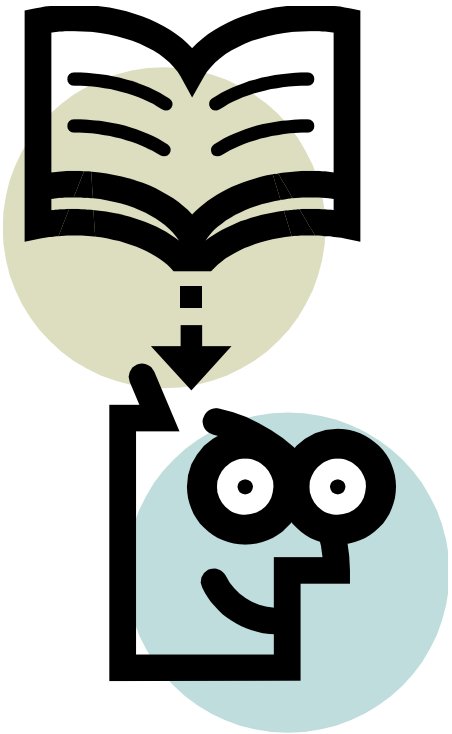
Projektowanie i Realizacja Sieci Komputerowych

Wykład 12

- **Bezpieczeństwo sieci**



dr inż. Artur Sierszeń asiersz@kis.p.lodz.pl

dr inż. Łukasz Sturgulewski luk@kis.p.lodz.pl

Strategia bezpieczeństwa.

- Co to jest bezpieczeństwo komputerowe ?
- Czy możliwe jest stworzenie bezpiecznej sieci ?
- Strategia bezpieczeństwa – kwestia zarządzania czy postępu technicznego ?

Planowanie.

- **Poufność**
- **Spójność danych**
- **Dostępność**
- **Prawidłowość**
- **Sterowanie**
- **Audyt**

Szacowanie ryzyka.

- Określenie zasobów – „Co chronić ?”
- Identyfikacja zagrożeń - „Przed czym chronić ?”
- Wyznaczanie wymiaru zagrożeń – „Ile czasu, wysiłku i środków można poświęcić, aby zapewnić należytą obronę ?”.

Analiza kosztów i zysków.

- SZACOWANIE KOSZTÓW:
  - Koszty napraw
  - Koszty zaprzestania usług
  - Koszt dodatkowych szkoleń
  - Reputacja firmy
- PŁYNNA SKALA STRAT:
  - Niedostępność (okres krótki, średni, długi)
  - Trwała utrata lub destrukcja
  - Przypadkowe/umyślne straty i uszkodzenia

Bezpieczny personel.

- Przyjmowanie nowych pracowników
- Podczas pracy
- Opuszczenie firmy
- Goście

UWAGA !!

80% przestępstw komputerowych jest wynikiem działania ludzi, którzy mają obecnie legalny dostęp do sieci lub mieli taki w przeszłości.

Przyjmowanie nowych

- Weryfikacja przeszłości kandydata

  (przerwy w ciągłości zatrudnienia, powody opuszczenia poprzedniej pracy, itp.)
- Weryfikacja referencji.
- Sprawdzenie informacji o wykształceniu i zdobytych certyfikatach

Podczas pracy.

- Ciągła edukacja personelu (także kadry kierowniczej)
- Dawka „nowych” informacji z dziedziny bezpieczeństwa
- Kontrolowany i monitorowany dostęp do sprzętu, oprogramowania i danych
- Stosowanie zasad:
  - minimalnych przywilejów
  - podziału obowiązków

Opuszczenie firmy.

- Zamknięcie kont
- Przekierowanie adresów poczty elektronicznej
- Zmiana ważnych haseł i ich kombinacji
- Dokonanie wszystkich niezbędnych operacji uniemożliwiające dostęp do systemu

Goście.

- Goście:
  - serwisanci
  - podwykonawcy
  - producenci oprogramowania i sprzętu komputerowego
  - inni..

UWAGA !!

Włamywacze najczęściej korzystają z informacji uzyskanych od „gości” lub próbują się pod nich podszyć.

ZAGROŻONE OBIEKTY

- Sprzęt:
  - Środowisko
  - Dostęp fizyczny
- Oprogramowanie
- Dane
- Linie komunikacyjne i sieci
- Serwery (WWW)
- Usługi sieciowe

Sprzęt.

- Zagrożenia środowiskowe:
  - Ogień
  - Dym
  - Kurz
  - Temperatura
  - Wilgotność
  - Insekty
- Dostęp fizyczny:
  - Zabezpieczenia antywłamaniowe
- Zakłócenia elektryczne i magnetyczne
- Wyładowania atmosferyczne
- Wibracje

Oprogramowanie.

- Zabezpieczenie dostępności dla użytkowników wewnętrznych i zewnętrznych
- Kontrola instalowanego oprogramowania (czy wszyscy powinni mieć taką możliwość)
- Testowanie

Linie komunikacyjne i sieci.

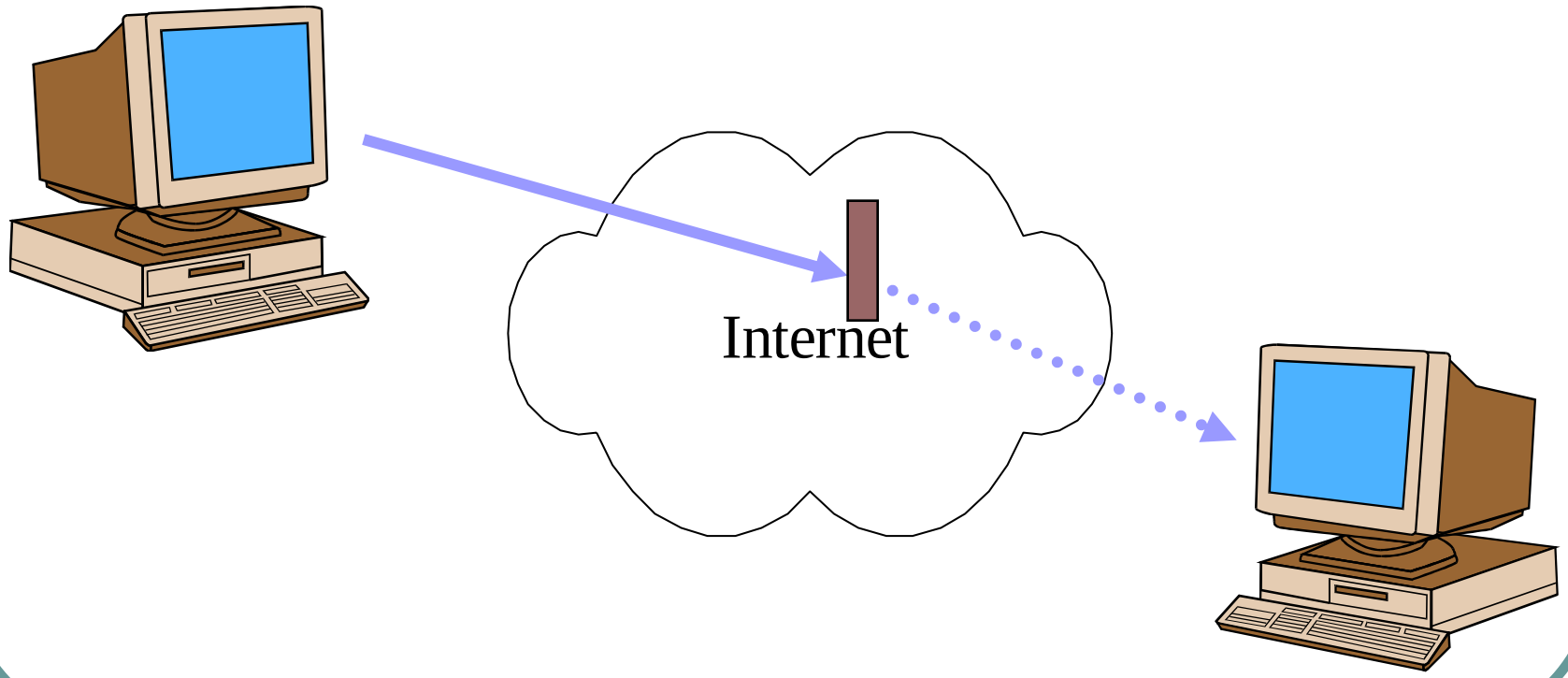
- Zagrożenia pasywne:
  - podsłuch wiadomości
  - analiza ruchu
- Zagrożenia aktywne:
  - modyfikacja informacji
  - przerwanie obsługi wiadomości
  - przechwycenie
  - fabrykacja

Zagrożenia danych.

- Przerwanie
- Modyfikacja
- Przechwycenie
- Fabrykacja

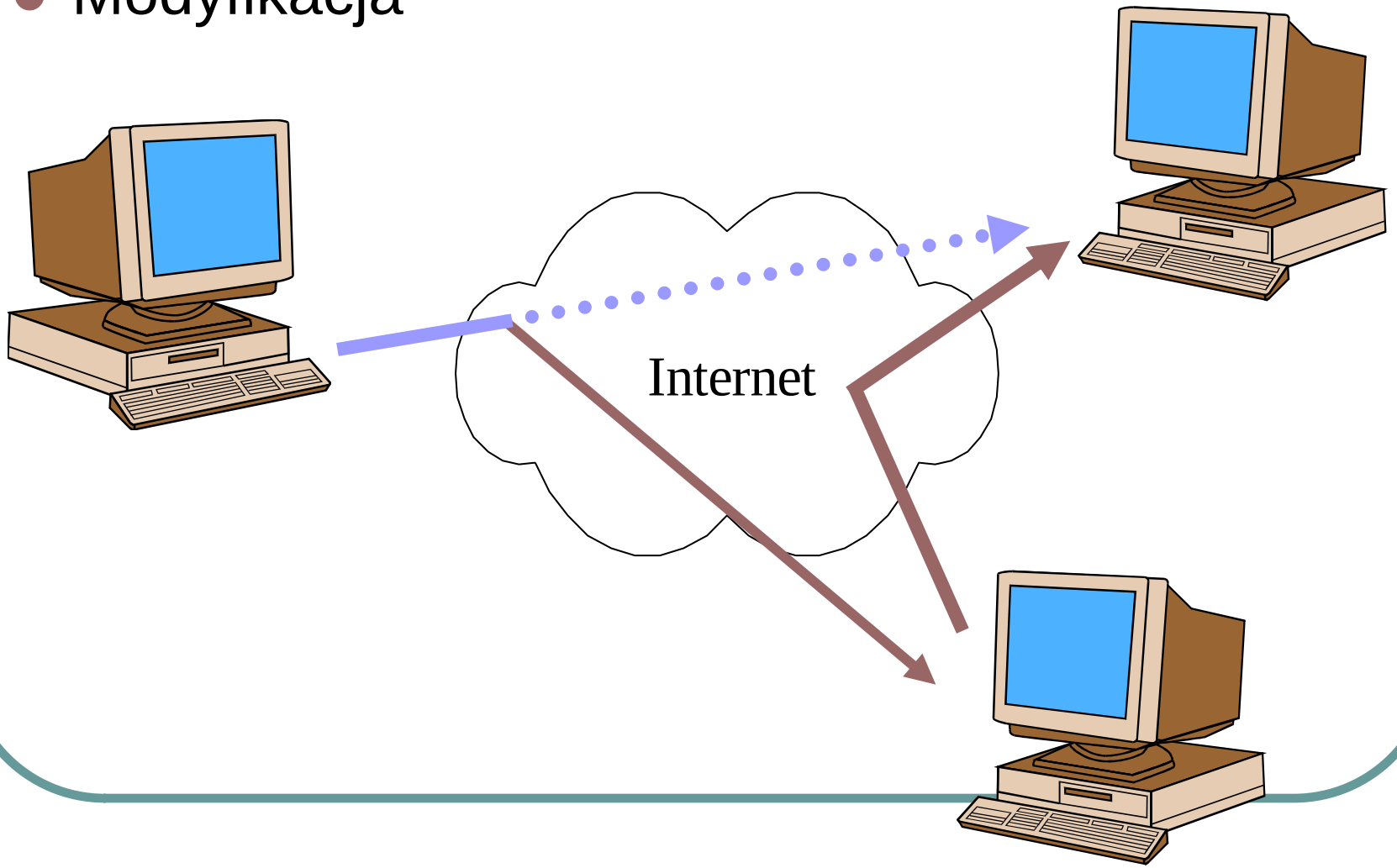
Zagrożenia danych.

- Przerwanie



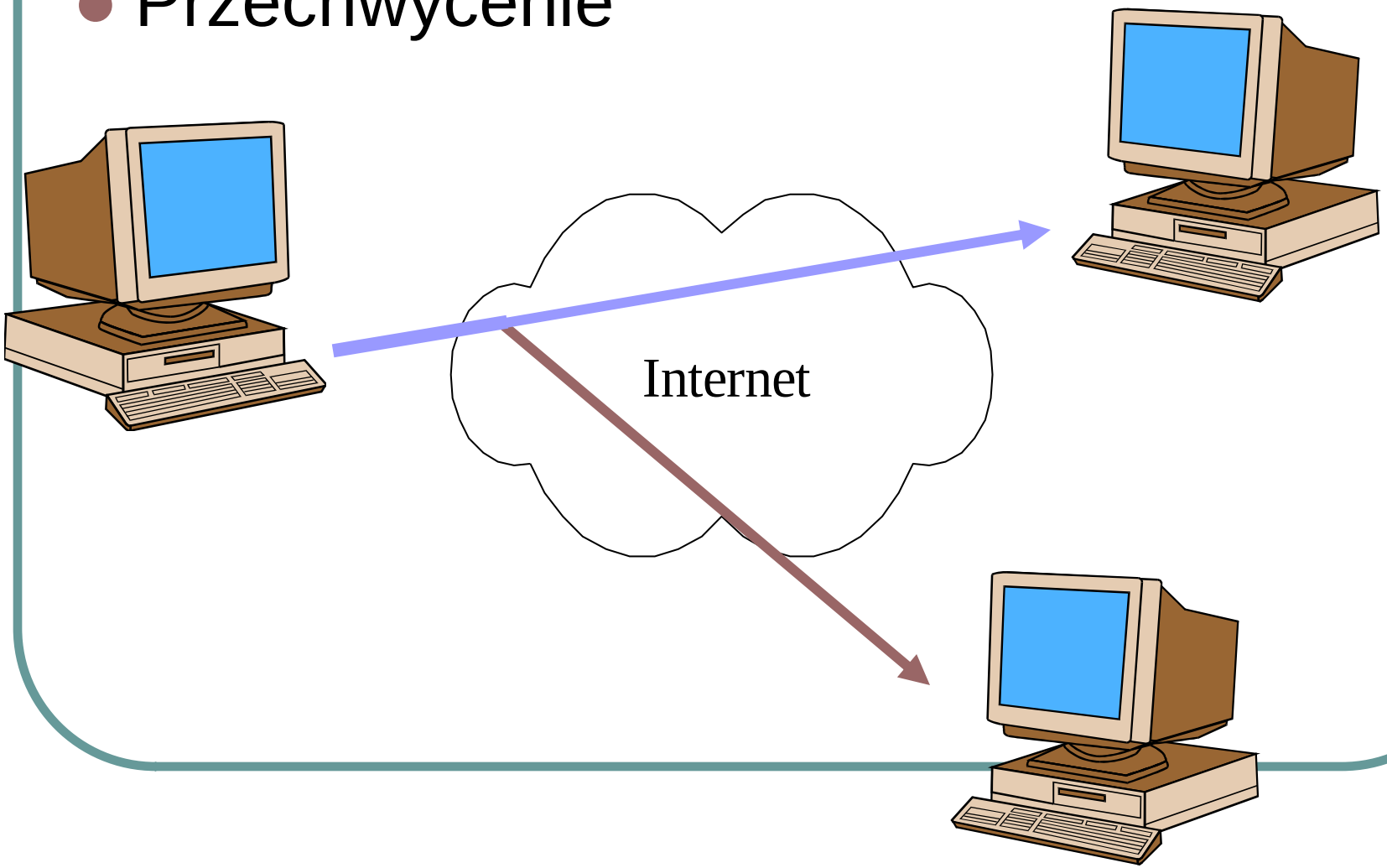
Zagrożenia danych.

- Modyfikacja



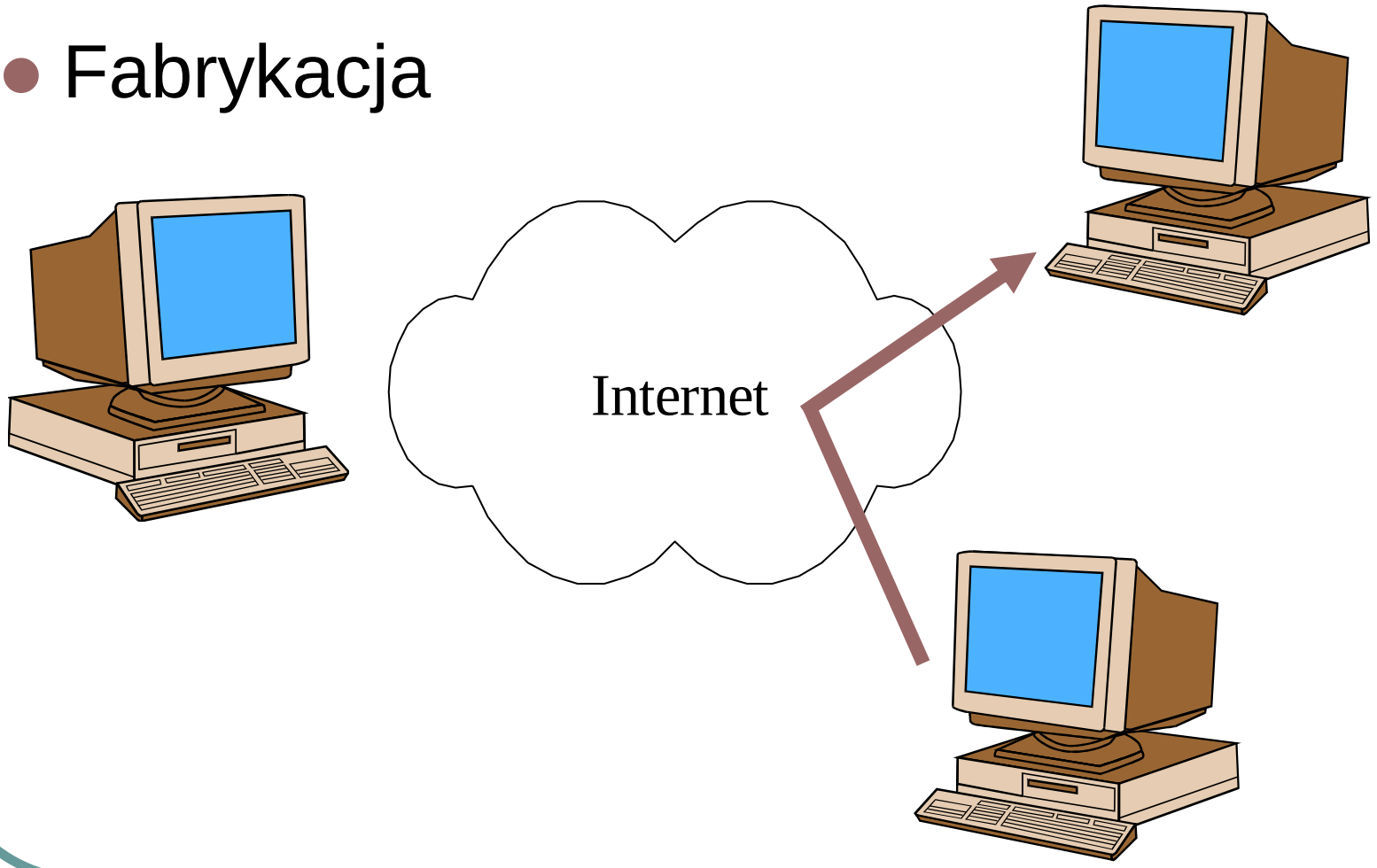
Zagrożenia danych.

- Przechwycenie



Zagrożenia danych.

- Fabrykacja



Usługi sieciowe.

- System przechowywania informacji
  - Weryfikacja poufności danych
- Mechanizm aktualizacji informacji
  - Weryfikacja spójności danych
- Mechanizm udostępniania informacji
  - Weryfikacja serwera
  - Weryfikacja autentyczności klienta i użytkownika

Popularne metody kryptograficzne.

Katedra Informatyki Stosowanej

Politechniki Łódzkiej

Wyjaśnienie pojęć (1).

- Tekst jawny (*plaintext*)
- Algorytm szyfrowania (*encryption algorithm*)
- Tajny klucz (*secret key*)
- Kryptogram (*ciphertext*)
- Algorytm deszyfrowania (*decryption algorithm*)

Wyjaśnienie pojęć (2).

- **Poufność.**
- **Uwierzytelnianie (autoryzacja).**
- **Autentyczność wiadomości.**
- **Integralność wiadomości.**

Bezpieczeństwo metod kryptograficznych.

- Zastosowanie bardzo dobrego (silnego) algorytmu szyfrowania.
- Maksymalna ochrona tajnego klucza.

Sposoby ataku na kryptogram (1).

- Analiza kryptogramu.

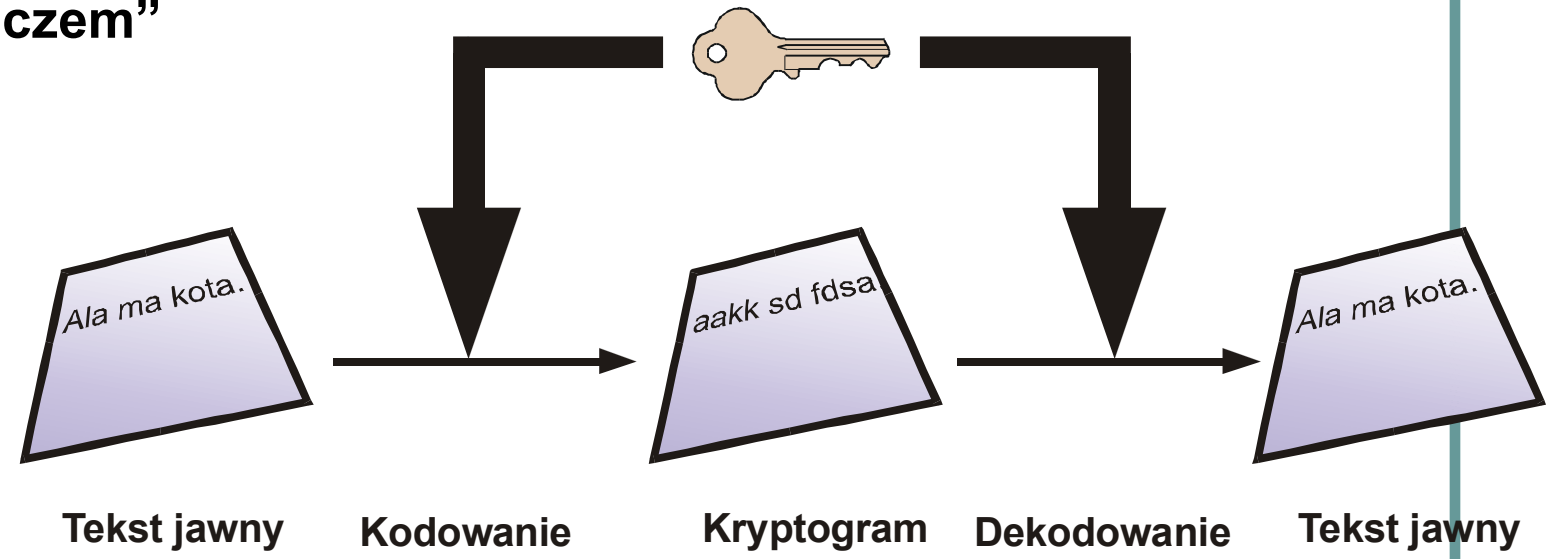
Sposoby ataku na kryptogram (2)

- Atak „siłowy”.

Rozmiar klucza (bity)	*Liczba możliwych kombinacji*	*Czas wyszukiwania klucza (1 klucz na mikrosekund ę*	*Czas wyszukiwania klucza (10^6 kluczy na mikrosekund ę*
32	2^{32} $4.3x10^9$	35.8 minut	2.15 ms
56	2^{56} $7.2x10^{16}$	1142 lat	10.01 godzin
128	2^{128} $3.4x10^{38}$	$5.4x10^{24}$ lat	$5.4x10^{18}$ lat

Metody kryptograficzne (1)

- Kryptografia symetryczna. **„z jednym kluczem”**

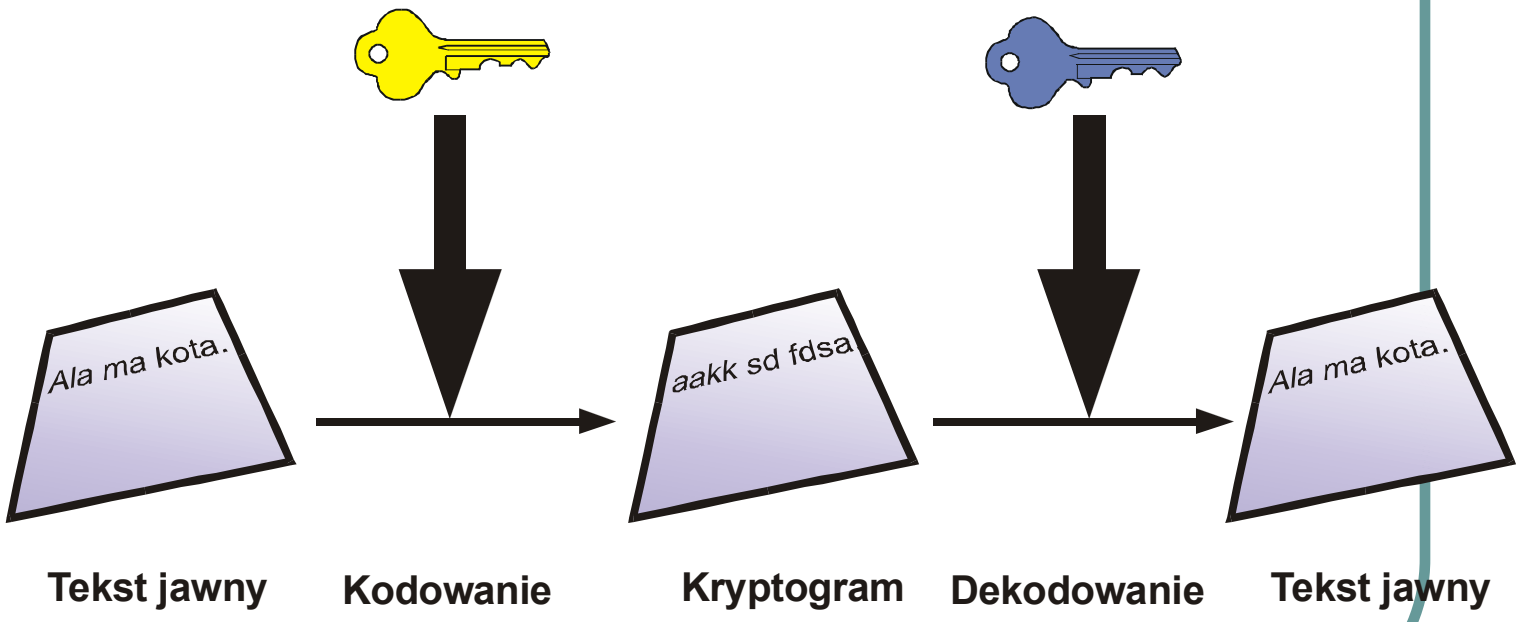


UWAGA !!

Należy bardzo uważać podczas przesyłania klucza pomiędzy jednostkami przez niebezpieczne medium.

Metody kryptograficzne (2)

- Kryptografia asymetryczna. **„z dwoma kluczami”**



Podpisy elektroniczne.

- Główne cechy:

  Łatwe do sprawdzenia;

  Trudne do podrobienia;

  Jednoznacznie określający nadawcę.

- Zastosowanie poznanych metod kodowania.
- Zastosowanie funkcji mieszających.

UWAGA !!

Algorytm generujący podpis nie musi być odwracalny.

Funkcje mieszające.

- **Główne cechy dobrej funkcji mieszającej:**

  - spójność;
  - unikalność;
  - jednokierunkowość;
  - małe zmiany na wejściu = duże zmiany na wyjściu.

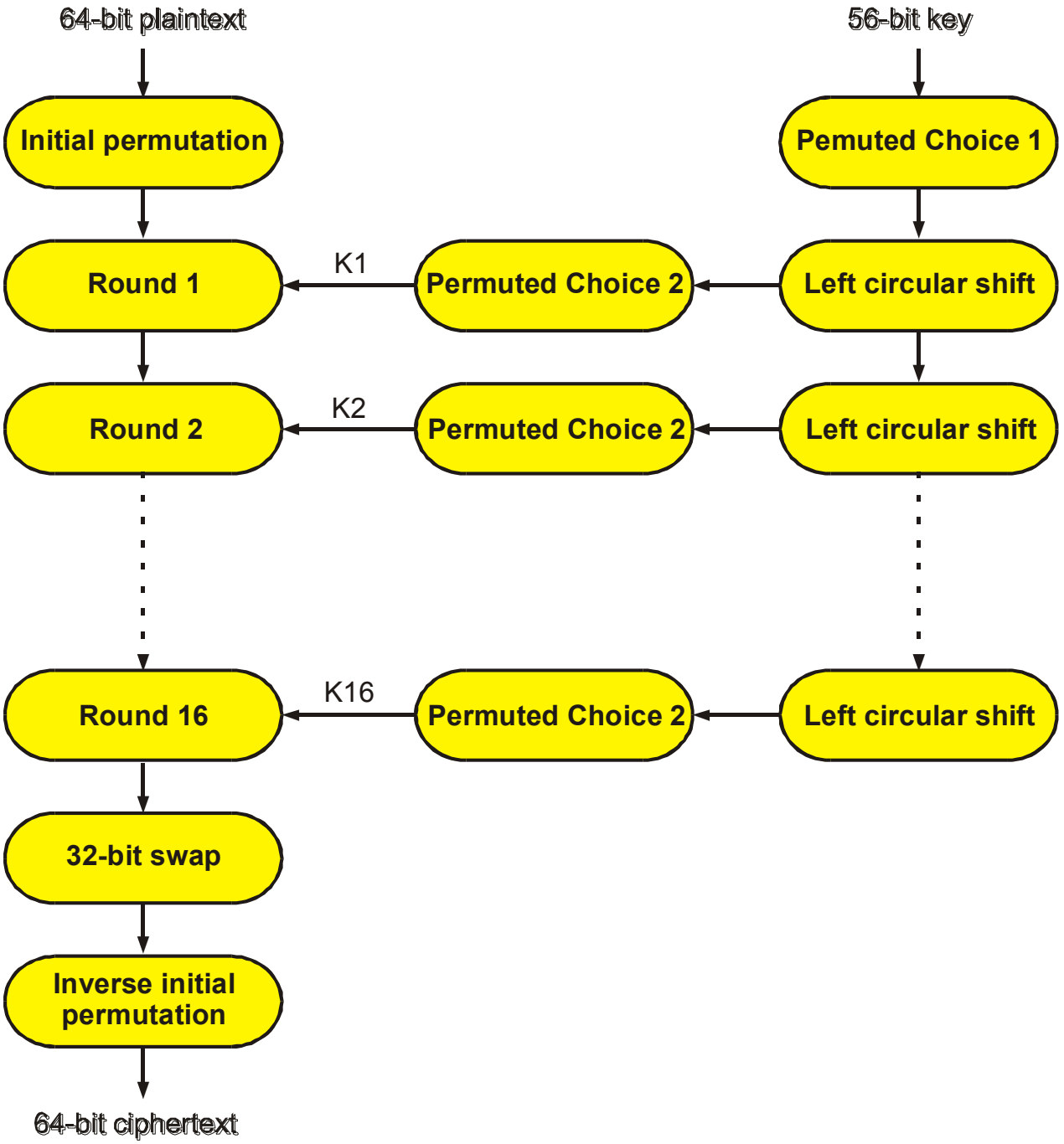
Przykładowy proces szyfrowania.

- Nadawca koduje wiadomość (użycie klucza publicznego otrzymanego od adresata).
- Nadawca dołącza podpis elektroniczny (użycie klucza prywatnego nadawcy).
- Wysłanie tak spreparowanej wiadomości niebezpiecznym kanałem.
- Adresat rozkodowuje wiadomość (użycie klucza prywatnego).
- Adresat weryfikuje podpis (użycie klucza publicznego otrzymanego od nadawcy).

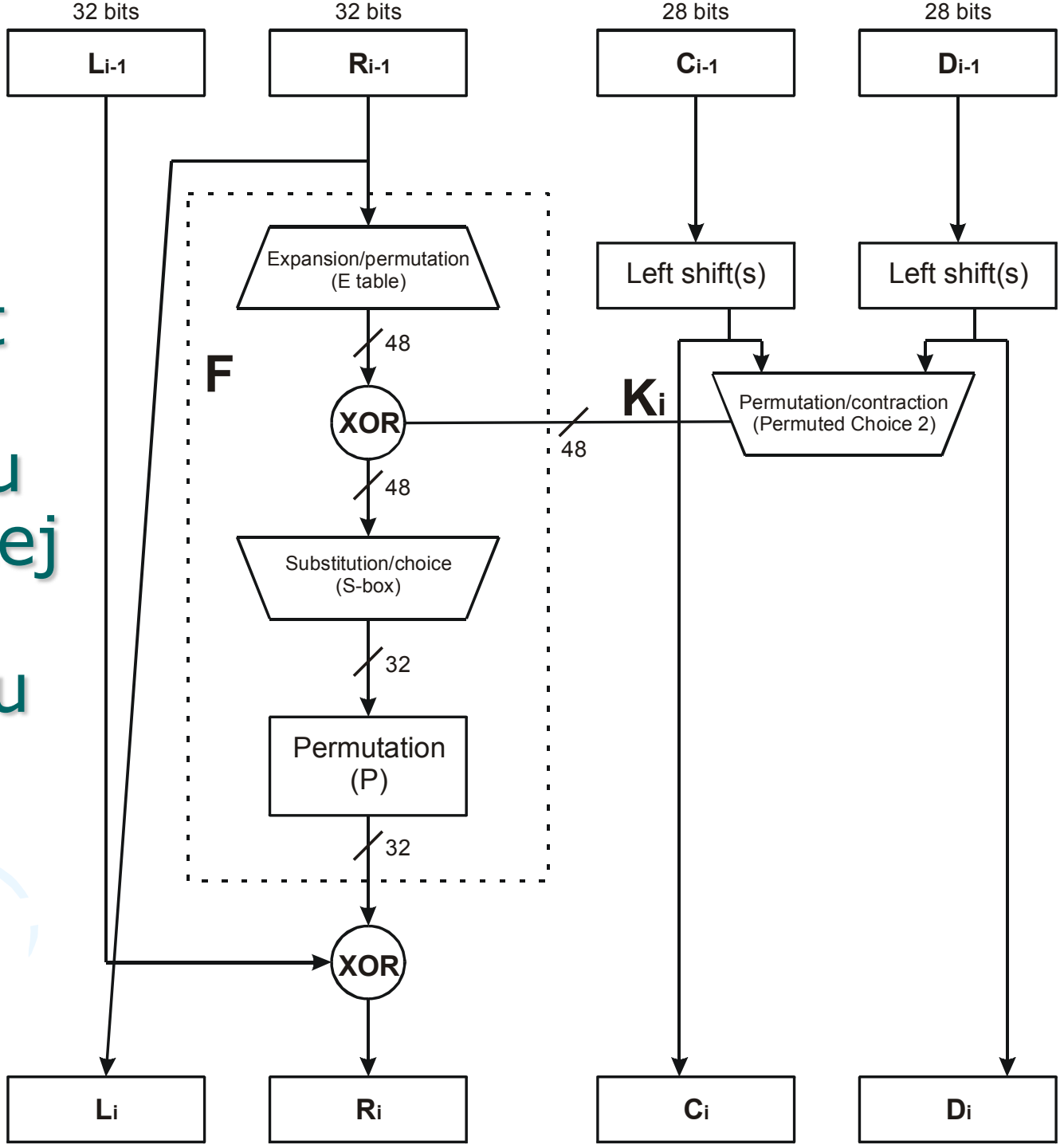
Metody szyfrowania danych.

- Najsławniejsze metody szyfrowania:
  - Kod Juliusza Cezara.
  - Enigma.
    - Opracowana pod koniec lat dwudziestych;
    - Wykorzystywana przez armię niemiecką w czasie II Wojny Światowej.
    - Złamanie zasady działania przez polskich naukowców: Rejewski, Różycki, Zygalski
- DES (*Data Encryption Standard*)

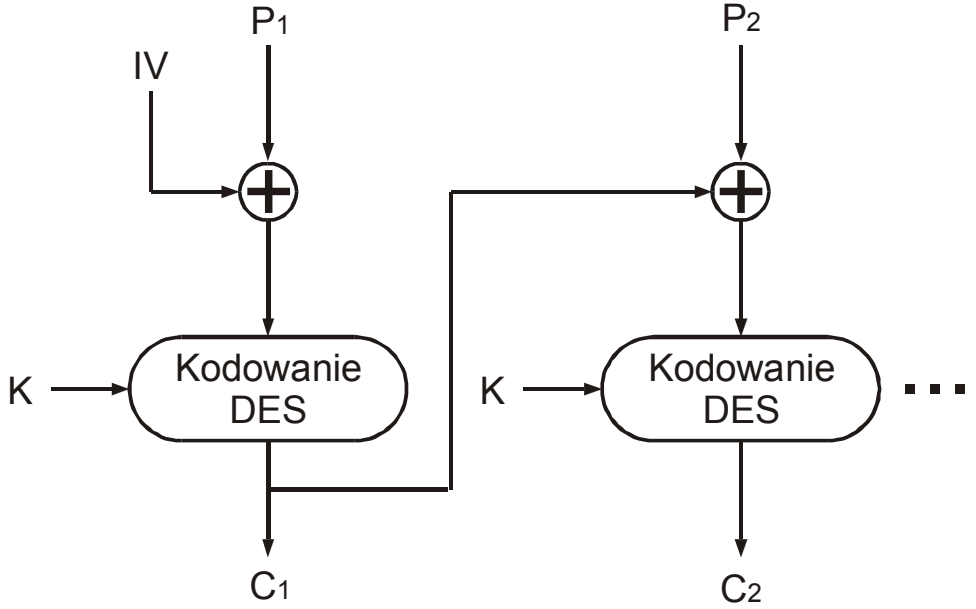
Schemat blokowy algorytmu kodowania DES.



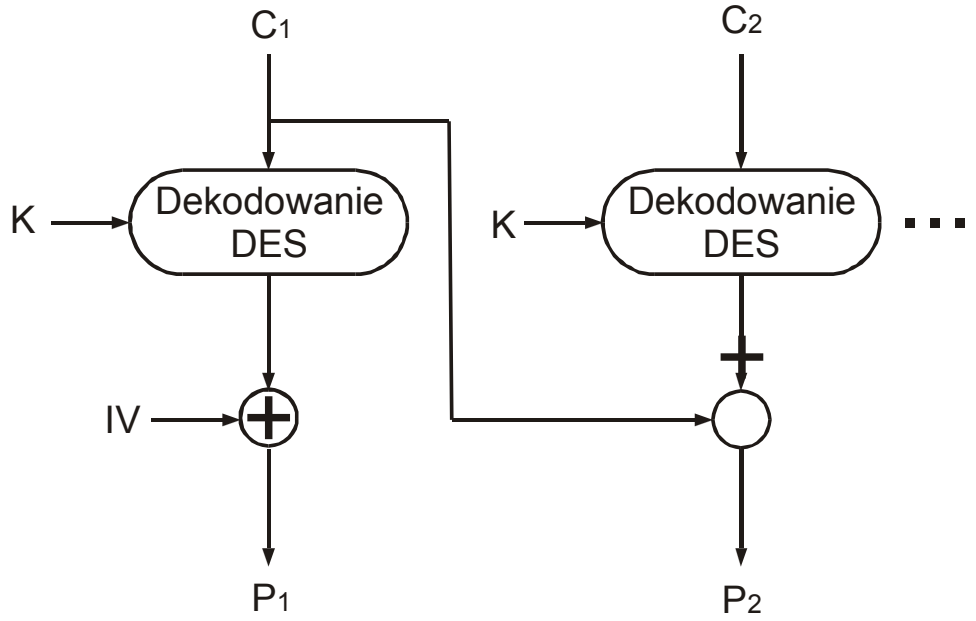
Schemat blokowy przebiegu pojedynczej rundy algorytmu DES.



Szyfrowanie bloków złożonego tekstu jawnego.



a.) kodowanie



b.) dekodowanie

Funkcje mieszające.

- Najpopularniejsze funkcje mieszające:
  - MD5.
  - SHA-1.
- Kolejne etapy działania funkcji:
  - Dodanie bitów *paddingu.*
  - Dodanie informacji o długości wiadomości.
  - Inicjalizacja bufora.
  - Przetwarzanie wiadomości w 512-bitowych blokach.
  - Wynik.

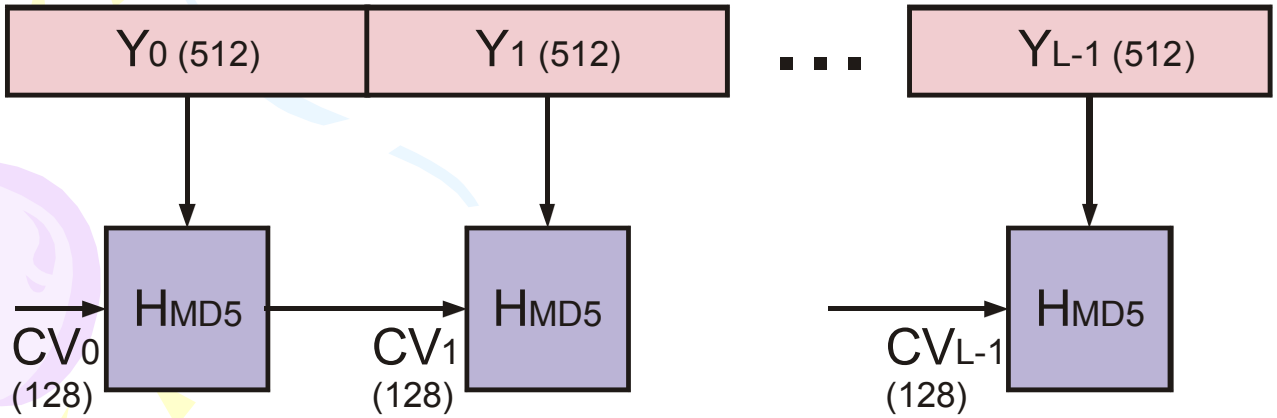
Algorytm MD5

Message = K-bits

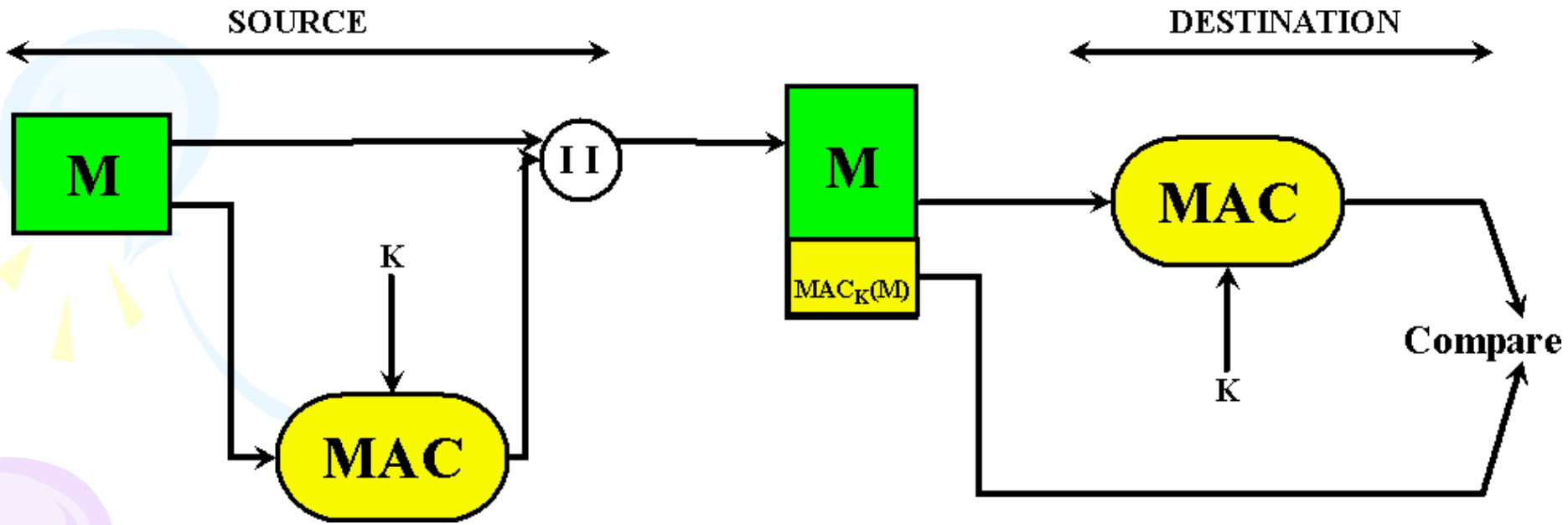
Padding = 1 -512 bits

Message length = K mod 2^64

Message + Padding + Message length = Lx512 bits



Kod autentyczności wiadomości.



Źródła.

- Merike Kaeo: *Tworzenie bezpiecznych sieci.*
  MIKOM, Warszawa, 2000
- William Stallings: *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*.
  Addison Wesley Longman, Massachusetts, 1999
- *Enigmatyczne wyzwania*.
  PC Kurier 18/99

Źródła:

- Grupy dyskusyjne:
  - ***comp.security.announce***
  - ***comp.security.misc***
  - ***comp.security.firewalls***
  - ***comp.security.virus***
  - ***alt.security***
  - ***comp.admin.policy***
  - ***comp.protocols.tcp-ip***
  - ***sci.crypt***