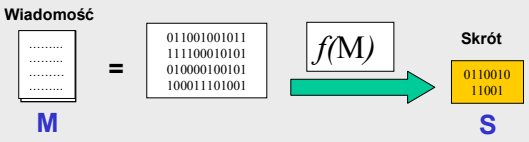
Ochrona integralności i autentyczności danych

Podpisy cyfrowe

Funkcje skrótu

Sformułowanie zagadnienia



= taki zbiór danych, że:

- Mając dane S nie sposób odtworzyć M — Jednokierunkowość
- $\forall_{\mathbf{M}\neq\mathbf{Y}} : f(\mathbf{M}) \neq f(\mathbf{Y})$ — Unikatowość
- Dla dowolnego M, skrót S_M jest podobnie nieuporządkowany jak skrót losowego ciągu U - S_U

Maksymalizacja entropii skrótu

Funkcje skrótu

Idea postępowania - przekształcenie redukujące rozmiar wektora

$$\mathbf{A} = [2 \quad 1 \quad 0 \quad 4] \qquad \mathbf{M} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \\ 2 & -1 \\ 2 & 0 \end{bmatrix} \qquad \mathbf{B} = \mathbf{AM} = [10 \quad 5]$$

A - wiadomość **M - parametry przekształcenia** **B - skrót wiadomości**

Mnożenie macierzy jest zbyt proste - nie spełnia żadnego ze sformułowanych postulatów

Stosowane algorytmy wyznaczania skrótu ...

- **MD5 - 128 bitów (16 bajtów)**
- **SHA-1 - 160 bitów (20 bajtów)**

...są złożone ale nie ma dowodu, że spełniają postawione założenia.

Bezpieczeństwo systemów informatycznych

Funkcje skrótu

Wyznaczanie skrótu

1. **Dopełnienie wiadomości do 512b x n**
   Argument wejściowy procedur SHA-1, MD5 - bloki o długości 512b

Wiadomość

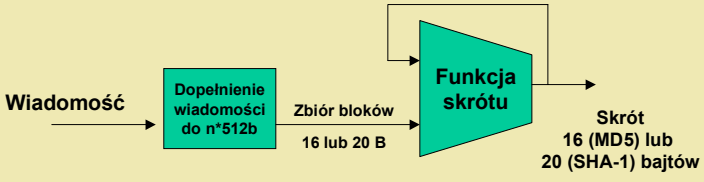
010100001 = 50H →

Dodanie '1', zer i długości wiadomości (64b)

50800000 00000000 00000000 00000000
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000008

2. **Obliczenie skrótu**

Funkcja skrótu - wielokrotne operacje wyznaczania różnic symetrycznych dla 16 (20) bajtowych fragmentów bloku wejściowego, z użyciem specjalnie dobranych stałych

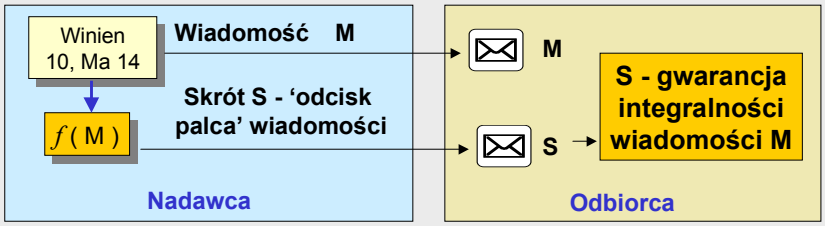


Krzysztof Ślot © 2002

Funkcje skrótu - podsumowanie

Funkcja skrótu - ang. 'hash', 'message digest'

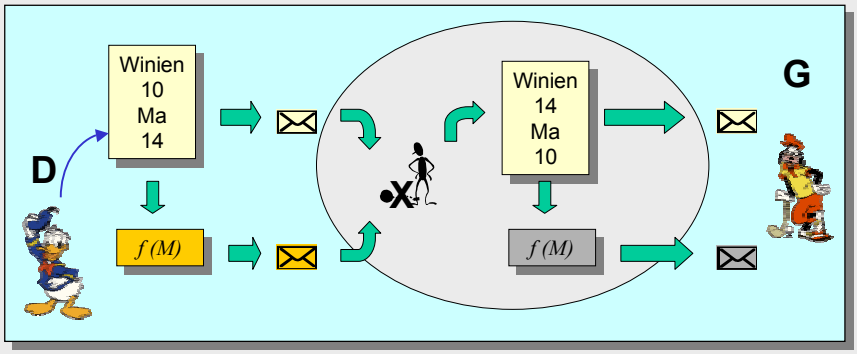
- $f(M)$ - **funkcja jednokierunkowa**
- $M_i \neq M_j \Rightarrow f(M_i) \neq f(M_j)$



Zastosowanie funkcji skrótu pozwala na ochronę integralności wiadomości

Ochrona autentyczności wiadomości

Zastosowanie funkcji skrótu nie pozwala na ochronę autentyczności wiadomości

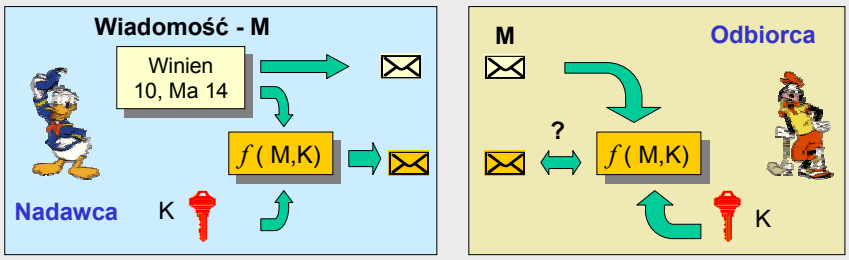


Każdy może zmienić wiadomość i wyznaczyć dla niej skrót

MAC (message authentication code)

Istota metody

- Nadawca: Wyznaczenie skrótu na podstawie wiadomości powiększonej o tajną informację, identyfikującą autora (klucz)
- Odbiorca: Sprawdzenie skrótu na podstawie wiadomości i współdzielonego klucza autora



MAC zapewnienia autentyczność wiadomości

Odbiorca musi posiadać ten sam klucz w celu uwiarygodnienia treści (klucz symetryczny)

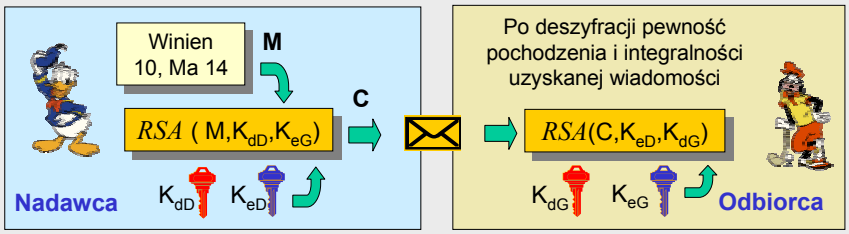
Podpisy cyfrowe

MAC - pozwala sporządzić podpis cyfrowy wiadomości, ale ma wady:

- Konieczność posiadania tego samego klucza przez obydwu uczestników korespondencji
- Możliwość wyparcia się autorstwa tekstu - tekst może być podpisany przez dowolną osobę posiadającą klucz

RSA - ?

Pożądana metoda wykorzystująca ideę kluczy publicznych



Podpisy cyfrowe

Podstawową wadą metody RSA jako metody zapewniającej ochronę autentyczności i integralności wiadomości jest duża złożoność obliczeniowa algorytmu

⇓ Zmniejszenie czasochłonności operacji

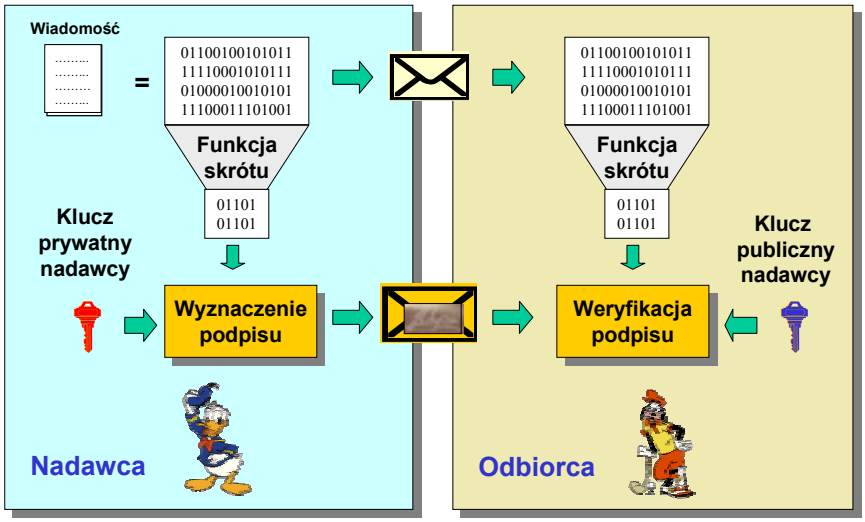
Zamiast przetwarzania całej wiadomości przy użyciu RSA wyznaczyć i podpisać wyłącznie skrót wiadomości

⇓

Efekt to przetwarzanie niewielkiego bloku danych o stałym rozmiarze (16 lub 20 bajtów)

Realizacja idei - algorytm DSA (digital signature algorithm)

Algorytm DSA



Algorytm DSA

Podstawowe charakterystyki

- Długość kluczy - jak w RSA
- Struktura klucza - składniki p,q,g (wspólne dla kluczy tajnego i jawnego) oraz x (tajny) i y (jawny)
- Stosowana funkcja skrótu - SHA-1
- Wielkość podpisu cyfrowego - 20 bajtów

Funkcja

- Zapewnia autentyczność wiadomości - może ją sporządzić tylko posiadacz klucza tajnego
- Zapewnia integralność podpisywanej wiadomości - podpis zgadza się tylko dla wiadomości w oryginalnej postaci

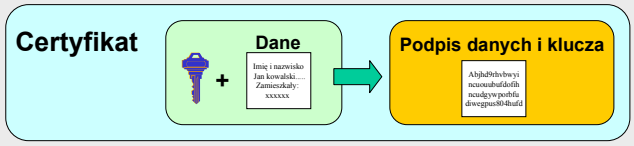
g:
7e1a085d69b3ddecbbcab5C36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107
108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa
213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492

q:
9760508f15230bccb292b982a2eb840bf0581cf5

Rozpowszechnianie kluczy - certyfikaty

Powszechnie przyjętym sposobem dystrybucji kluczy publicznych stały się certyfikaty

- **Składniki certyfikatu**
  - **Klucz publiczny**
  - **Informacje o posiadaczu klucza (imię, nazwa instytucji itp.)**
  - **Podpis (podpisy) cyfrowe całej zawartości**

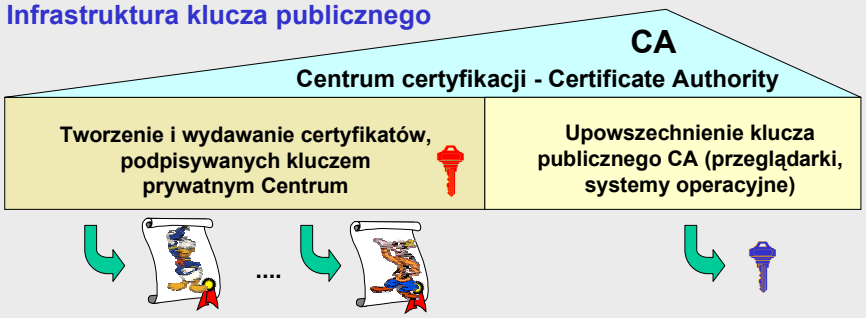


Dystrybucja certyfikatów

Metody dystrybucji certyfikatów

- **Bezpośrednia (osobista - e-mail, dyskietka z plikiem)**
- **Serwery certyfikatów (bazy danych kluczy)**
- **Infrastruktura klucza publicznego (PKI)**
  - **bazy danych kluczy + struktura i procedury**

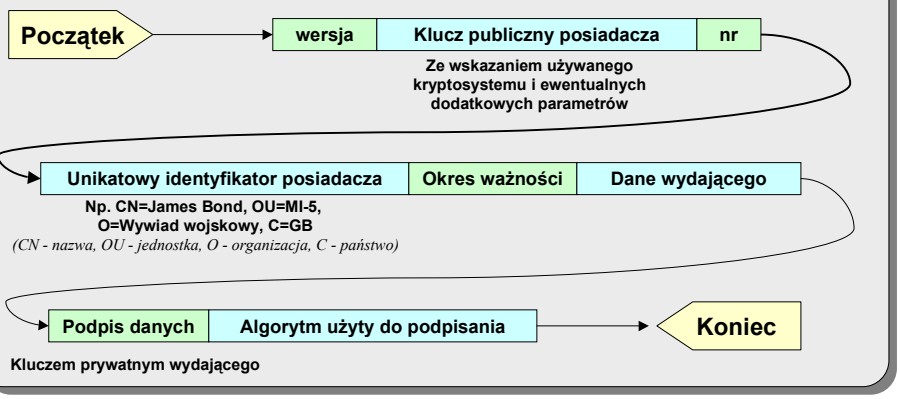
Infrastruktura klucza publicznego



Stosowane standardy certyfikatów

- X.509 Przeglądarki

Struktura certyfikatu X.509



Formaty certyfikatów

- Podstawowe niedogodności formatu

Certyfikat można uzyskać tylko od CA (Verisign, Thawte)

Certyfikat jest podpisywany tylko jednym podpisem (przez jeden organ)

c.d.n.