Bezpieczeństwo i ochrona danych

Andrzej Bobyk
http://www.alfabeta.lublin.pl/BiOD/

Literatura

- S. Garfinkel, G. Spafford: *Bezpieczeństwo w Unixie i Internecie.* RM, Warszawa 1997.
- W. Stallings: *Ochrona danych w sieci i intersieci. W teorii i praktyce.* WNT, Warszawa 1997.
- M. Kutyłowski, W.-B. Strothmann: *Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych, wydanie drugie rozszerzone.* Read Me, Warszawa 1999.
- D. Ferbrache: *Patologia wirusów komputerowych.* WNT, Warszawa 1993.

Literatura (c.d.)

- C. Adams, S. Lloyd: *Podpis elektroniczny. Klucz publiczny.* Robomatic, Warszawa 2002.
- M. Kaeo: *Tworzenie bezpiecznych sieci.* Mikom, Warszawa 1999.
- M. Wrona: *Niebezpieczeństwo komputerowe.* RM, Warszawa 2000
- D. E. Robling Denning: *Kryptografia i ochrona danych.* WNT, Warszawa 1993.
- E. Amoroso: *Sieci: Wykrywanie intruzów.* RM, Warszawa 1999.

Co to jest bezpieczeństwo komputerowe?

- Komputer jest bezpieczny, jeżeli jego użytkownik może na nim polegać, a zainstalowane oprogramowanie działa zgodnie ze stawianymi mu oczekiwaniami.
- Praktyczne bezpieczeństwo jest kwestią **zarządzania i administracji**.
- Zbiór technicznych rozwiązań nietechnicznych problemów.
- Nie ma systemów 100% bezpiecznych – **każdy** system może być zagrożony lub uszkodzony.

Polityka bezpieczeństwa

Zasady efektywnej strategii i polityki bezpieczeństwa:

- Świadomość strategii i bezpieczeństwa musi spływać **z góry na dół** w hierarchii organizacji.
- Bezpieczeństwo musi należeć do **priorytetowych** zadań zarządów firm.
- Efektywne bezpieczeństwo komputerowe oznacza ochronę **danych**.

Etapy tworzenia struktur bezpieczeństwa

- Planowanie
- Ocena ryzyka
- Analiza kosztów i zysków
- Tworzenie strategii odpowiadającej konkretnym potrzebom
- Implementacja
- Audyt i reagowanie na incydenty

Usługi związane z ochroną informacji

Generalnie:

- **Poufność:** Ochrona informacji przed odczytem przez osoby nieupoważnione (drukowanie, wyświetlanie, inne formy ujawniania, w tym ujawnianie istnienia jakiegoś obiektu).
- **Uwierzytelnienie:** Poprawne określenie pochodzenia informacji z zapewnieniem autentyczności źródła.
- **Spójność (nienaruszalność):** Ochrona informacji przed nieautoryzowanymi zmianami (pisanie, zmiany, zmiany stanu, kasowanie, tworzenie, opóźnianie i powtarzanie).
- **Dostępność (dyspozycyjność):** Ochrona świadczonych usług przed zniekształceniem i uszkodzeniem, zapewnienie uprawnionym osobom możliwości korzystania z systemu w każdej chwili.

Usługi związane z ochroną informacji (c.d.)

- **Niezaprzeczalność:** Uniemożliwienie tak nadawcy, jak i odbiorcy informacji zaprzeczenia faktowi jej przesłania.
- **Prawidłowość:** Zapewnienie pracy systemu zgodnej z oczekiwaniami.
- **Kontrola dostępu (sterowanie):** Regulowanie dostępu do systemu, autoryzacja.
- **Audyt:** Niepodatny na zniszczenia i uszkodzenia zapis zdarzeń w systemie.

Przykłady:

- **Środowisko bankowe**: spójność, audyt > poufność, dostępność.
- **Systemy obrony narodowej**: poufność >> dostępność.
- **Uczelnia**: integralność, dostępność >> sterowanie, audyt.

Usługi związane z ochroną informacji (c.d.)

W kontekście przesyłania wiadomości przez sieci teleinformatyczne:

- **Integralność zawartości:** Zapewnia możliwość sprawdzenia tego, czy przesyłane dane nie zostały w żaden sposób zmodyfikowane podczas transmisji.
- **Integralność sekwencji:** Chroni przed przechwyceniem i opóźnionym przesłaniem wiadomości, zmianą kolejności wiadomości oraz przed powieleniem, dodaniem lub usunięciem wiadomości.
- **Uwierzytelnienie nadawcy:** Zapewnia możliwość sprawdzenia, czy nadawca wiadomości jest tym użytkownikiem sieci, za którego się podaje.

Usługi związane z ochroną informacji (c.d.)

- **Poufność zawartości:** Takie przekształcenie przesyłanych danych, by były one niemożliwe do odczytania przez żadną inną osobę poza właściwym odbiorcą wiadomości.
- **Niezaprzeczalność nadania:** Chroni przed możliwością wyparcia się przez nadawcę faktu wysłania określonej wiadomości.
- **Niezaprzeczalność odbioru wiadomości:** Chroni nadawcę komunikatu przed wyparciem się przez odbiorcę faktu odbioru komunikatu.

Niezaprzeczalność nadania

⬇

Uwierzytelnienie nadawcy

⬇

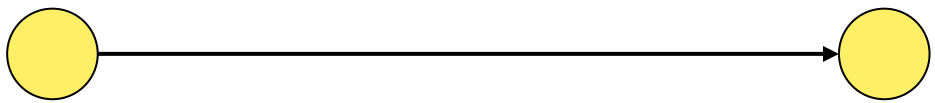
Integralność zawartości

Ataki na informację

- **Przechwycenie:** Nieupoważniony dostęp do zasobów (atak na poufność)
  - odkrycie treści komunikatu;
  - analiza przesyłu.
- **Przerwanie:** Zniszczenie części systemu albo spowodowanie jej niedostępności lub niemożności użycia (atak na dyspozycyjność).
- **Modyfikacja:** Nieupoważniony dostęp do zasobów połączony z wprowadzeniem zmian (atak na nienaruszalność).
- **Podrobienie:** Wprowadzenie do systemu fałszywych obiektów (atak na autentyczność).

Przechwycenie jest atakiem **pasywnym**, pozostałe są **aktywne**.

Ataki na informację (c.d.)

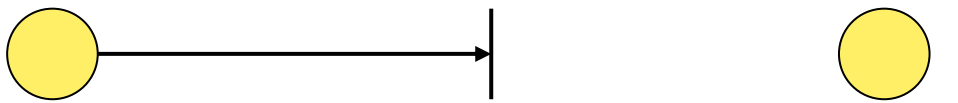


Źródło informacji

Miejsce przeznaczenia

a) Przepływ normalny

Ataki na informację (c.d.)

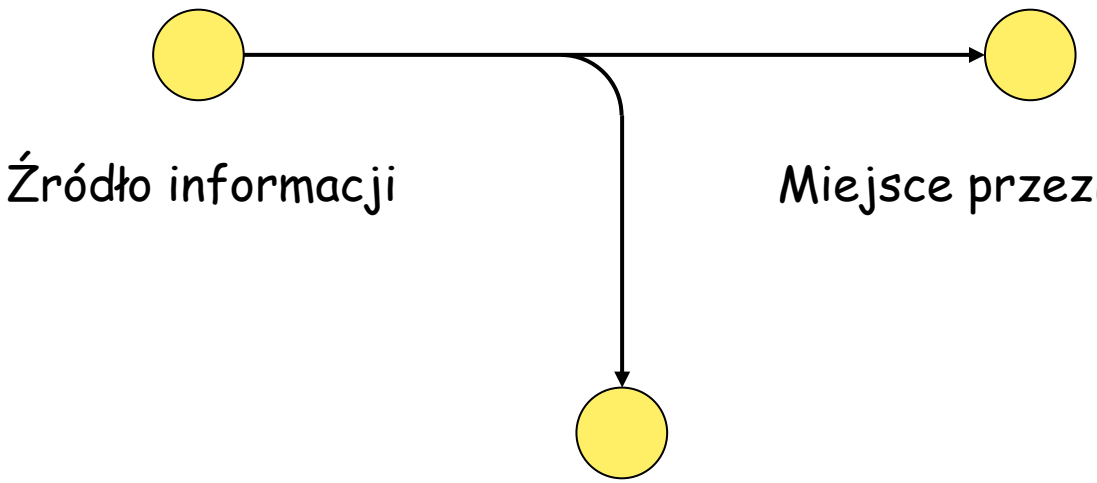


Źródło informacji

Miejsce przeznaczenia

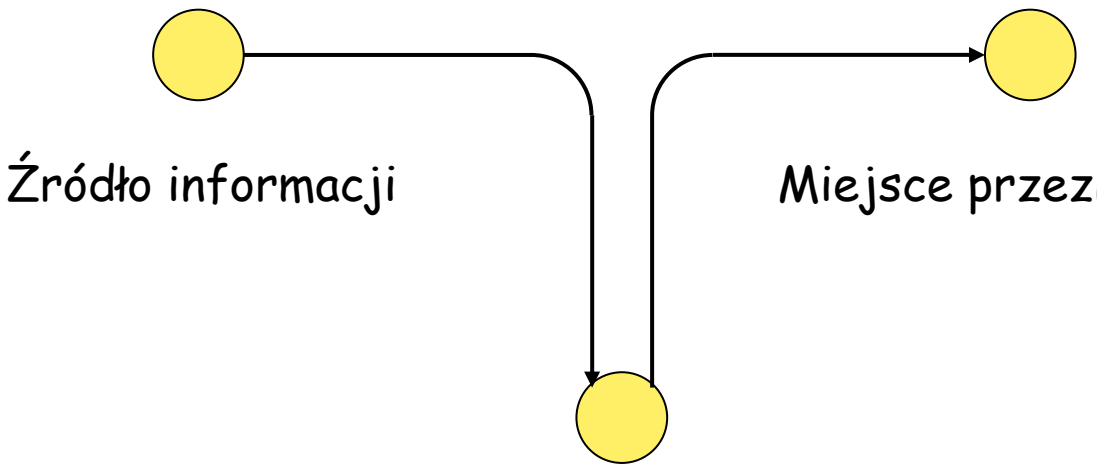
b) Przerwanie

Ataki na informację (c.d.)



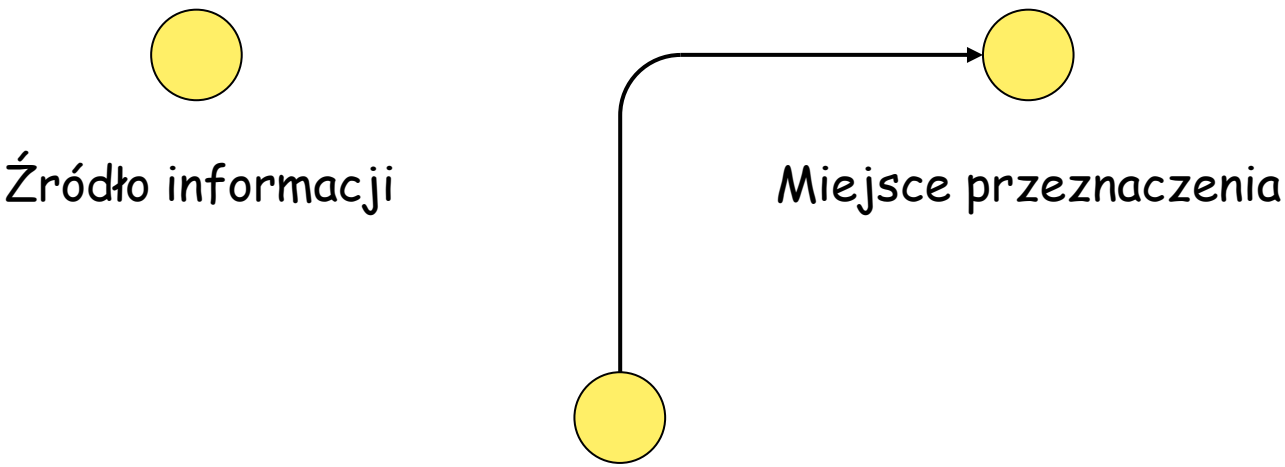
c) Przechwycenie

Ataki na informację (c.d.)



d) Modyfikacja

Ataki na informację (c.d.)



e) Podrobienie

Kategorie zagrożeń

- Zagrożenia fizyczne:
  - kradzież sprzętu, plików lub danych;
  - celowe zniszczenie;
  - bezmyślne zniszczenie danych lub programów.
- Siły wyższe:
  - powódź;
  - pożar;
  - wyładowania atmosferyczne;
  - trzęsienie ziemi;
  - ...

Kategorie zagrożeń (c.d.)

- Inne katastrofy:
  - zwiazane z użytkownikami:
    - pomyłki i nieuwaga;
    - celowe działania na szkodę firmy;
    - wykorzystywanie służbowego sprzętu i oprogramowania (nielegalne kopiowanie) do celów niezgodnych z przeznaczeniem.
  - związane z technologią:
    - awarie sprzętowe;
    - awarie systemowe i błędy programów;
    - wirusy i bomby logiczne w programach.
  - związane z komunikacją:
    - zdalny dostęp do sieci dla legalnych użytkowników;
    - nielegalny dostęp do sieci (hakerzy);
    - celowe podsłuchiwanie komunikacji.

Etapy tworzenia struktur bezpieczeństwa

- Planowanie
- Ocena ryzyka
- Analiza kosztów i zysków
- Tworzenie strategii odpowiadającej konkretnym potrzebom
- Implementacja
- Audyt i reagowanie na incydenty

Proces szacowania ryzyka

- Określanie zasobów – co chronić?
- Określanie zagrożeń – przed czym chronić?
- Wyliczanie ryzyka – ile czasu, wysiłku i pieniędzy można poświęcić, aby zapewnić sobie należytą ochronę?

Określanie zasobów

- Należy sporządzić **listę elementów**, wymagających ochrony.
- Powinna ona być oparta na **biznesplanie i zdrowym rozsądku**.
- Powinna zawierać wszystko to, co przedstawia pewną wartość z punktu widzenia strat wynikających z nieosiągniętych zysków, kosztów straconego czasu oraz wartości napraw i wymian niesprawnych elementów systemu.

Lista elementów wymagających ochrony

- Składniki materialne:
  - komputery,
  - dane o charakterze strategicznym,
  - kopie zapasowe i archiwa,
  - podręczniki i książki,
  - wydruki,
  - nośniki z komercyjnym oprogramowaniem,
  - urządzenia i okablowanie komunikacyjne,
  - dane osobowe,
  - dane audytu.

Lista elementów wymagających ochrony

- Składniki niematerialne:
  - bezpieczeństwo i zdrowie pracowników,
  - prywatność użytkowników,
  - hasła pracowników,
  - wizerunek publiczny i reputacja,
  - dobre imię klientów,
  - zdolności produkcyjne lub do prowadzenia usług,
  - dane konfiguracyjne.

Proces szacowania ryzyka

- Określanie zasobów – co chronić?
- Określanie zagrożeń – przed czym chronić?
- Wyliczanie ryzyka – ile czasu, wysiłku i pieniędzy można poświęcić, aby zapewnić sobie należytą ochronę?

Identyfikowanie zagrożeń

- choroby ważnych osób,
- jednoczesna choroba wielu osób (np. epidemia grypy),
- utrata kluczowych pracowników (rezygnacja z pracy, wygaśnięcie umowy, śmierć),
- utrata możliwości korzystania z łączy telekomunikacyjnych
- utrata mediów (telefon, woda, prąd),
- uderzenie pioruna,
- powódź,

Identyfikowanie zagrożeń (c.d.)

- kradzież taśm lub dysków,
- kradzież komputera przenośnego lub domowego pracownika,
- infekcja wirusem komputerowym,
- bankructwo producenta komputerów,
- błędy w programach,
- destrukcyjni pracownicy,
- destrukcyjni współpracownicy z innych firm (np. personel zewnętrznego serwisu),
- złośliwość przedmiotów martwych,

Identyfikowanie zagrożeń (c.d.)

- terroryzm polityczny i gospodarczy,
- przypadkowi włamywacze systemowi,
- użytkownicy wysyłający anarchiczne lub strategiczne informacje do grup dyskusyjnych,
- …

Proces szacowania ryzyka

- Określanie zasobów – co chronić?
- Określanie zagrożeń – przed czym chronić?
- Wyliczanie ryzyka – ile czasu, wysiłku i pieniędzy można poświęcić, aby zapewnić sobie należytą ochronę?

Wyznaczanie wymiaru zagrożeń

Określenie prawdopodobieństwa każdego ze zdarzeń w wymiarze rocznym

- Firmy ubezpieczeniowe
- Zakłady energetyczne
- Dział kadr
- Dane statystyczne i raporty
- Własne doświadczenia i szacunki

Nie zapominajmy o **weryfikacji ryzyka**!

Etapy tworzenia struktur bezpieczeństwa

- Planowanie
- Ocena ryzyka
- Analiza kosztów i zysków
- Tworzenie strategii odpowiadającej konkretnym potrzebom
- Implementacja
- Audyt i reagowanie na incydenty

Koszty strat

Przypisanie przedziału kosztów do każdego z zagrożeń

- Niedostępność
  - krótkookresowa (7-10 dni),
  - średniookresowa (1-2 tygodnie),
  - długookresowa (ponad 2 tygodnie),
  - trwała utrata lub destrukcja.
- Błędy i uszkodzenia
  - przypadkowe,
  - umyślne,
  - wymiana i naprawa.

Koszty strat (c.d.)

- Wyjawienie zastrzeżonych informacji
  - wewnątrz organizacji,
  - poza organizacją,
  - na zewnątrz – konkurencji i prasie.
- …

Koszty prewencji

- Wyliczenie kosztów zabezpieczeń przed poszczególnymi rodzajami strat.
- Amortyzacja kosztów w określonym czasie.
- Mogą pojawić się dodatkowe koszty (ew. zyski) lub zagrożenia.

Porównanie kosztów i zysków

- Bilans dla każdej z potencjalnych strat.
- Czy koszty prewencji są adekwatne do potencjalnych zysków?
- Wynik: lista priorytetowych zadań, jakimi należy się zająć.

W wielu środowiskach pożar, czy utrata kluczowych osób z personelu są **o wiele bardziej prawdopodobne** i brzemienne w skutkach niż wirusy i włamania przez sieć.

Rachunek zysków i strat – przykład 1

- Zagrożenie: utrata zasilania
- P = 0,5%
- k = 25000 zł + 10000 zł = 35000 zł
- $k_r = P \times k = 175$ zł/rok

- Prewencja: zakup UPS-a i generatora
- k = 150000 zł
- t = 10 lat
- $k_r = k/t = 15000$ zł/rok

?

Rachunek zysków i strat – przykład 2

- Zagrożenie: ujawnienie hasła
- $n = 50$
- $P_1 = 2\%$
- $P = 1 - (1 - P_1)^n = 63{,}6\%$
- $k = 1000000$ zł
- $k_r = P \times k = 636000$ zł/rok

- Prewencja: system haseł jednorazowych
- $k = 20000$ zł $+ n \times 75$ zł $= 23750$ zł
- $t = 5$ lat
- $k_r = k/t = 4750$ zł/rok

!!!

Co dalej?

- Bezpieczeństwa nie uzyskuje się za darmo
- Inwestowanie w strategie opłacalne
- Przekonanie zarządu firmy
- Lista priorytetowych działań i wydatków
- Ryzyko można oszacować, zredukować, ale nie wyeliminować!
- „Czynnik ludzki" jest często najsłabszym ogniwem

Etapy tworzenia struktur bezpieczeństwa

- Planowanie
- Ocena ryzyka
- Analiza kosztów i zysków
- Tworzenie strategii odpowiadającej konkretnym potrzebom
- Implementacja
- Audyt i reagowanie na incydenty

Strategia

Zadania strategii:

- wyjaśnia, **co** ma być chronione i **dlaczego**,
- wyznacza **odpowiedzialność** za ochronę,
- zapewnia **grunt** do interpretacji zdarzeń i rozstrzygania sporów.

Strategia (c.d.)

- Może być **ogólna**, lub **szczegółowa** – dla każdego chronionego zasobu.
- Nie powinna zawierać np. listy **konkretnych** zagrożeń, czy osób – powinna być **ogólna, ponadczasowa**.
- Strategia powinna być taka, by można ją było **pokazać osobom z zewnątrz**.

Normy

- Kodyfikują **skuteczną** praktykę bezpieczeństwa w organizacji.
- Są zazwyczaj **niezależne** od platformy.
- Służą do określenia **kryteriów**, jakie muszą być spełnione przez rzecz, której dotyczą.

Procedury

- Służą do interpretacji norm dla **konkretnego** środowiska.
- W przeciwieństwie do norm – mogą być **łamane** w razie konieczności.
- Są przeznaczone dla **konkretnego** systemu; **zmieniają się** o wiele częściej niż normy.

Zasady tworzenia strategii

- Przypisywanie właściciela
- Pozytywne nastawienie
- Pracownicy to też ludzie
- Nacisk na edukację
- Władza proporcjonalna do odpowiedzialności
- Wybór prostej filozofii
- Obrona w głąb

Cztery proste zalecenia

- Oceń, jak ważne jest bezpieczeństwo w Twoim środowisku.
- Szkol użytkowników i anagażuj ich w sprawy związane z bezpieczeństwem.
- Opracuj procedurę sporządzania i przechowywania kopii zapasowych.
- Bądź czujny i podejrzliwy.

Problem bezpieczeństwa przez ukrywanie

- Ang. „security through obscurity"
- Koncepcja „wiedzy koniecznej"
- Utajnianie to postawienie wszystkiego na jedną kartę
- Co i kiedy ujawniać?

Etapy tworzenia struktur bezpieczeństwa

- Planowanie
- Ocena ryzyka
- Analiza kosztów i zysków
- Tworzenie strategii odpowiadającej konkretnym potrzebom
- Implementacja
- Audyt i reagowanie na incydenty

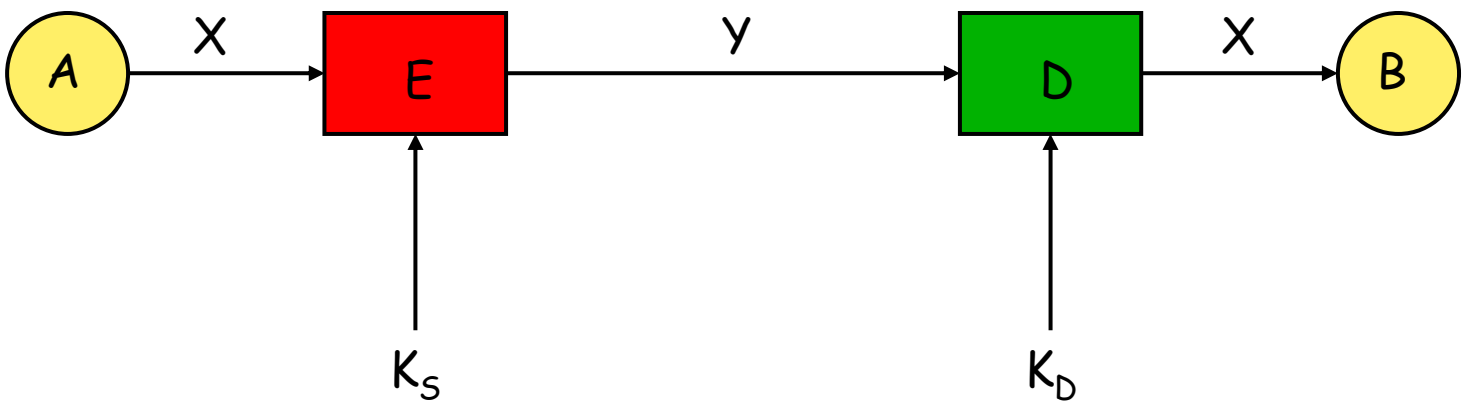
Kryptologia

- Kryptologia = kryptografia + kryptoanaliza
- Szyfrowanie: takie przekształcenie wiadomości (tekstu jawnego), by była ona dla osoby trzeciej jedynie przypadkowym ciągiem znaków (tekst zaszyfrowany, szyfrogram), nie pozwalającym na odtworzenie żadnej użytecznej informacji.

Historia kryptologii

- ok. 1900 r. p.n.e. – zaszyfrowane inskrypcje grobowe
- ok. 475 r. p.n.e. – kryptografia w łączności (Sparta), szyfr transpozycyjny
- ok. 350 r. p.n.e. – traktat Eneasza o kryptografii
- ok. 60 r. p.n.e. – szyfr Cezara
- 1412 – traktat Kalkashandiego o kryptoanalizie
- 1917 – maszyna rotorowa (Hebern)
- 1971 – system Lucifer (IBM)
- 1975 – standard DES (zaaprobowany w 1977 r.)
- 1976 – koncepcja klucza jawnego (Diffie, Hellmann)
- 1978 – algorytm RSA (Rivest, Shamir, Adelman)

Proces szyfrowania



- $Y = E_{K_S}(X)$; $X = D_{K_D}(Y)$;
- $E_{K_S} = (D_{K_D})^{-1}$

Kryteria podziału systemów kryptograficznych

- Ze względu na rodzaj operacji
  - podstawieniowe
  - przestawieniowe
  - kaskadowe
- Ze względu na liczbę używanych kluczy
  - symetryczne, z jednym kluczem, z tajnym kluczem, konwencjonalne
  - asymetryczne, z dwoma kluczami, z jawnym kluczem
- Ze względu na sposób przetwarzania tekstu jawnego
  - blokowe
  - strumieniowe

Bezpieczeństwo algorytmów szyfrowania

- bezwarunkowo bezpieczne – tekst zaszyfrowany nie zawiera dostatecznej ilości informacji, by jednoznacznie określić odpowiadający mu tekst jawny
- obliczeniowo bezpieczne - spełnione przynajmniej jedno z kryteriów:
  - kryterium czasu
  - kryterium kosztów

Metoda brutalna

Rozmiar klucza	Liczba możliwych kluczy	Czas odkrycia klucza (1/μs)	Czas odkrycia klucza (10^6/μs)
32 bity	$2^{32} = 4{,}3 \times 10^9$	35,8 min	2,15 ms
56 bitów	$2^{56} = 7{,}2 \times 10^{16}$	1142 lata	10,01 h
128 bitów	$2^{128} = 3{,}4 \times 10^{38}$	$5{,}4 \times 10^{24}$ lat	$5{,}4 \times 10^{18}$ lat
26 znaków	$26! = 4{,}03 \times 10^{26}$	$6{,}4 \times 10^{12}$ lat	$6{,}4 \times 10^{6}$ lat

$$k \times t \approx \text{const}$$