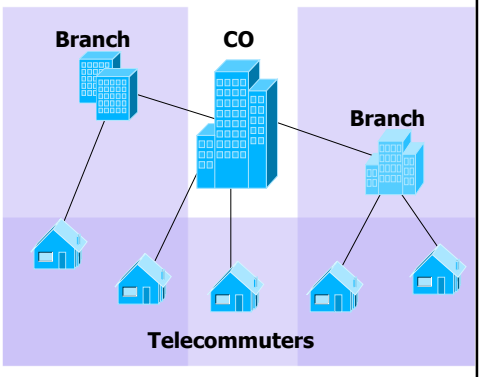
## Wirtualne sieci prywatne

- Wprowadzenie
- Szyfrowanie symetryczne i asymetryczne
- Bezpieczne sumy kontrolne
- Typy VPN
- IP Security Architecture (IPSec)
- Internet Key Exchange (IKE)
- Etapy wdrażania VPN

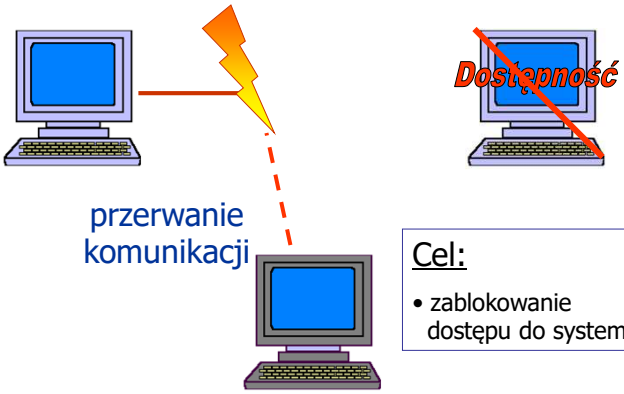
## Wprowadzenie

- Typowa sieć korporacyjna: centrum (central office, CO) + oddziały (branch office)
- Użytkownik zdalny jest to użytkownik nie pracujący w danej chwili w CO
- VPN (wirtualna sieć prywatna) jest to sieć zrealizowana na infrastrukturze publicznie dostępnej, zapewniająca poziom bezpieczeństwa porównywalny z występującym w rzeczywistej prywatnej sieci



**Bezpieczeństwo**

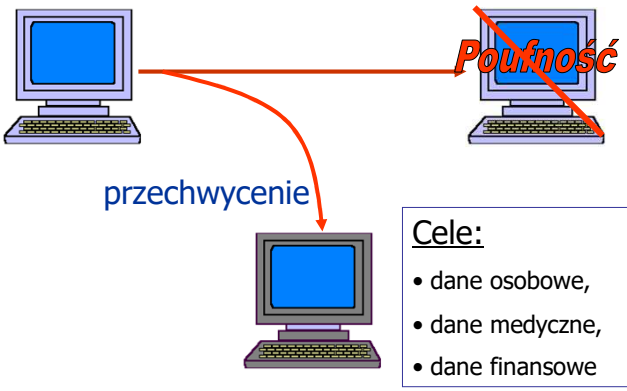
## Rodzaje ataków




Cel:

- zablokowanie dostępu do systemu

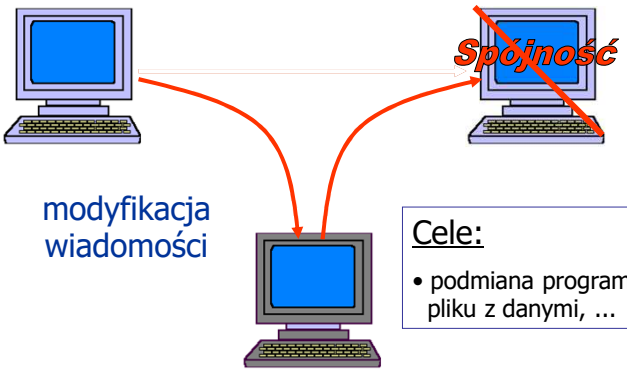
## Rodzaje ataków




Cele:

- dane osobowe,
- dane medyczne,
- dane finansowe

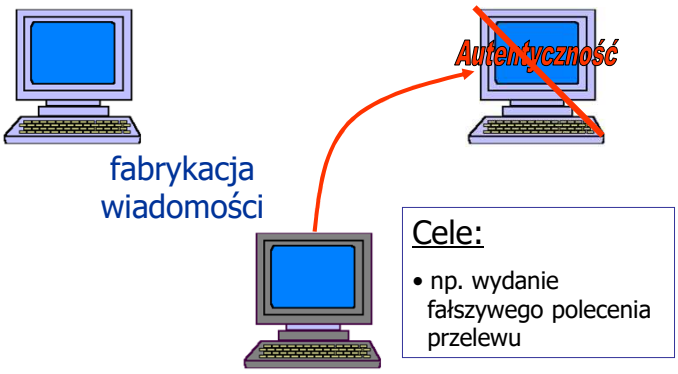
## Rodzaje ataków




Cele:

- podmiana programu, pliku z danymi, ...

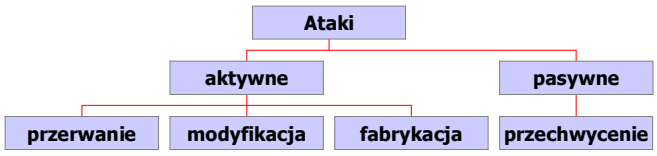
## Rodzaje ataków




Cele:

- np. wydanie fałszywego polecenia przelewu

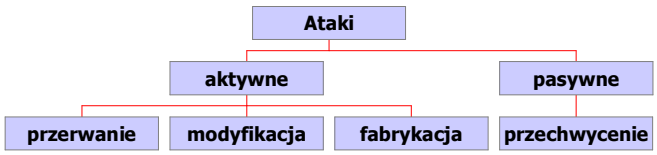
## Klasyfikacja ataków




***ATAKI AKTYWNE***

- masquerade attack (podszycie się) - np. uzyskanie sekwencji identyfikacji w celu późniejszego odtworzenia
- replay attack (powtórzenie) - przechwycenie strumienia i odtworzenie
- modyfikacja strumienia, np. zamiana „`chmod u+x plik1`" na „`chmod a+w plik2`"
- denial of service

## Klasyfikacja ataków




***ATAKI PASYWNE***

- uzyskanie treści przesyłanej informacji
- analiza ruchu w sieci - obserwacja natury komunikacji

## Zabezpieczenia


Cel: zapewnienie dostępu do systemu dla uprawnionych użytkowników

Przykład: program wykrywający skanowanie portów

Uwaga: sam fakt skanowania portów jeszcze nie jest włamaniem, choć nikt nie lubi, gdy się mu porty przegląda

Analogia: oglądanie samochodów na parkingu

## Zabezpieczenia


Cel: zapewnienie ochrony ważnych danych, np. przyszłych cen produktów, ...

Przykłady:

firewall - blokada dostępu z określonych miejsc,

transmisja szyfrowana

Uwaga: czasami sam fakt istnienia jakiegoś obiektu jest informacją tajną

Ataki na poufność zazwyczaj są atakami pasywnymi, w związku z czym trudno je wykryć - można im tylko (np. poprzez szyfrowanie) zapobiegać.

## Zabezpieczenia


Cel: umożliwienie stwierdzenia źródła komunikatu

Przykłady:

zabezpieczenie hasłem,

transmisja z szyfrowaniem asymetrycznym

Podstawowym celem tych zabezpieczeń jest uniemożliwienie fabrykacji wiadomości, nieuprawnionemu włączaniu się osób „trzecich”.

## Zabezpieczenia


Cel: zapobieganie modyfikacjom np. bazy danych

Przykłady:

sumy kontrolne,

transmisja z szyfrowaniem („przy okazji" zapewniamy poufność),

przykład praktyczny: SNMPv2

Ważnym aspektem zabezpieczeń integralności systemu (lub jego części) jest istnienie procedur odzyskiwania integralności (ang. recovery).

"Nieodwołalność" (non-repudiation)

## Wartość informacji

System jest bezwarunkowo bezpieczny, gdy niezależnie od nakładów (czasowych i finansowych) nie można złamać jego zabezpieczeń.

System jest warunkowo bezpieczny, gdy do złamania jego zabezpieczeń potrzeba większych nakładów, niż wynoszą potencjalne korzyści związane z chronioną informacją.

## Technologie VPN

## Wprowadzenie

- Przy konstruowaniu wirtualnej sieci prywatnej ważne są trzy aspekty bezpieczeństwa:
  - poufność,
  - spójność danych,
  - autentykacja źródła.
- Inne wymagania odnośnie bezpieczeństwa systemów sieciowych, np. zapewnienie niemożliwości odwołania transakcji też są ważne, ale nie są realizowane za pomocą VPN.

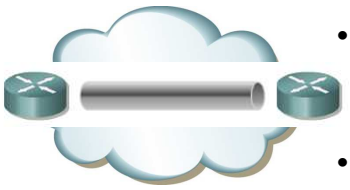
## Wprowadzenie

- Podstawowe mechanizmy, wykorzystywane do konstrukcji wirtualnych sieci prywatnych to:
  - tunele (dedykowane połączenia pomiędzy urządzeniami końcowymi),
  - silne szyfrowanie.
- Wirtualne sieci prywatne mogą być zrealizowane na (prawie) każdej warstwie modelu OSI!
  - na pierwszej nie są wirtualne ☺
- Na obecnym etapie połączenia przez VPN uzupełniają lub nawet zastępują linie dzierżawione bądź prywatne sieci Frame Relay lub ATM.

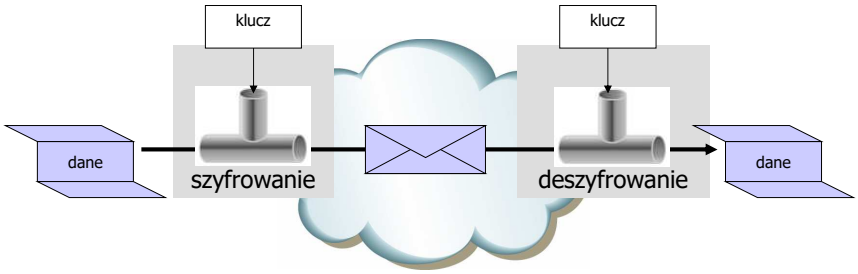
## Dlaczego stosuje się VPN?

- Bo jest taniej:
  - łącza dzierżawione są najdroższym rozwiązaniem,
  - zastąpienie łącza dzierżawionego przez połączenie VPN wykorzystujące **publicznie dostępną** infrastrukturę może obniżyć koszty utrzymania łącza nawet o 40%
- Bo VPN są bardziej elastyczne od tradycyjnych sieci WAN:
  - można łatwo zmieniać końce połączenia (dziś pracuję w Gdańsku, a jutro w Wąchocku)
  - łatwiej utrzymywać VPN, niż klasyczną sieć WAN (?)

## Wirtualna sieć prywatna



- tunel: **wirtualne** połączenie punkt-punkt służące do przenoszenia danych jednego protokołu wewnątrz PDU innego protokołu
- klucze szyfrowania/deszyfrowania są utajnione (**prywatne**)

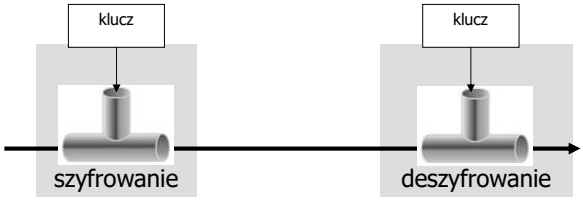



## Podstawowe pojęcia – c.d.

- **autentykacja**: stwierdzenie, że użytkownik lub urządzenie jest tym, za kogo się podaje
- **autoryzacja**: proces przyznawania praw dostępu poszczególnym użytkownikom
- **centrum autoryzacji** (certificate of authority service, CA): instytucja lub usługa wspomagająca bezpieczną komunikację pomiędzy urządzeniami poprzez wystawianie certyfikatów oraz (czasami) generowanie kluczy szyfrowania

## Szyfrowanie symetryczne

- szyfrowanie i deszyfrowanie jest mniej złożone obliczeniowo
- w obydwu przekształceniach wykorzystywany jest **ten sam klucz**
- problem: jak dystrybuować kopie klucza szyfrowania?




- przykłady szyfrów symetrycznych:
  - historyczne: szyfr Cezara, szyfr Vigenere'a, Playfair, ...
  - współczesne: DES, 3DES, AES, ...
- szyfrowanie symetryczne jest stosowane do przesyłania dużych ilości danych
- w czasie transmisji klucze **mogą się zmieniać**

## Tradycyjne metody kodowania

1937 Kornel Makuszyński

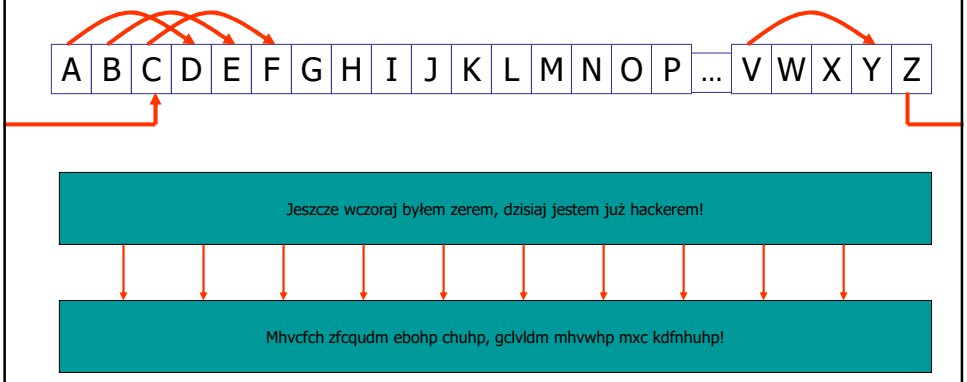
„Szatan z siódmej klasy":
- [...] PILNUJCIE DOMU [...]

- nakłucia tekstu,
- atrament sympatyczny
- zaznaczanie

Kodak Photo CD:
- 2048x3072 punktów

Zalety i wady:
(+) tę metodę można wykorzystać do ukrycia faktu istnienia komunikacji
(-) raz odkryty schemat jest bezużyteczny

## Szyfr Cezara



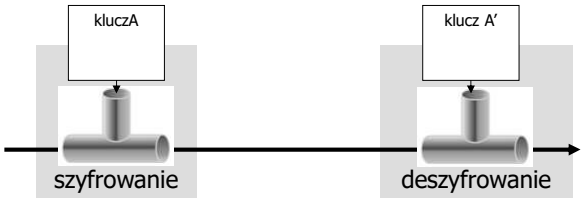

**Bardzo łatwy do złamania (ilość kluczy)**

## Szyfrowanie symetryczne

- Data Encryption Standard (DES)
  - wynaleziony w latach 70-tych ubiegłego stulecia
  - oparty na tablicach permutacji, które służą do minimalizacji ilości przenoszonych informacji statystycznych
  - długość klucza: 56 bitów
  - nie jest już tak trudny do złamania, jak kiedyś, ale nadal dość często używany
  - ten sam algorytm służy do szyfrowania i deszyfrowania informacji
- wariant 3DES – potrójny DES
  - ten sam algorytm jest stosowany trzykrotnie z tym samym bądź różnymi kluczami

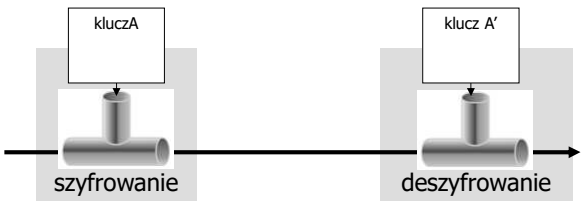
## Szyfrowanie asymetryczne

- zwane jest także szyfrowaniem z kluczem publicznym
  - jeden klucz (prywatny) zazwyczaj służy do szyfrowania, a drugi (publiczny) do deszyfrowania
  - dla danego klucza prywatnego istnieje tylko jeden odpowiadający mu klucz publiczny (i odwrotnie)
- procedury szyfrowania i deszyfrowania są znacznie bardziej złożone obliczeniowo (nawet o kilka rzędów wielkości)
  - są to algorytmy o złożoności wielomianowej, problem tkwi jednak w stopniu wielomianu

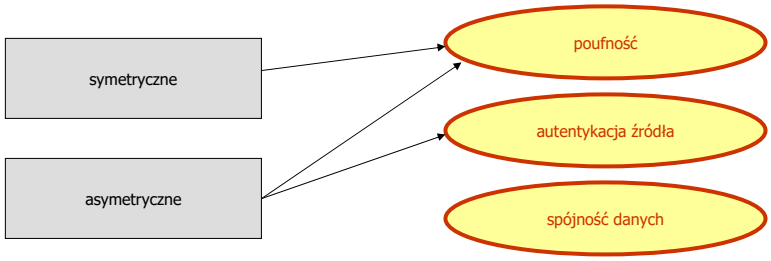



## Szyfrowanie asymetryczne

- często bazuje na bardzo dużych liczbach pierwszych (lub przynajmniej względnie pierwszych)
  - szyfry mają przez to mniej możliwych kluczy ➔ klucz musi być dłuższy
  - operacje na bardzo dużych liczbach zajmują stosunkowo dużo czasu
- stosowane jest do przesyłania małych ilości danych (np. podpisy elektroniczne lub klucze szyfrowania symetrycznego)
- przykładem często stosowanego szyfru asymetrycznego jest RSA (Ron **R**ivest, Adi **S**hamir, Leonard **A**dleman)

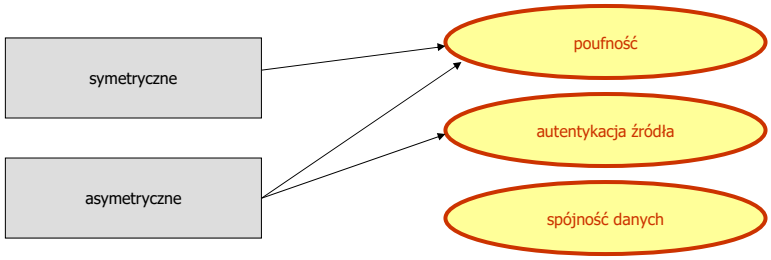


## Co nam daje szyfrowanie...




- **poufność**: należy dobrać szyfr na tyle mocny, aby nakłady poniesione na jego złamanie były większe, niż wartość przesyłanych informacji (szyfr jest **obliczeniowo** (względnie) **bezpieczny**)
- **autentykacja**: jeśli możemy odczytać dane za pomocą czyjegoś klucza publicznego i mamy pewność, że istnieje tylko jeden klucz prywatny odpowiadający danemu kluczowi publicznemu, to wiemy, kto nadał dane

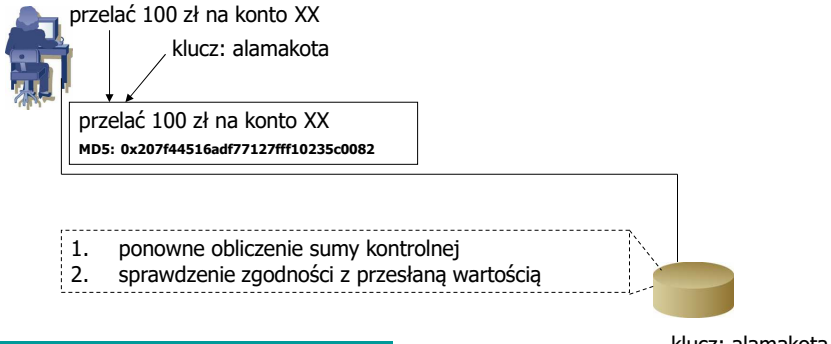
## Co nam daje szyfrowanie...




- **spójność danych**: do sprawdzania, czy dane nie zostały zmodyfikowane stosuje się ... sumy kontrolne
  - przykłady algorytmów obliczających tzw. bezpieczne sumy kontrolne: MD5, SHA
- **UWAGA**! Algorytmy szyfrowania są zazwyczaj publicznie znane, nieznane są natomiast ich parametry, czyli **klucze**.

## Bezpieczne sumy kontrolne

- **MD5, SHA-1** – funkcje jednokierunkowe obliczające sumy kontrolne o stałej długości na podstawie porcji danych o zmiennej długości oraz (tajnego) klucza




Długość kluczy i danych wyjściowych:
MD5: 128 bitów, SHA-1: 160 bitów

## Ile czasu zajmie złamanie?

| Rozmiar klucza | Ilość kluczy | 1 klucz/us | 1 mln kluczy/us |
|---|---|---|---|
| 32 bity | $2^{32} = 4{,}3*10^{9}$ | $2^{31}$ us =35,8 min | 2,15 us |
| 56 bitów (DES) | $2^{56} = 7{,}2*10^{16}$ | 1142 lata | 10,01 godz. |
| 128 bitów | $2^{128} = 3{,}4*10^{38}$ | $5{,}4*10^{24}$ lat | $5{,}4*10^{18}$ lat |
| 26 znaków (permutacja) | $26! = 4{,}03*10^{26}$ | $6{,}4*10^{12}$ lat | $6{,}4*10^{6}$ lat |

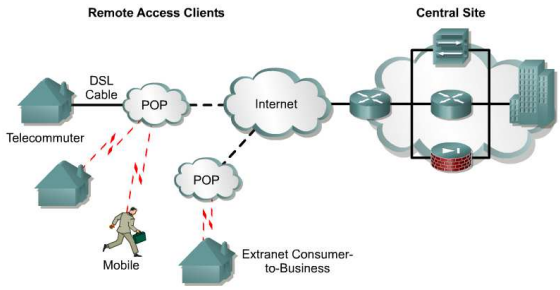
Wnioski:

- włamywacz stosujący wyłącznie metodę „brute-force” nie jest w stanie wyżyć ze swojego fachu,
- atak siłowy jest skuteczny niezmiernie rzadko,
- kryptoanalityk musi znaleźć elementy, które przetrwały proces kodowania

## Z powrotem do VPN

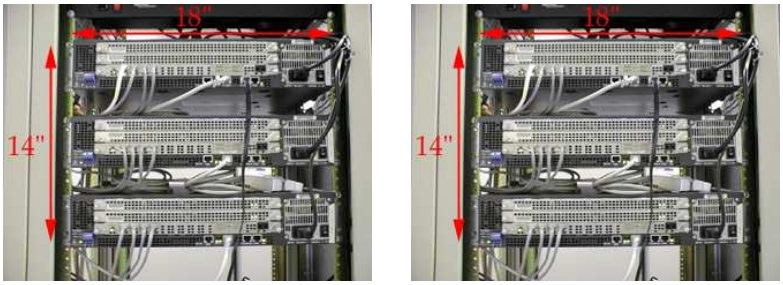
- Wirtualne sieci prywatne konstruowane są pomiędzy:
  - urządzeniami sieciowymi należącymi do danego przedsiębiorstwa,
  - stacjami roboczymi użytkowników zdalnych (np. klientów) a punktami dostępowymi sieci przedsiębiorstwa (połączenia B2B,B2C)
- Tworzenie wirtualnej sieci prywatnej może być zainicjowane przez:
  - **klienta**: użytkownik zdalny używa odpowiedniego oprogramowania aby dostać się za pomocą sieci publicznej do sieci przedsiębiorstwa,
  - **serwer dostępowy**: ruch generowany przez użytkownika pracującego w oddziale firmy jest szyfrowany przy wychodzeniu do sieci publicznej bez udziału samego użytkownika
- **Za chwilę będzie jaśniej...** ☺

## VPN inicjowany przez klienta



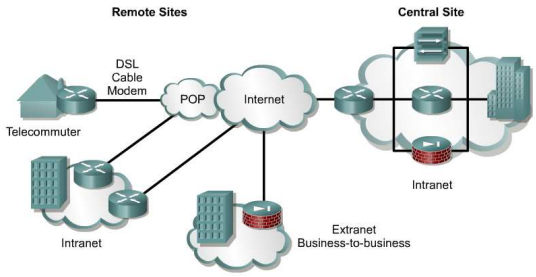

- Dwa pojęcia:
  - **intranet**: zabezpieczona sieć łącząca oddziały danego przedsiębiorstwa
  - **extranet**: zabezpieczona sieć łącząca dane przedsiębiorstwo z partnerami
- Technicznie, obydwa typy sieci realizowane są podobnie.

## VPN inicjowany przez klienta



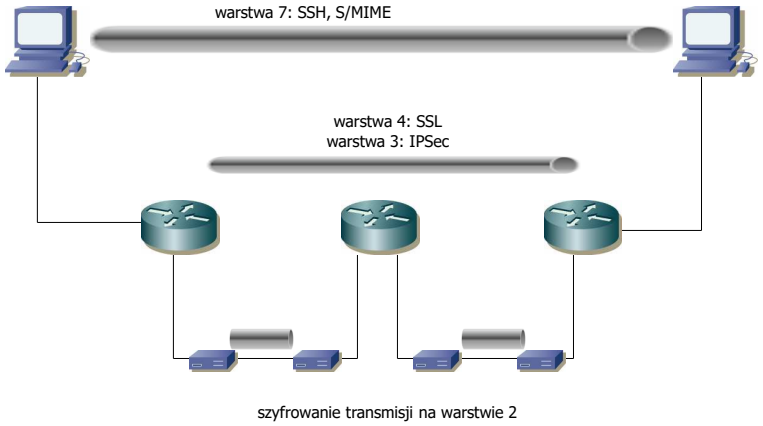

- Dawniej zdalny dostęp do firmy oparty był na posiadaniu odpowiedniej liczby łączy telefonicznych. Użytkownik „wdzwaniał się" do sieci firmy.
- Zastosowanie VPN pozwala na tańsze rozwiązanie – użytkownik „wdzwania się" do swojego ISP – dalej transmisja (szyfrowana) przechodzi zabezpieczonym tunelem.

## VPN inicjowany przez serwer dostępowy




- Dawniej połączenie dwóch (lub więcej) oddziałów firmy wymagało posiadania łącza dzierżawionego albo przynajmniej kanału Frame Relay lub ATM. Połączenie z siecią publiczną realizowane było za pomocą osobnej infrastruktury.
- Zastosowanie VPN pozwala na wykorzystanie jednego łącza zarówno w charakterze „wyjścia na świat", jak i końca tunelu.

## Technologie wspomagające tworzenie VPN

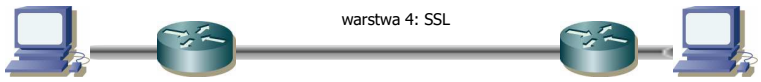



## Technologie wspomagające tworzenie VPN


- Secure/Multipurpose Internet Mail Extensions (S/MIME) jest standardem IETF dla aplikacji VPN
- w zastosowaniach szerokiej skali stosowanie VPN na lub nad warstwą aplikacji jest kłopotliwe, gdyż każda nowa aplikacja wykorzystywana w ramach intra- lub extranetu musi być dostosowana do istniejących mechanizmów
  - a co dopiero, gdy nadejdzie czas wymiany mechanizmów...

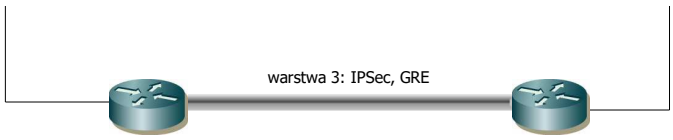
- SSH jest technologią bardzo często używaną, ale ograniczoną pod względem spektrum zastosowań
  - tylko aplikacje interaktywne

## Technologie wspomagające tworzenie VPN



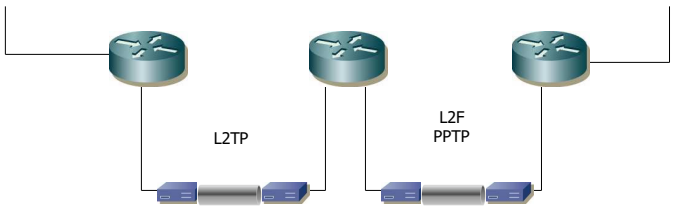

- Secure Sockets Layer jest ustandaryzowaną technologią pozwalającą na zapewnienie poufności i integralności danych oraz autentykację źródła dla aplikacji opartych na protokole TCP
  - technologia ta jest często używana w nowoczesnych rozwiązaniach e-commerce
  - ma jednak swoje wady:
    - ograniczona elastyczność,
    - niezbyt łatwe wdrażanie,
    - duży, ale ograniczony zakres stosowania (tylko TCP),
    - szyfrowanie programowe – obciąża CPU końcówki.

## Technologie wspomagające tworzenie VPN



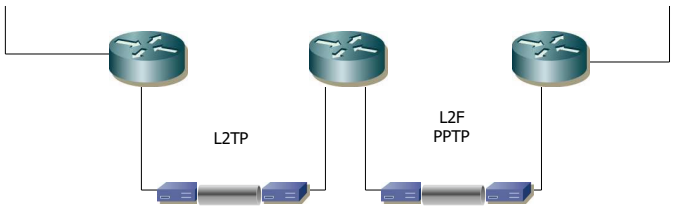

- IPSec (RFC 2401) jest zestawem mechanizmów tworzących połączenie punkt-punkt z wykorzystaniem (bezpołączeniowego) protokołu IP
  - zapewnia poufność i sprawdzanie integralności danych oraz autentykację źródła
  - wykorzystuje tzw. Internet Key Exchange (IKE) do negocjacji algorytmów kryptograficznych oraz ich parametrów (kluczy)
- GRE (Generic Routing Encapsulation, RFC 1701, 2784) pozwala na przenoszenie wielu protokołów, tworzy tunele (połączenia punkt-punkt), ale nie zapewnia mechanizmów szyfrowania

## Technologie wspomagające tworzenie VPN



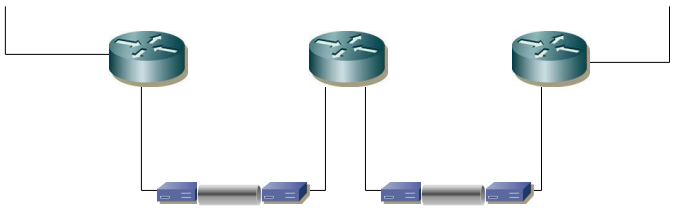

- L2TP (Layer 2 Tunnelling Protocol) jest wykorzystywany do tworzenia „wdzwanianych" wieloprotokołowych wirtualnych sieci prywatnych (VPDN)
  - powstał w roku 1999 jako unifikacja L2F (Cisco) oraz PPTP (Microsoft)
  - **uwaga**... nie definiuje mechanizmów szyfrowania (!)
  - w celu zapewnienia wymaganych właściwości sieci musi być stosowany wraz z innymi technologiami

## Technologie wspomagające tworzenie VPN




- wieloprotokołowość – na czym to polega?
  1. przychodzi pakiet do routera ...
  2. ... zostaje opakowany w pakiet IP adresowany do drugiego końca ...
  3. ... router na drugim końcu tunelu odpakowuje powłoczkę ...
  4. ... i pakiet sam wędruje dalej
- nigdzie nie jest powiedziane, że musi to być pakiet IP!
  - w szczególności może to być nawet ramka np. Frame Relay

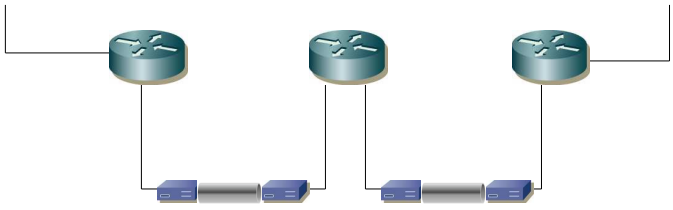
## Technologie wspomagające tworzenie VPN



- szyfrowanie na warstwie 2:
  - istnieją techniki szyfrowania na warstwie 2, ale ich użyteczność jest kontrowersyjna – nawet adresy IP są szyfrowane (!), co spowalnia routing
  - nie ma szans, aby skonstruować w ten sposób tunel wykorzystujący publiczną sieć WAN

## Technologie wspomagające tworzenie VPN

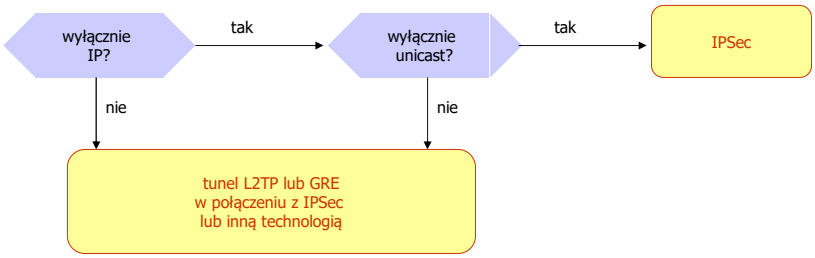
szyfrowanie transmisji na warstwie 2



- technologie warstwy 2 **były** dość często stosowane do zabezpieczania pojedynczych połączeń, ale:
  - ciężko (drogo) stosować je na większą skalę,
  - są wrażliwe na ataki typu „man-in-the-middle”, bo każde urządzenie warstwy 3 kończy tunel realizowany przy ich wykorzystaniu
    - np. ISP może podsłuchiwać nasz ruch...

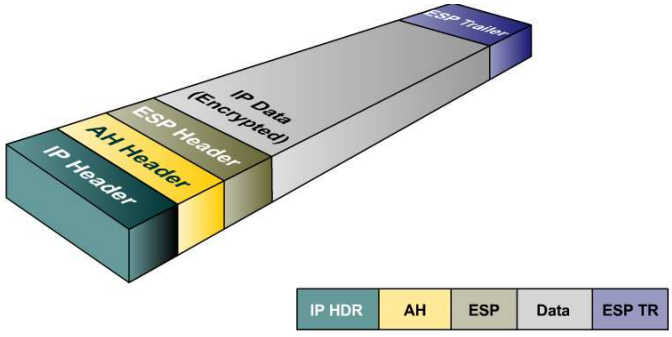
## Jak wybrać technologię realizacji VPN

- technologie warstw wyższych niż 3 mają dość dobrze zdefiniowany zakres zastosowań
- wybór technologii warstw 3 i 2 może przebegać według następującego (bardzo prostego) algorytmu:



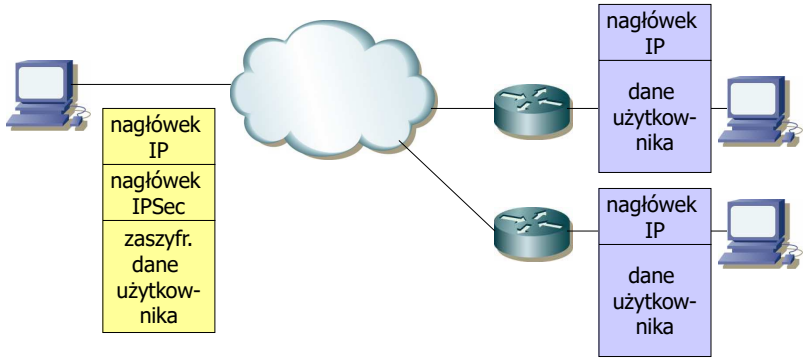

  - unicastowe pakiety IP wystarczy opakować w nagłówek IPSec,
  - multicast IP lub inne protokoły np. przed przesłaniem przez sieć IP (w postaci jawnej bądź szyfrowanej) muszą być opakowane np. przez L2TP lub GRE

## IP Security Architecture (IPSec)

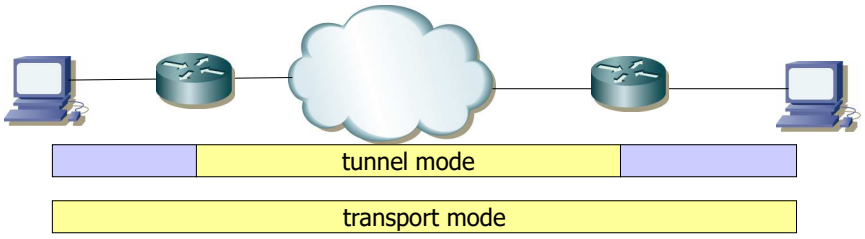


## Jak działa IPSec?

- IPSec w zależności od trybu pracy może zachowywać oryginalny nagłówek IP lub też dodawać nowy,
- może również zapewniać autentykację (AH – authentication header) oraz szyfrowanie przenoszonych danych (ESP – encapsulating security payload)




## Jak działa IPSec?



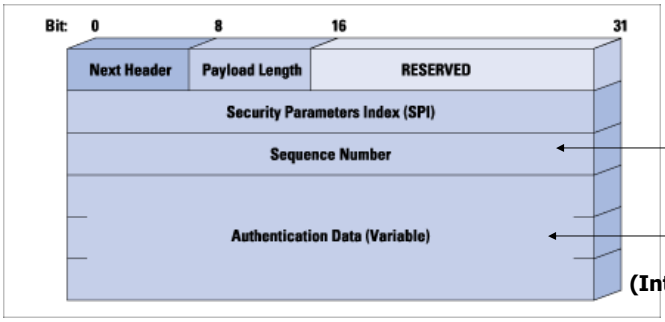

**Tryby pracy IPSec:**

- **tunnel mode**: urządzenie końcowe tunelu dodaje nowy nagłówek IP (cały źródłowy pakiet IP zostaje umieszczony w polu danych)
  → stosowany przez routery lub podobne urządzenia

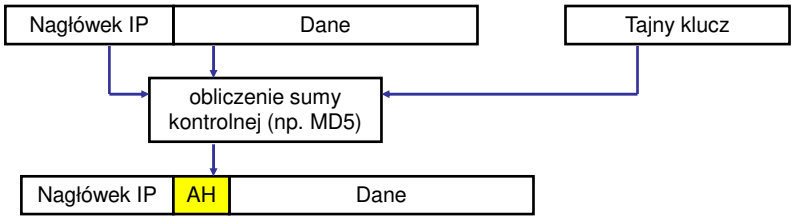
- **transport mode**: urządzenie końcowe dokonuje modyfikacji źródłowego pakietu IP, ale zachowuje nagłówek
  → stosowany przez hosty – routery nie muszą obsługiwać IPSec
  → mniejszy narzut związany z przetwarzaniem pakietów

## Authentication Header

- Authentication Header (AH) jest **protokołem** wchodzącym w skład IPSec, który pozwala na autentykację źródła danych, sprawdzenie integralności danych oraz (opcjonalnie) zabezpiecza przed atakami przez powtórzenie

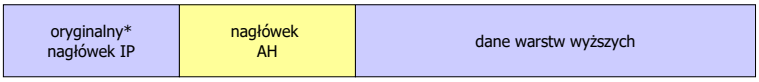



## Algorytm tworzenia AH



## Gdzie umieszczany jest AH?

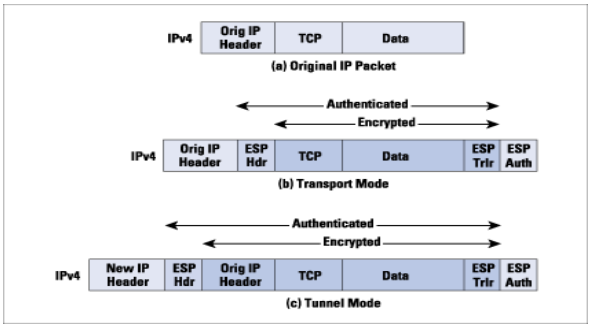
- W trybie *transport* jest dodawany tuż za nagłówkiem IP
  - w polu „protokół” nagłówka IP umieszczana jest zarezerwowana dla AH liczba 51, zaś oryginalna wartość tego pola przenoszona jest do pola „*next header*” AH
  - nie wszystkie pola nagłówka brane są pod uwagę przy obliczaniu sumy kontrolnej (np. TTL zmniejsza się na każdym routerze)




- W trybie *tunnel* jest dodawany tuż za nowym nagłówkiem IP


## Encapsulating Security Payload

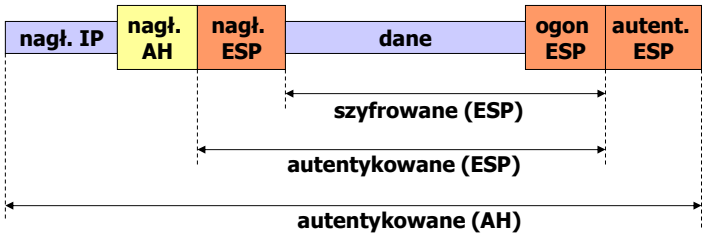
- Encapsulating Security Payload (ESP) jest **protokołem** wchodzącym w skład IPSec zapewniającym poufność oraz integralność danych; opcjonalnie także autentykację źródła oraz zabezpieczenie przed atakami przez powtórzenie

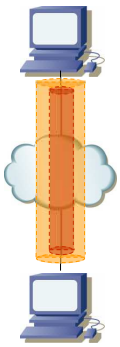



- ESP enkapsuluje zabezpieczane dane
- często stosuje się wyłącznie ESP (bez AH)

## Warianty stosowania AH i ESP

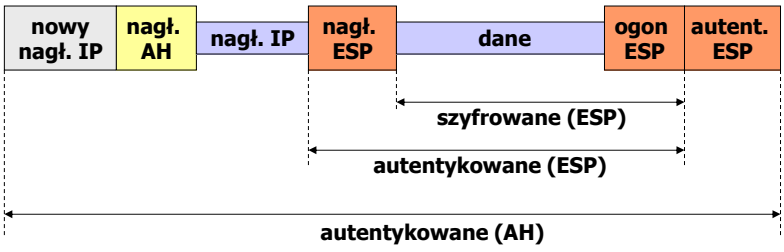
- AH i ESP mogą być stosowane niezależnie
- mogą nawet być stosowane jednocześnie a mimo to mieć różne „końce działania”
- mogą być (i czasami są) wykorzystywane kaskadowo...
- typowe warianty to:
  - ***tryb transportowy*** pomiędzy dwoma hostami
    - zarówno AH, jak i ESP pracują w tym trybie

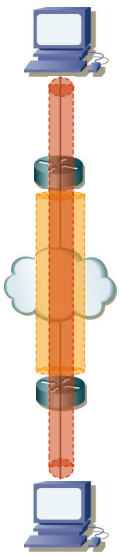


## Warianty stosowania AH i ESP

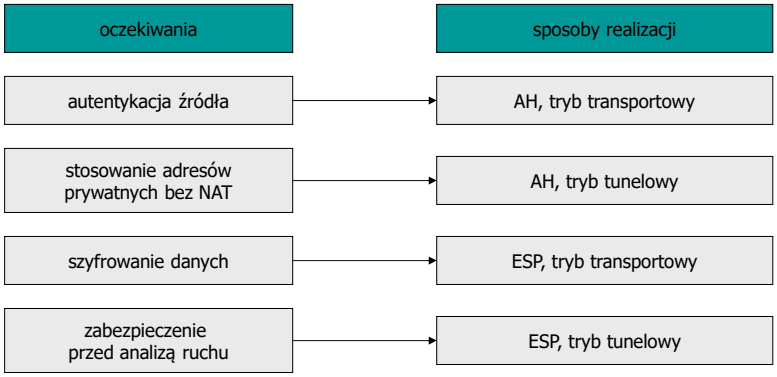
- typowe warianty to:
  - ***tryb transportowy ESP*** pomiędzy dwoma hostami
  - ***tryb tunelowy AH*** pomiędzy routerami



Ciekawa właściwość: w obydwu łączonych oddziałach firmy może działać adresacja prywatna bez translacji adresów!

## Tryby pracy VPN - podsumowanie




## Literatura:


- http://www.cisco.com
- http://cisco.netacad.net
- http://www.redbooks.ibm.com
- http://www.microsoft.com
- http://computer.howstuffworks.com
- http://www.watchguard.com

- D. Elizabeth, R. Denning, *Kryptografia i ochrona danych*
- M. Murhammer i in., *A Comprehensive Guide to Virtual Private Networks,* vol. I-III, www.redbooks.ibm.com

**KONIEC**