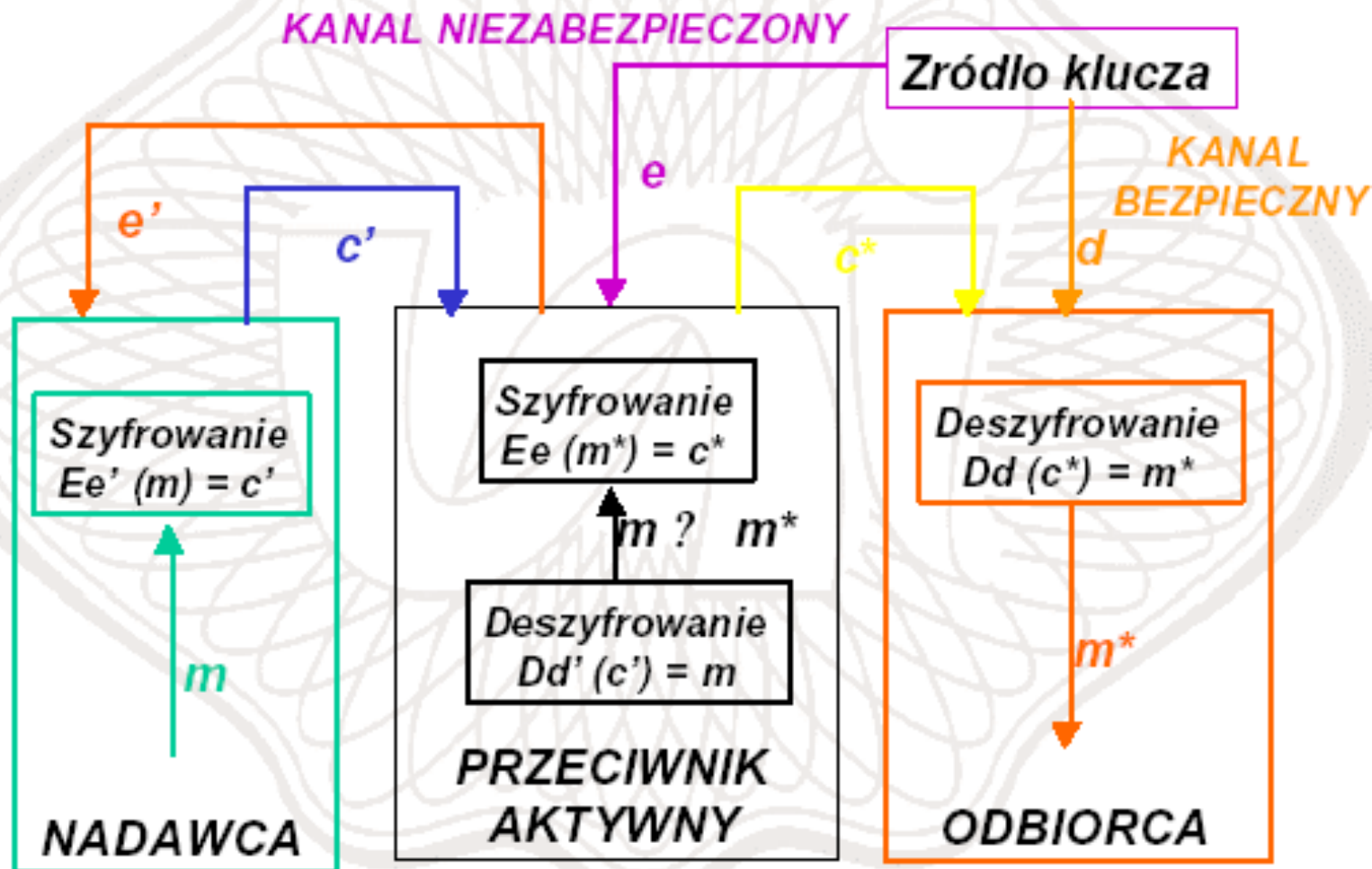


Atak czynny

Przeciwnik w celu uzyskania korzyści stara się wprowadzić do protokołu nowe komunikaty, usunąć istniejące komunikaty, podstawić nowe komunikaty w miejsce istniejących, zniszczyć kanał łączności lub zmienić informacje przechowywane na komputerze.

Łamanie czynne jest bardziej groźne, szczególnie w protokołach, w których odmienne strony niekoniecznie sobie ufają. Napastnik może być legalnym użytkownikiem systemu, może być nawet jedną ze stron³¹ uczestniczących w protokole.

Asymetryczny system kryptograficzny “Impersonation attack”





Kryptografia symetryczna - zalety

- duże prędkości przetwarzania danych
- względnie krótkie klucze szyfrujące
- szeroki zakres zastosowań przy konstrukcji różnorodnych mechanizmów kryptograficznych (generatory binarnych ciągów pseudolosowych, funkcje skrótu, itp.)
- możliwość “składania” silnych przekształceń szyfrujących ze słabych algorytmów symetrycznych



Kryptografia symetryczna - wady

- ***konieczność utrzymywania w sekrecie klucza wspólnego dla obu komunikujących się stron***
- ***w systemach o dużej liczbie uczestników konieczność zarządzania wieloma parami kluczy - w konsekwencji konieczność zaangażowania do tego celu bezwarunkowo zaufanej trzeciej strony, która powinna świadczyć swoje usługi w sposób ciągły, tzn. w trybie “on-line”***
- ***praktyka wskazuje na konieczność częstej zmiany kluczy, nawet przy każdej nowej sesji komunikacyjnej***



Inne algorytmy klucza publicznego

- Algorytm Diffiego-Hellmana
- Algorytm Plecakowy
- Algorytm Rabina
- Algorytm Williamsa
- Algorytm ElGamala
- Probablistyczny Algorytm Bluma-Goldwassera



Kryptografia asymetryczna - zalety

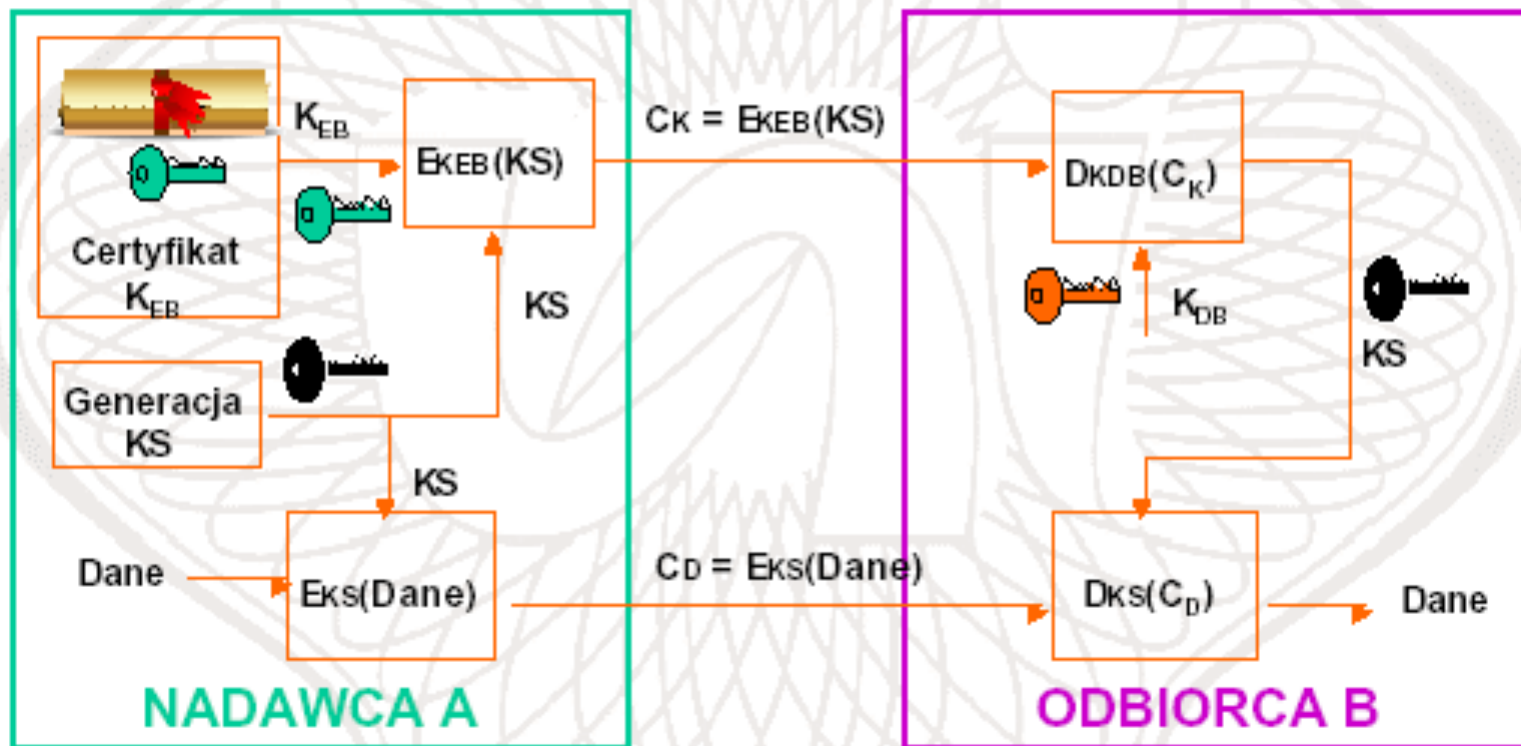
- *w sekrecie musi być utrzymywany tylko klucz prywatny, co nie zmienia faktu, że musi być zagwarantowana autentyczność klucza publicznego*
- *zarządzanie kluczami wymaga istnienia tylko funkcjonalnie zaufanej trzeciej strony, może ona świadczyć swoje usługi w trybie “off-line”*
- *w zależności od trybu zastosowania pary kluczy mogą pozostawać ważne (bez konieczności zmiany) przez dłuższe okresy czasu (wiele sesji komunikacyjnych)*
- *w systemach o dużej liczbie uczestników liczba kluczy o wiele mniejsza, niż w przypadku systemu z kryptografia symetryczna*



Kryptografia asymetryczna - wady

- *prędkość przetwarzania danych w większości stosowanych systemów kryptografii asymetrycznej jest o rzędy wielkości mniejsza od najlepszych znanych systemów kryptografii symetrycznej*
- *długości kluczy o wiele większe niż w systemach kryptografii symetrycznej*
- *w stosunku do żadnego z systemów asymetrycznych formalnie nie udowodniono bezpieczeństwa (ich konstrukcja jest oparta na niewielkiej liczbie problemów obliczeniowych, o których przypuszcza się, że są trudne)*

Bezpieczne przekazanie klucza sesyjnego (symetrycznego)





Funkcje skrótu

Jednokierunkowe funkcje skrótu

wykorzystywane do zapewniania integralności przesyłanych danych, pozwalają stwierdzić, czy informacja przesyłana od nadawcy do odbiorcy nie została poddana modyfikacji. Załoženiami działania takiej funkcji skrótu są:

- uzyskiwany wynik jest stałej długości (niezależnie od długości tekstu, który poddawany jest operacji),
- funkcja działa jednokierunkowo – tzn. nie ma możliwości uzyskania tekstu źródłowego z posiadanego wyniku operacji.

Funkcje skrótu - właściwości

"Dobra" funkcja skrótu musi być pseudolosowa, tzn. dowolna wartość funkcji skrótu powinna być jednakowo prawdopodobna, zaś zmiana jednego bitu argumentu funkcji skrótu („skracanej” wiadomości) powinna powodować zmianę około połowy bitów wartości funkcji dla tego nowego argumentu

Kolizja - dwie różne wiadomości x_1 i x_2 są w kolizji wtedy, gdy $h(x_1) = h(x_2)$

Funkcje skrótu odporne na kolizje - obliczeniowo trudne jest wyznaczenie takiej pary różnych wiadomości x_1 i x_2 , by były one w kolizji

Funkcja jednokierunkowa

Obliczanie wartosci funkcji: $y = F(x)$



Odtwarzanie argumentu na podstawie wartosci funkcji: $x = F^{-1}(y)$



Kryptograficzne funkcje skrótu

Funkcja skrótu (hash function) - efektywna obliczeniowo funkcja jednokierunkowa odwzorowująca ciągi binarne o dowolnej długości na ciągi binarne o ustalonej długości

Funkcja skrótu bez klucza: $h = f(x)$



Funkcja skrótu z kluczem (kryptograficzna funkcja kontrolna): $h = f(x, k)$





Własności protokołów kryptograficznych

- Każdy użytkownik protokołu musi go znać i kolejno wykonywać wszystkie kroki
- Każdy użytkownik musi zgodzić się na jego stosowanie
- Protokół nie może być mylący – każdy krok powinien być dobrze zdefiniowany i nie może wystąpić szansa na jakiegokolwiek nieporozumienie
- Protokół powinien być kompletny – dla każdej możliwej sytuacji musi być podany odpowiedni sposób postępowania.



Cele stosowania protokołów kryptograficznych

Strony uczestniczące w protokole:

- Dzielą się częścią swoich tajemnic
- Wspólnie generują liczbę losową (klucz kryptograficzny)
- Przekonują się wzajemnie do swojej tożsamości
- Podpisują jednocześnie umowę

Stosowanie protokołów kryptograficznych umożliwia współpracę całkowicie nie ufających sobie stron w obrębie sieci komputerowej.



Podpis cyfrowy

Technicznie **podpis cyfrowy** jest ciągiem bitów (krótszym od przesyłanej informacji) będącym funkcją podpisywanej informacji oraz klucza prywatnego nadawcy. W odróżnieniu od podpisu ręcznego zależy od zawartości dokumentu, a dokładniej - od skompensowanej próbki dokumentu.

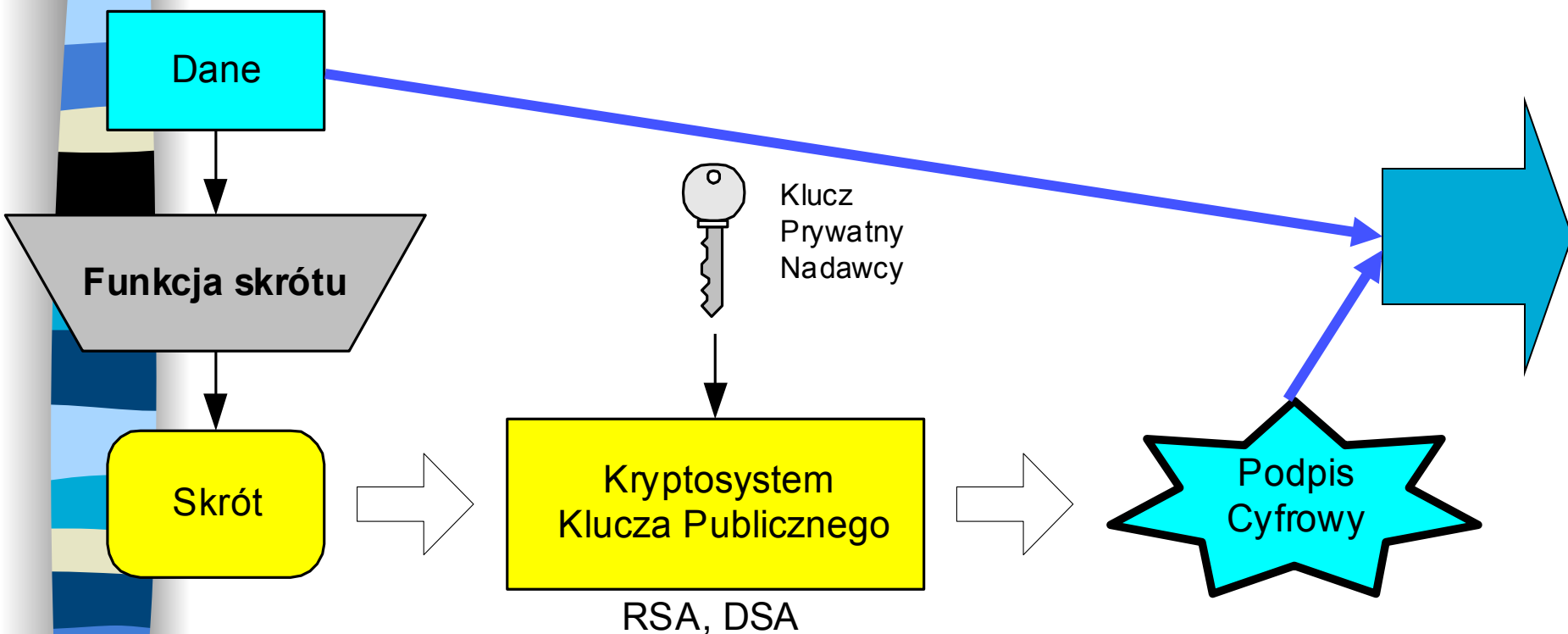
Odwzorowanie informacji z dokumentu na jej skompensowaną próbkę dokonuje się za pomocą jednokierunkowej funkcji szyfrującej, tzw. funkcji skrótu, inaczej haszującej (*hash*).



Algorytm generowania i weryfikacji podpisu cyfrowego

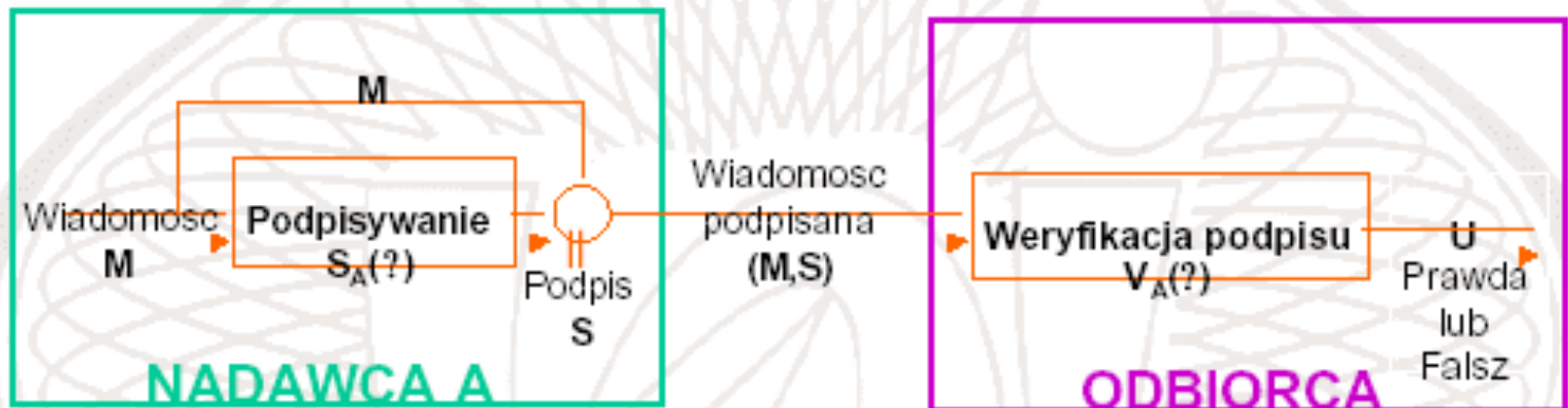
1. **Nadawca** *oblicza* skrót wiadomości za pomocą funkcji skrótu.
2. *Szyfruje* kluczem prywatnym nadawcy skrót wiadomości i *dołącza* do wiadomości jako jej podpis cyfrowy.
3. **Odbiorca** *deszyfruje* kluczem publicznym nadawcy jego podpis cyfrowy oraz *wylicza* z niego skrót przesłanej wiadomości.
4. *Porównuje* ze skrótem uzyskanym po zaszyfrowaniu funkcją skrótu otrzymanej wiadomości.
5. **Zgodność** oznacza, że podpis cyfrowy dotyczy przesłanej wiadomości oraz świadczy o nienaruszalności informacji.

Wykonywanie podpisu cyfrowego



Podpis cyfrowy z załącznikiem

zasada działania



$S = S_A(M) =$ podpis nadawcy A na wiadomości M

$U = V_A(M, S) =$ prawda lub fałsz

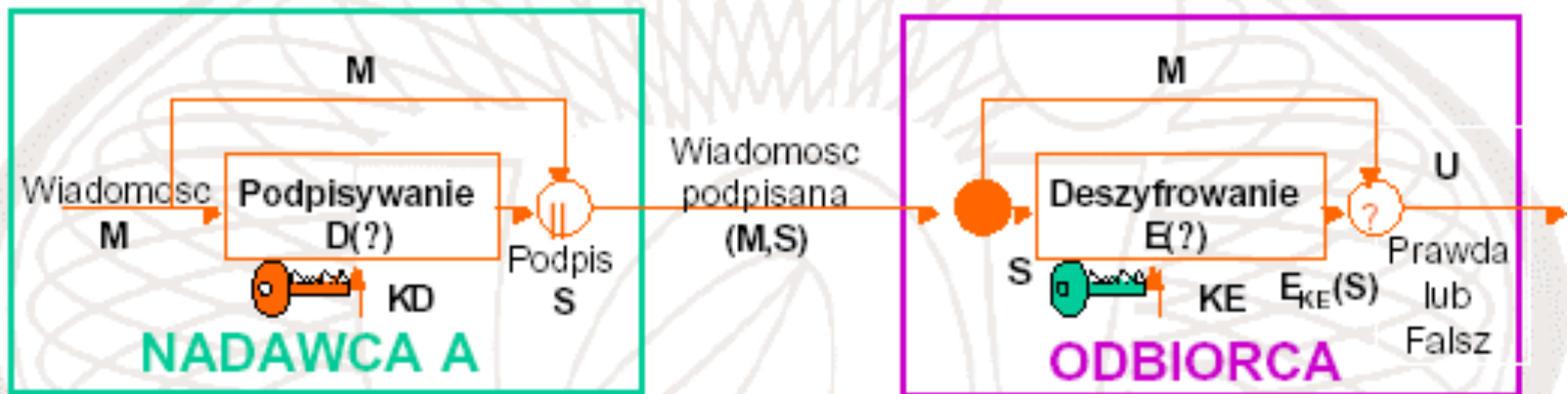
S_A – funkcja podpisująca (tajna)

V_A – funkcja weryfikująca (publicznie dostępna)

Dla dowolnej wiadomości M' wyznaczenie przez podmiot inny niż A takiej wartości S' , że $V_A(M', S') =$ prawda jest obliczeniowo niewykonalne

Podpis cyfrowy z zalacznikiem

wykorzystanie kryptografii asymetrycznej



Odwracalne przekształcenie kryptografii asymetrycznej

$$D_{KD}(E_{KE}(M)) = E_{KE}(D_{KD}(M)) = M$$

KD – klucz prywatny

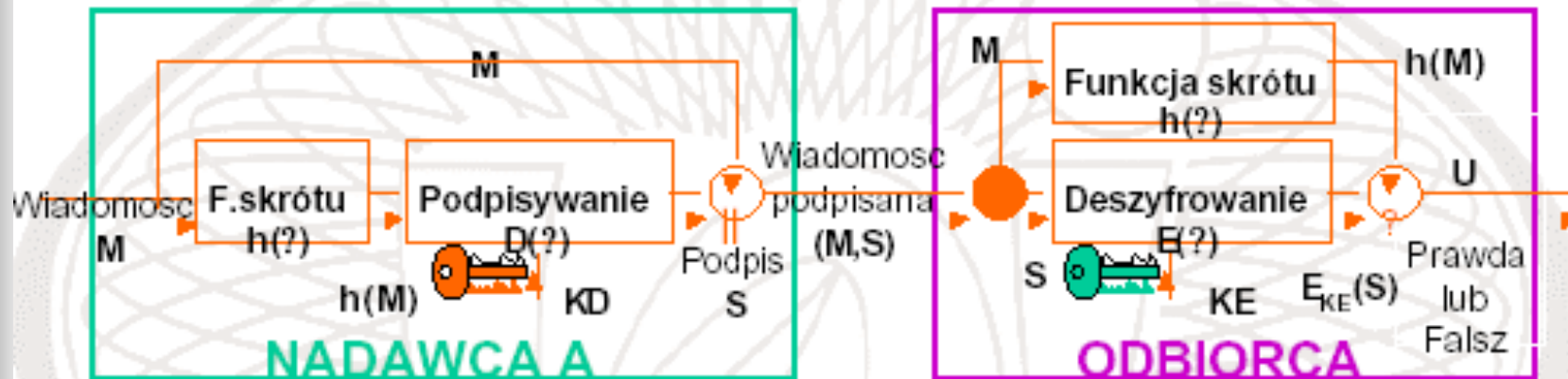
KE – klucz publiczny

$$S = S_A(M) = D_{KD}(M)$$

$$U = V_A(M, S) = \begin{cases} \text{prawda, gdy } E_{KE}(S) = M \\ \text{falsz, gdy } E_{KE}(S) \neq M \end{cases}$$

Podpis cyfrowy z zalacznikiem

zastosowanie funkcji skrótu



$$S = S_A(h(M)) = D_{KD}(h(M))$$

$$U = V_A(M, S) = \begin{cases} \text{prawda, gdy } E_{KE}(S) = h(M) \\ \text{fałsz, gdy } E_{KE}(S) \neq h(M) \end{cases}$$



Cechy podpisu elektronicznego

Podpis elektroniczny ma wszystkie istotne cechy podpisu odręcznego: potwierdza jednoznacznie tożsamość osoby podpisującej, uniemożliwia zaprzeczenie faktu podpisania i dokonania transakcji, jest też powiązany z treścią, która została podpisana. Dodatkową zaletą stosowania podpisu elektronicznego jest możliwość stwierdzenia na podstawie samego podpisu, czy dokument nie był zmieniany już po podpisaniu. Dzięki temu może być wykorzystywany do jednoznacznej autoryzacji wszelkich dokumentów i transakcji elektronicznych.



Certyfikacja podpisu cyfrowego

Łatwo wyobrazić sobie scenariusz, w którym intruz podmienia klucz publiczny określonego użytkownika, a następnie przechwytuje i swobodnie deszyfruje wiadomości kierowane do tego użytkownika.

Skutecznym i efektywnym rozwiązaniem tego problemu są tzw. **urzędy certyfikacji** (*ang. certificate authority*) odpowiadające za dystrybucję kluczy publicznych użytkowników.

Użytkownik, aplikacja lub urządzenie, które zamierza prowadzić szyfrowanie w systemie klucza publicznego najpierw powinni zarejestrować się w urzędzie certyfikacji oraz dostarczyć swoje klucze publiczne wraz z danymi identyfikacyjnymi.

Certyfikat

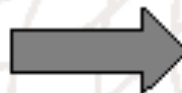
Klucz prywatny



Klucz publiczny



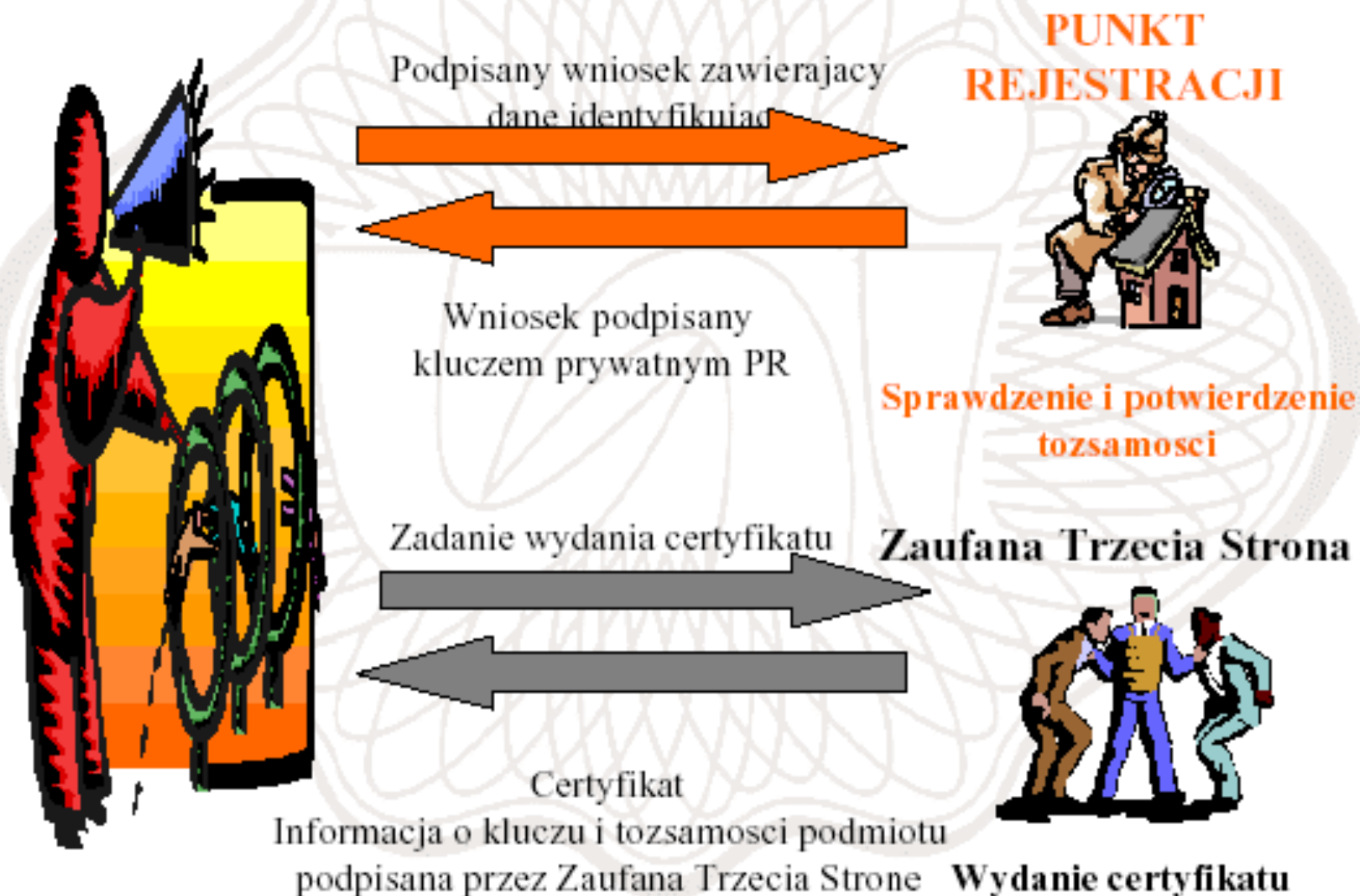
Zaufana Trzecia Strona



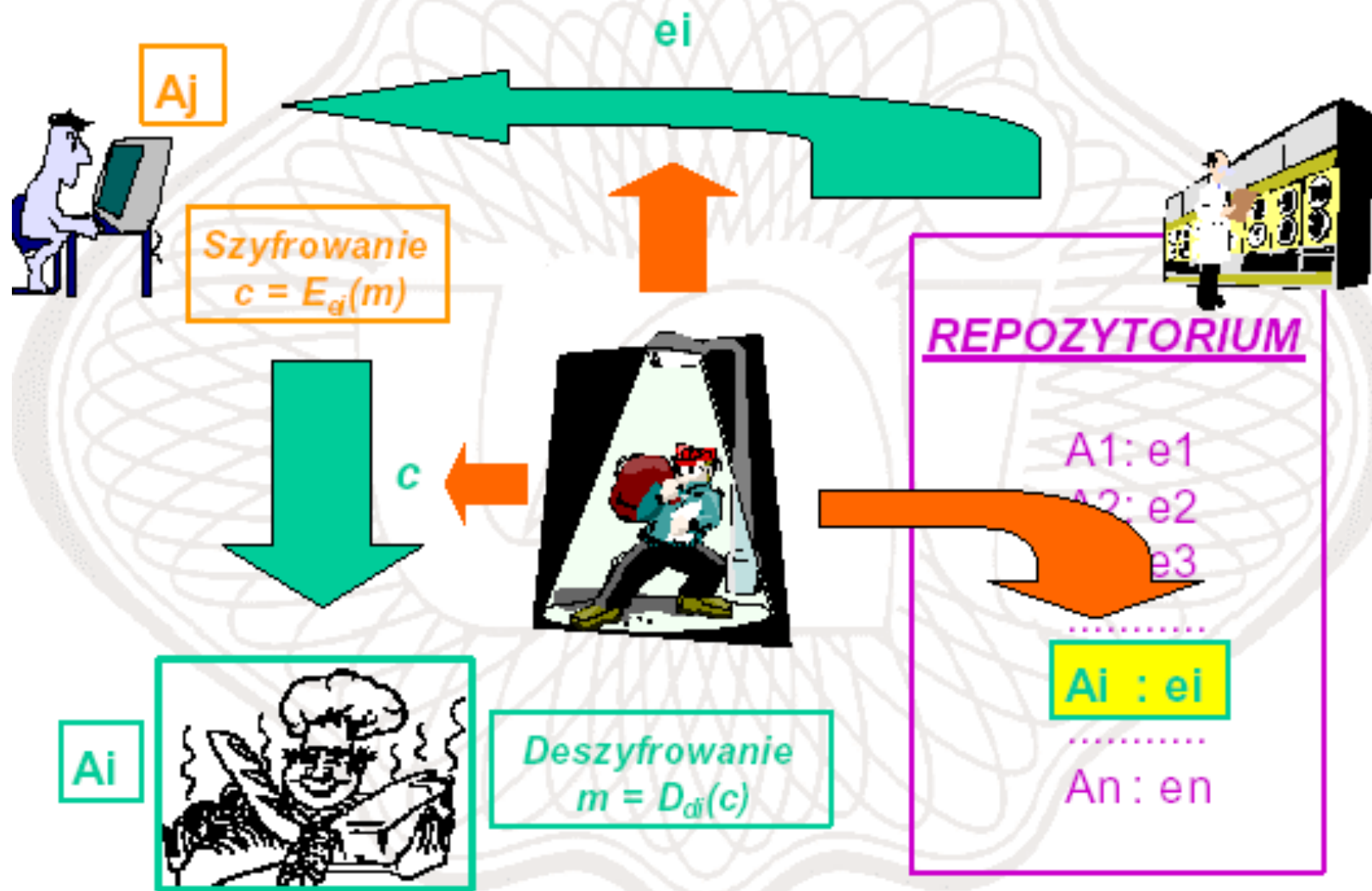
Certyfikat
klucza publicznego



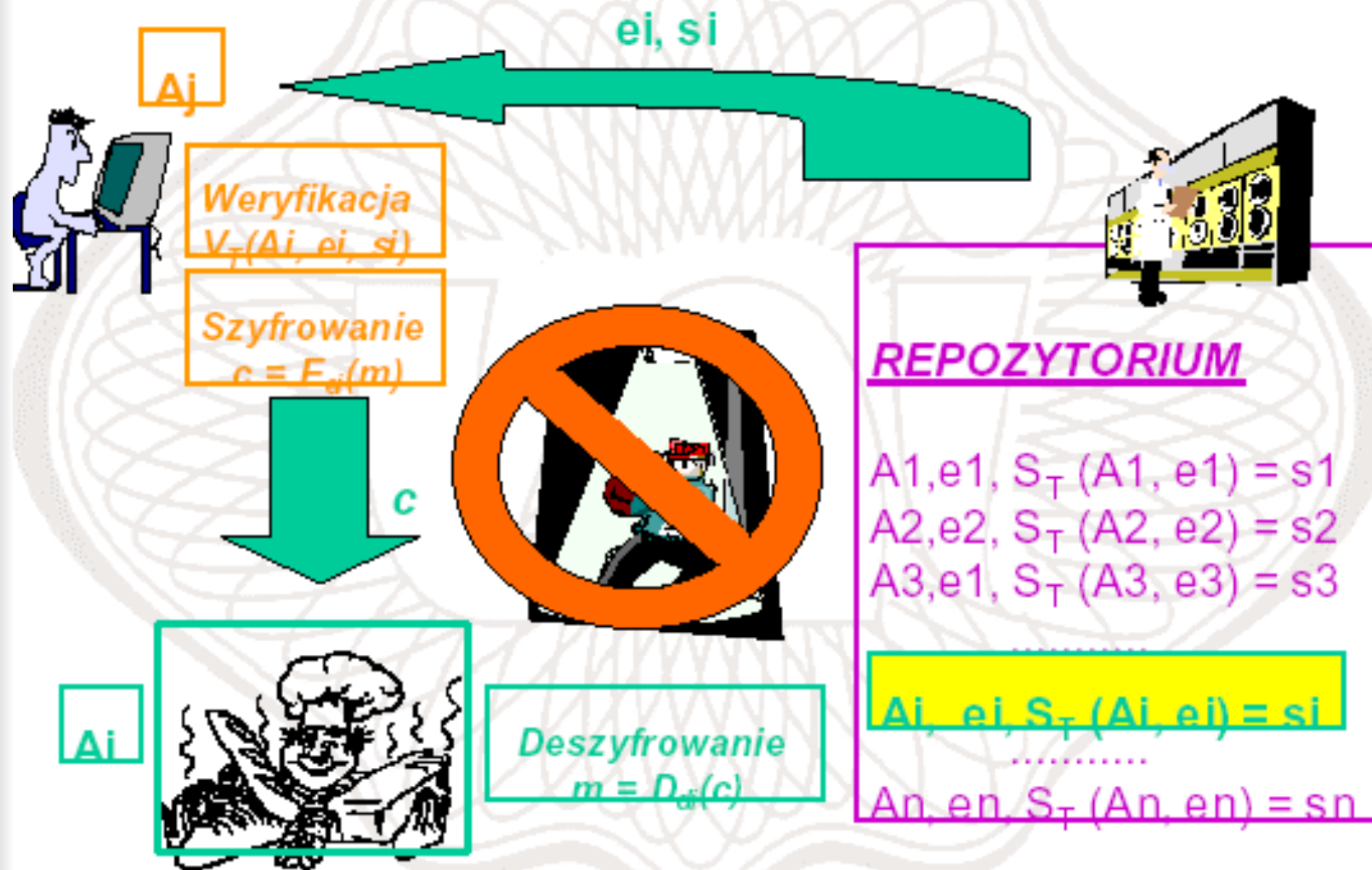
Uzyskanie certyfikatu



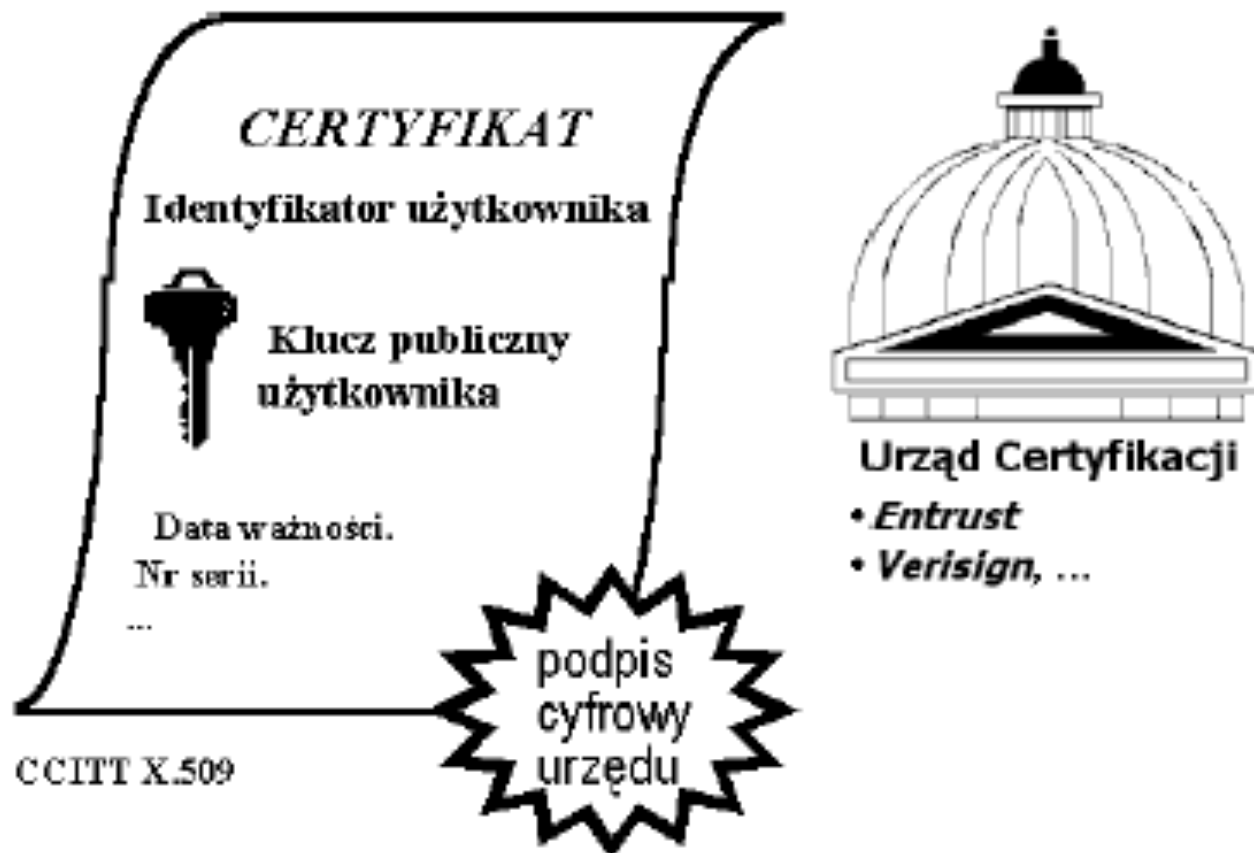
“Poufna wymiana danych”



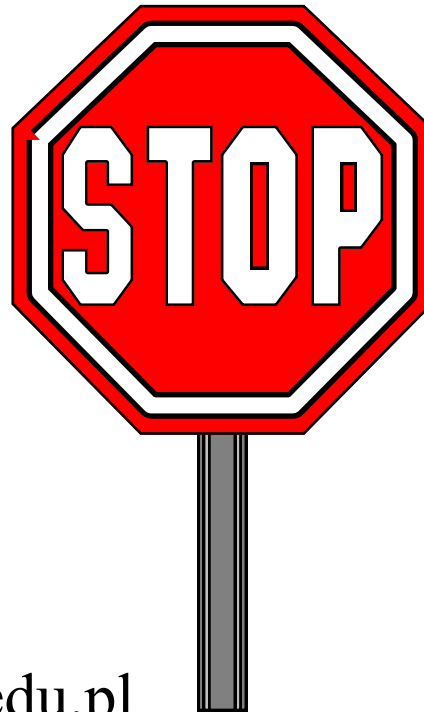
Certyfikaty klucza publicznego



Elementy certyfikatu cyfrowego



Dziękuję za uwagę



jczerniak@ukw.edu.pl