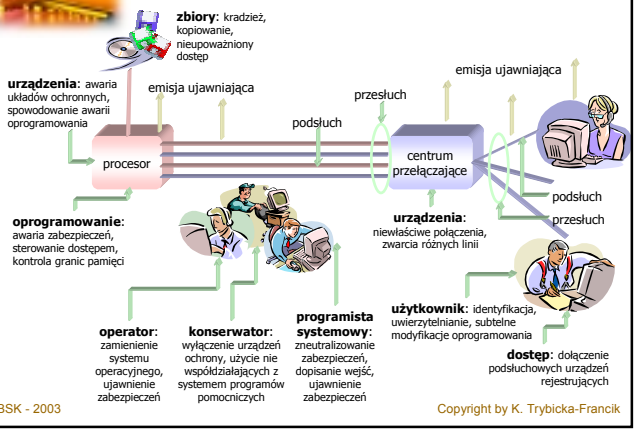
# Bezpieczeństwo systemów komputerowych

## Zagrożenia i konsekwencje

mgr Katarzyna Trybicka-Francik
kasiat@zeus.polsl.gliwice.pl
pok. 503

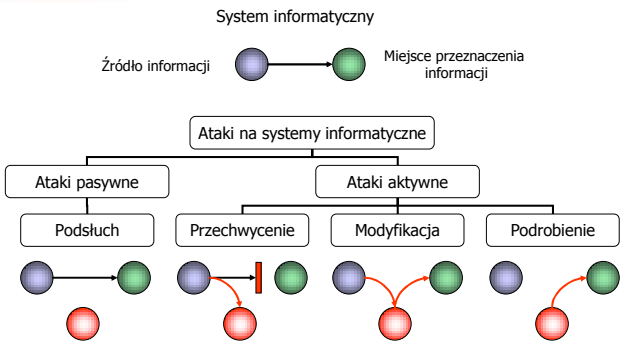
## Słabe punkty sieci komputerowych



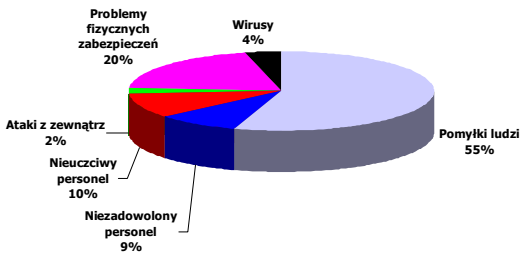




## Klasyfikacja zagrożeń



## Typy zagrożeń – częstotliwość występowania



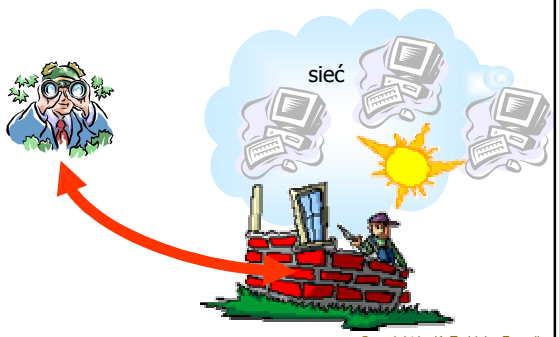

BSK - 2003 Copyright by K. Trybicka-Francik

## Usługi ochrony

- Poufność
- Uwierzytelnienie
- Nienaruszalność
- Niezaprzeczalność
- Kontrola dostępu
- Dyspozycyjność

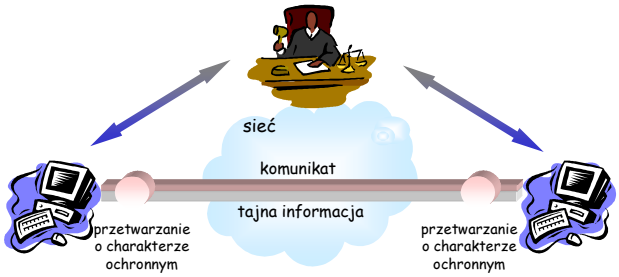
BSK - 2003 Copyright by K. Trybicka-Francik

## Model ochrony dostępu do sieci




BSK - 2003 Copyright by K. Trybicka-Francik

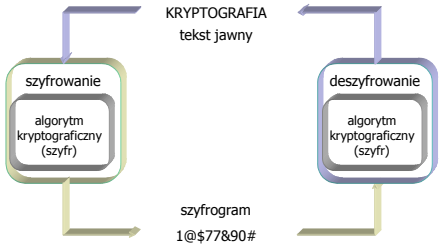
## Model ochrony dostępu do sieci







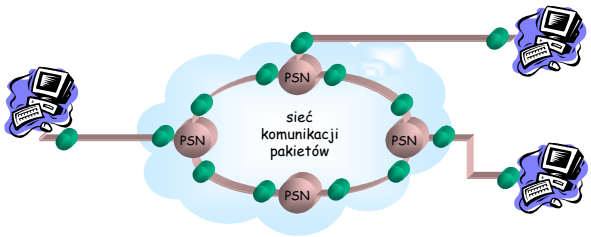
## Terminologia



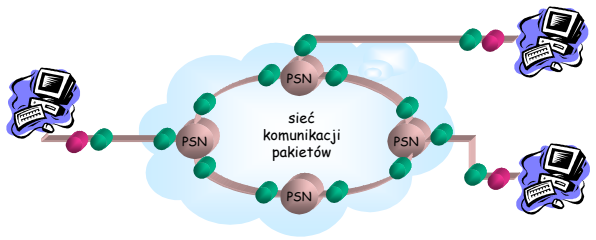




## Szyfrowanie w sieci komunikacji pakietów



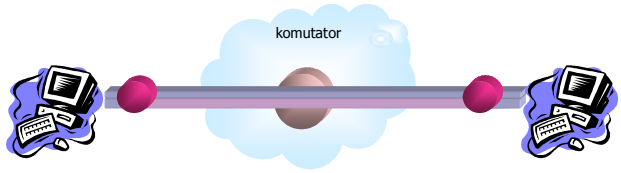
## Szyfrowanie w sieci komunikacji pakietów







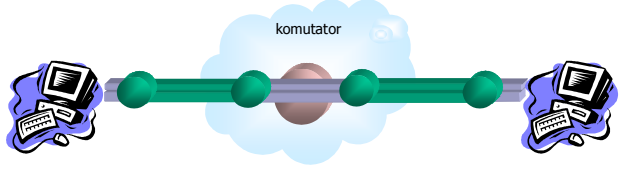
## Szyfrowanie w sieci komunikacji pakietów




szyfrowanie na całej drodze przesyłu

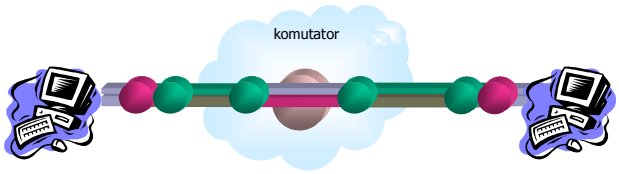



## Szyfrowanie w sieci komunikacji pakietów




szyfrowanie na łączu

## Szyfrowanie w sieci komunikacji pakietów




oba rodzaje szyfrowania




## Teoria informacji

- ✓ Teoretyczne podstawy kryptografii opracował w 1949 r. Shannon.

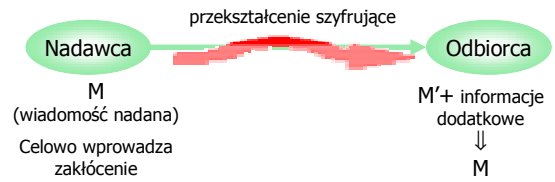
  Zaproponował by teoretyczną poufność szyfru mierzyć nieokreślonością treści jawnej uzyskanej z przekazanego tekstu zaszyfrowanego.

- ✓ Teoria informacji dotyczy dwu zagadnień:
  - ✓ problemu „kanału z szumem”
  - ✓ problemu poufności




## Teoria informacji

## Teoria informacji







## Teoria informacji

Jeżeli przyjmiemy, że $X_1, \ldots, X_n$ to warianty wszystkich możliwych treści wiadomości, a $p(X_1), \ldots, p(X_n)$ to prawdopodobieństwa, z jakimi one występują, przy czym

$$\sum_{i=1}^{n} p(X_i) = 1$$

to **entropię** definiujemy jako:

$$H(X) = \sum_{X} p(X) \log_2 \left( \frac{1}{p(X)} \right)$$

Innymi słowy, entropia to średnia ilość informacji przypadająca na wiadomość.




## Teoria informacji

**Wskaźnik języka** dla wiadomości *N* jest zdefiniowany jako:

$$r = \frac{H(X)}{N}$$

Jest to średnia ilość informacji przypadająca na słowo.

## Teoria informacji

**Wskaźnik bezwzględny języka** definiuje się jako maksymalną liczbę bitów informacji, które mogą być zakodowane w każdym znaku, pod warunkiem, że wszystkie słowa są jednakowo prawdopodobne. Jeżeli przyjmiemy, że alfabet danego języka zawiera *L* znaków, to **wskaźnik bezwzględny języka** jest dany jako

$$R = \log_2 L$$

maksimum entropii poszczególnych znaków.




## Teoria informacji

Języki naturalne charakteryzuje pewna nadmiarowość, redundancja, która wynika ze struktury języka.
**Nadmiarowość** tę definiuje się jako:

$$D = R - r$$




## Teoria informacji

Przyjmijmy że *Y* jest wiadomością ze zbioru wiadomości $Y_1, \ldots, Y_m$, przy czym

$$\sum_{i=1}^{m} p(Y_i) = 1$$

Przez *P(X|Y)* oznaczmy prawdopodobieństwo warunkowe wystąpienia wiadomości *X* przy znanym *Y*. Natomiast *p(X,Y)* oznacza łączne prawdopodobieństwo wystąpienia wiadomości *X* i *Y*, czyli $p(X,Y) = P(X|Y)p(Y)$.

**Entropia warunkowa** *X* przy danym *Y* jest określona wzorem:

$$H(X \mid Y) = \sum_{X,Y} p(X,Y) \log_2 \left( \frac{1}{P(X \mid Y)} \right)$$

## Teoria informacji

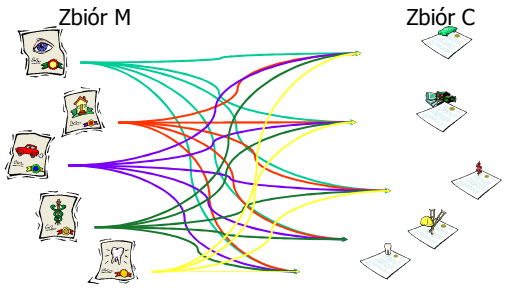
Oznaczmy przez ***M*** zbiór wiadomości jawnych, a przez ***C*** zbiór szyfrogramów.
Shannon warunek na bezpieczeństwo doskonałe wyraził wzorem:

$$H(M \mid C) = H(M)$$

innymi słowy, zbiory ***M*** i ***C*** są statystycznie niezależne.




## Teoria informacji







## Teoria informacji

Oznacza to,
że dla uzyskania rozwiązania doskonale bezpiecznego:

- klucz musi być co najmniej tak długi, jak długi jest tekst jawny
- musi być ciągiem losowym,
- może być użyty tylko jednokrotnie.

każdy algorytm kryptograficzny
jest możliwy do złamania !!!

## Teoria informacji - odległość jednostkowa

Dla wiadomości o długości *n* liczba kluczy deszyfrujących dany szyfrogram do zrozumiałego tekstu jest dana wzorem:

$$2^{H(K)-nD}-1$$

Odległość jednostkowa (punkt jednostkowy),U , jest to taka przybliżona długość szyfrogramu, że suma rzeczywistej informacji (entropii) w odpowiednim tekście jawnym i entropii klucza jest równa liczbie bitów szyfrogramu.

Dla większości symetrycznych systemów kryptograficznych

$$U=H(K)/D$$




**Sukces**
przy przełamywaniu
**algorytmów obliczeniowo bezpiecznych**
uzależniony jest od dostępnych zasobów:
**mocy obliczeniowej** i **czasu**.




## Złożoność obliczeniowa

Złożoność obliczeniowa algorytmu mierzona jest za pomocą dwu zmiennych:

- **T** dla złożoności czasowej
- **S** dla złożoności pamięciowej

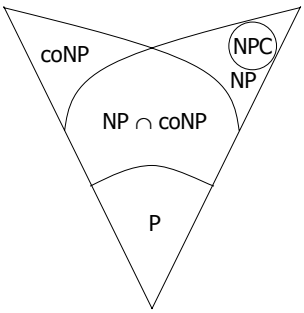
## Złożoność obliczeniowa

Klasyfikacja

- złożoność algorytmu jest stała, gdy nie zależy od *n*, ***O(1)***,
- złożoność algorytmu jest liniowa, gdy rośnie liniowo ze wzrostem *n*, ***O(n)***,
- złożoność algorytmu jest wielomianowa, gdy wynosi $O(n^{f(t)})$ przy stałym *t*,
- algorytmy których złożoność wynosi $O(n^{f(t)})$, gdzie *t* jest stałą, a *f(n)* jest wielomianem zmiennej *n*, nazywamy algorytmami o złożoności wykładniczej,
- algorytmy których złożoność wynosi $O(n^{f(t)})$, gdzie *t* jest stałą, a *f(n)* jest więcej niż stałą, a mniej niż liniową, nazywamy algorytmami o złożoności superwielomianowej.




## Złożoność obliczeniowa - klasy złożoności







**Kryptografowie**
dążą do tego aby
złożoność obliczeniowa szyfrów nie była większa niż
**liniowa**

**Kryptoanalitycy**
dążą do tego aby
złożoność obliczeniowa algorytmów łamiących
nie była większa niż
**wykładnicza**

Złożoność superwielomianowa

## Teoria liczb
## - arytmetyka modularna

$a \equiv b \pmod n$, jeśli $a = b + kn$ gdzie $k$ to liczba całkowita

(a+b) mod n = ((a mod n) + (b mod n)) mod n
(a- b) mod n = ((a mod n) - (b mod n)) mod n
(a*b) mod n = ((a mod n) * (b mod n)) mod n
(a*(b+c)) mod n = (((a*b) mod n)+((a*c) mod n)) mod n

$a^x \bmod n$
np.
$a^8 \bmod n = (a*a*a*a*a*a*a*a) \bmod n =$
$= ((a^2 \bmod n)^2 \bmod n)^2 \bmod n$




## Teoria liczb
## - arytmetyka modularna

Odwrotności modulo pewna liczba

$$a^{-1} \equiv x \pmod n,$$

czyli szukamy takiego x, że

$$1 = (a*x) \bmod n$$

np.

$$1/4 \equiv x \pmod 7$$
$$1 = (4 * x) \bmod 7$$
$$x = 2$$




## Teoria liczb
## - chińskie twierdzenie o resztach

Jeśli $n=p_1*p_2*...*p_t$ jest rozkładem liczby $n$ na czynniki pierwsze, to układ równań

$$(x \bmod p_i) = a_i \text{ przy czym } i=1,2,...,t$$

ma jedno rozwiązanie $x$, przy czym $x$ jest mniejsze niż $n$.

np.
n = 3*5 = 15
x = 14
(14 mod 3) = 2; (14 mod 5) = 4

Istnieje tylko jedna liczba mniejsza od 15 posiadająca reszty 2 i 4

## Teoria liczb
## - reszty kwadratowe

Jeśli p jest liczbą pierwszą i liczba a jest większa niż 0 i mniejsza niż p, to a jest resztą kwadratową modulo p, gdy zachodzi

$x^2 \equiv a \pmod p$ dla wszystkich x.

Nie wszystkie wartości liczby a spełniają to równanie.

np.

p=7 resztami kwadratowymi są 1, 2 i 4

$1^2=1\equiv1 \pmod 7$ $2^2=4\equiv4 \pmod 7$

$3^2=9\equiv2 \pmod 7$ $4^2=16\equiv2 \pmod 7$

$5^2=25\equiv4 \pmod 7$ $6^2=36\equiv1 \pmod 7$

liczby 3,5 i 6 są nieresztami kwadratowymi modulo 7

$x^2=3 \pmod 7$ $x^2=5 \pmod 7$ $x^2=6 \pmod 7$

BSK - 2003 Copyright by K. Trybicka-Francik

## Teoria liczb
## - liczby pierwsze

- Liczba pierwsza
  - jest większa niż 1,
  - posiada dwa dzielniki 1 i samą siebie
- Liczby względnie pierwsze
  - nie posiadają wspólnych dzielników różnych od 1, lub inaczej, jeśli ich największy wspólnym dzielnikiem jest 1

BSK - 2003 Copyright by K. Trybicka-Francik

## Problemy

- Faktoryzacja
- Generatory liczb pierwszych
- Logarytmy dyskretne w skończonym ciele dyskretnym
- Generatory liczb pseudolosowych

BSK - 2003 Copyright by K. Trybicka-Francik

Dziękuję za uwagę