WSIZ Copernicus we Wrocławiu

Bezpieczeństwo sieci komputerowych

Wykład 4.

Robert Wójcik

Wyższa Szkoła Informatyki i Zarządzania
„Copernicus” we Wrocławiu

Plan wykładu

Sylabus - punkty:

4. **Usługi ochrony**: poufność, integralność, dostępność, uwierzytelnianie, kontrola dostępu (autoryzacja), niezaprzeczalność.
5. **Mechanizmy kryptograficzne** wykorzystywane do realizacji usług ochrony: kryptografia symetryczna, kryptografia asymetryczna, funkcje haszujące, podpis cyfrowy, certyfikaty kluczy kryptograficznych.
6. **Zastosowanie kryptografii symetrycznej i asymetrycznej** do realizacji poufności, autentyczności oraz uwierzytelnienia podmiotów i dokumentów.
7. **Struktura certyfikatu klucza publicznego** definiowana w oparciu o standard X.509. Zasada działania hierarchicznego systemu certyfikatów oparta o centra certyfikacji (CA) – infrastruktura klucza publicznego PKI.

Usługi ochrony informacji

Systemy bezpieczeństwa sieci komputerowych powinny zapewniać:

- bezpieczeństwo informacji składowanych w węzłach sieci oraz przesyłanych w sieci;

- bezpieczny dostęp do systemu - zasobów i usług, dla uprawnionych podmiotów (osoby, komputery);

- nieprzerwany dostęp do zasobów i usług sieciowych.

Usługi ochrony informacji

Podstawowe usługi ochrony realizowane w sieciach komputerowych:

- **poufność danych** oraz ich transmisji (confidentiality): zabezpieczanie przed podsłuchem lub nielegalnym odczytem; informacje składowane lub przesyłane mogą być odczytane tylko przez podmioty uprawnione (zapewnienie prywatności danych, np. poprzez ich szyfrowanie);

- **integralność danych** (integrity): zagwarantowanie nienaruszalności (autentyczności) danych, informacji przesyłanych; tylko podmioty uprawnione mogą dokonywać modyfikacji danych; powinna istnieć możliwość wykrycia zdarzeń polegających na celowym lub przypadkowym naruszeniu integralności przesyłanych wiadomości (np. poprzez zastosowanie funkcji haszujących do wyznaczenia sumy kontrolnej);

- **dostępność danych i usług** (availability): zapewnienie uprawnionym użytkownikom możliwości korzystania z danych i usług w każdej chwili; zabezpieczenie przed zakłóceniami działania usług i dostępu do danych (np. poprzez serwery rezerwowe, archiwizację danych).

Usługi ochrony informacji

Inne usługi zapewniania bezpieczeństwa informacji:

- **uwierzytelnianie użytkowników** (user authentication): oznacza możliwość weryfikacji tożsamości użytkownika, który podał identyfikator (nazwę: user login) w oparciu o podane hasło lub inny mechanizm potwierdzania tożsamości (np. token, certyfikat). lub zabezpieczanie przed podsłuchem lub nielegalnym odczytem; informacje składowane lub przesyłane mogą być odczytane tylko przez podmioty uprawnione (zapewnienie prywatności danych, np. poprzez ich szyfrowanie);

- **uwierzytelnianie wiadomości** (message authentication): oznacza możliwość potwierdzenia autentyczności źródła pochodzenia komunikatu (dokumentu), tj. weryfikacji, czy wiadomość została utworzona przez dany podmiot, czy też nie (np. w oparciu o dołączony podpis cyfrowy);

- **niezaprzeczalność przesłania komunikatu** (nonrepudiation): sprowadza się do uniemożliwienia zarówno nadawcy jak i odbiorcy komunikatu zaprzeczenia faktowi jego przesłania;

Usługi ochrony informacji

- **kontrola dostępu, autoryzacja** (access control, authorization): ma na celu zapewnienie, aby dostęp do zasobów i usług sieciowych był kontrolowany (autoryzowany) przez system w sposób automatyczny zgodnie z obowiązującymi uprawnieniami użytkowników (np. zastosowanie ról i uprawnień użytkowników, list kontroli dostępu).

Do realizacji wymienionych usług ochrony informacji mogą być wykorzystywane różne mechanizmy kryptograficzne:

- kryptografia symetryczna (z kluczem tajnym),

- kryptografia asymetryczna (z kluczem publicznym),

- funkcje haszujące (generowanie haszu wiadomości - „odcisk palca”),

- podpis cyfrowy wiadomości,

- certyfikaty kluczy publicznych.

Mechanizmy kryptograficzne

Kryptografia: dziedzina wiedzy zajmująca się szyfrowaniem, czyli metodami utajniania treści wiadomości.

W wyniku szyfrowania (encryption) tekst jawny (plaintext), nazywany też tekstem otwartym (cleartext), zostaje przekształcony w tekst zaszyfrowany zwany kryptogramem lub szyfrogramem (ciphertext).

Proces odtwarzania treści kryptogramu nazywamy deszyfrowaniem (decryption).

Mechanizmy kryptograficzne

Algorytm kryptograficzny (szyfr) - funkcja matematyczna służąca do szyfrowania i deszyfrowania wiadomości.

Szyfrowanie tekstu jawnego - algorytm szyfrujący (encryption algorithm).

Deszyfrowanie kryptogramów - algorytm deszyfrujący (decryption algorithm).

Szyfrowanie i deszyfrowanie - z udziałem **kluczy kryptograficznych**.

Klucze przyjmują wiele wartości z określonego zbioru - **przestrzeń klucza**.

Na ogół algorytmy kryptograficzne nie są tajne. Tajność operacji szyfrowania zapewnia się poprzez tajne klucze kryptograficzne.

System kryptograficzny:
- algorytm kryptograficzny,
- klucze kryptograficzne,
- metoda implementacji (sprzęt i oprogramowanie).

Mechanizmy kryptograficzne

Systemy kryptograficzne z kluczem tajnym (secret-key systems):

- *ten sam klucz* służy do szyfrowania i deszyfrowania informacji; systemy takie nazywane są *systemami symetrycznymi*, a stosowane w nich algorytmy *algorytmami symetrycznymi* (przykłady algorytmów symetrycznych: DES, 3DES, IDEA, AES, Blowfish, RC4).

Systemy kryptograficzne z kluczem jawnym lub publicznym (public-key systems):

- używają *dwóch oddzielnych kluczy* do szyfrowania i deszyfrowania; system taki nosi nazwę *systemu asymetrycznego*, a stosowane w nich algorytmy *algorytmami asymetrycznymi* (przykłady algorytmów asymetrycznych: RSA, ElGamala, DSA – Digital Signature Algorithm);

- klucz szyfrujący - *klucz jawny*, nazywany kluczem publicznym (public key);

- klucz deszyfrujący - *klucz tajny*, nazywany kluczem prywatnym (private key).

Mechanizmy kryptograficzne

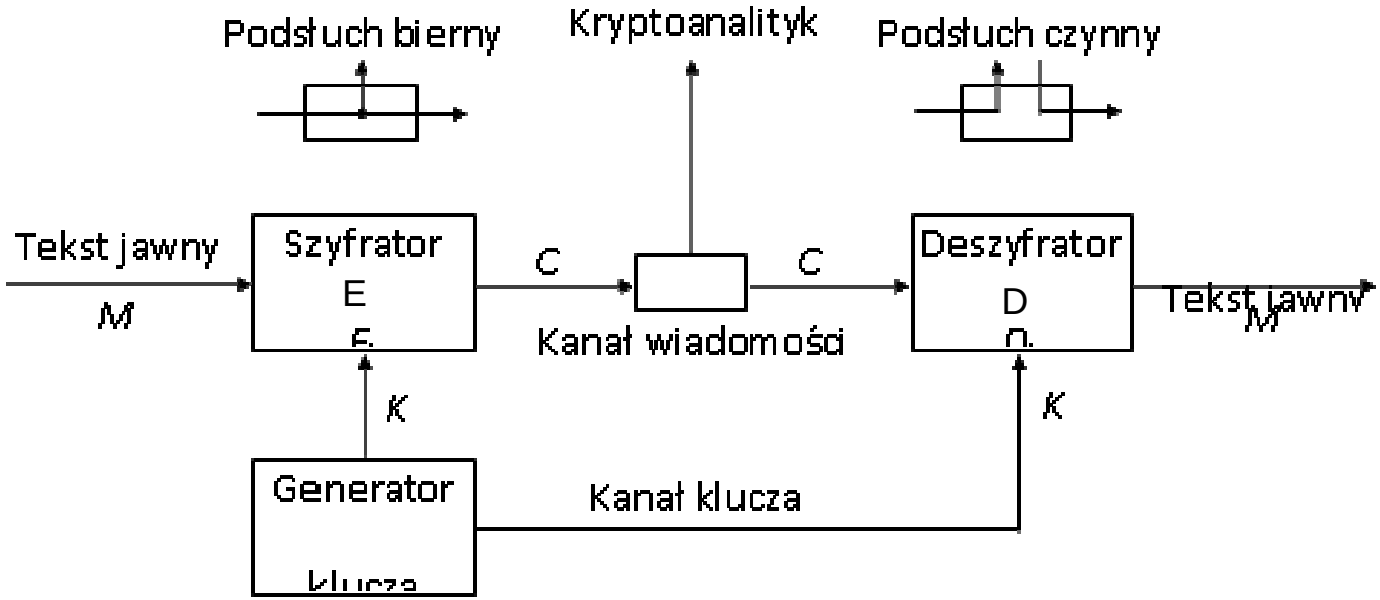
Elementy systemu kryptografii symetrycznej

Algorytmy i klucze kryptograficzne:
- wiadomość jawna *M*,
- wiadomość zaszyfrowana (kryptogram) *C*,
- klucz *K* (klucz wykorzystywany do szyfrowania i deszyfrowania wiadomości); *przesyłany kanałem tajnym*,
- algorytm szyfrowania *E*,
- algorytm deszyfrowania *D*.

Elementy sprzętowe:
- szyfrator - realizuje algorytm szyfrowania *E*; generuje kryptogram C z wiadomości *M*, z udziałem klucza kryptograficznego *K;*
- deszyfrator – realizuje algorytm deszyfrowania *D*; odtwarza wiadomość jawną *M* z kryptogramu *C*, z udziałem tego samego klucza *K*;
- generator klucza: generuje klucze kryptograficzne.

Mechanizmy kryptograficzne

Schemat blokowy systemu symetrycznego



[1] Mochnacki W., Kody korekcyjne i kryptografia, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław, 2000.

Mechanizmy kryptograficzne

Zastosowania kryptografii symetrycznej

• Szyfrowanie wiadomości i danych: **$C = E_K(M)$**
(dane na dyskach, wiadomości przesyłane w kanałach komunikacyjnych)

• Deszyfrowanie wiadomości: **$M = D_K(C)$**

Z definicji: $M = D_K(C) = D_K(E_K(M))$ – szyfrowanie jest przekształceniem odwracalnym. Jednak **bez znajomości klucza tajnego K** odwrócenie przekształcenia jest niemożliwe w rozsądnym czasie.

• Szyfrowanie kluczem tajnym zabezpiecza wiadomości przed modyfikacjami (zapewnia integralność, autentyczność informacji).

• Szyfrowanie można traktować jak rodzaj kodowania: umożliwia wykrywanie błędów transmisji danych, gdyż przypadkowe modyfikacje kryptogramu uniemożliwią odszyfrowanie informacji.

Mechanizmy kryptograficzne

Zastosowania kryptografii symetrycznej

• Uwierzytelnianie wiadomości: zaszyfrowanie wiadomości kluczem tajnym (prywatnym) jednoznacznie identyfikuje jej nadawcę (rodzaj podpisu).

• Uwierzytelnianie podmiotów: aby sprawdzić, czy dany podmiot jest tym za kogo się podaje należy zrealizować procedurę sprawdzającą, która polega na wysłaniu do podmiotu losowej liczby x, zaszyfrowanej algorytmem kryptografii symetrycznej oraz posiadanym kluczem tajnym K; badany podmiot jest tym za kogo się podaje, jeśli odeśle zaszyfrowaną wartość (x-1).

Wniosek:

W przypadku kryptografii symetrycznej poufność oraz integralność przesyłanych informacji jest zagwarantowana poprzez ich szyfrowanie oraz zapewnienie tajności klucza prywatnego.

Mechanizmy kryptograficzne

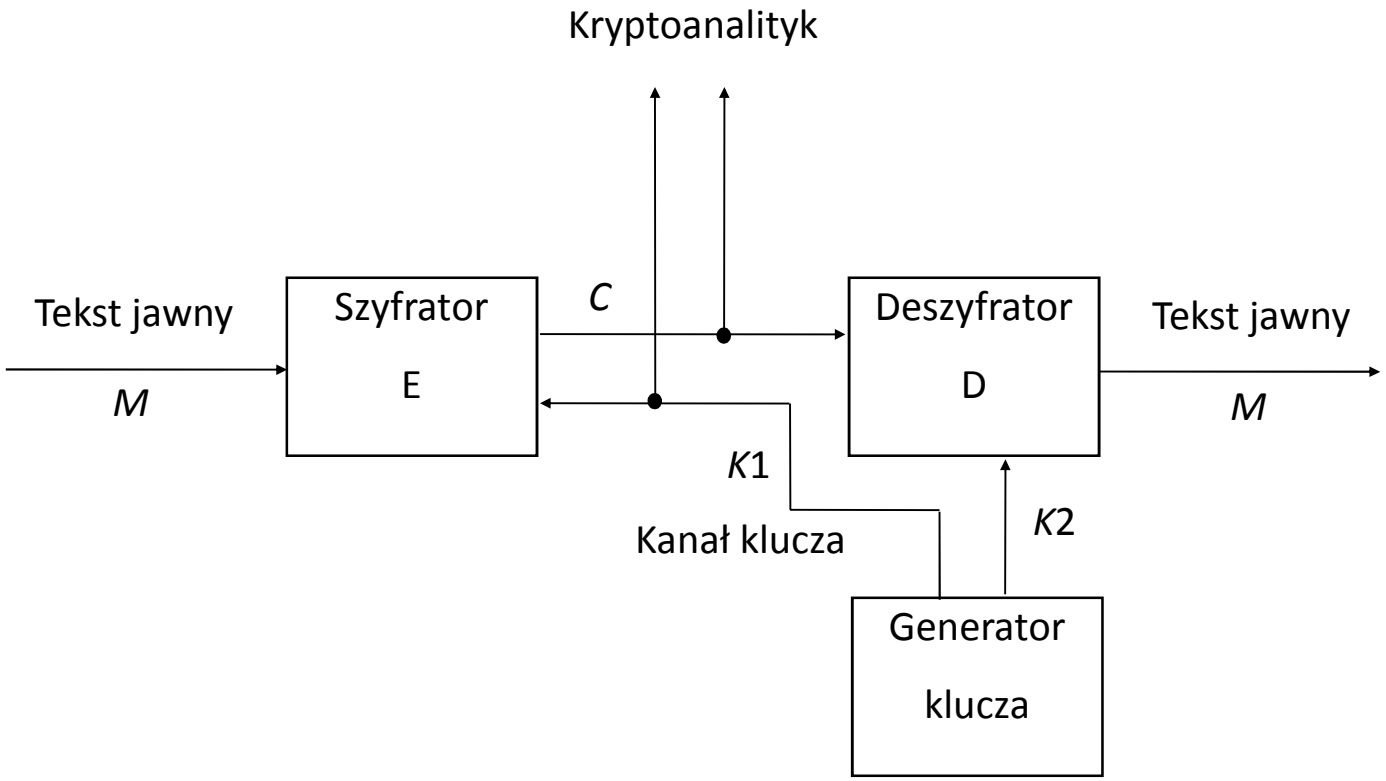
Elementy systemu kryptografii asymetrycznej

Algorytmy i klucze kryptograficzne:
- wiadomość jawna *M*,
- wiadomość zaszyfrowana (kryptogram) *C*,
- klucz ***K1*** (**klucz jawny**, publiczny wykorzystywany do szyfrowania wiadomości); *przesyłany kanałem otwartym*;
- klucz ***K2*** (**klucz tajny**, prywatny wykorzystywany do deszyfrowania wiadomości); *przesyłany kanałem tajnym*;
- algorytm szyfrowania *E*,
- algorytm deszyfrowania *D*.

Elementy sprzętowe:
- szyfrator - realizuje algorytm szyfrowania *E*; generuje kryptogram C z wiadomości *M*, z udziałem klucza publicznego (jawnego) *K1;*
- deszyfrator – realizuje algorytm deszyfrowania *D*; odtwarza wiadomość jawną *M* z kryptogramu *C*, z udziałem klucza prywatnego (tajnego) *K2*;
- generator klucza: generuje klucze kryptograficzne.

Mechanizmy kryptograficzne

Schemat blokowy systemu asymetrycznego



Mechanizmy kryptograficzne

Zastosowania kryptografii asymetrycznej

• Szyfrowanie wiadomości i danych **kluczem publicznym K1**: **$C = E_{K1}(M)$**
(na ogół krótkie wiadomości ze względu na niską wydajność algorytmów kryptografii asymetrycznej oraz podatność na złamanie przy dużej liczbie danych).

• Deszyfrowanie wiadomości kluczem prywatnym: **$M = D_{K2}(C)$**

Z definicji: $M = D_{K2}(C) = D_{K2}(E_{K1}(M))$ – szyfrowanie jest przekształceniem odwracalnym. Jednak **bez znajomości klucza tajnego K2** odwrócenie przekształcenia jest niemożliwe w rozsądnym czasie.

• Szyfrowanie kluczem tajnym K2 zabezpiecza wiadomości przed modyfikacjami (zapewnia integralność, autentyczność informacji);

Mechanizmy kryptograficzne

Zastosowania kryptografii asymetrycznej

• Uwierzytelnianie wiadomości: zaszyfrowanie wiadomości kluczem tajnym K2 jednoznacznie identyfikuje jej nadawcę (rodzaj podpisu).

$P = D_{K2}(M);$ podpis realizowany poprzez szyfrowanie całej wiadomości (w praktyce zastąpione podpisem cyfrowym, tj. szyfrowaniem haszu z wiadomości);

$M = E_{K1}(P) = E_{K1}(D_{K2}(M));$ weryfikacja podpisu, źródła pochodzenia wiadomości, np. wysyłamy $(M, D_{K2}(M))$;

• Uwierzytelnianie podmiotów: aby sprawdzić, czy dany podmiot jest tym za kogo się podaje należy zrealizować procedurę sprawdzającą, która polega na wysłaniu do podmiotu losowej liczby x, zaszyfrowanej kluczem publicznym K1 podmiotu; badany podmiot jest tym za kogo się podaje, jeśli odeśle wartość, np. (x-1) lub wartość (x-1) zaszyfrowaną naszym kluczem publicznym.

Mechanizmy kryptograficzne

Zastosowania kryptografii asymetrycznej

Wniosek:

W przypadku kryptografii asymetrycznej, aby zapewnić równocześnie poufność oraz integralność wiadomości przesyłanych od podmiotu A do podmiotu B, należy zastosować złożenie przekształceń szyfrowania i podpisywania z udziałem dwóch par kluczy (jawny, tajny): dla podmiotu A - (K1A, K2A) oraz dla podmiotu B – (K1B, K2B).

Wariant 1:

- podpis wiadomości M, kluczem prywatnym K2A podmiotu A (integralność), następnie szyfrowanie kluczem publicznym K1B podmiotu B (poufność);
  $P = D_{K2A}(M);$ $C = E_{K1B}(P);$ np. system ochrony poczty PGP;

Wariant 2:

- szyfrowanie wiadomości M, kluczem publicznym K1B podmiotu B (poufność), następnie podpis kluczem prywatnym K2A podmiotu A (integralność);
  $C = E_{K1B}(M);$ $P = D_{K2A}(C);$ np. system ochrony poczty PEM;

Mechanizmy kryptograficzne

Weryfikacja:

Wariant 1:

• odszyfrowanie wiadomości za pomocą klucza prywatnego K2B, następnie odczytanie wiadomości M kluczem publicznym K1A podmiotu A;

$$\mathbf{P = D_{K2B}(C);} \quad \mathbf{M = E_{K1A}(P);}$$

Wariant 2:

• odczytanie podpisu za pomocą klucza publicznego K1A, następnie odszyfrowanie wiadomości kluczem prywatnym K2B podmiotu B;

$$\mathbf{C = E_{K1A}(P);} \quad \mathbf{M = D_{K2B}(C);}$$

(szybszy do sprawdzenia; podpis nie pasuje to odrzucamy; mniej bezpieczny niż wariant 1);

Mechanizmy kryptograficzne

Własności systemów kryptografii symetrycznej i asymetrycznej

- kryptografia symetryczna: szybsza w działaniu, bardziej odporna na złamanie; stosowna do szyfrowania strumieniowego oraz blokowego dużych ilości danych;

- kryptografia asymetryczna wolna, podatna na złamanie przy dużej liczbie szyfrowanych danych; stosowna do szyfrowania krótkich zbiorów danych, (np. wiadomości pocztowych, kluczy sesji dla kryptografii symetrycznej, sum kontrolnych (haszy) wiadomości.

Dyskusja ze studentami:

- rozpatrzyć wariant zabezpieczania wiadomości poczty elektronicznej poprzez ich szyfrowanie po stronie nadawcy za pomocą algorytmu kryptografii symetrycznej; tajny klucz sesji algorytmu symetrycznego jest generowany losowo po stronie nadawcy;

Mechanizmy kryptograficzne

Funkcje haszujące

W praktyce zapewnianie integralności informacji oraz uwierzytelnianie źródła ich pochodzenia poprzez szyfrowanie całych wiadomości za pomocą klucza prywatnego (tajnego) nadawcy jest nieefektywne dla dużych zbiorów danych.

W praktyce integralność wiadomości zapewnia się poprzez dodanie do wiadomości M jej haszu h(M) zaszyfrowanego kluczem prywatnym nadawcy, tj. zastosowanie **podpisu cyfrowego**.

Funkcja haszująca h umożliwia wyznaczenie dla danej wiadomości M ciągu bitowego, który stanowi rodzaj odcisku palca i w praktyce jest inny dla każdej wiadomości. Funkcje haszujące są realizowane za pomocą tzw. funkcji jednokierunkowych, które posiadają następujące własności:

- dla każdej wiadomości M łatwo jest obliczyć h(M);
- h(M) ma zawsze stałą długość niezależnie od długości M;
- dla zadanego haszu X znalezienie M takiego, że h(M) = X, jest praktycznie niemożliwe.

Mechanizmy kryptograficzne

Podstawowe funkcje haszujące

Funkcja MD5: hasz128 bitów;

Funkcja SHA-1: hasz 160 bitów.

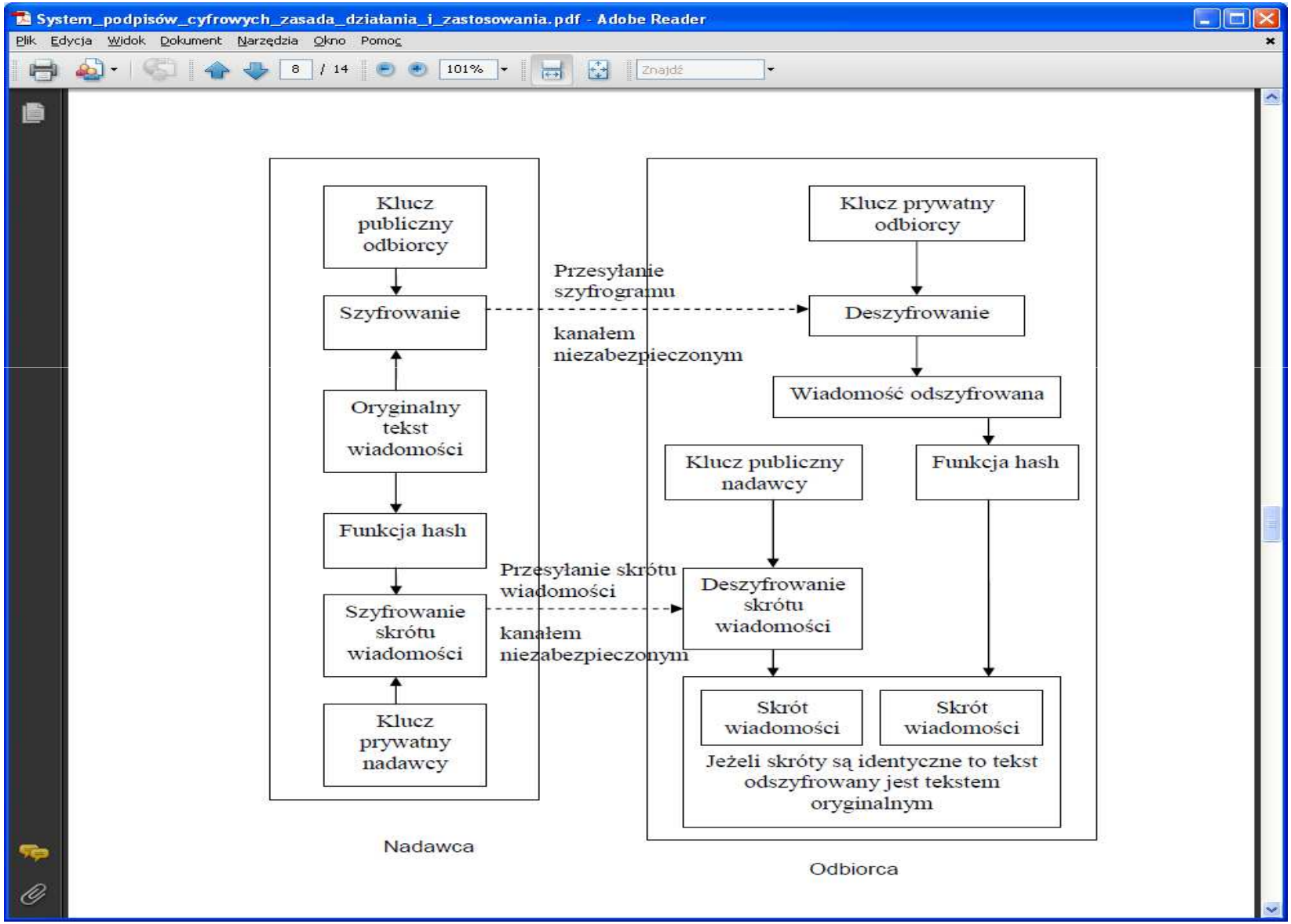
Należy podkreślić, że w przypadku wymienionych funkcji może dochodzić do konfliktów, polegających na tym, że dwie różne wiadomości X i Y dadzą ten sam hasz h(X) = h(Y), ale jest to w praktyce zjawisko rzadkie.

Mechanizmy kryptograficzne

Zastosowania funkcji haszujących

- podpis cyfrowy: hasz z wiadomości zaszyfrowany kluczem prywatnym nadawcy;
- zabezpieczanie umów przed zmianami (pozostawiamy hasz z odpowiednią datą u notariusza lub ogłaszamy na stronie WWW);
- potwierdzenie istnienia dokumentu bez ujawniania jego treści (np. opis technologii, wzoru; dowód, że go posiadamy);
- zabezpieczanie przed modyfikacjami kodu programu przez wirusy (podczas pobierania programów sprawdzana suma kontrolna, np. md5).

Generowanie i weryfikacja podpisu cyfrowego



Dziękuję za uwagę!