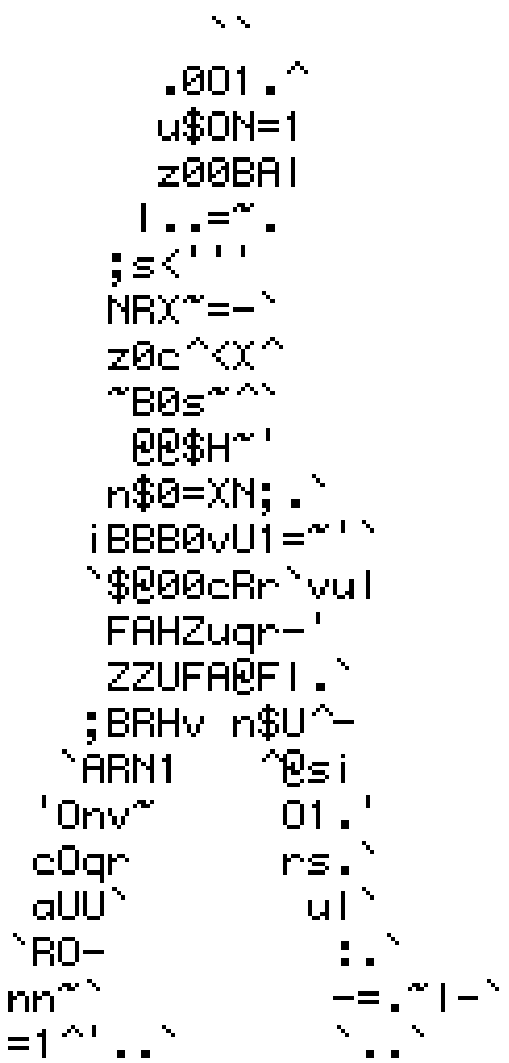


Podstawowe elementy kryptografii

część II

Zagadnienia

1. Terminologia
2. Szyfry symetryczne
3. Szyfry asymetryczne
4. Funkcje skrótu i podpis cyfrowy
5. Zarządzanie kluczami (PKI)
6. Zastosowania kryptografii
7. Aspekty prawne wykorzystania kryptografii
8. Steganografia

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 h[M]
- jednoznaczny wynik $d=h$[M] – skrót (*message digest*, *fingerprint*) o stałym rozmiarze
- przy wieloznacznym argumencie (M)
- jej zadaniem jest dostarczyć odbiorcy narzędzia do zweryfikowania czy treść wiadomości nie została zmodyfikowana

Skrót

Rys historyczny:

- w transmisji danych skróty wiadomości powszechnie wykorzystywane są od lat 70
- suma kontrolna (*checksum*) – negatywne potwierdzenia, retransmisje
- funkcja kontrolna (*data integrity check*)
- funkcja kontrolna wiadomości (*message integrity check*)
- funkcja ściągająca (*contraction function*)
- kod uwierzytelniający informacji (*data authentication code*)

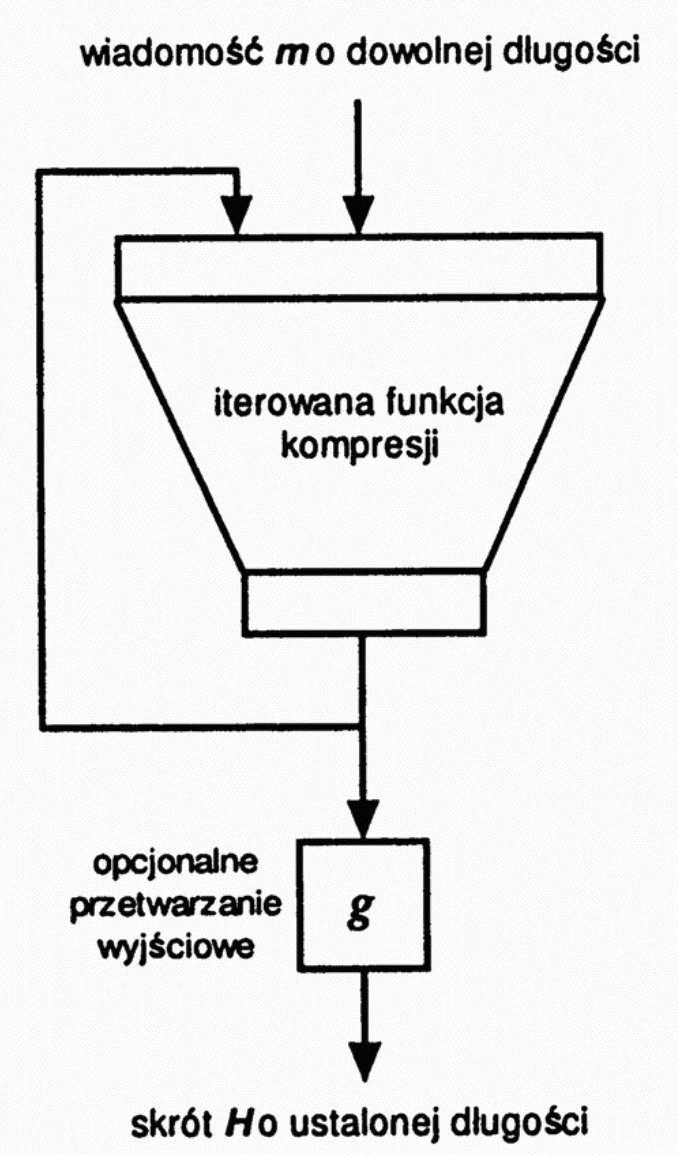
Skrót

Wymagane własności:

- kompresja: $|d| < |M|$
- 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 $M \neq M'$ :: $h[M] = h[M']$

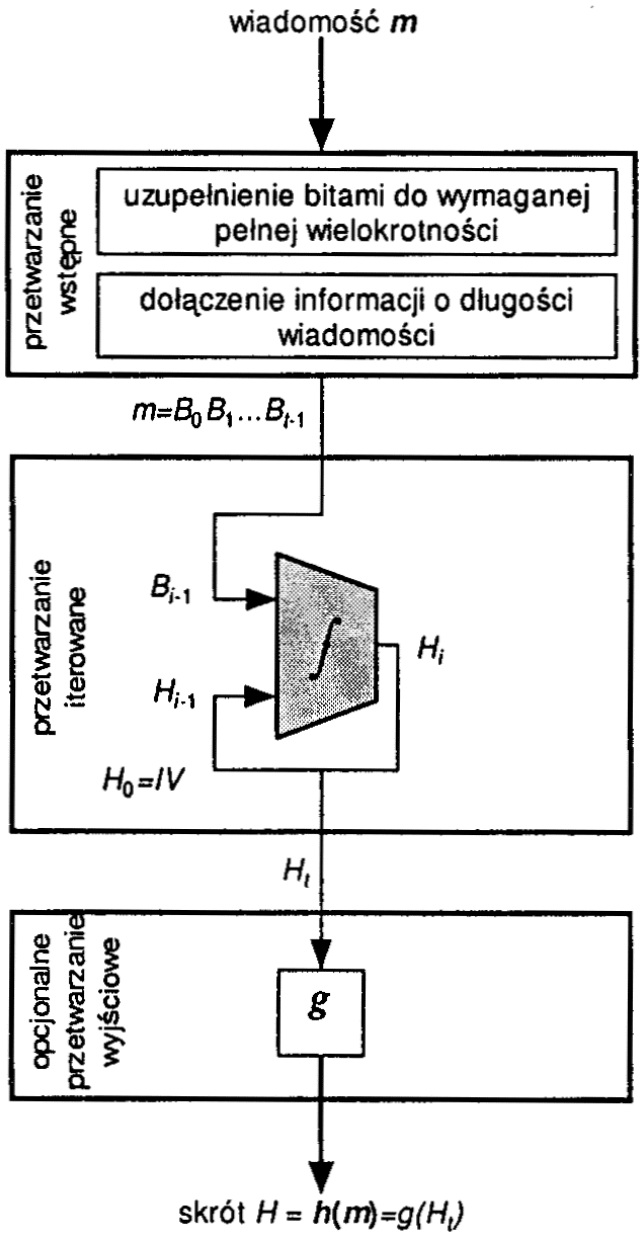
Skrót

Idea:



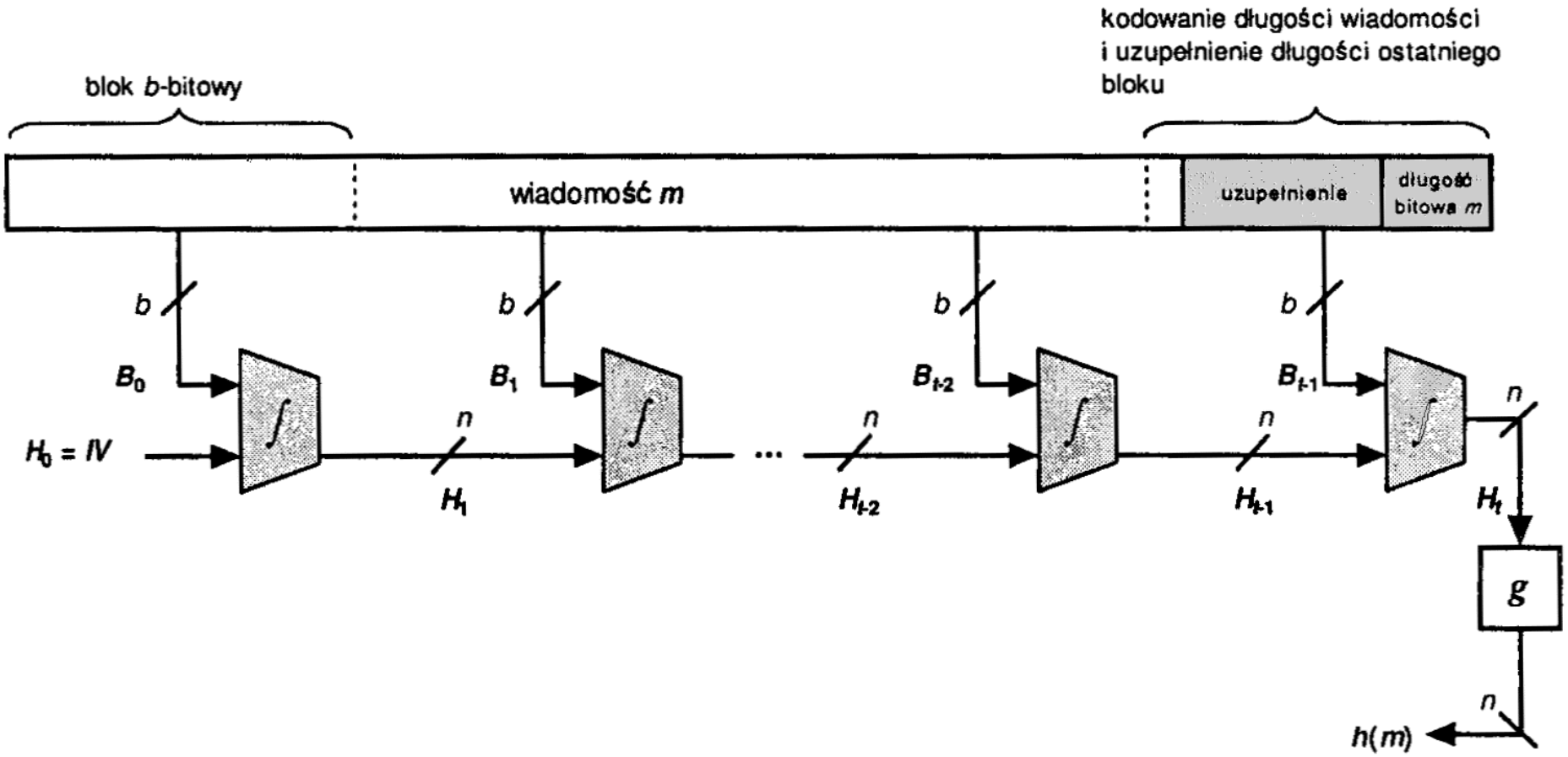
Skrót

Schemat:



Skrót

Działanie:



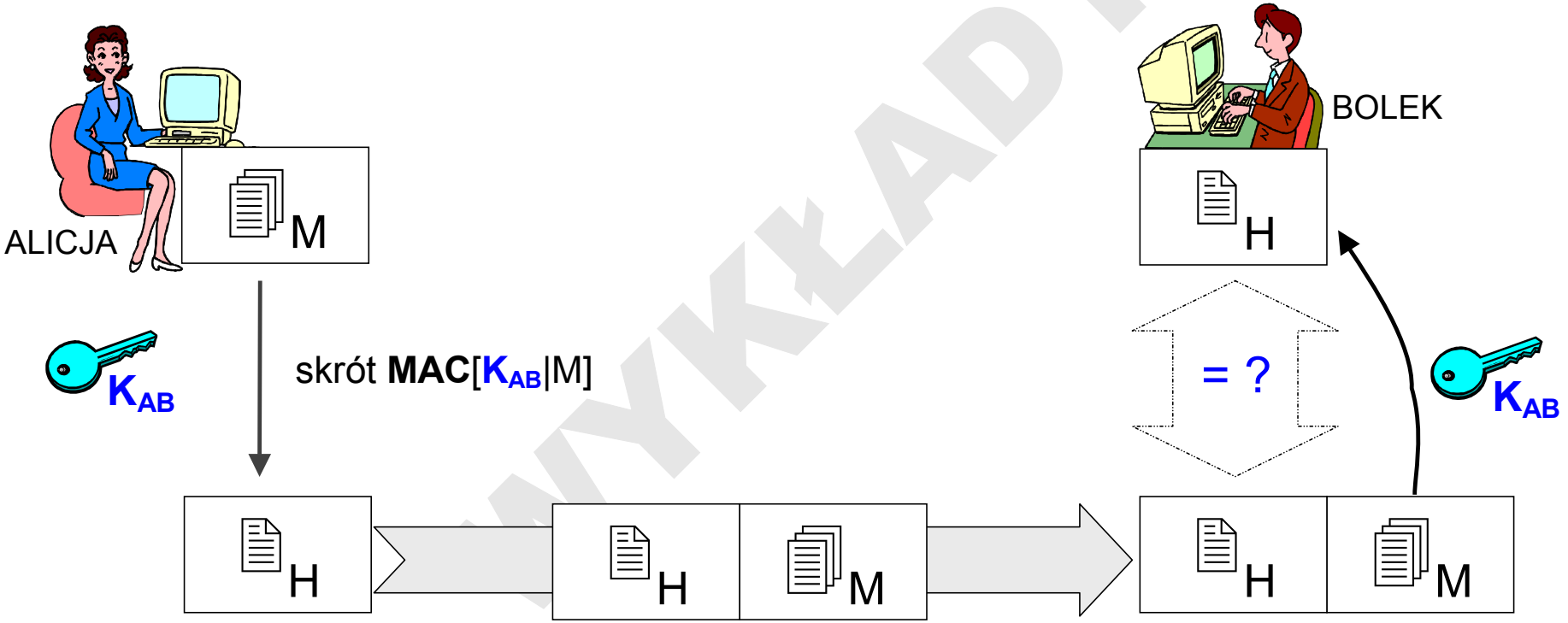
Skrót

Zastosowanie funkcji skrótu:

- zapewnienie integralności wiadomości: **MDC** – *message digest code* (bez klucza kryptograficznego)
- zapewnienie integralności oraz autentyczności wiadomości: **MAC** – *message authentication code* (z kluczem kryptograficznym)

Skrót

Zastosowanie funkcji skrótu:



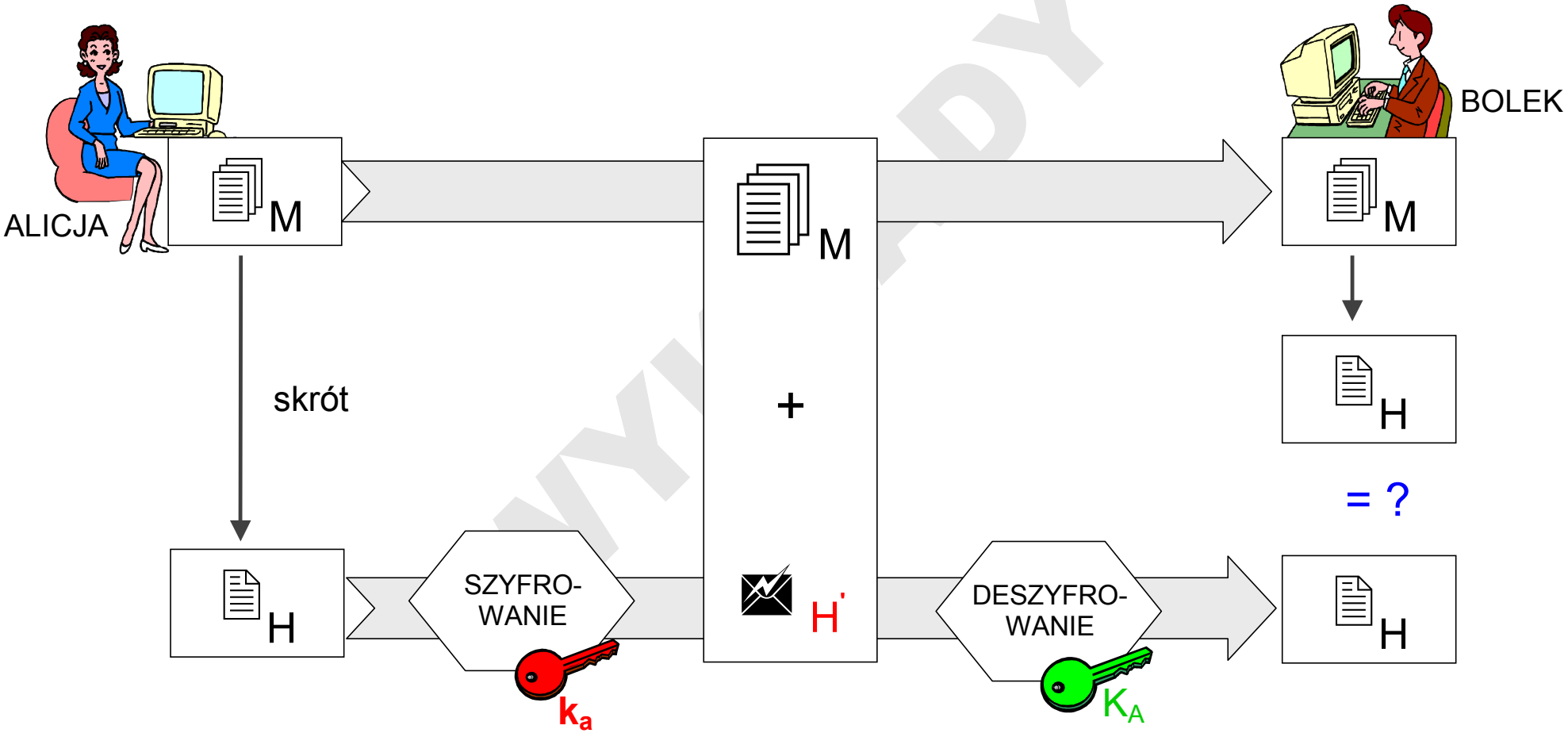
Podpis cyfrowy

Podpis cyfrowy HMAC

- najczęściej wykorzystywana funkcja mieszająca (*hash function*) h[M]
- z kluczem k asymetrycznym (*keying hash function*) h_k[M]
  (wartość skrótu HMAC jest zaszyfrowana kluczem prywatnym nadawcy)
- być może z wykorzystaniem ziarna (*salt*) lub zawołania (*challenge*)

Podpis cyfrowy

Generowanie i weryfikowanie HMAC:



All in one

ALICJA

integralność
autentyczność
i poufność

BOLEK

k_a

K_A

k_b

K_B

M

H

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

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

M | H'

S

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

M | H'

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

H = H

Algorytmy skrótu

Rys historyczny:

- Algorytmy MD i MD2 (Ron Rivest) powstały w latach ’80. jako alternatywa dla autentyczności osiąganej metodą 1 (RSA)
- MD nie został nigdy oficjalnie opublikowany, był wykorzystywany jako autorskie rozwiązanie w systemie pocztowym RSADSI, MD2 – RFC 1319
- w 1990 Ralph Merkle (Xerox) zaproponował algorytm HMAC o nazwie SNEFRU – kilkukrotnie szybszy od MD2
- na to Rivest odpowiedział MD4 (RFC 1320) – wykorzystuje operacje 32b
- w 1992 złamano SNEFRU i wykryto pewną słabość MD4 w wersji 2-rund
- Rivest wzmocnił algorytm otrzymując trochę wolniejszy MD5 (RFC1321)

Algorytmy skrótu

MD5

- skrót 128b
- teoretyczna odporność na kolizje 2^{64} jest współcześnie uznawana za zbyt słabą
- 128b wektor IV
- 64 iteracje (4 rundy po 16 kroków)
- little endian

Algorytmy skrótu

SHA (*Secure Hash Algorithm*)

- SHA został opracowany przez NSA (*National Security Agency*)
- i przyjęty przez NIST jako standard federalny w 1993r.
- SHA (SHA-0) jest zbliżony do MD4
- przekształca wiadomość o długości do 2^{64}b w skrót 160b
- 160b wektor IV
- 80 iteracji (4 rundy po 20 kroków)
- big endian
- szybko wykryto słabości (ich natury nigdy nie opublikowano)
- i opracowano SHA-1 (ratyfikowany przez NIST)
- odporność na kolizje 160b skrótu – 2^{80} jest współcześnie uznawana za zbyt słabą

Algorytmy skrótu

SHA-256 / SHA-384 / SHA-512

- zupełnie nowe funkcje
- przystosowane do współpracy z kluczami AES (128b, 192b i 256b)
- dają skróty 256b, 384b i 512b
- nie doczekały się jeszcze szerszej analizy
- złożone obliczeniowo
- SHA-384 ma identyczny koszt co SHA-512 – w praktyce bezużyteczna

Algorytmy skrótu

RIPE-MD

- europejski (EU) projekt RACE Integrity Primitives Evaluation – Message Digest
- skrót 128b
- ulepszony wariant MD4 (zmodyfikowane rotacje i kolejność słów wiadomości)
- równoległe 2 przebiegi (z różnym zadanym parametrem) w każdej iteracji
- po każdej iteracji oba wyniki łączone z rejestrem strumieniowym
- prawdopodobnie duża odporność na ataki

Algorytmy skrótu

HAVAL

- skrót o zmiennej długości: 128b, 160b, 192b, 224b lub 256b
- wariant MD4
- stosuje wyrafinowane funkcje nieliniowe (o własności lawinowości)
- w każdej iteracji wykonuje inne permutacje
- zmodyfikowano rotacje
- prawdopodobnie duża odporność na ataki

Algorytmy skrótu

ElGamal

- algorytm ten początkowo opracowano właśnie dla podpisu cyfrowego HMAC
- podpisem wiadomości M jest para (a, b) ::

  $a = g^k \bmod p$

  b:: M = $(xa + kb) \bmod p$-1 (rozszerzone równanie Euklidesa)

- weryfikacja podpisu cyfrowego:

  jeśli $(y^a\ a^b) \bmod p == g^M \bmod p$

Podpis cyfrowy

Podpis cyfrowy UMAC

- *universal hashing MAC* – UMAC$_{k|x}$[M] wykorzystuje entropię x klucza k do przyspieszenia działania
- wyrażona w bitach entropia określa „niepewność” klucza – ilość bitów klucza nieznanych atakującemu
- algorytmy UMAC-STD-30, UMAC-MMX-60, UMAC16, UMAC32
- szybkie, ale dalece niedoskonałe

Systemy podpisu cyfrowego

Standardy

Standard DSS (*Digital Signature Standard*)

- standard NIST z kategorii FIST (*Federal Information processing STandard*) 1991 i 1993
- obejmuje użycie skrótu SHA-1 oraz algorytmu DSA (*Digital Signature Algorithm*)

Standard SHS (*Secure Hash Standard*)

- projekt NIST z 2001: SHA-256 / SHA-384 / SHA-512

Ataki na funkcje skrótu

Atak urodzinowy

Paradoks dnia urodzin:

- ile osób potrzeba na tej sali, aby z prawdopodobieństwem 50% znalazła się wśród nich taka, która obchodzi urodziny tego samego dnia co autor tych slajdów?
  (funkcja mieszająca: 🧍 → 366 dni)
- odp.: 183
- a ile potrzeba osób, aby wśród nich znalazły się 2 obchodzące urodziny tego samego dnia?
- odp.: [Schneier]

Ataki na funkcje skrótu

Atak urodzinowy

Uogólnienie:

- mamy rozmiar danych wejściowych: n (input)
- rozmiar zbioru wynikowego: k (output)
- dla n mamy możliwych $n(n\text{-}1)/2$ par danych wejściowych
- dla każdej pary oba elementy dadzą ten sam wynik (output) z prawdop. $1/k$
- zatem, potrzeba $k/2$ par aby z prawdop. 50% wśród nich była taka jak szukamy
- jeśli $n > \sqrt{k}$ to są duże szanse powodzenia
- dla skrótu 128b potrzeba 2^{128} wiadomości aby znaleźć tę, która dała określony skrót
- ale wystarczy 2^{64} wiadomości aby znaleźć 2 o identycznym skrócie

Ataki na funkcje skrótu

Kolizje w MD5 (Xuejia Lai et al. 17.08.2004):

2 ciągi po 128 B różniące się 6-cioma bajtami:

```
00000000  d1 31 dd 02 c5 e6 ee c4  69 3d 9a 06 98 af f9 5c
00000010  2f ca b5 87 12 46 7e ab  40 04 58 3e b8 fb 7f 89
00000020  55 ad 34 06 09 f4 b3 02  83 e4 88 83 25 71 41 5a
00000030  08 51 25 e8 f7 cd c9 9f  d9 1d bd f2 80 37 3c 5b
00000040  96 0b 1d d1 dc 41 7b 9c  e4 d8 97 f4 5a 65 55 d5
00000050  35 73 9a c7 f0 eb fd 0c  30 29 f1 66 d1 09 b1 8f
00000060  75 27 7f 79 30 d5 5c eb  22 e8 ad ba 79 cc 15 5c
00000070  ed 74 cb dd 5f c5 d3 6d  b1 9b 0a d8 35 cc a7 e3
```

MD5 = a4c0d35c95a63a805915367dcfe6b751

```
00000000  d1 31 dd 02 c5 e6 ee c4  69 3d 9a 06 98 af f9 5c
00000010  2f ca b5 07 12 46 7e ab  40 04 58 3e b8 fb 7f 89
00000020  55 ad 34 06 09 f4 b3 02  83 e4 88 83 25 f1 41 5a
00000030  08 51 25 e8 f7 cd c9 9f  d9 1d bd 72 80 37 3c 5b
00000040  96 0b 1d d1 dc 41 7b 9c  e4 d8 97 f4 5a 65 55 d5
00000050  35 73 9a 47 f0 eb fd 0c  30 29 f1 66 d1 09 b1 8f
00000060  75 27 7f 79 30 d5 5c eb  22 e8 ad ba 79 4c 15 5c
00000070  ed 74 cb dd 5f c5 d3 6d  b1 9b 0a 58 35 cc a7 e3
```

MD5 = a4c0d35c95a63a805915367dcfe6b751

Co jeśli taki ciąg będzie IV ?

Ataki na funkcje skrótu

Kolizje w SHA (Xiaoyun Wang et al. 15.01.2005):

- SHA-1: kolizje dla 2^{69} operacji (przy teoretycznej 2^{80})
- SHA-1 uproszczona wersja (58-rund): 2^{33}
- SHA-0: 2^{39}

. . .

- ale dla zastosowań HMAC kolizje funkcji nie przesądzają jeszcze o jej nieprzydatności

Zarządzanie kluczami

Problemy

- jak partnerowi komunikacji przekazać w sposób bezpieczny klucz niezbędny do szyfrowania / deszyfrowania?
- jak go regularnie zmieniać?
- tajny klucz symetryczny? – 10 os. = 45 kluczy, 100 os. = 4950 kluczy
- publiczny klucz asymetryczny? – skąd pewność jego prawdziwości

Metoda Diffiego-Hellmana (DH) Whitfield Diffie, Martin Hellman

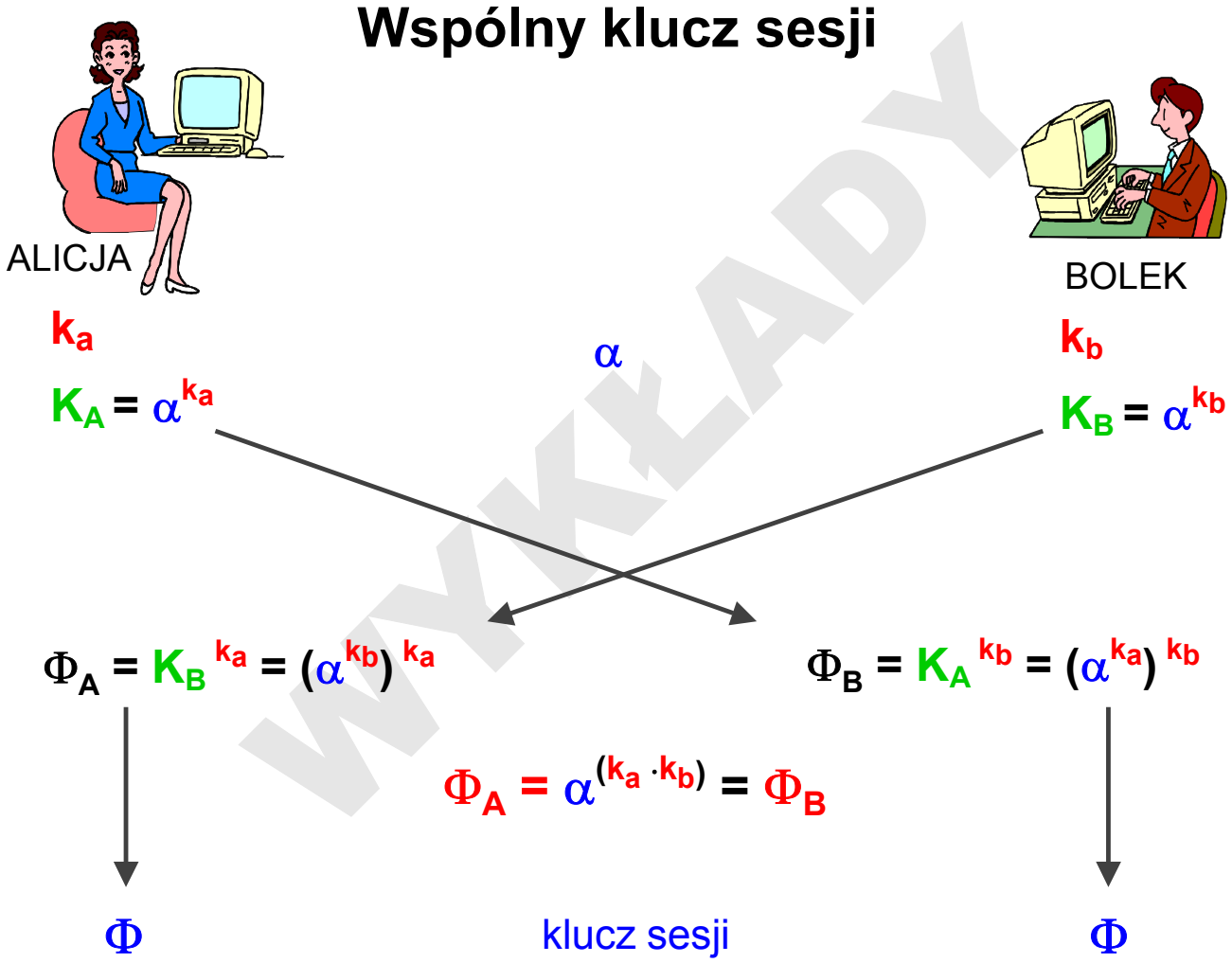
- jest częściowym rozwiązaniem tego problemu
- pozwala partnerom uzgodnić tajny klucz bez ryzyka ujawnienia go podsłuchującym

Metoda Diffiego-Hellmana

Idea:

- ustalamy wspólny jednorazowy symetryczny **klucz sesji** (dla każdej sesji inny)
- na potrzeby ustalenia klucza sesji wykorzystamy model asymetryczny
- na scenę wkraczają ponownie liczby pierwsze
- DH wykorzystuje multiplikatywną grupę modulo p – $\mathbb{Z}_p^*$
- α jest elementem pierwotnym grupy $\mathbb{Z}_p^*$ (α generujące całą grupę)
- czyli zamiast 1, ..., p-1 możemy grupę traktować jako 1, α, α^2, ... , α^{p-2}

Metoda Diffiego-Hellmana



Metoda Diffiego-Hellmana

Atak *man-in-the-middle*:

- Edziu, znając α, może skutecznie wkroczyć na etapie negocjacji klucza
- Alicja i Bolek będą porozumiewać się poprzez Edzia za pomocą kluczy, które – jak im się będzie wydawać – wymienili ze sobą

Przypadek szczególny:

- co jeśli Edziu przechwytując komunikację zastąpi $K_A = \alpha^{k_a}$ oraz $K_B = \alpha^{k_b}$ przez wartość 1?

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 E 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
- nazywaną urzędem poświadczającym 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

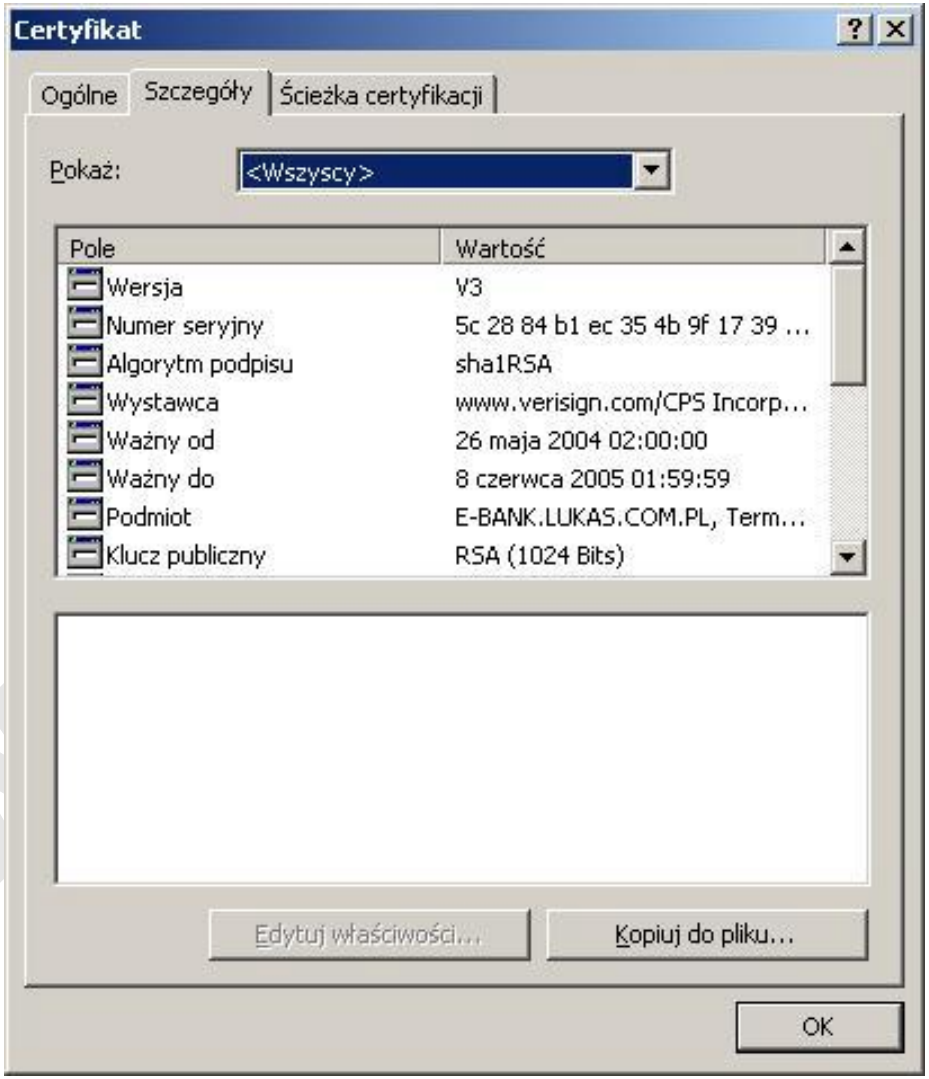
Certyfikaty kluczy publicznych

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

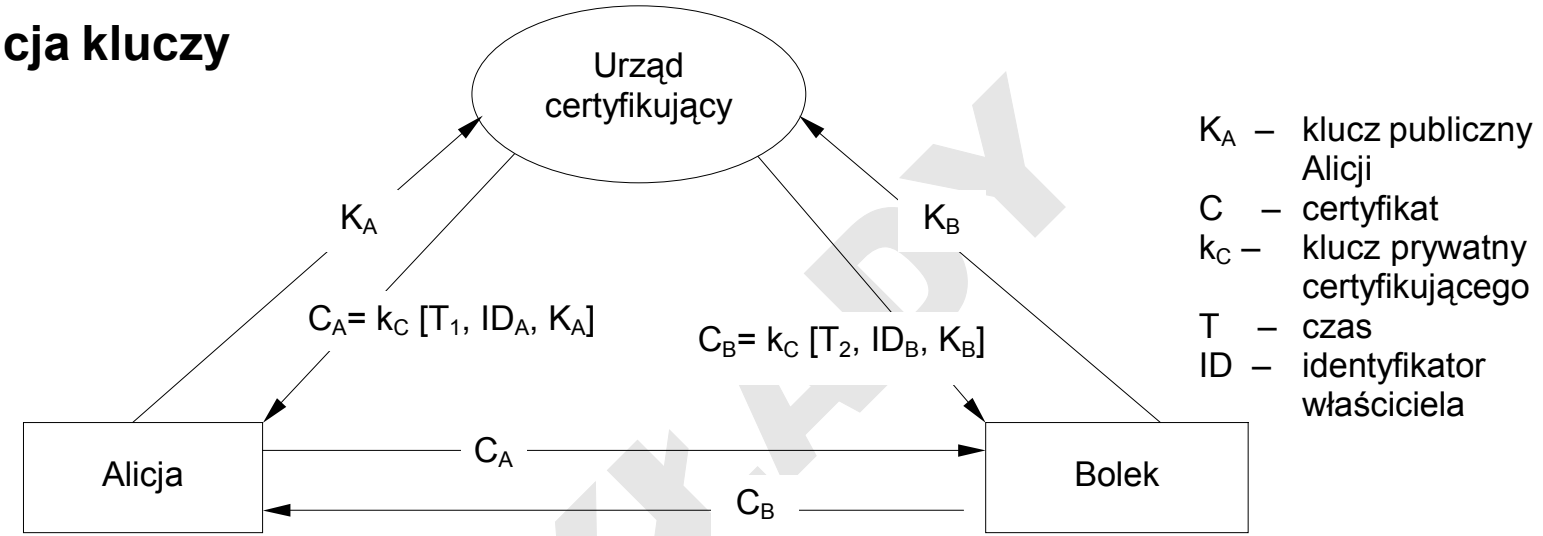
Standard ITU-T X.509

Budowa certyfikatu X.509 v.3:

- struktura podstawowa uzupełniona o zestaw danych identyfikacyjnych podmiotu certyfikatu
- sposób wykorzystania klucza (przeznaczenie, np. do szyfrowania danych, do szyfrowania kluczy, do uzgadniania kluczy, do podpisywania danych, do osiągnięcia niezaprzeczalności)
- informacje o polityce certyfikacji wydawcy certyfikatu (np. ograniczenia długości ścieżki certyfikacji, punkty dystrybucji list certyfikatów unieważnionych)
- oraz opcjonalna możliwość tworzenia dodatkowych pól / parametrów identyfikacyjnych, wg potrzeb komunikujących się podmiotów

Certyfikaty kluczy publicznych

Dystrybucja kluczy



- w celu uzyskania certyfikatu użytkownik zwraca się do urzędu certyfikującego CA dostarczając mu swój klucz publiczny
- do odczytania certyfikatu niezbędny jest tylko i wyłącznie klucz publiczny urzędu certyfikującego
- użytkownik może przesłać swój certyfikat do innych użytkowników w celu poświadczenia jego autentyczności

Certyfikaty kluczy publicznych

Hierarchia urzędów poświadczających

dylemat

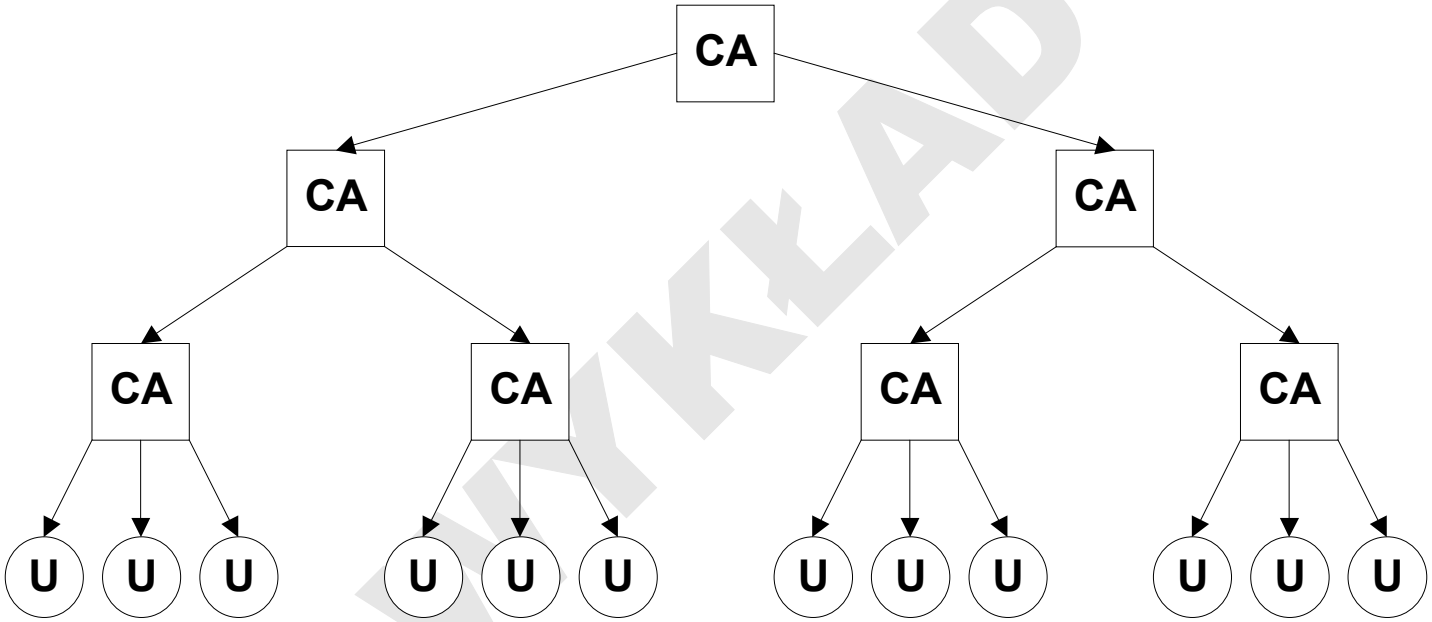
- komu na tyle zaufać, aby mógł być w pełni wiarygodny i wydawać certyfikaty?

rozwiązanie

- certyfikat musi przebyć pewną procedurę uwierzytelniającą
- urzędy CA mogą tworzyć wielopoziomową hierarchię
- urzędy na danym poziomie wystawiają certyfikaty kluczy publicznych urzędom lub użytkownikom (U) znajdującym się na niższym poziomie

Certyfikaty kluczy publicznych

Hierarchia urzędów poświadczających



Infrastruktura kluczy publicznych

PKI (*Public Key Infrastructure*)

sprzęt, oprogramowanie, ludzie, polityki i procedury

konieczne do utworzenia, zarządzania, przechowywania, dystrybucji i unieważniania certyfikatów kluczy publicznych

- w Internecie PKI wykorzystuje specyfikację X.509 (PKIX, RFC 2459)
- PKI oferuje często dodatkowe certyfikaty, np. Certyfikaty Znacznika Czasu (dla wiarygodnego potwierdzania czasu)

Infrastruktura kluczy publicznych

Usługi PKI

Hierarchiczny urząd certyfikujący oferujący publicznie swoje usługi.

Do jego funkcji należy między innymi:

- weryfikacja tożsamości użytkowników ubiegających się o certyfikaty
- zarządzanie kluczami kryptograficznymi
  - generowanie par kluczy dla użytkowników
  - bezpieczne przechowywanie kluczy
- zarządzanie certyfikatami
  - wystawienie certyfikatów kluczy publicznych
  - generowanie list certyfikatów unieważnionych CRL (*Certificate Revocation List*)

Infrastruktura kluczy publicznych

Komponenty PKI

- 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

Infrastruktura kluczy publicznych

Repozytoria certyfikatów

- serwery LDAP
- respondery OCSP
- serwery WWW
- serwery FTP
- serwery DNS (DNSsec)
- agenci systemu katalogowego X.500 (DSA – *Directory System Agents*)
- korporacyjne bazy danych

Infrastruktura kluczy publicznych

Problemy

wielość hierarchicznych ośrodków certyfikacji

- możliwa współpraca pomiędzy niezależnymi strukturami

problem jednoznacznej identyfikacji podmiotu

- jaki kompromis pomiędzy pełnymi danymi identyfikującymi a prywatnością?
- różne klasy certyfikacji o różnym poziomie zaufania, np. VeriSign:

Class 1	poświadczenie adresu e-mail	darmowe
Class 2	weryfikacja użytkownika w bazie danych podmiotów	20$ (operacje z gwarancją do 5 tys.$)
Class 3	weryfikacja danych osobowych	300$ (gwar. do 100 tys.$)

Infrastruktura kluczy publicznych

Problemy

problem pierwszego certyfikatu

- jak bezpiecznie certyfikować CA?
- wzajemna certyfikacja różnych urzędów z PKI
- certyfikaty wbudowane w aplikacje (przeglądarki WWW, np. Netscape ma ponad 30 predefiniowanych certyfikatów urzędów CA)

standardowy mechanizm pobierania certyfikatów CA

- przekazywanie jako typ MIME application/x-x509-ca-cert

Infrastruktura kluczy publicznych

Zarządzanie

protokoły służące do wymiany informacji niezbędnych

do właściwego zarządzania infrastrukturą kluczy publicznych:

- CMP (*Certificate Management Protocol*)
- SCVP (*Simple Certificate Validation Protocol*)

Infrastruktura kluczy publicznych

Polska

Certyfikaty zwykłe (tzw. powszechne)

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

Certyfikaty kwalifikowane

- wywołują skutki prawne równoważne podpisowi własnoręcznemu (Ustawa z dn. 18.09.2001 o podpisie elektronicznym)
- przeznaczone dla osób fizycznych, wydawane na podstawie umowy i po weryfikacji tożsamości w Punkcie Rejestracji
- znajdują zastosowanie w każdym przypadku składania oświadczenia woli (również e-faktury)
- nie służą do szyfrowania dokumentów

Infrastruktura kluczy publicznych

Instytucje certyfikujące w Polsce

- Unizeto Certum www.certum.pl
- Signet www.signet.pl
- Sigillum www.sigillum.pl
- . . .

Infrastruktura kluczy publicznych

Ceny

	Cena	*Okres ważności*
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)

	Cena	*Okres ważności*
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)

Zastosowania kryptografii

Kryptograficzne zabezpieczenie danych

- ogromna ilość aplikacji szyfrowania plików,
- ... i całych katalogów (fragmentów systemu plików):
  - moduł jądra Linux *loop-AES* (od k.2.4 *cryptoloop*) – szyfrowanie całego systemu plików na poziomie jądra za pomocą urządzenia blokowego /dev/loop[1-8]

```
mount -t ext3 crypto.raw /mnt/crypto -oencryption=aes-256
```

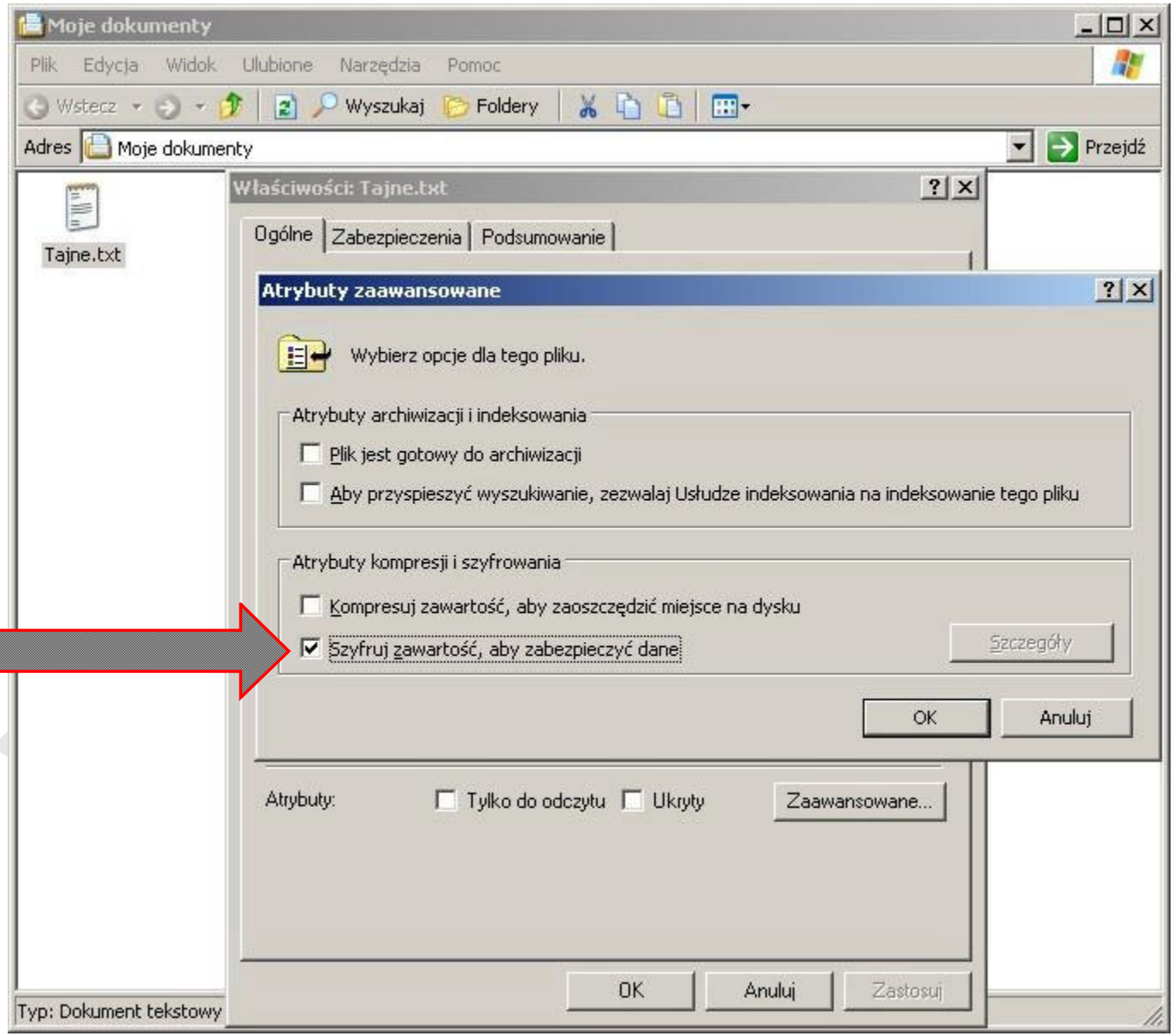
  - EncFS – tworzy z wybranego katalogu wirtualny system plików w przestrzeni użytkownika, korzysta z modułu jądra FUSE (*Filesystem in USErspace*)

```
encfs ~/.crypto.vfs ~/tajne_dane
fusermount -u ~/tajne_dane
```

Zastosowania kryptografii

EFS

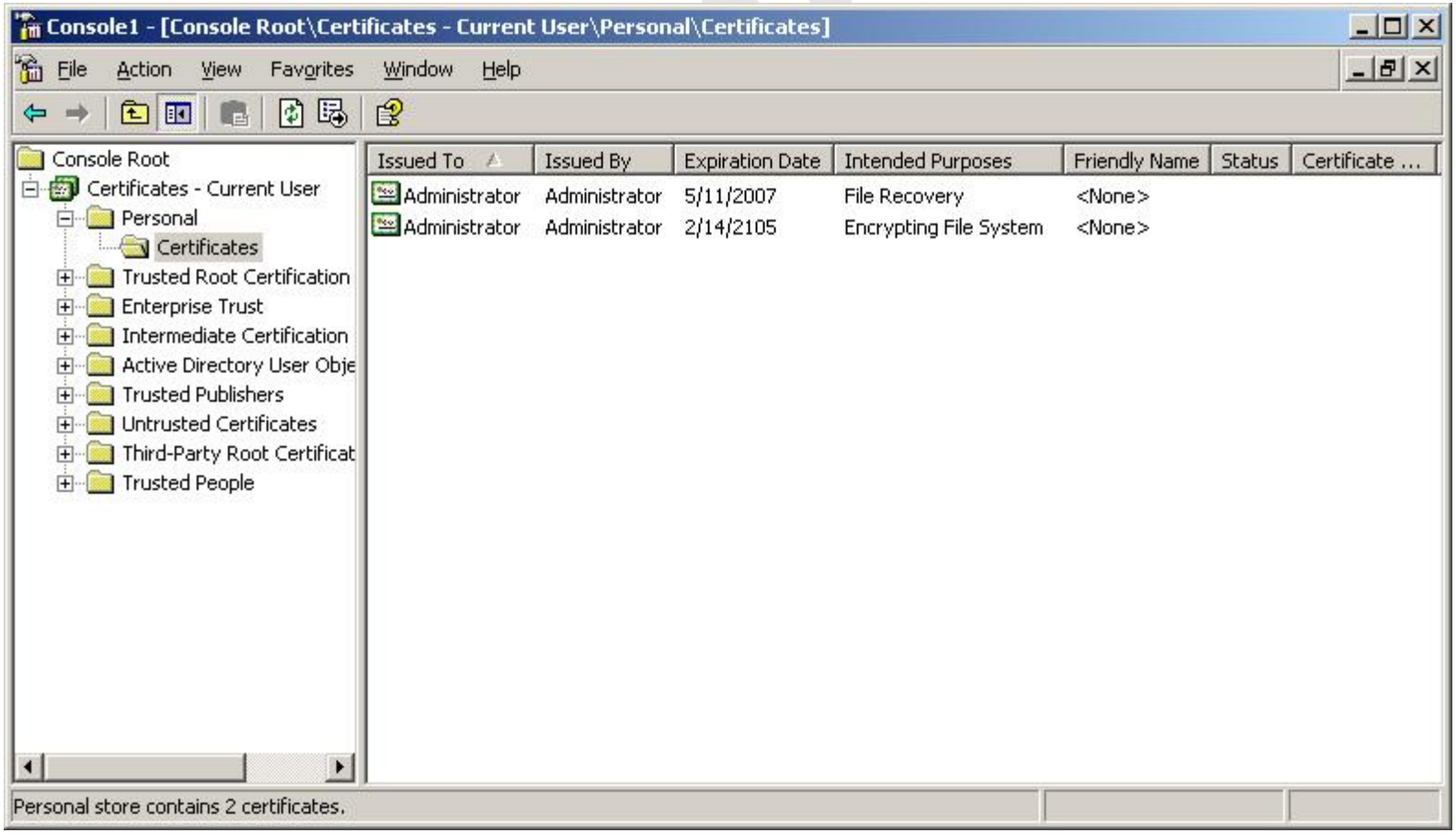
EFS (*Encrypted File System*) – na partycjach NTFS od Windows 2000, działa jako usługa systemowa (przeźroczyście dla aplikacji); DESX i 3DES



Zastosowania kryptografii

Klucze EFS

- klucz właściciela pliku przechowywany w certyfikacie użytkownika
- klucz uniwersalny usługi systemowej Data Recovery Agent



Zastosowania kryptografii

Kryptograficzne zabezpieczenie komunikacji

Protokoły komunikacyjne:

- SSH (*Secure Shell*)
- SSL (*Secure Sockets Layer*) / TLS (*Transport Layer Security*)
- PCT (*Private Communication Technology*)

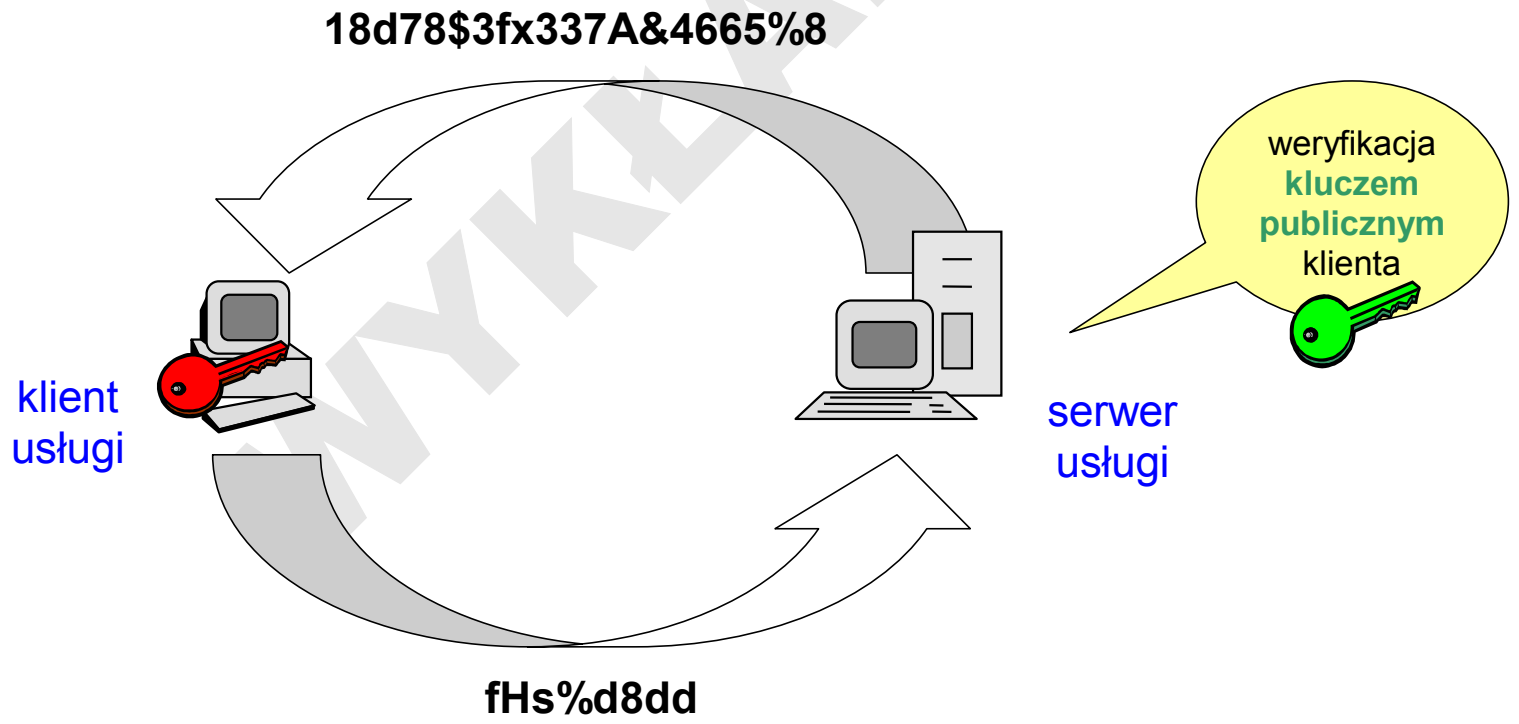
Komponenty aplikacji użytkowych:

- poczta elektroniczna: PGP, PEM, S/MIME, MIME/PGP, MSP
- www: S-HTTP
- e-commerce: SET (Secure Electronic Transactions)

Uwierzytelnianie

Metoda zawołanie-odzew (*challenge-response*):

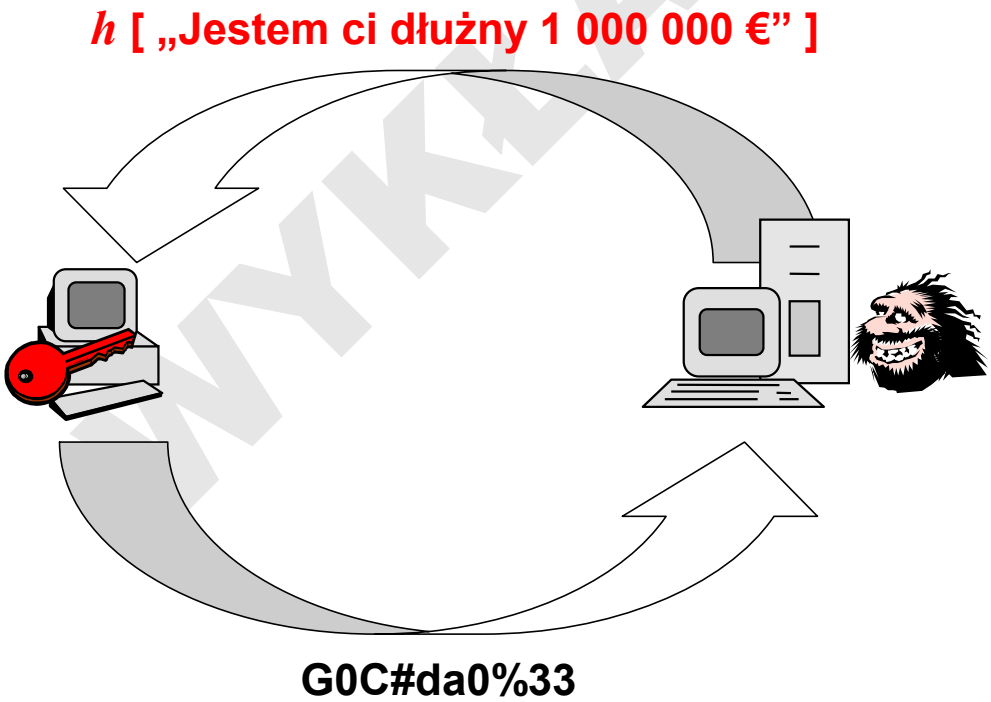
- serwer pyta o nazwę użytkownika, a następnie przesyła unikalny ciąg („zawołanie”)
- klient **podpisuje** otrzymany ciąg **kluczem prywatnym** i podpis odsyła jako „odzew”



Uwierzytelnianie

Uwaga:

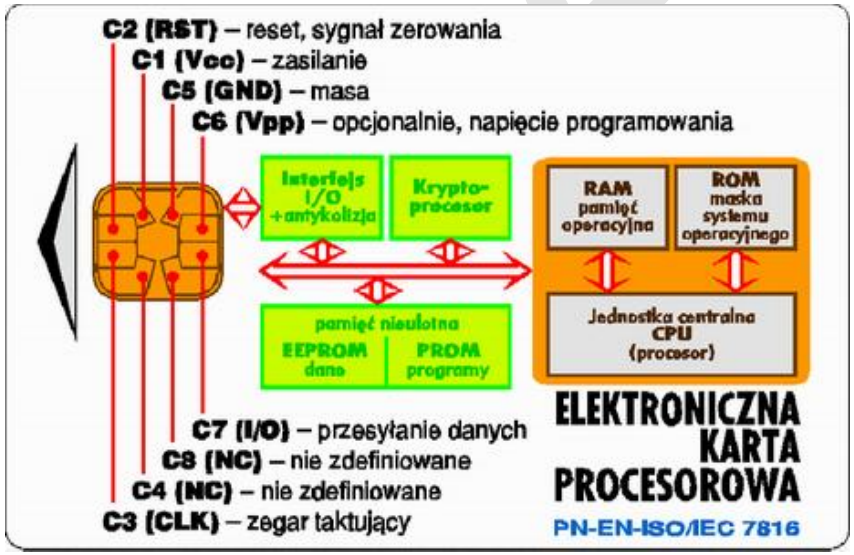
- kryptografia asymetryczna jest wystarczająca do uwierzytelniania
- jednak stosowanie jej w takim prostym schemacie „zawołanie-odzew” rodzi pole do nadużyć niezaprzeczalności:



Zastosowania kryptografii

Kryptograficzne mechanizmy uwierzytelniające

- system Kerberos
- kryptograficzne żetony uwierzytelniające (*cryptographic tokens*)

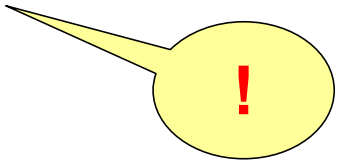


Narzędzia

Przykładowe pakiety kryptograficzne

RSA Secure (RSA Data Security)

- szyfrowanie plików
- algorytm RC4
- klucz „master” (możliwy podział na części – do zebrania pełnego klucza potrzeba np. 3 ludzi spośród 5 posiadających poszczególne części)
- Windows, Macintosh



Compaq iTP Certificate Security Solution (CSS)

- system kryptograficzny z algorytmem symetrycznym
- licencja eksportowa USA dla klucza 128b

Narzędzia

Przykładowe biblioteki kryptograficzne

darmowe:

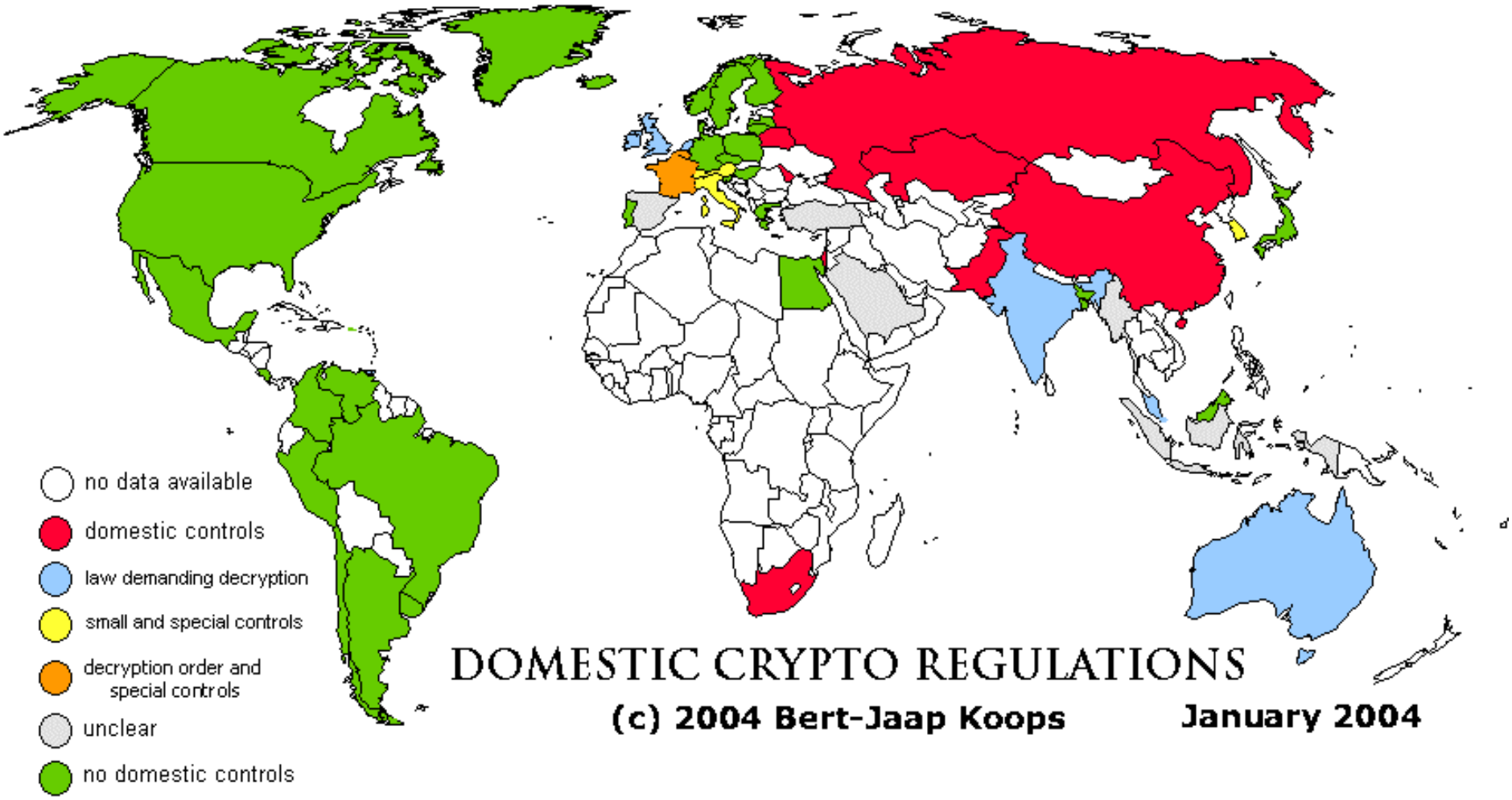
- crypto++ www.cryptopp.com
- cryptix www.cryptix.org
- boucy castle www.bouncycastle.org
- flexiprovider www.flexiprovider.de
- botan (OpenCL) botan.randombit.net

komercyjne:

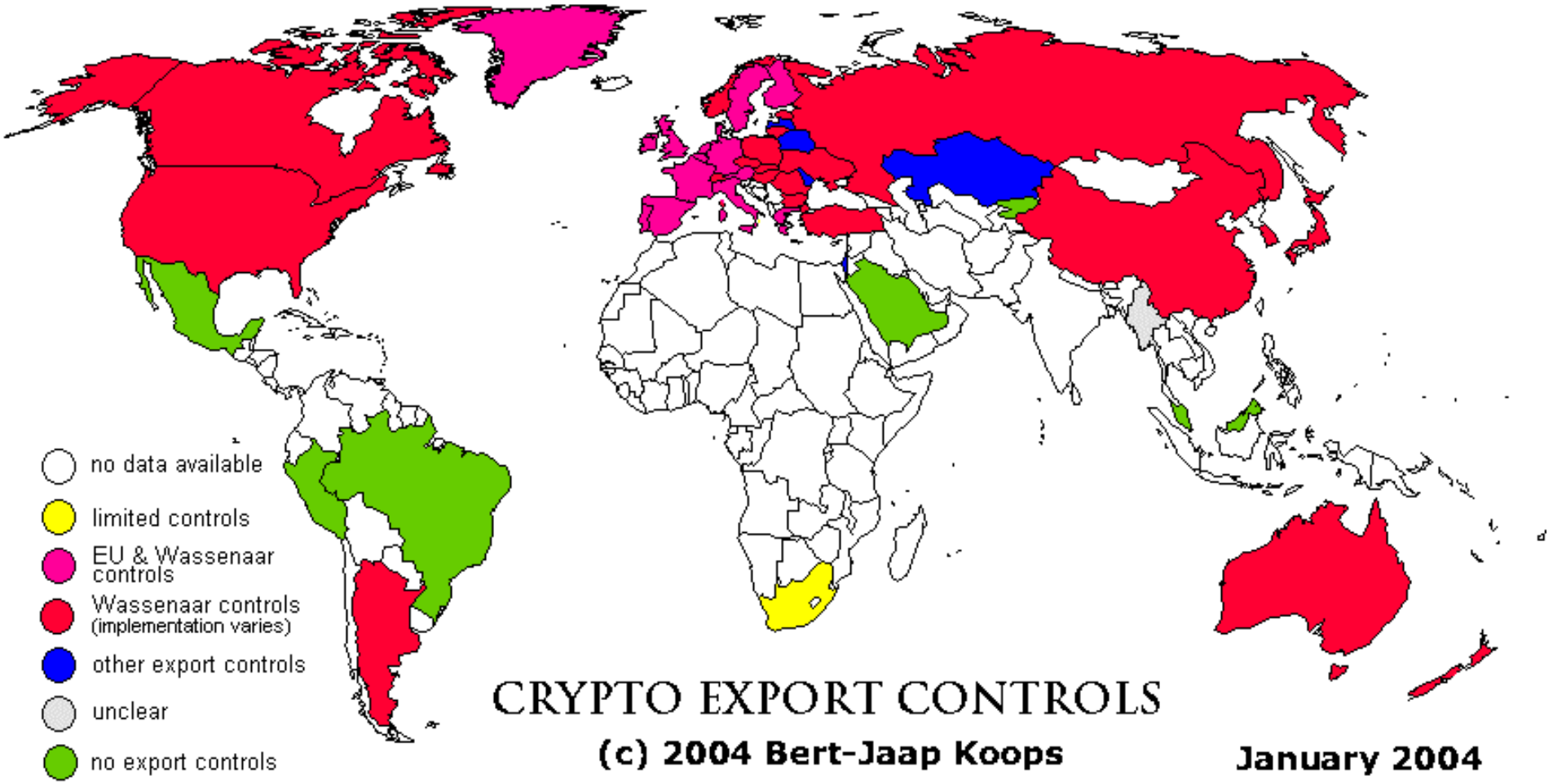
- cryptlib www.cryptlib.com
- nCiphers www.ncipher.com
- RSA BSAFE www.rsasecurity.com

.NET – standardowa biblioteka `System.Security.Cryptography`

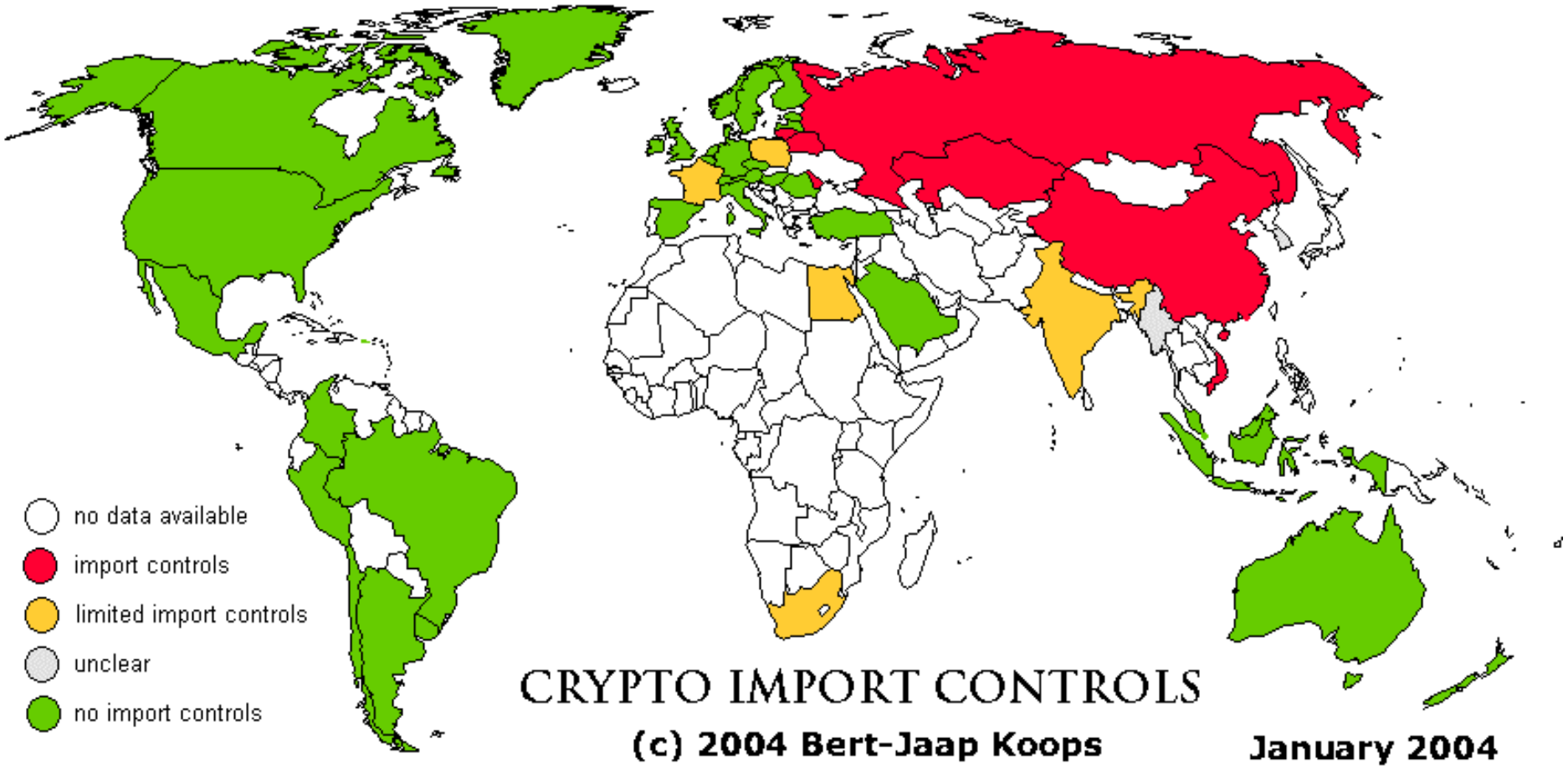
Obwarowania prawne



Obwarowania prawne



Obwarowania prawne



Obwarowania prawne

Polska

- eksport ograniczony przez COCOM (*Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*), jak w całej UE:

  - free for export are: all symmetric crypto products of up to 56 bits, all asymmetric crypto products of up to 512 bits, and all subgroup-based crypto products (including elliptic curve) of up to 112 bits;
  - mass-market symmetric crypto software and hardware of up to 64 bits are free for export;
  - the export of products that use encryption to protect intellectual property (such as DVDs) is relaxed;
  - export of all other crypto still requires a license.

- oprogramowanie kryptograficzne public-domain wolne od ograniczeń eksportowych
- co prawda niejasna pozostaje kwestia eksportu drogą elektroniczną (via Internet)
- w grudniu 2000 usunięto klauzulę eksportową 5A2 (limit 64-bit) na produkty użytku powszechnego (mass-market)
- od 1993r. potrzebne jest zezwolenie na import zagranicznych produktów kryptograficznych wykraczających poza listę COCOM (wymaga wyspecyfikowania sposobu i miejsca wykorzystania produktu)

Przyszłość kryptografii ?

1. Zwiększanie mocy obliczeniowej:

- inżynieria biogenetyczna
- procesory kwantowe (www.qubit.org)

2. Silniejsze szyfry:

Szyfry oparte o teorię krzywych eliptycznych (ECC, *Elliptic Curve Cryptography*):

- analog eliptyczny kłódki Masseya-Omury
- analog eliptyczny systemu ElGamala
- przykładowe implementacje: EC DSA

Przyszłość kryptografii ?

Bezpieczne długości kluczy asymetrycznych

rok	długość bitowa	
	algorytmy klasyczne	bazujące na krzywych eliptycznych
2000	952	132
2002	1028	139
2005	1149	147
2010	1369	160
2015	1613	173
2020	1881	188

Steganografia

Ukrywanie informacji wewnątrz większych zbiorów danych

- może być wykorzystane w celu ochrony poufności danych niejawnych a nawet ukrycia faktu ich istnienia
- tworzenie zamaskowanych kanałów komunikacyjnych
- znaki wodne (*watermarking*) wykonywanie podpisów identyfikujących porcje danych (znaki wodne w grafice i strumieniach video) – ochrona praw autorskich

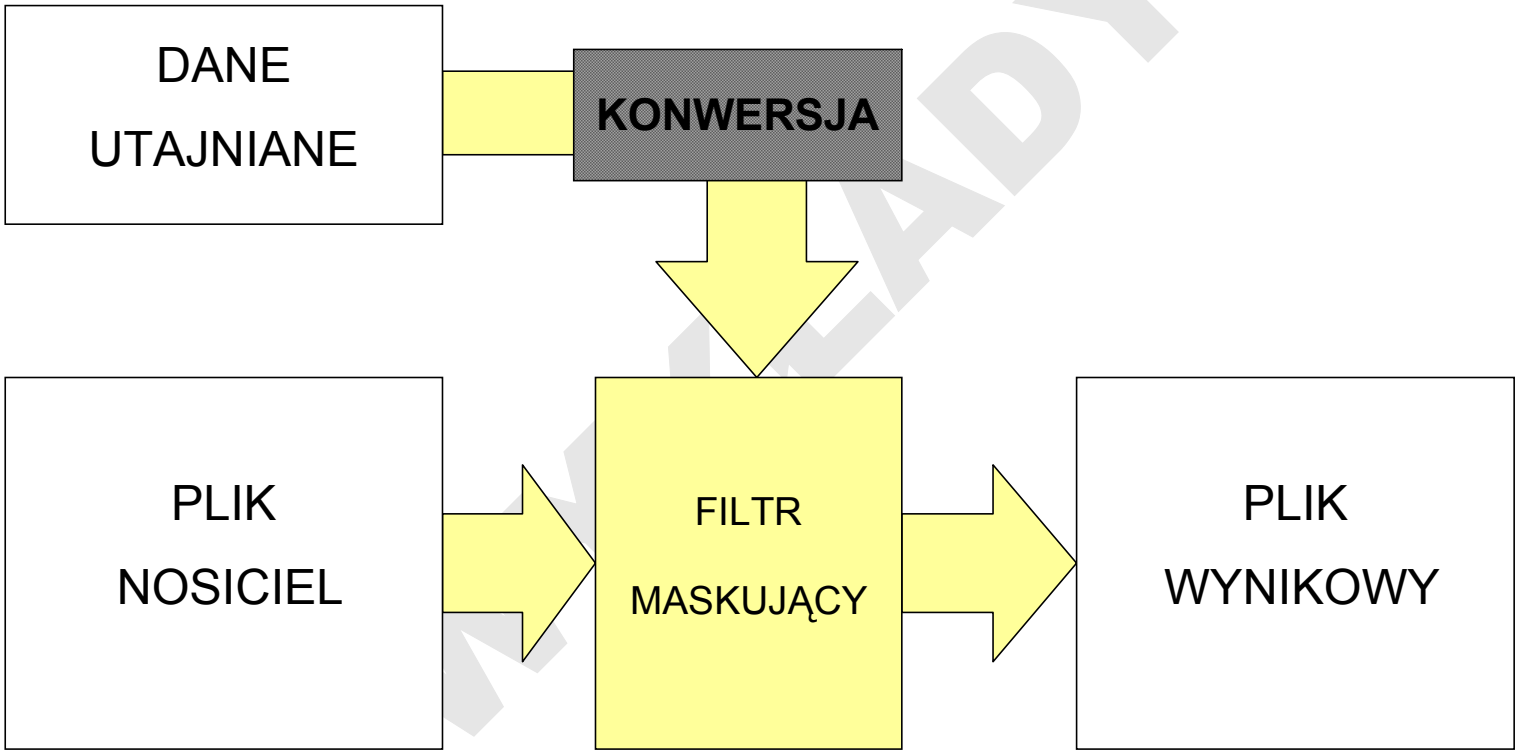
http://www.securityfocus.com/infocus/1684

http://www.jjtc.com/stegdoc/steg1995.html

http://www.cotse.com/tools/stega.htm

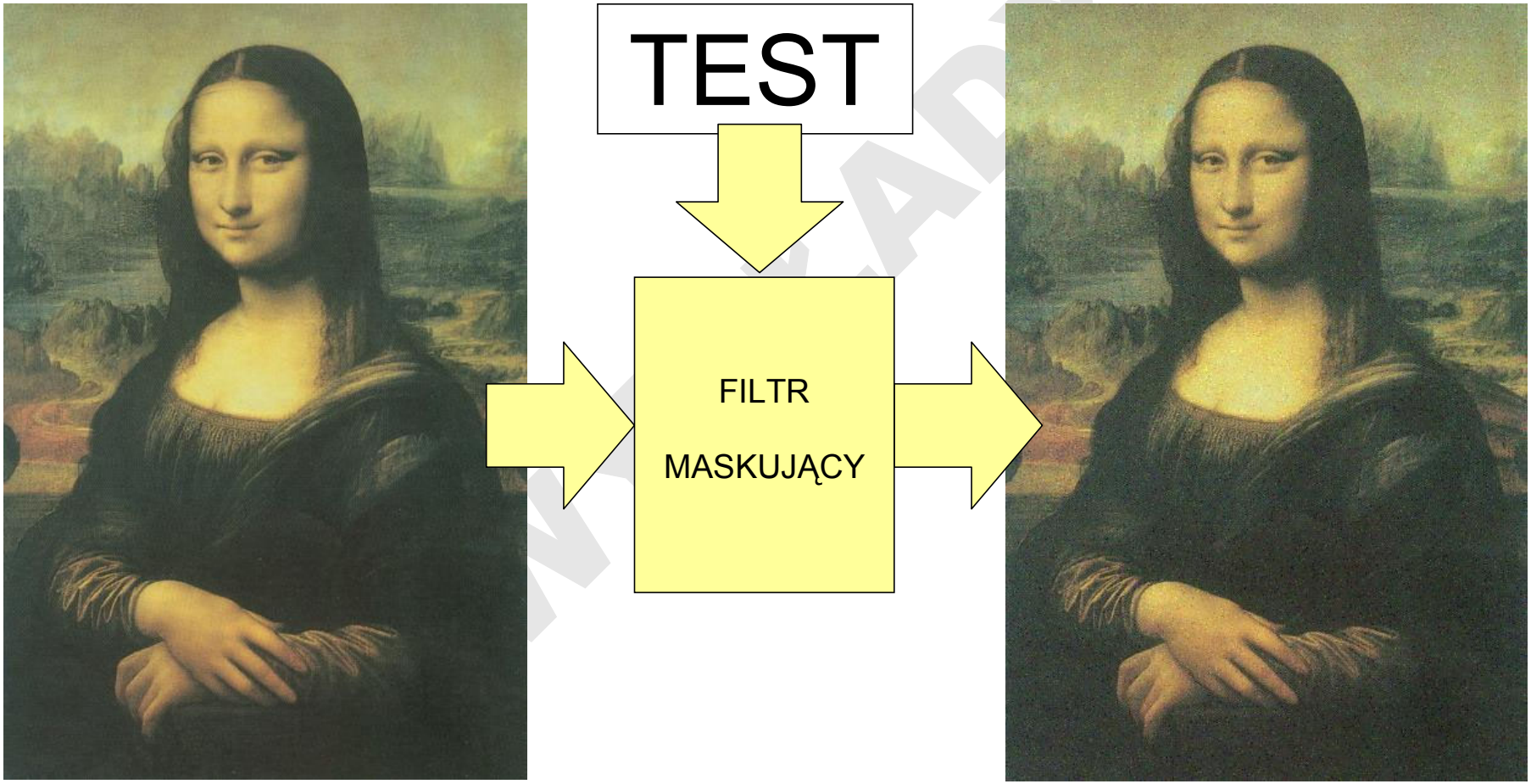
Steganografia

Schemat kodowania



Steganografia

Przykład kodowania (znak wodny)



Steganografia

Przykład dekodowania