Mapa wykładu

- 7.1 Co to jest ochrona informacji?
- 7.2 Zasady działania kryptografii
- 7.3 Uwierzytelnienie
- 7.4 Integralność
- 7.5 Dystrybucja kluczy i certyfikacja
- 7.6 Kontrola dostępu: ściany ogniowe
- 7.7 Ataki i środki zaradcze
- 7.8 Wykrywanie włamań i cyfrowa kryminalistyka
- 7.9 Ochrona informacji w wielu warstwach

Podpisy cyfrowe

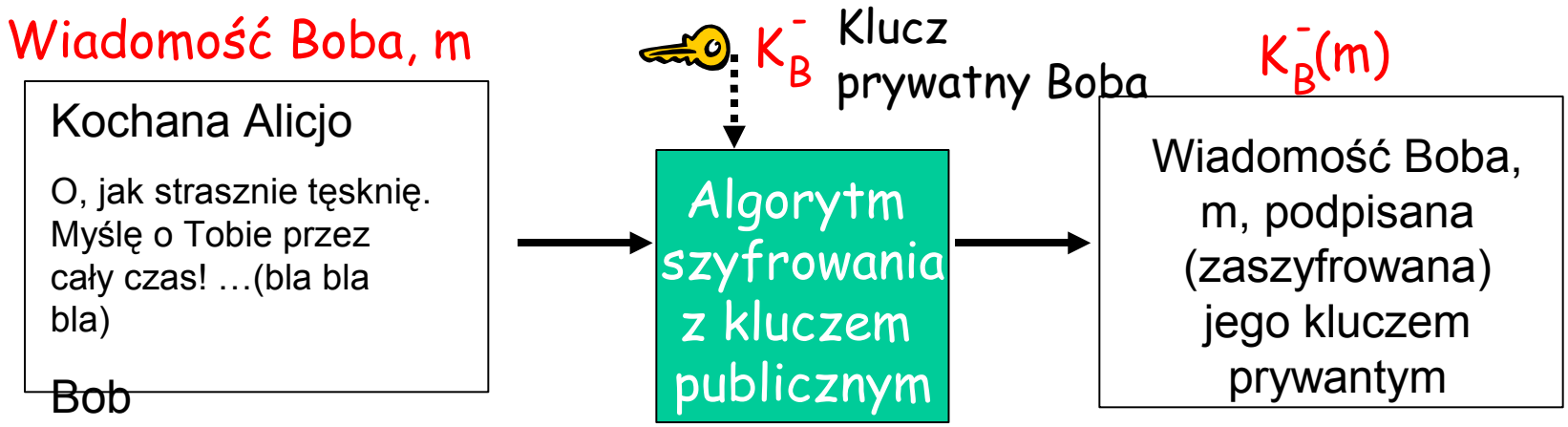
Technika kryptograficzna analogiczna do podpisów odręcznych.

- nadawca (Bob) podpisuje dokument cyfrowo, twierdząc że jest właścicielem/twórcą dokumentu.
- weryfikacja, zabezpieczenie przed fałszerstwem: odbiorca (Alicja) może udowodnić komuś, że Bob, i nikt inny (również sama Alicja), podpisał dokument

Podpisy cyfrowe

Prosty podpis cyfrowy dla wiadomości m:

- Bob podpisuje m przez zaszyfrowanie wiadomości z pomocą swojego klucza ***prywatnego*** K_B^-, tworząc "podpisaną" wiadomość, $K_B^-(m)$



Podpisy cyfrowe (cd)

- Załóżmy, że Alicja otrzymuje wiadomość m, podpis cyfrowy $K_B^-(m)$
- Alicja sprawdza m podpisaną przez Boba przez użycie klucza publicznego Boba K_B^+ do $K_B^+(m)$ i sprawdzenie, czy $K_B^+(K_B^-(m)) = m$.
- Jeśli $K_B^+(K_B^-(m)) = m$, to osoba, która podpisywała m, musiała użyć klucza prywatnego Boba.

Alicja sprawdza, że:

- Bob podpisał m.
- Nikt inny nie podpisał m.
- Bob podpisał m, a nie m'.

Niezaprzeczalność:

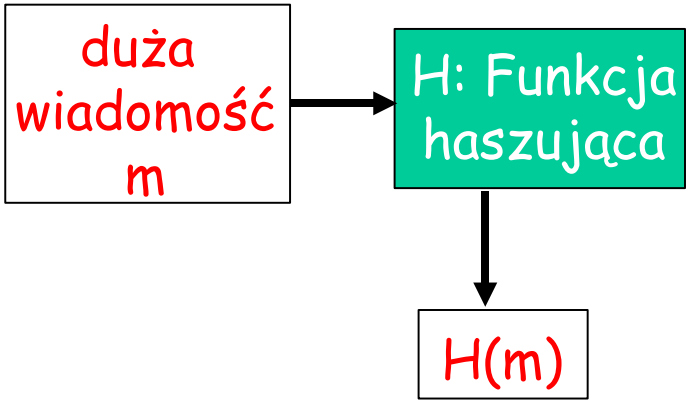
- ✓ Alicja może wziąć m, oraz podpis $K_B^-(m)$ do sądu i udowodnić, że Bob podpisał m.

Skróty wiadomości

Szyfrowanie długich wiadomości w kryptografii klucza publicznego jest drogie obliczeniowo

Cel: prostu do obliczenia, cyfrowy skrót wiadomości

- zastosuj funkcję haszującą H do *m*, uzyskując skrót wiadomości o ustalonej długości, *H(m)*.



Własności funkcji haszujących:

- nie są różnowartościowe
- tworzą skróty ustalonej długości
- mając dany skrót x, znalezienie m takiego, że x = H(m), jest bardzo trudne obliczeniowo

Internetowa suma kontrolna: słaba funkcja haszująca

Internetowa suma kontrolna ma niektóre własności funkcji haszującej:

- tworzy skróty ustalonej długości (16-bitowe)
- nie jest różnowartościowa

Jednak znając wiadomość i jej skrót, łatwo jest znaleźć inną wiadomość o tym samym skrócie:

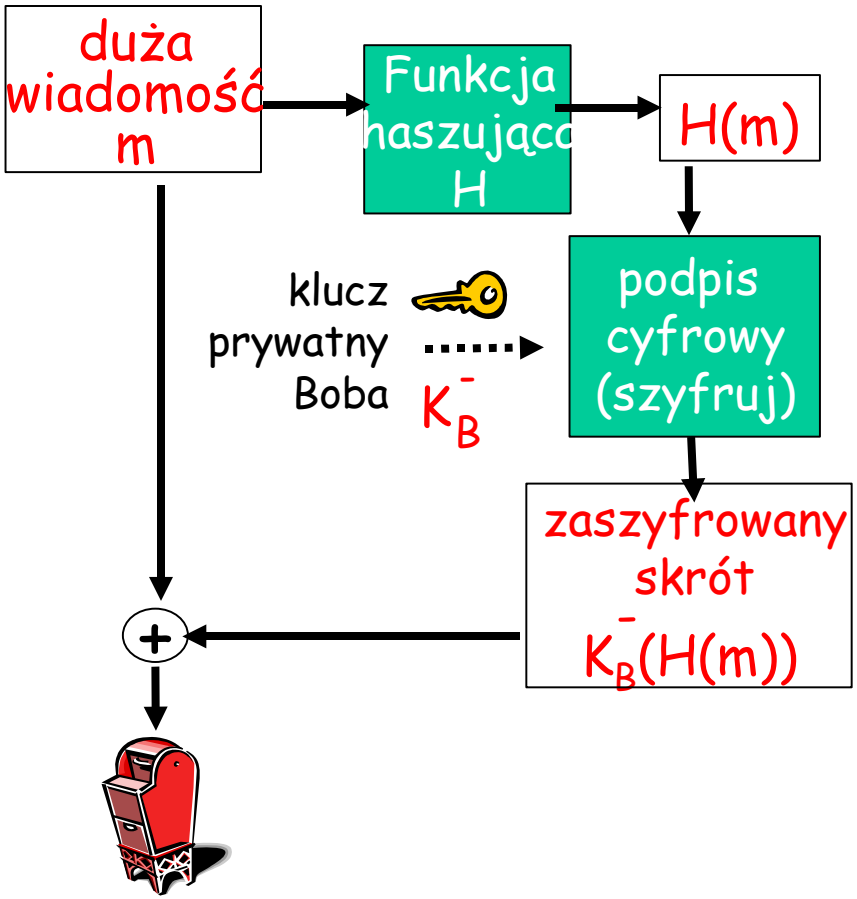
wiadomość	format ASCII
I O U 1	49 4F 55 31
0 0 . 9	30 30 2E 39
9 B O B	39 42 D2 42
	B2 C1 D2 AC

wiadomość	format ASCII
I O U 9	49 4F 55 39
0 0 . 1	30 30 2E 31
9 B O B	39 42 D2 42
	B2 C1 D2 AC

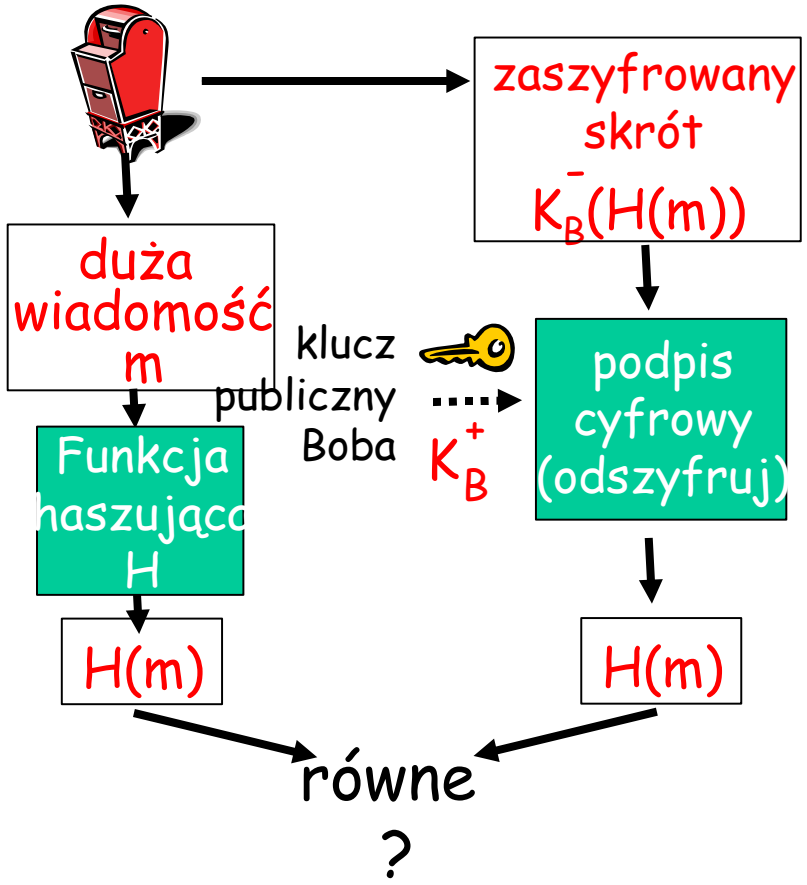
różne wiadomości
lecz identyczne skróty!

Podpis cyfrowy = podpisany skrót wiadomości

Bob wysyła wiadomość podpisaną cyfrowo:



Alicja sprawdza podpis o integralność podpisanej wiadomości:



Algorytmy funkcji haszujących

- Szeroko używana funkcja MD5 (RFC 1321)
  - oblicza 128-bitowy skrót wiadomości w czterostopniowym procesie.
  - mając dowolny 128-bitowy ciąg x, trudno jest skonstruować wiadomość m której hasz MD5 jest równy x.
- SHA-1 także jest używany.
  - Standard amerykański [NIST, FIPS PUB 180-1]
  - skrót 160-bitowy

Mapa wykładu

- 7.1 Co to jest ochrona informacji?
- 7.2 Zasady działania kryptografii
- 7.3 Uwierzytelnienie
- 7.4 Integralność
- 7.5 Dystrybucja kluczy i certyfikacja
- 7.6 Kontrola dostępu: ściany ogniowe
- 7.7 Ataki i środki zaradcze
- 7.8 Wykrywanie włamań i cyfrowa kryminalistyka
- 7.9 Ochrona informacji w wielu warstwach

Zaufani pośrednicy

Dystrybucja kluczy symetrycznych:

- Jak dwie jednostki mają uzgodnić tajny klucz w sieci?

Rozwiązanie:

- zaufane centrum dystrybucji kluczy (CDK) działające jako pośrednik pomiędzy jednostkami

Dystrybucja kluczy publicznych:

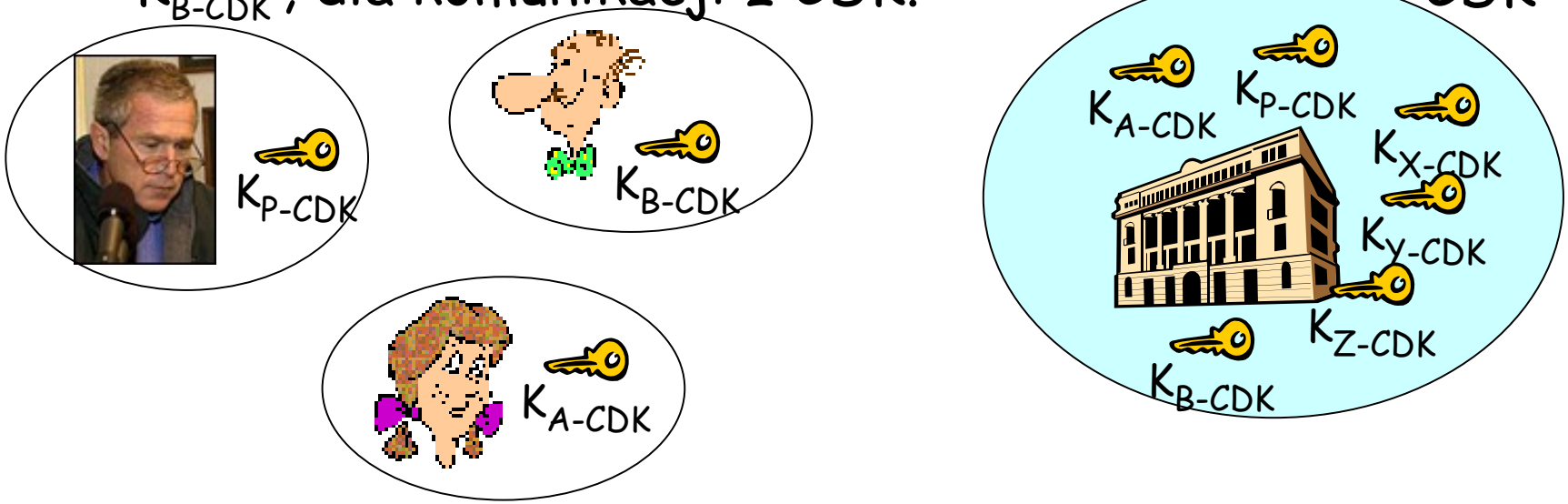
- Gdy Alicja otrzymuje klucz publiczny Boba (ze strony WWW, przez e-mail, dyskietkę), to skąd wie, że jest to klucz Boba, a nie klucz Trudy?

Rozwiązanie:

- zaufane centrum certyfikatów (ang. *Certificate Authority*, CC)

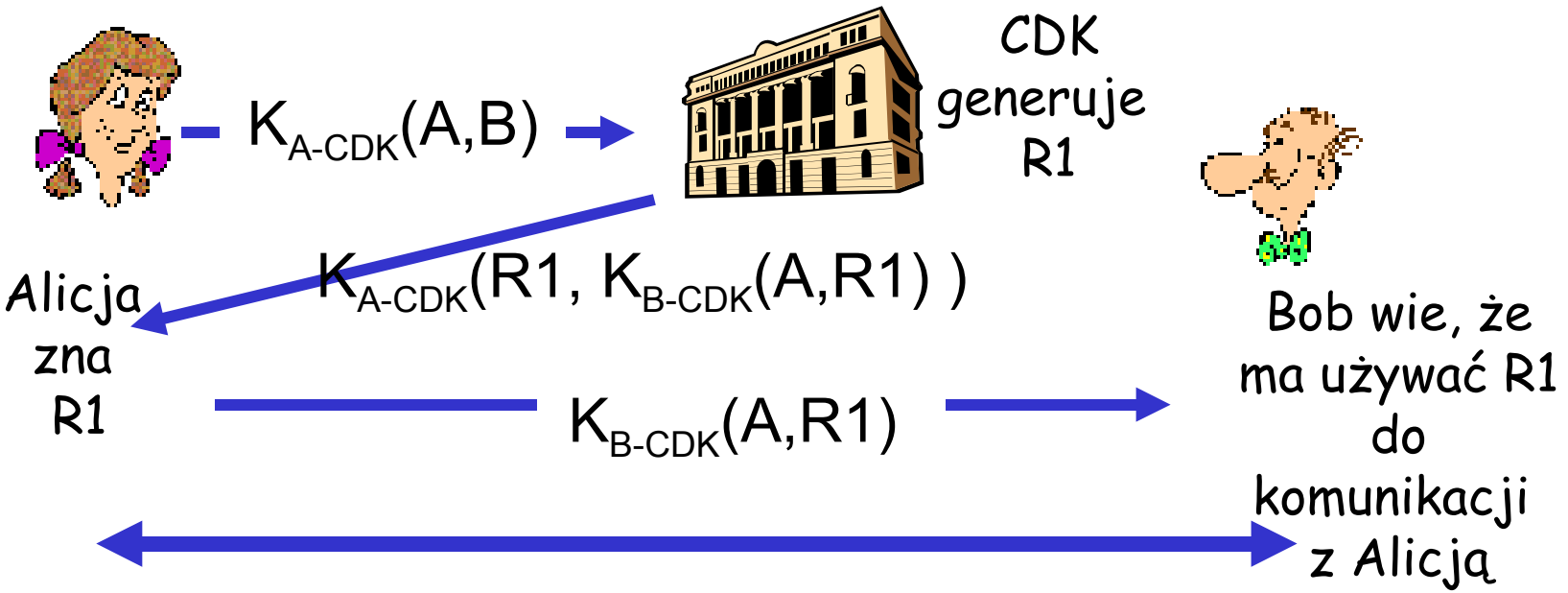
Centrum Dystrybucji Kluczy (CDK)

- Alicja i Bob potrzebują wspólnego symetrycznego klucza.
- CDK: serwer ma wspólny klucz symetryczne z *każdym* zarejestrowanym użytkownikiem (wielu użytkowników)
- Alicja, Bob znają swoje klucze symetryczne, $K_{A\text{-}CDK}$ i $K_{B\text{-}CDK}$, dla komunikacji z CDK.



Centrum Dystrybucji Kluczy (CDK)

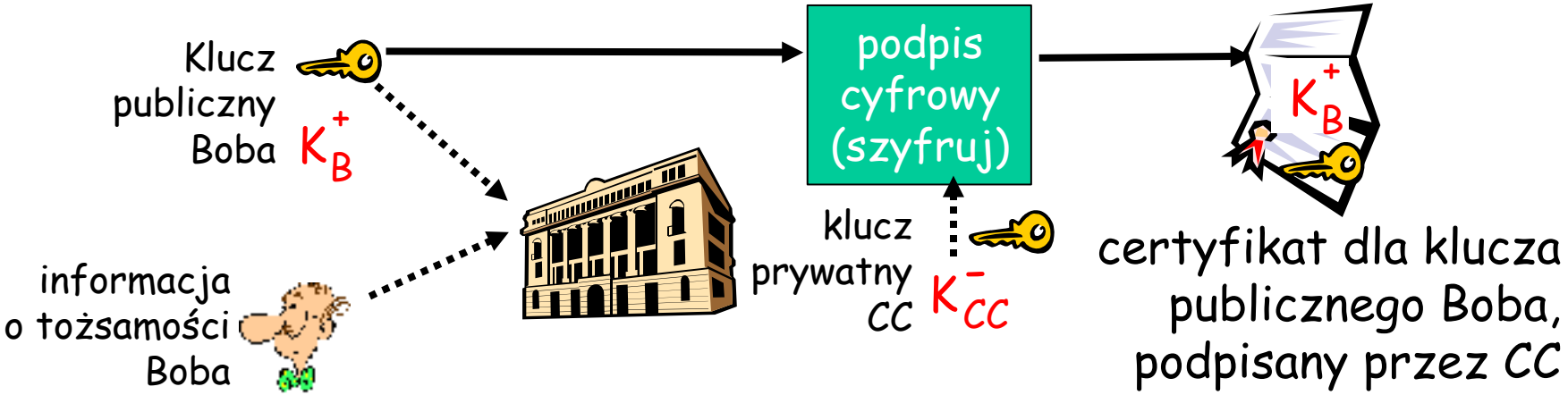
P: W jaki sposób CDK pozwala Bobowi i Alicji ustalić klucz symetryczny dla komunikacji między sobą?



Alicja i Bob komunikują się: używają R1 jako *klucza sesji* dla szyfru z kluczem symetrycznym

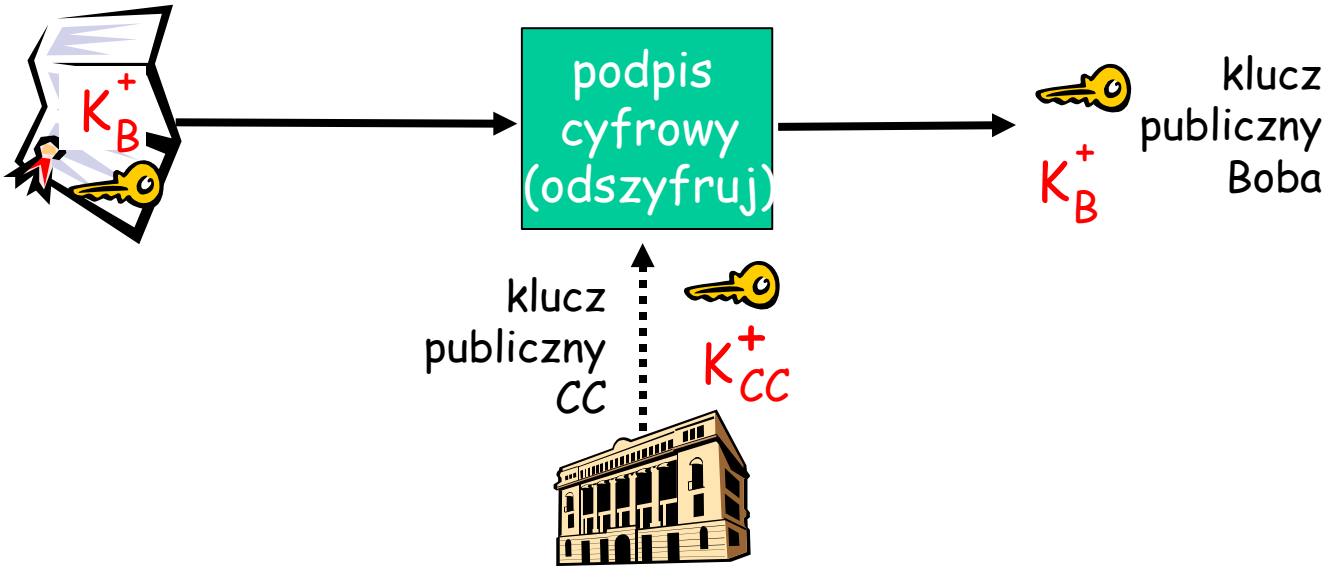
Centra Certyfikatów

- Centrum Certyfikatów (CC): wiąże klucz publiczny z tożsamością jednostki E.
- E (osoba, ruter) rejestruje swój klucz publiczny u CC.
  - E udostępnia "dowód tożsamości" dla CC.
  - CC tworzy certyfikat wiążący tożsamość E z kluczem publicznym.
  - certyfikat, zawierający klucz publiczny E, zostaje cyfrowo podpisany przez CC – CC stwierdza "to jest klucz publiczny E"



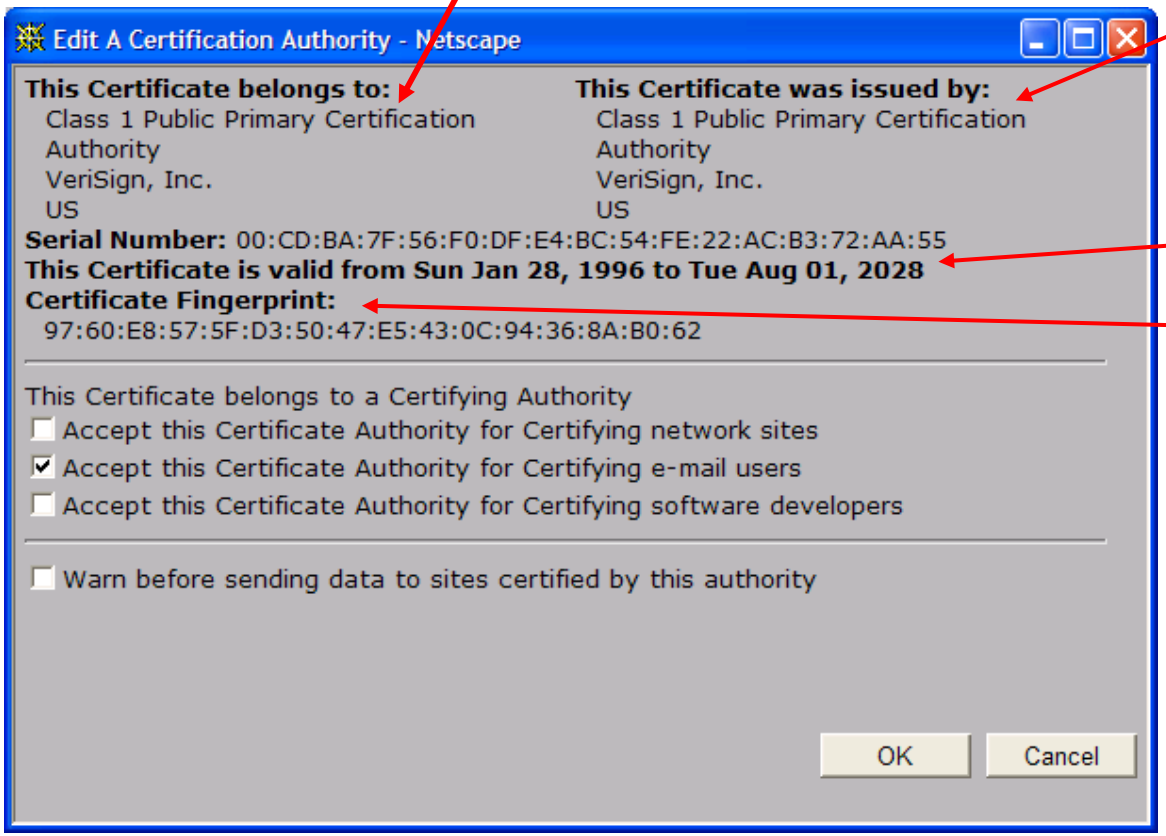
Centra Certyfikatów

- Kiedy Alicja potrzebuje klucza publicznego Boba:
  - bierze certyfikat Boba (od Boba lub skądinąd).
  - używa klucza publicznego *CC*, uzyskuje klucz publiczny Boba



Certyfikat zawiera:

- Numer seryjny (niepowtarzalny u nadawcy)
- informacja o właścicielu certyfikatu, oraz o algorytmach szyfrowania i skrótu, a także wartość klucza (nie pokazana)



- informacja o wydawcy certyfikatu (CC)
- daty ważności
- podpis cyfrowy wydawcy

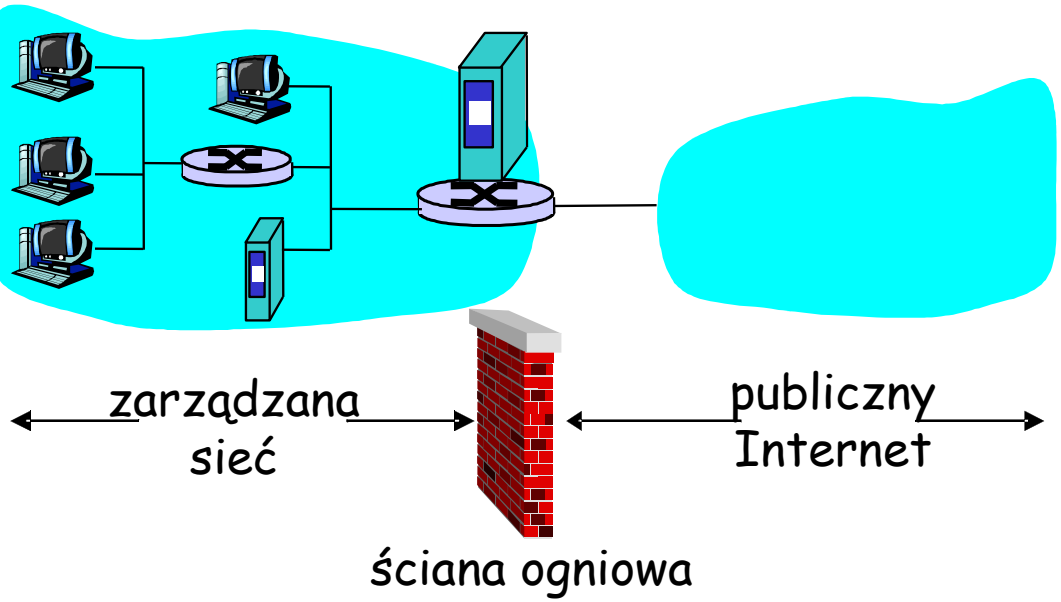
Mapa wykładu

- 7.1 Co to jest ochrona informacji?
- 7.2 Zasady działania kryptografii
- 7.3 Uwierzytelnienie
- 7.4 Integralność
- 7.5 Dystrybucja kluczy i certyfikacja
- 7.6 Kontrola dostępu: ściany ogniowe
- 7.7 Ataki i środki zaradcze
- 7.8 Wykrywanie włamań i cyfrowa kryminalistyka
- 7.9 Ochrona informacji w wielu warstwach

Ściany ogniowe

ściana ogniowa

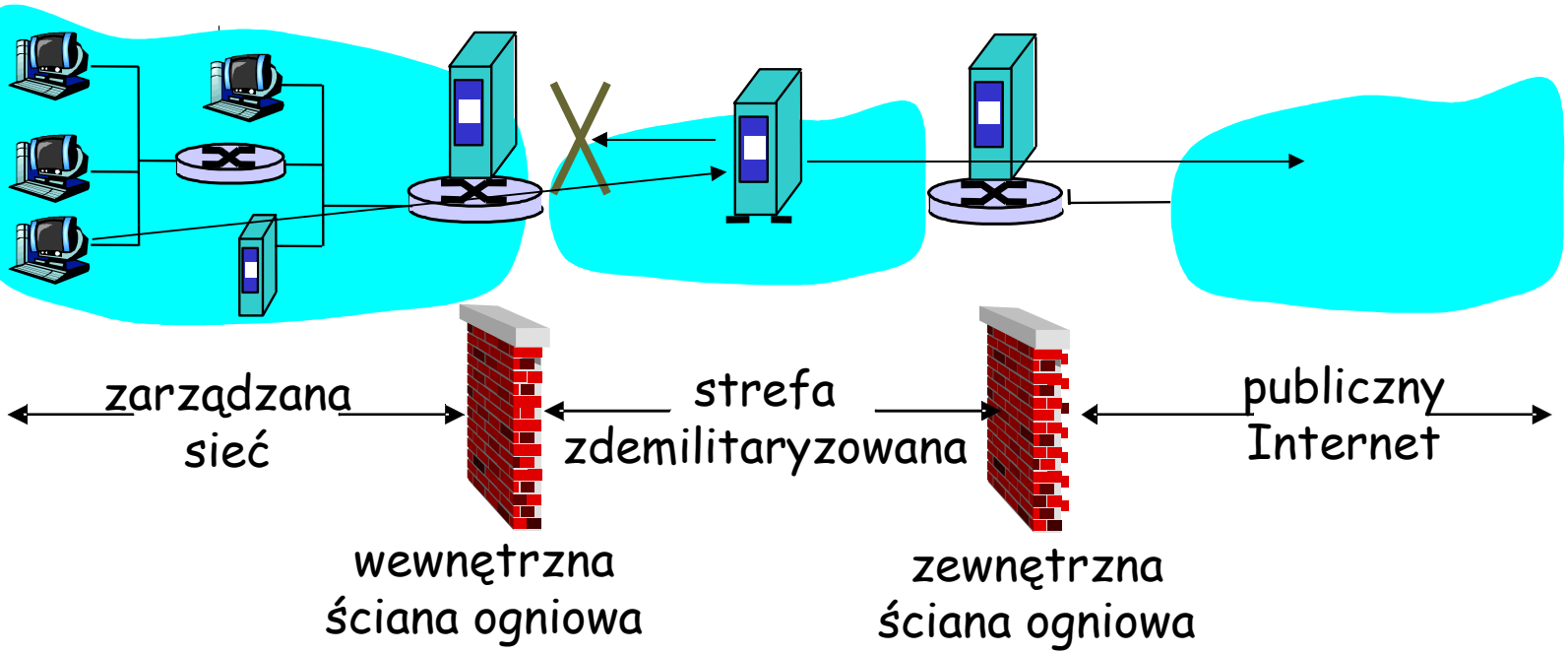
(ang. *firewall*) izoluje wewnętrzną sieć organizacji od Internetu, pozwalając na niektóre rodzaje komunikacji, a blokując inne.



Strefy zdemilitaryzowane

strefa zdemilitaryzowana

(ang. *Demilitarized Zone*) część sieci pomiędzy wewnętrzną siecią a publicznym Internetem, chroniona ścianą ogniową, w której mogą się znajdować serwery proxy.



Ściany ogniowe: Dlaczego

zapobiegają atakom DoS:

- zalew SYN (ang. *SYN flooding*): napastnik otwiera wiele fałszywych połączeń TCP, nie starcza zasobów dla "prawdziwych" połączeń.

zapobieganie nielegalnym modyfikacjom/dostępowi do danych.

- n.p., napastnik zastępuje stronę domową banku przez inną stronę

pozwolić tylko na uprawniony dostęp do wewnętrznej sieci (zbiorowi uwierzytelnionych użytkowników/hostów)

dwa rodzaje ścian ogniowych:

- w warstwie aplikacji
- w warstwie sieci (filtry pakietów)

Filtrowanie pakietów

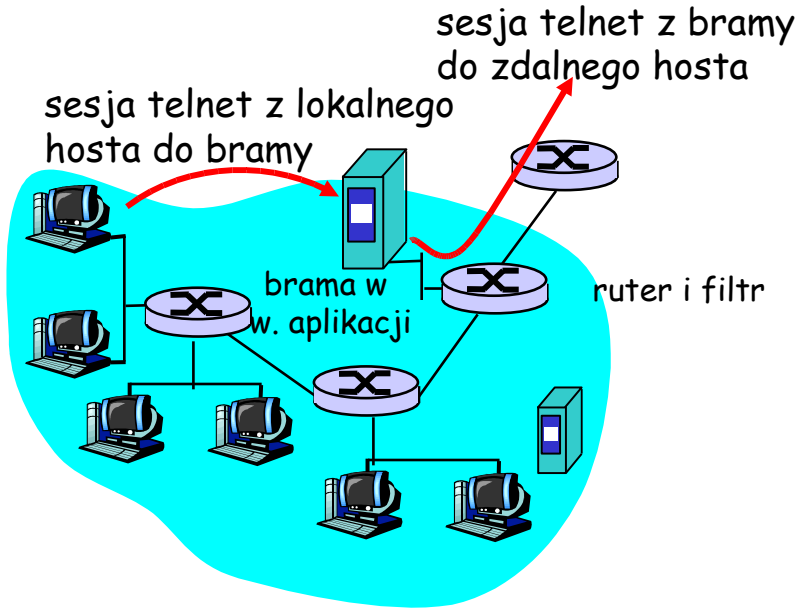
- wewnętrzna sieć jest połączona przez ścianę ogniową zintegrowaną z ruterem
- ruter filtruje pakiety, decyduje o przekazaniu/zatrzymaniu pakietu w oparciu o (m.in):
  - adres IP źródła, adres IP celu
  - numery portów TCP/UDP źródła i celu
  - typ komunikatu ICMP
  - bity SYN, ACK segmentu TCP

Filtrowanie pakietów

- Przykład 1: blokuj pakiety z polem protokołu w pakiecie IP = 17 i z portem celu lub źródła = 23.
  - wszystkie przychodzące lub wychodzące pakiety UDP oraz wszystkie połączenia telnet zostaną zablokowane.
- Przykład 2: Blokuj przychodzące segmenty TCP z ACK=0.
  - Uniemożliwia zewnętrznym hostom otwieranie połączeń TCP do wewnętrznych hostów, ale pozwala wewnętrznym hostom tworzyć połączenia TCP na zewnątrz.

Bramy w wstie aplikacji

- Analizuje dane aplikacji oprócz nagłówków IP/TCP/UDP.
- Przykład: pozwól wybranym użytkownikom wewnętrznym na telnet na zewnątrz.



1. Wszyscy użytkownicy telnet muszą przejść przez bramę.
2. Dla uprawnionych użytkowników, brama otwiera sesję telnet do celu. Brama przekazuje dane między dwoma połączeniami
3. Filtrujący ruter blokuje wszystkie sesje telnet nie nawiązane przez bramę.

Ograniczenia ścian ogniowych

- IP spoofing: ruter nie może wiedzieć, czy dane "rzeczywiście" pochodzą z podanego źródła
- jeśli wiele aplikacji potrzebuje specjalnego traktowania, każda musi mieć własną bramę.
- oprogramowanie klienta musi wiedzieć, jak współpracować z bramą.
  - n.p., adres IP pośrednika musi być podany w przeglądarce WWW
- filtry często używają polityki "wszystko albo nic" dla UDP.
- wymiana: stopień swobody komunikacji ze światem, poziom bezpieczeństwa
- wiele bardzo chronionych hostów nadal podlega atakom.

Mapa wykładu

- 7.1 Co to jest ochrona informacji?
- 7.2 Zasady działania kryptografii
- 7.3 Uwierzytelnienie
- 7.4 Integralność
- 7.5 Dystrybucja kluczy i certyfikacja
- 7.6 Kontrola dostępu: ściany ogniowe
- 7.7 Ataki i środki zaradcze
- 7.8 Wykrywanie włamań i cyfrowa kryminalistyka
- 7.9 Ochrona informacji w wielu warstwach

Zagrożenia bezpieczeństwa w Internecie

Mapowanie:

- przed atakiem: sprawdzenie, jakie usługi są udostępniane w sieci
- Używa się `ping` do stwierdzenia, jakie adresy mają hosty w sieci
- Skanowanie portów: próba nawiązania połączenia TCP na każdy port (sprawdzenie reakcji)
- program mapujący *nmap* (http://www.insecure.org/nmap/) : "network exploration and security auditing"

Środki zaradcze?

Zagrożenia bezpieczeństwa w Internecie

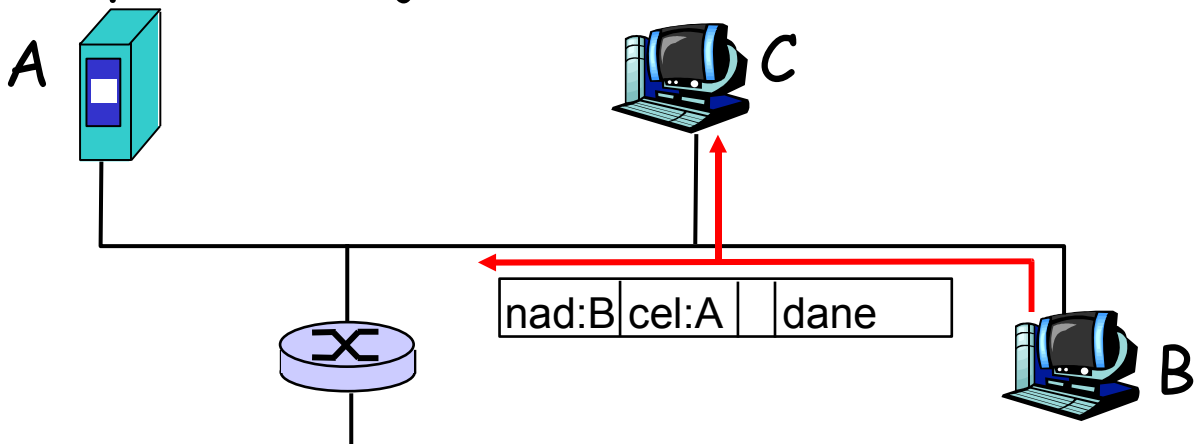
Mapowanie: środki zaradcze

- prowadzenie dzienników informacji wysyłanych do sieci
- poszukiwanie podejrzanej aktywności (wzorców skanowania adresów IP, portów)
- modyfikacja reguł filtrów w celu blokowania skanowania za pomocą reguł stanowych filtrów

Zagrożenia bezpieczeństwa w Internecie

Podsłuch pakietów:

- media rozgłaszające
- karta NIC w trybie odbierania (*promiscuous*) czyta wszystkie ramki
- może przeczytać wszystkie niezaszyfrowane informacje (n.p. hasła)
- n.p.: C podsłuchuje ramki B

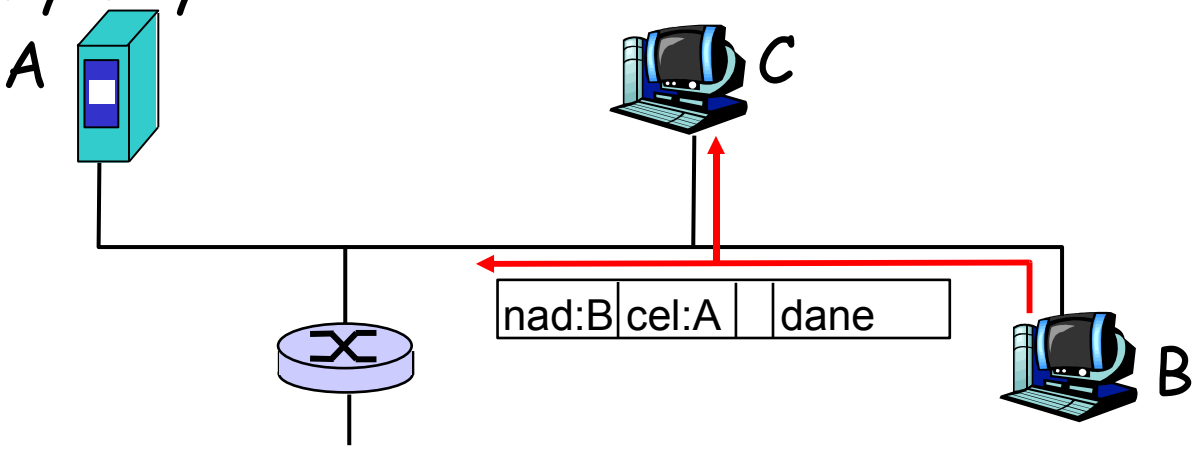


Środki zaradcze?

Zagrożenia bezpieczeństwa w Internecie

Podsłuch: środki zaradcze w w. łącza

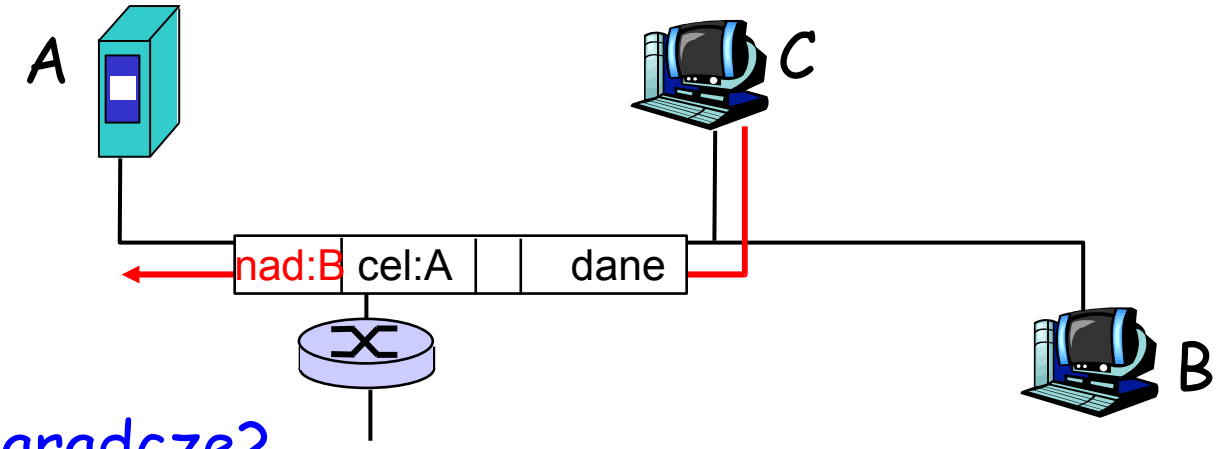
- na wszystkich hostach w organizacji działa oprogramowanie, które sprawdza, czy karta jest w trybie odbierania.
- po jednym hoście w każdym segmencie z medium rozgłaszającym (przełącznik Ethernet w centrum gwiazdy)
- kontrola dostępu do sieci przy pomocy adresów fizycznych



Zagrożenia bezpieczeństwa w Internecie

Podszywanie się (*spoofing*):

- aplikacja może tworzyć "surowe" pakiety IP, umieszczając dowolną wartość w adresie IP nadawcy
- odbiorca nie może sprawdzić, czy adres został zmieniony
- n.p.: C podszywa się pod B

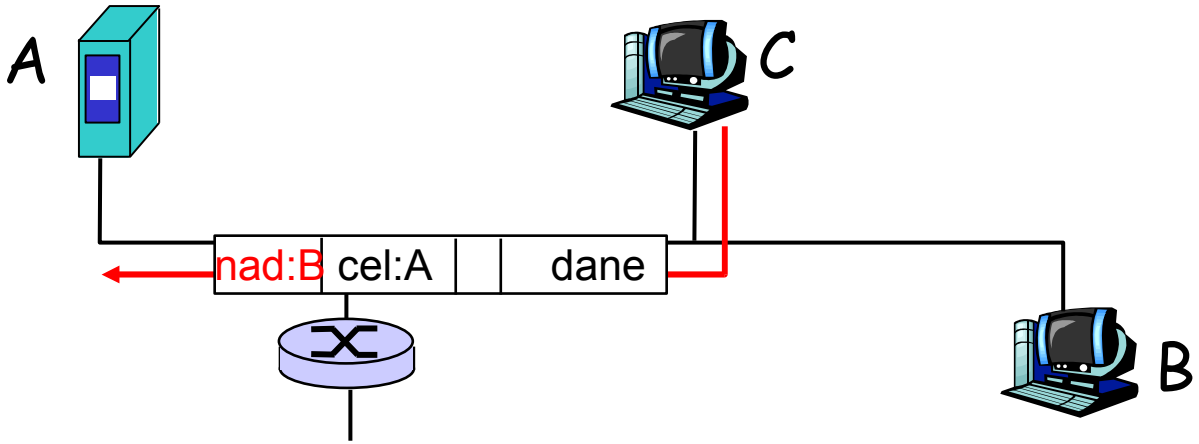


Środki zaradcze?

Zagrożenia bezpieczeństwa w Internecie

Podszywanie się: filtrowany dostęp

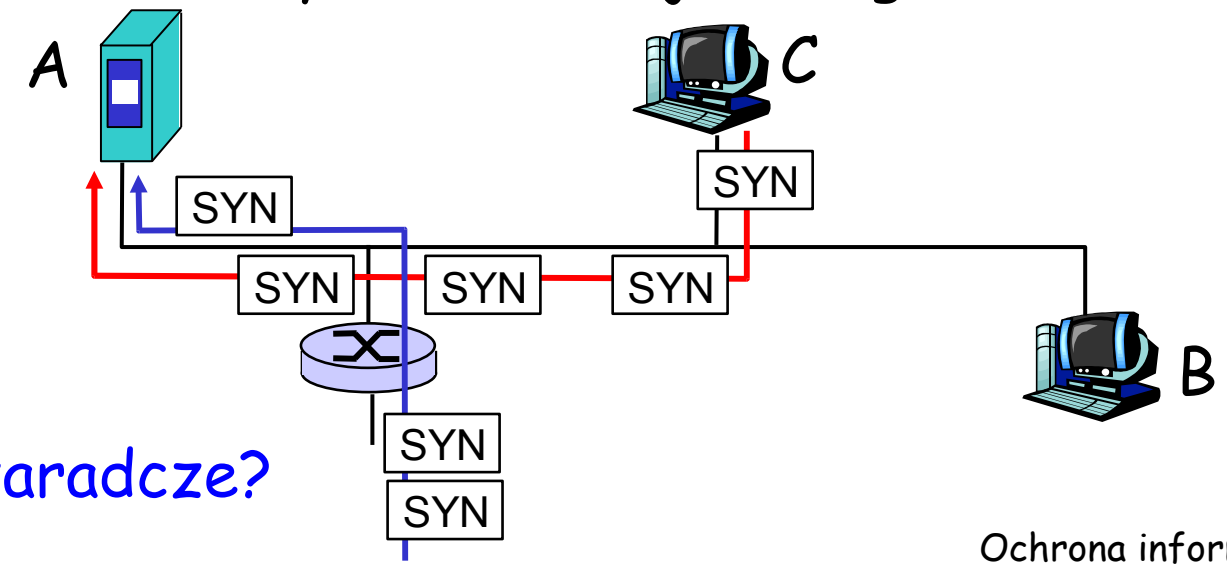
- rutery nie powinny przekazywać pakietów z niewłaściwymi adresami nadawcy (n.p., adres nadawcy pakietu nie jest w podsieci rutera)
- świetnie, ale filtrowany dostęp nie może być wymuszony we wszystkich sieciach



Zagrożenia bezpieczeństwa w Internecie

Zablokowanie usług (ang. *Denial of service*, DOS):

- zalew złośliwie wygenerowanych pakietów "zatapia" odbiorcę
- *Distributed DOS* (DDOS): wiele skoordynowanych źródeł zalewa odbiorcę
- n.p., C i zdalny host atakują A segmentami SYN

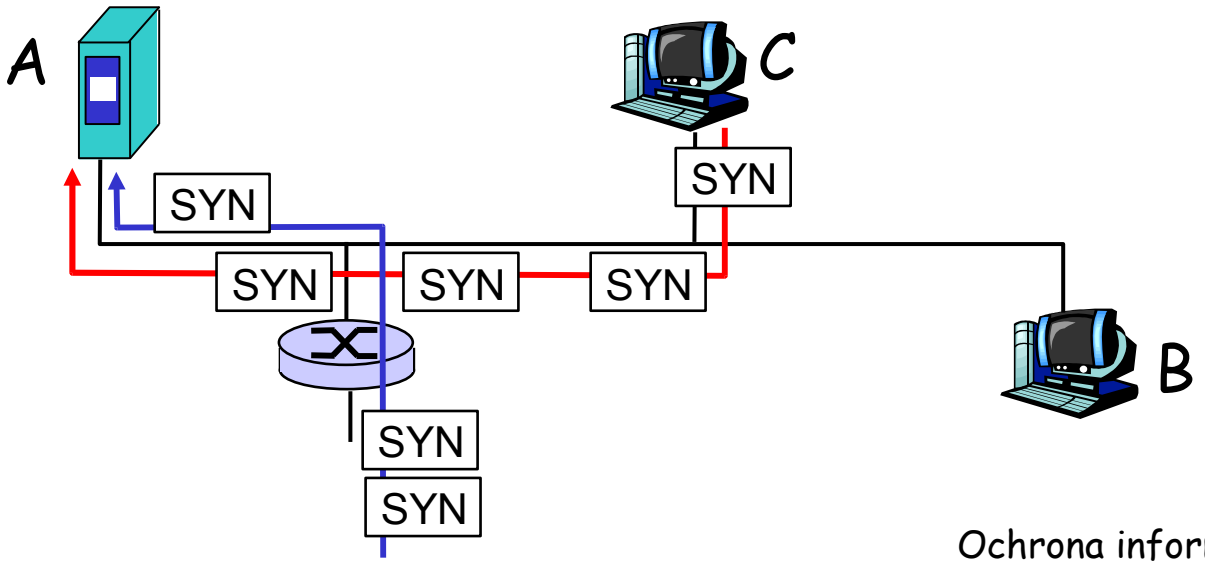


Środki zaradcze?

Zagrożenia bezpieczeństwa w Internecie

Denial of service (DOS): środki zaradcze

- odfiltrowanie zalewających pakietów poprzez reguły stanowe: może wyrzucać dobre pakiety razem ze złymi
- traceback do nadawcy pakietów (najprawdopodobniej niewinny host, na który było włamanie)
- łamigłówki, CAPTCHA



Wykrywanie włamań

Czasami nie da się zapobiegać: trzeba umieć wykryć chorobę i ją wyleczyć!

- ściana ogniowa zapobiega atakom
- jednak wiele ataków przeprowadza się od wewnątrz
  - połączenia modemowe
  - złośliwi pracownicy
  - konie trojańskie, wirusy
- Systemy wykrywania włamań (*Intrusion Detection Systems*, IDS): wykrywają zdarzenia, które świadczą o wystąpieniu włamania do sieci
  - modyfikacje systemu plików
  - niedozwolony ruch w sieci

Cyfrowa kryminalistyka

Metody gromadzenia dowodów przestępstwa

- wykrycie włamania
- odtworzenie przebiegu
- próba identyfikacji napastnika

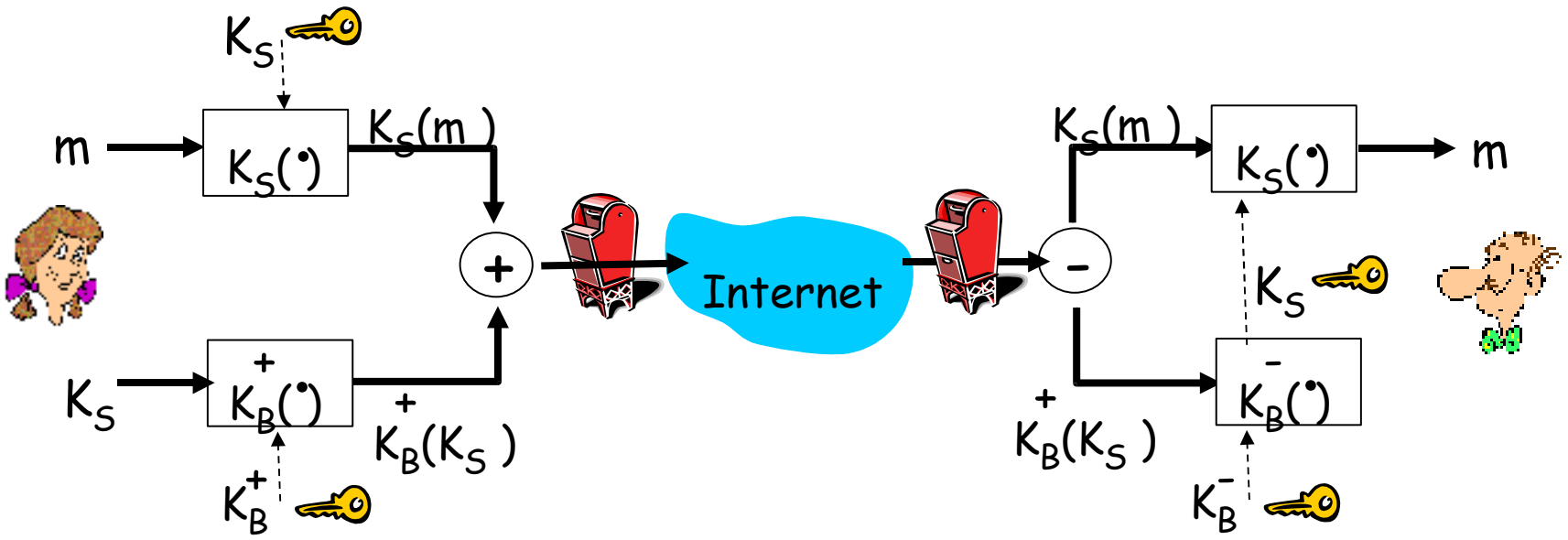
- Rola regulacji prawnych
  - gromadzenie obowiązkowych informacji przez operatorów sieci
  - udostępnianie informacji na żądanie prokuratury

Mapa wykładu

7.1 Co to jest ochrona informacji?
7.2 Zasady działania kryptografii
7.3 Uwierzytelnienie
7.4 Integralność
7.5 Dystrybucja kluczy i certyfikacja
7.6 Kontrola dostępu: ściany ogniowe
7.7 Ataki i środki zaradcze
7.8 Wykrywanie włamań i cyfrowa kryminalistyka
7.9 Ochrona informacji w wielu warstwach
- 7.8.1. Bezpieczna poczta
- 7.8.2. Bezpieczne gniazda
- 7.8.3. IPsec
- 7.8.4. 802.11 WEP
- 7.8.5. TEMPEST i poufność w warstwie fizycznej

Bezpieczna poczta

- Alicja chce wysłać poufny list, m, do Boba.

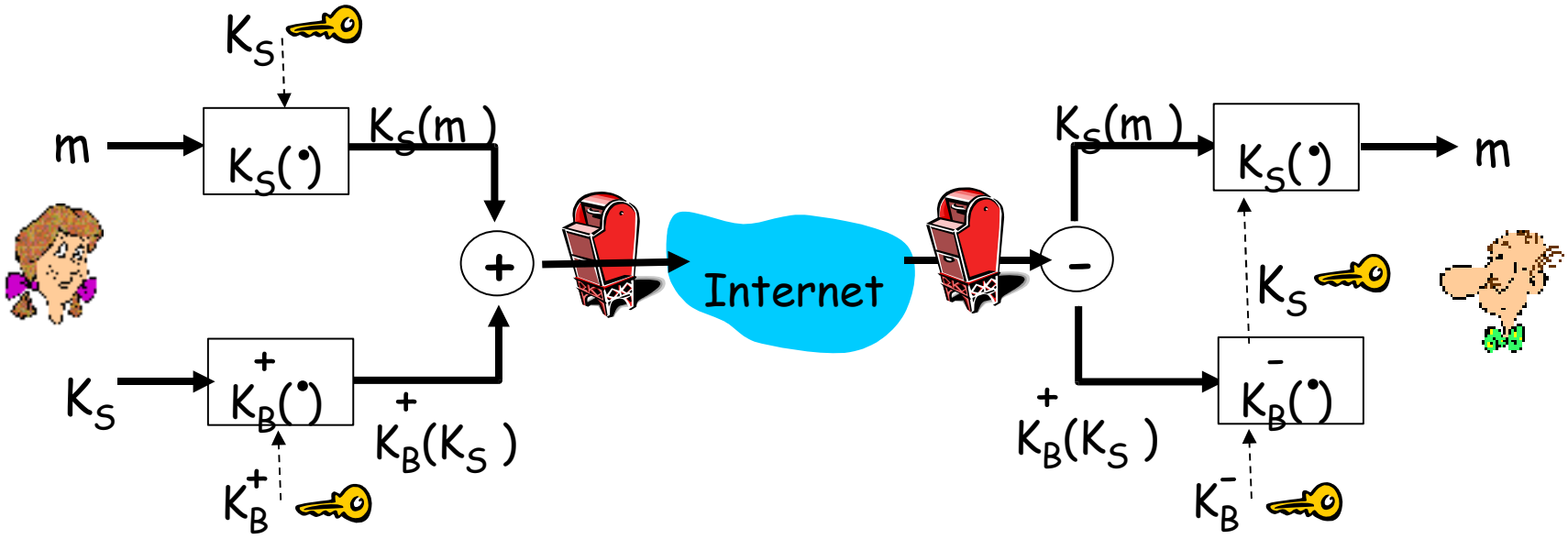


Alicja:

- generuje losowy *symetryczny* klucz prywatny, K_S.
- szyfruje wiadomość kluczem K_S (dla wydajności)
- szyfruje także K_S kluczem publicznym Boba.
- wysyła zarówno $K_S(m)$ jak i $K_B(K_S)$ do Boba.

Bezpieczna poczta

- Alicja chce wysłać poufny list, m, do Boba.

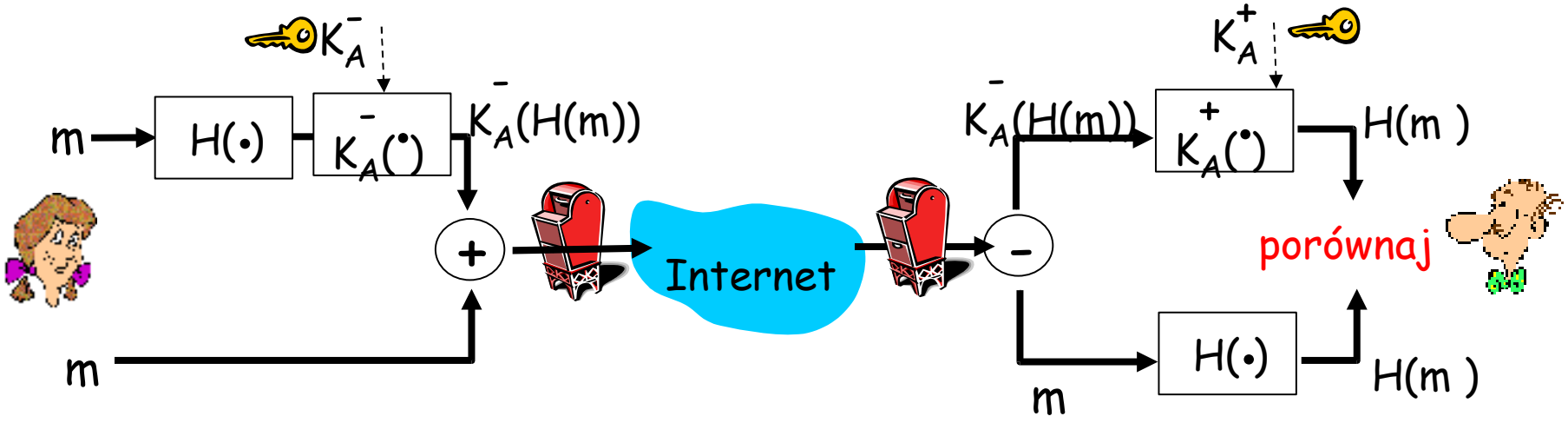


Bob:

- używa swojego prywatnego klucza do odszyfrowania K_S
- używa K_S do odszyfrowania $K_S(m)$ i odzyskania m

Bezpieczna poczta (cd)

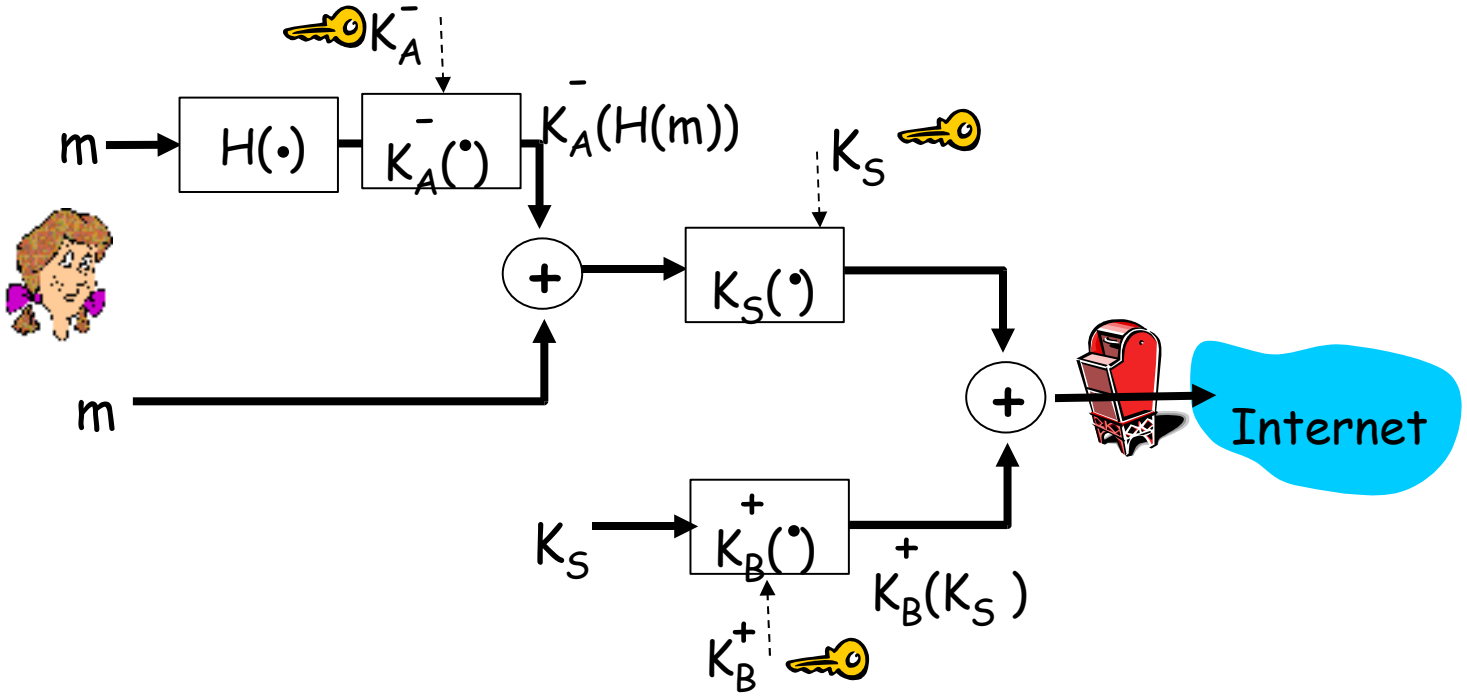
• Alicja chce zapewnić integralność listu i uwierzytelnić się Bobowi.



• Alicja podpisuje list cyfrowo.
• wysyła list (otwartym tekstem) i podpis cyfrowy.

Bezpieczna poczta (cd)

- Alicja chce zapewnić poufność, uwierzytelnienie nadawcy, integralność listu.



Alicja używa trzech kluczy: swojego prywatnego, publicznego Boba, nowego klucza symetrycznego

Pretty good privacy (PGP)

- Mechanizm szyfrowania poczty elektronicznej, standard de-facto.
- używa kryptografii symetrycznej, kryptografii z kluczem publicznym, funkcji haszujących, i podpisów cyfrowych.
- zapewnia poufność, uwierzytelnienie nadawcy, integralność.
- wynalazca, Phil Zimmerman, był obiektem śledztwa w USA przez 3 lata.

Wiadomość podpisana przez PGP:

```
---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1

Kochany Bobie: Mój mąż wyjechał
   dziś w delegację. Ubóstwiam
   Cię, Alicja

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3mqJh
   FEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

Secure sockets layer (SSL)

- usługa SSL: ochrona informacji w warstwie transportu dla aplikacji używających TCP.
- używane pomiędzy przeglądarkami i serwerami WWW w celu handlu elektronicznego (https).
- usługi ochrony informacji:
  - uwierzytelnienie serwera
  - poufność
  - uwierzytelnienie klienta (opcjonalne)
- uwierzytelnienie serwera:
  - przeglądarka używająca SSL zawiera klucze publiczne zaufanych CC.
  - Przeglądarka żąda certyfikatu serwera, wydanego przez zaufane CC.
  - Przeglądarka używa klucza publicznego CC w celu uzyskania klucza publicznego serwera z certyfikatu.
- sprawdźcie w swoich przeglądarkach, jakie mają zaufane CC.

SSL (cd)

Szyfrowana sesja SSL:

- Przeglądarka generuje *symetryczny klucz sesji*, zaszyfrowuje go kluczem publicznym serwera, wysyła serwerowi.
- Używając prywatnego klucza, serwer odszyfrowuje klucz sesji.
- Przeglądarka i serwer znają klucz sesji
  - Wszystkie dane wysyłane do gniazda TCP (przez klienta lub serwera) są szyfrowane kluczem sesji.

- SSL: podstawa standardu IETF Transport Layer Security (TLS).
- SSL może być używane dla aplikacji innych niż WWW, n.p., IMAP.
- Uwierzytelnienie klienta można osiągnąć przy użyciu certyfikatów klienta.

IPsec: Bezpieczeństwo w w. sieci

- Poufność w warstwie sieci:
  - nadawca szyfruje dane w pakiecie IP
  - segmenty TCP i UDP; komunikaty ICMP i SNMP.
- Uwierzytelnienie w w. sieci
  - odbiorca może uwierzytelnić adres IP nadawcy
- Dwa główne protokoły:
  - *authentication header*, AH
  - *encapsulation security payload* , ESP

- Zarówno w AH jak i ESP, źródło i cel wymagają wstępnej komunikacji:
  - tworzą kanał logiczny w w. sieci, zwany związkiem bezpieczeństwa (*security association*, SA)
- Każdy SA jest jednokierunkowy.
- Jednoznacznie określony przez:
  - protokół (AH or ESP)
  - adres IP nadawcy
  - 32-bitowy identyfikator połączenia

Protokół Authentication Header (AH)

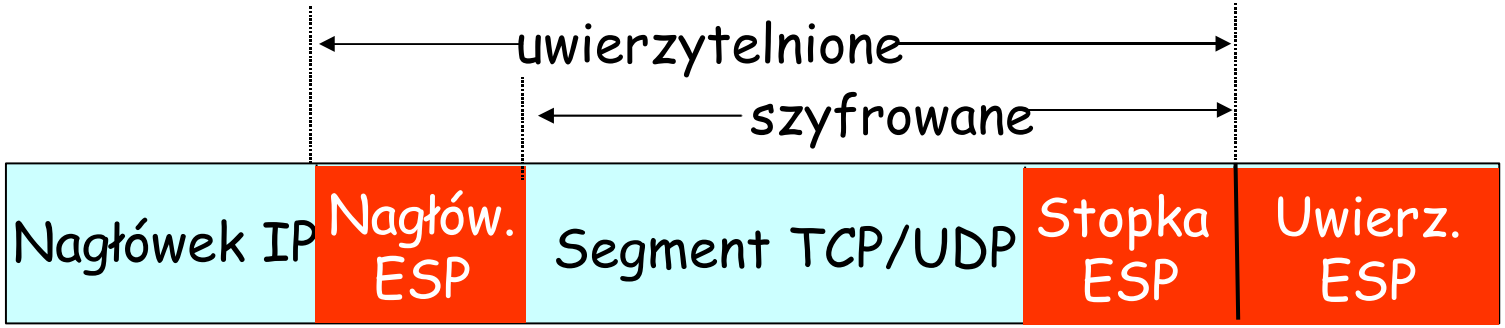
- umożliwia uwierzytelnienie źródła, integralność, ale nie poufność
- Nagłówek AH jest dodawany między nagłówkiem IP a polem danych pakietu.
- pole protokołu: 51
- pośrednie rutery obsługują pakiety jak zwykle

Nagłówek AH zawiera:

- identyfikator połączenia
- dane uwierzytelniające: skrót oryginalnego pakietu IP podpisany przez źródło.
- pole *next header*: określa rodzaj danych (n.p., TCP, UDP, ICMP)

Protokół ESP

- udostępnia poufność, uwierzytelnienie, integralność.
- dane, stopka ESP są szyfrowane.
- pole *next header* jest w stopce ESP.
- Uwierzytelnienie ESP jest podobne do uwierzytelnienia AH.
- Protokół = 50.



Ochrona informacji w IEEE 802.11

- *War-driving:* jeżdżąc wokół Los Angeles w Kalifornii, jakie sieci 802.11 są dostępne?
  - Ponad 9000 jest dostępne z dróg publicznych
  - 85% nie używa szyfrowania/uwierzytelnienia
  - podsłuch i inne ataki są proste!
- *Wired Equivalent Privacy (WEP):* uwierzytelnienie jak w protokole *uwierz4.0*
  - host wymaga uwierzytelnienia od punktu dostępowego
  - punkt dostępowy wysyła jednorazowy identyfikator długości 128 bitów
  - host szyfruje identyfikator używając wspólnego klucza symetrycznego
  - punkt dostępowy odszyfrowuje identyfikator, uwierzytelnia hosta

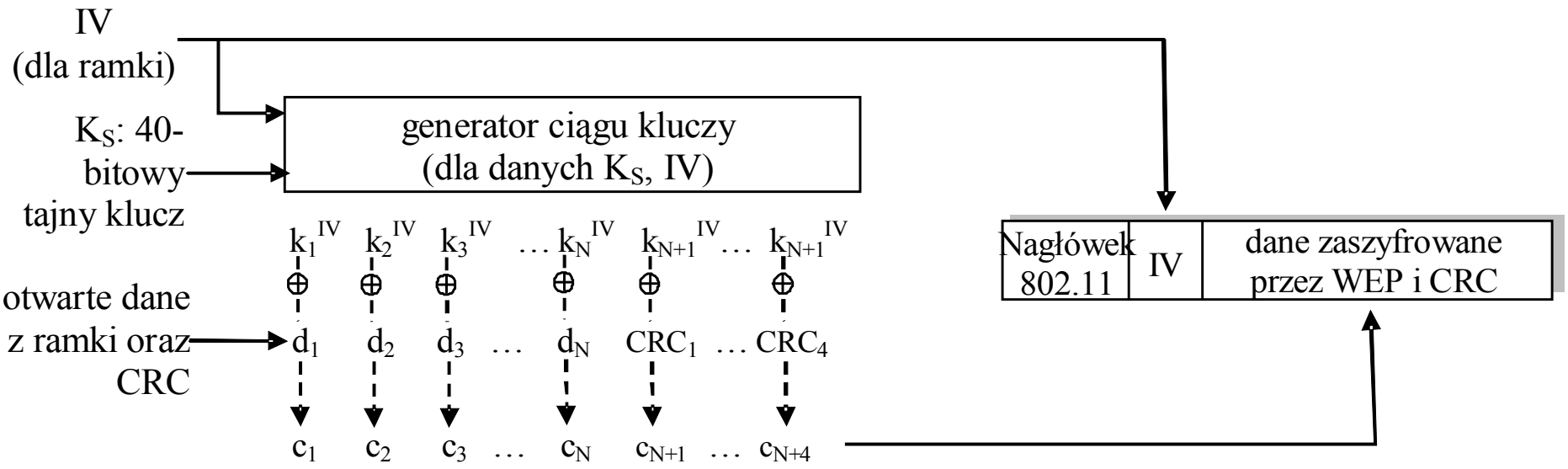
Ochrona informacji w IEEE 802.11

- *Wired Equivalent Privacy (WEP):* szyfrowanie
  - Host/punkt dostępowy mają wspólny, 40 bitowy klucz symetryczny (rzadko zmienny)
  - Host dołącza 24-bitowy wektor inicjujący (IV) żeby stworzyć 64-bitowy klucz
  - 64 bitowy klucz służy do generacji ciągu kluczy, k_i^{IV}
  - k_i^{IV} szyfruje i-ty bajt, d_i, w ramce:

$$c_i = d_i \text{ XOR } k_i^{IV}$$

  - IV oraz zaszyfrowane bajty, c_i są wysyłane w ramce

Szyfrowanie 802.11 WEP



Szyfrowanie WEP u nadawcy

Łamanie szyfru 802.11 WEP

Luka w bezpieczeństwie:

- 24-bitowy IV, jeden IV dla każdej ramki, -> w końcu IV się będą powtarzać
- IV wysyłany otwartym tekstem -> wykryje się powtarzanie
- **Atak:**
  - Trudy powoduje, że Alicja szyfruje znaną wiadomość $d_1\ d_2\ d_3\ d_4$ …
  - Trudy widzi: $c_i = d_i$ XOR k_i^{IV}
  - Trudy zna c_i d_i, więc może obliczyć k_i^{IV}
  - Trudy zna ciąg kluczy, $k_1^{IV}\ k_2^{IV}\ k_3^{IV}$ …
  - Następnym razem, gdy użyty jest IV, Trudy może odszyfrować wiadomość!

Ochrona informacji w w. fizycznej

- *TEMPEST (Transient Electromagnetic Pulse Emanation Standard)*
  - tajny standard rządu USA o ochronie informacji przed podsłuchem promieniowania elektromagnetycznego
  - problem: nawet promieniowanie monitora komputerowego jest dość silne, żeby je można było podsłuchać
  - podsłuchujący widzi na monitorze to, co piszący
  - inne źródło podsłuchu: okablowanie elektryczne
  - istnieje wiele rozwiązań i firm ekranujących urządzenia elektroniczne!

Ochrona informacji w sieciach (podsumowanie)

Podstawowe techniki……

- kryptografia (symetryczna i z kluczem publicznym)
- uwierzytelnienie
- integralność
- dystrybucja kluczy

…. używane w wielu różnych scenariuszach

- bezpieczna poczta
- bezpieczny transport (SSL)
- IP sec
- 802.11 WEP

Plan całości wykładu

- Wprowadzenie (2 wykłady)
- Warstwa aplikacji (2 wykłady)
- Warstwa transportu (3 wykłady)
- Warstwa sieci (3 wykłady)
- Warstwa łącza i sieci lokalne (2 wykłady)
- Podstawy ochrony informacji (3 wykłady)
  - studium przypadku z ochrony informacji w sieciach komputerowych