Szyfrowanie informacji

Szyfrowanie jest sposobem ochrony informacji przed zinterpretowaniem ich przez osoby niepowołane, lecz nie chroni przed ich odczytaniem lub skasowaniem.

Informacje niezaszyfrowane przechowywane czy przesyłane w systemach informatycznych (sieciach) można traktować jako informacje ujawnione, pomimo użycia innych środków ochrony przed niepowołanym dostępem.

Szyfrowanie to jedyny znany, skuteczny sposób realizacji ochrony informacji przesyłanej w sieci. W szyfrowaniu informacji wykorzystuje się szyfry – tj. rodzinę przekształceń służących do nadawania informacji postaci niezrozumiałej lub bezużytecznej dla napastnika.

Sam proces szyfrowania polega na przekształceniu informacji (jawnej) w inną (tzw. kryptogram lub tekst zaszyfrowany) za pomocą funkcji matematycznej oraz hasła szyfrowania (tzw. klucza). Proces odwrotny, nazywany deszyfrowaniem polega na tym, że kryptogram jest przekształcany z powrotem w oryginalną informację jawną za pomocą pewnej funkcji matematycznej i klucza.

W praktyce zachodzi potrzeba szyfrowania łańcuchów znaków (hasła, dane informacyjne), liczb (dane typu byte, word, integer, longint) oraz rekordów i zbiorów. Rodzaj szyfrowanej informacji, a przede wszystkim sposób jej wykorzystania, wpływa na wybór systemu kryptograficznego (systemu szyfrowania).

Z szyfrowaniem związane są takie pojęcia jak:

- **kryptologia** – nauka o szyfrach;
- **kryptografia** – nauka o konstruowaniu i stosowaniu szyfrów;
- **kryptoanaliza** – nauka o łamaniu szyfrów.

Podstawowe typy algorytmów kryptograficznych

Obecnie najczęściej są stosowane systemy szyfrowania wykorzystujące przekształcenia matematyczne. W ramach tej grupy systemów można wyróżnić dwa podstawowe typy algorytmów szyfrowych:

- algorytmy z kluczem prywatnym, w których tego samego klucza używa się do szyfrowania i odszyfrowania informacji (tzw. algorytmy z kluczem symetrycznym);
- algorytmy z kluczem publicznym (tzw. algorytmy z kluczem asymetrycznym), w których używa się klucza publicznego do zaszyfrowania informacji, a klucza prywatnego do jej odszyfrowania (klucz publiczny – bo można go udostępnić publicznie bez utraty tajności informacji oraz klucza do deszyfrowania).

Występujący w podanych typach algorytmów termin „klucz", oznacza klucz kryptograficzny, czyli ciąg symboli, od którego w sposób istotny zależy wynik przekształcenia kryptograficznego (np. szyfrowania, deszyfrowania, obliczania kryptograficznej funkcji kontrolnej, obliczania podpisu lub weryfikacji podpisu).

W publikacjach związanych z szyfrowaniem informacji można znaleźć szereg innych kontekstów użycia terminu 'klucz":

- **klucz podpisu** – element danych specyficzny dla podmiotu i stosowany jedynie przez ten podmiot w procesie podpisywania;
- **klucz prywatny** – element pary kluczy asymetrycznych podmiotu, stosowany jedynie przez ten podmiot, który w przypadku systemu szyfrowania asymetrycznego określa przekształcenie deszyfrujące, a w przypadku systemu podpisywania asymetrycznego określa przekształcenie podpisu. Oznacza również:

  $\Rightarrow$ w kryptografii klucz, który jest przeznaczony do deszyfrowania, stosowany wyłącznie przez właściciela,

⇒ w systemie kryptograficznym klucz z pary kluczy użytkownika, który jest znany jedynie przez użytkownika.

- **klucz prywatny podpisu** – element pary kluczy asymetrycznych podmiotu, który służy do określenia prywatnego przekształcenia podpisu;
- **klucz publiczny –** klucz przeznaczony do stosowania przez dowolny podmiot w celu szyfrowania komunikowania się z właścicielem odpowiedniego klucza prywatnego. Oznacza również:

  ⇒ klucz, który jest publicznie znany, ale niekoniecznie jest ogólnie dostępny. Może być dostępny jedynie dla wszystkich członków wstępnie określonej grupy,

  ⇒ w systemie kryptograficznym klucz z pary kluczy użytkownika, który jest publicznie znany.
- **klucz do szyfrowania danych –** klucz kryptograficzny wykorzystywany do szyfrowania i deszyfrowania danych;
- **klucz szyfrowania kluczy** – klucz kryptograficzny stosowany do szyfrowania i deszyfrowania kluczy szyfrujących dane, lub innych kluczy szyfrujących klucze;
- **klucz tajny –** klucz stosowany przez ograniczoną liczbę korespondentów do szyfrowania i deszyfrowania danych;
- **klucz weryfikacji –** element danych odpowiadający kluczowi podpisu podmiotu i wykorzystywany w procesie weryfikacji.

Każdy klucz ma przypisany przedział czasu (tzw. okres ważności klucza kryptograficznego), w którym określony klucz uprawniony jest do użytku lub w którym klucze dla danego systemu mogą pozostawać skuteczne. Z kluczami związane jest zwykle centrum certyfikacji kluczy, tj. ośrodek generujący i wydający certyfikaty, nadzorowany przez organ certyfikacji. Certyfikat klucza jest to zatem informacja o kluczu podmiotu podpisana przez organ certyfikacji, co powoduje, że jest niemożliwa do podrobienia.

Porównanie typów systemów kryptograficznych pozwala uwypuklić ich następujące właściwości:

1. Algorytmy z kluczem prywatnym
   - wspólny tajny klucz – tajność klucza decyduje o bezpieczeństwie!
   - konieczne wcześniejsze bezpieczne uzgodnienia klucza,
   - łatwa realizacja poufności i uwierzytelniania,
   - duża szybkość działania,
   - bezpieczeństwo informacji jest zależne od rozmiaru przestrzeni kluczy,
   - Najbardziej znany system: DES (Data Encryption Standard).
2. Algorytmy z kluczem publicznym
   - para kluczy u każdego użytkownika,
   - klucz szyfrujący jest jawny, może być opublikowany,
   - klucz deszyfrujący jest tajny, ma go tylko właściciel,
   - łatwa realizacja niezaprzeczalności i dystrybucji kluczy,
   - mała szybkość działania,
   - konstrukcja związana z arytmetyką dużych liczb całkowitych,
   - bezpieczeństwo informacji jest zależne od znalezienia efektywnych rozwiązań problemów arytmetyki dużych liczb całkowitych,
   - najbardziej znany system: RSA (Rivest Shamir Adleman).

Ze względu na cechy charakterystyczne obu ww. algorytmów, w praktyce stosuje się tzw. algorytmy hybrydowe, w których algorytm z kluczem publicznym służy do wymiany losowych kluczy sesji, które są później używane do algorytmu z kluczem prywatnym.

Każdy z systemów (algorytmów) kryptograficznych będzie posiadał pewne wspólne elementy, takie jak:

- algorytm szyfrowania
- klucze szyfrowania
- długość klucza

- informację jawną (do zaszyfrowania)
- kryptogram (informację zaszyfrowaną).

Zdolność systemu kryptograficznego do ochrony informacji przed atakiem nazywana jest mocą kryptograficzną. Zależy ona od takich czynników jak:

- tajność klucza;
- stopień skomplikowania klucza (trudność odgadnięcia lub przebadania wszystkich możliwych kluczy);
- podatność na złamanie algorytmu szyfrowania (tj. możliwość odwrócenia algorytmu szyfrowania bez znajomości klucza szyfrującego);
- podatność na atak z tekstem jawnym (tj. możliwość odszyfrowania kryptogramu, jeżeli jest znana część informacji pierwotnej);
- znajomość przez napastnika cech charakterystycznych zaszyfrowanej informacji (regularności w przesyłanej informacji);
- inne, oprócz znajomości klucza, sposoby odczytywania informacji (tzw. tylne drzwi).

Inny sposób klasyfikacji algorytmów szyfrowania to ich podział na algorytmy tajne i jawne. Algorytm tajny (firmowy) posiada następujące cechy charakterystyczne:

- bezpieczeństwo oparte nie tylko na tajności klucza, ale i na **tajności algorytmu;**
- mniejsza liczba użytkowników – zatem mniejsza motywacja do złamania szyfru.

Algorytm jawny (powszechnie znany) posiada następujące cechy charakterystyczne:

- możliwość niezależnej oceny odporności na złamanie;
- możliwość zastosowania w międzynarodowej elektronicznej wymianie danych;

- możliwość normalizacji w ramach danego kraju;
- łatwość i wiarygodność testów;
- dostosowanie norm i zaleceń (ISO, CCITT) do właściwości systemów DES i RSA.

Na informację zaszyfrowaną można przeprowadzić ataki (tj. próby rozszyfrowania informacji) na szereg sposobów:

- **atak analityczny** – próba przełamania kodu lub znalezienia klucza metodami systematycznymi (np. statystyczna analiza wzorców symbolicznych; wykrywanie szczelin w algorytmie szyfrowania). Jest przeciwieństwem ataku na zasadzie pełnego przeglądu.
- **atak tekstem zaszyfrowanym** – atak analityczny, podczas którego kryptoanalityk dysponuje jedynie tekstem zaszyfrowanym;
- **atak za pomocą wybranego tekstu jawnego** – atak polegający na tym, że kryptoanalityk może wykonać eksperyment szyfrowania wiadomości i obserwowania skutków takiego szyfrowania;
- **atak znanym tekstem jawnym** – atak analityczny, podczas którego kryptoanalityk dysponuje w istotnych ilościachtekstem jawnym i odpowiadającym mu tekstem zaszyfrowanym;
- **atak na zasadzie pełnego przeglądu** – atak na zabezpieczenia systemu informatycznego poprzez wypróbowanie wszystkich możliwych wartości kluczy lub haseł. Jest przeciwieństwem ataku analitycznego.

Przegląd kryptosystemów

1. Kryptosystem DES

Został zaprojektowany przez IBM przy pomocy NSA *(National Security Agency)*. Co pięć lat poddawany jest ocenie bezpieczeństwa. W 1987r. NSA wycofała poparcie dla DES'a. W 1993r. został przyjęty przez NIST na kolejne 5 lat.

DES jest szyfrem blokowym, wykorzystującym wielowarstwową sieć podstawieniowo-przestawieniową. Posiada 64-bitowe bloki wiadomości jawnej i szyfrogramu oraz 64-bitowy klucz (efektywnie 56 bitów). Szybkości szyfrowania są różne w zależności od sposobu implementacji algorytmu:

- programowa: x*100kbps
- sprzętowa: x*10 Mbps (NIST dopuszcza tylko implementacje sprzętowe).

Możliwe tryby pracy kryptosystemu DES:

- **tryby blokowe:**
  - ⇒ **ECB** *Electronic Code Book),* zalecana tylko dla krótkich i losowych wiadomości. W tymtzw. „trybie elektronicznej książki kodowej", każdy blok danych wejściowych jest szyfrowany za pomocą tego samego klucza, a dane wejściowe są zapisywane w postaci bloku. Metoda ta nie zawiera mechanizmu informowania o tym, że jakąś wiadomość wstawiono lub usunięto;
  - ⇒ **CBC** *Clipher Block Chaining),* każdy blok szyfrogramu zależy od wszystkich poprzednich bloków wiadomości. W tym tzw. „trybie wiązania bloków zaszyfrowanych", na danym bloku tekstu jawnego jest przed zaszyfrowaniem wykonywana różnica symetryczna z zaszyfrowaną wiadomością z poprzedniego bloku. Wynik tej operacji jest następnie szyfrowany za pomocą zwykłego klucza.
- **tryby strumieniowe** (są k razy wolniejsze, $1 \leq k \leq 64$)
  - ⇒ **CFB** *(Cipher Feedback).* W tym trybie (tzw. sprzężenia zwrotnego zaszyfrowanego tekstu) dane wejściowe sąz powrotem wprowadzone na wejście. Część każdego zaszyfrowanego bloku jest przenoszona do rejestru przesuwnego. Zawartość rejestru jest szyfrowana z użyciem klucza szyfrowania za pomocą trybu ECB, a na wyniku wykonywana jest różnica symetryczna ze strumieniem danych, tworząc ostateczny wynik szyfrowania. Zaleta tego trybu to samosynchronizacja, umożliwiająca

deszyfrowanie małych porcji dużego ciągu danych, poczynając od miejsca leżącego w ustalonej odległości od początku.

⇒ **OFB** *(Output Feedback).* W tym trybie (tzw. sprzężenia zwrotnego bloków wyjściowych) dane wyjściowe są wprowadzone na wejście. Rejestr przesuwny jest inicjowany pewną znaną wartością (tzw. wektor inicjujący), a następnie zawarta w nim informacja jest szyfrowana z użyciem klucza szyfrującego w trybie ECB. Wynik jest używany jako klucz do szyfrowania bloku danych i jest również zapisywany z powrotem do rejestru do użycia w następnym bloku. Zaletą tego trybu jest brak propagacji błędów.

- **tryb wielokrotnego szyfrowania,** np.:

  ⇒ 2 klucze: $E_{K1}D_{K2}E_{K1}$

  ⇒ zgodny z pojedynczym przebiegiem gdy K1=K2.

Bezpieczeństwo oferowane przez kryptosystem DES można scharakteryzować następująco:

- nie znaleziono słabych punktów algorytmu;
- jedyny skuteczny atak, to przeszukiwanie przestrzeni kluczy przy ataku ze znanym tekstem jawnym;
- średnia ilość operacji przeszukiwania: 2^{55}. Potrzebny na to czas jest zależny od konfiguracji sprzętu, np. dla maszyny jednoprocesorowej (jedna operacja co 5μs) wynosi ponad 10 000 lat.

Możliwości zastąpienia kryptosystemu DES są następujące:

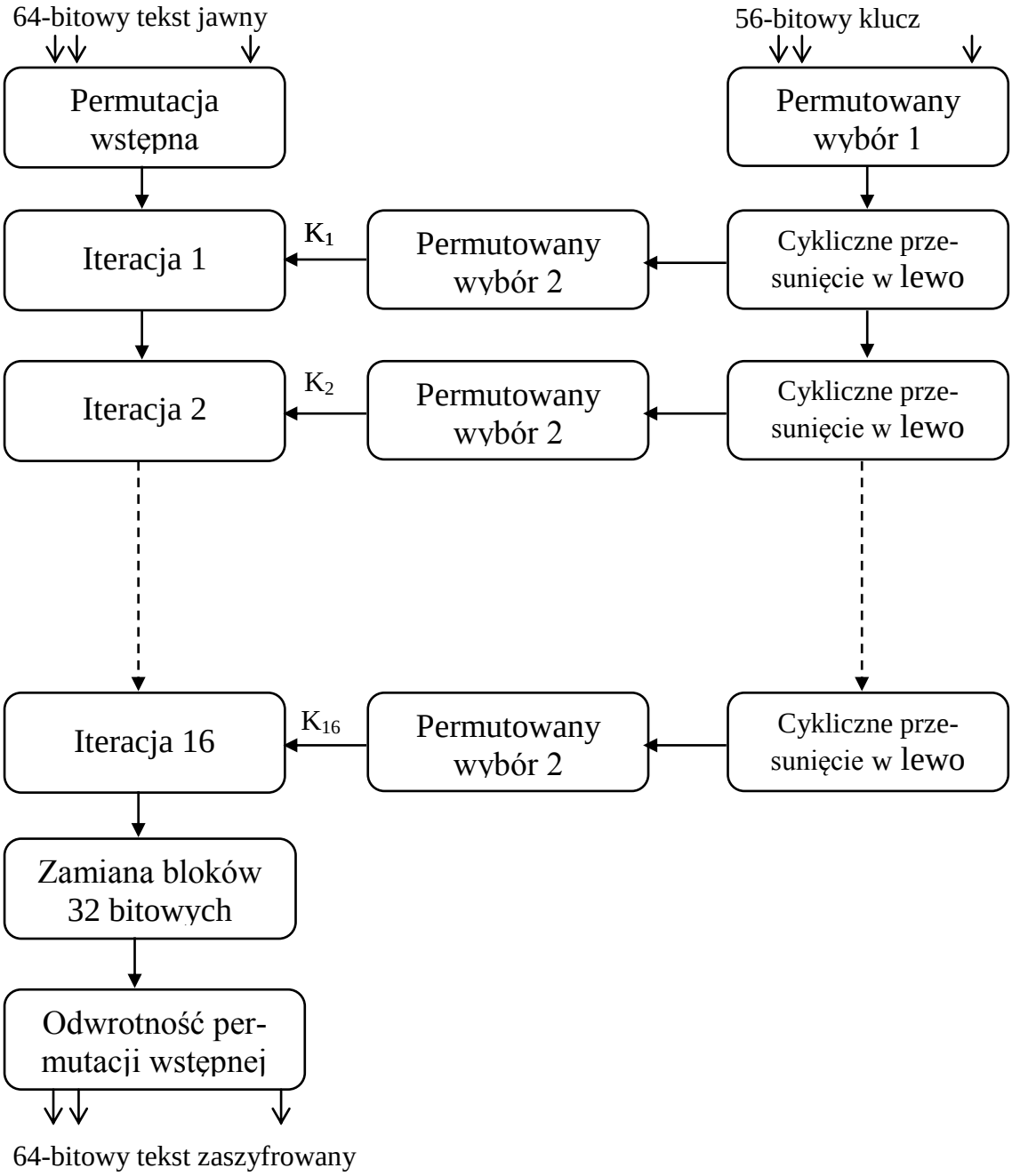
- potrójne szyfrowanie – 3 różne klucze, 3-krotnie mniejsza szybkość (największe szanse na rozpowszechnienie);
- schematy *NxM* DES (wiele kluczy, pojedynczy DES jako operacja składowa, dłuższe bloki, nie do końca rozpoznane własności);
- wykorzystanie kryptosystemu *IDEA*;
- wykorzystanie kryptosystemu *Clipper*.

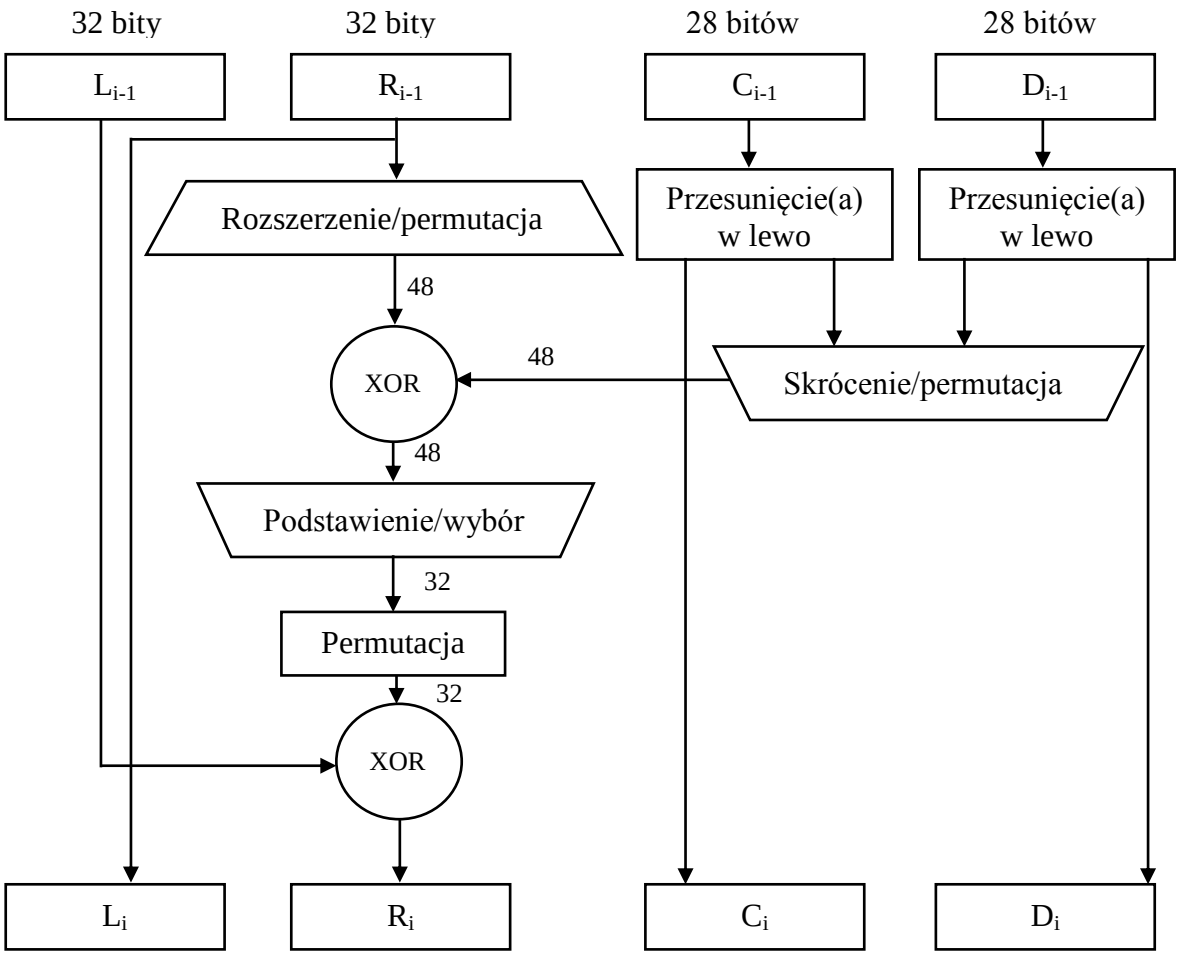
2. Kryptosystem IDEA *(International Data EncryptionAlgorithm)*

Został opracowany pod koniec lat 80-tych w ETH (Szwajcaria). Jest to szyfr blokowy, iteracyjny, oparty na trzech operacjach arytmetycznych. Zawiera 64-bitowe bloki i 128-bitowy klucz. Tryby pracy jak dla DES'a (jest ok. dwukrotnie szybszy od DES'a). Jego stosowanie jest ograniczone szeregiem patentów.

3, Kryptosystem *Clipper Chip*

Jest to w zasadzie propozycja rządu amerykańskiego, opublikowana w 1993r. jako zalecenie dla przemysłu. Zawiera tajny algorytm *Skipjack*, opracowany przez NSA. Posługuje się 80-bitowym kluczem (prędkość szyfrowania 14Mbps). Realizacja tego kryptosystemu jest wykonywana tylko w układzie scalonym produkowanym przez jedną firmę. Z założenia istnieje możliwość podsłuchu przez uprawnione agencje rządowe (z tego powodu kontrowersyjny technicznie i prawnie). Jego druga generacja nosi nazwę *Capstone.*


64-bitowy tekst jawny
56-bitowy klucz
Permutacja wstępna
Permutowany wybór 1
Iteracja 1
K1
Permutowany wybór 2
Cykliczne przesunięcie w lewo
Iteracja 2
K2
Permutowany wybór 2
Cykliczne przesunięcie w lewo
Iteracja 16
K16
Permutowany wybór 2
Cykliczne przesunięcie w lewo
Zamiana bloków 32 bitowych
Odwrotność permutacji wstępnej
64-bitowy tekst zaszyfrowany


32 bity
32 bity
28 bitów
28 bitów
L_{i-1}
R_{i-1}
C_{i-1}
D_{i-1}
Rozszerzenie/permutacja
Przesunięcie(a) w lewo
Przesunięcie(a) w lewo
48
XOR
48
Skrócenie/permutacja
48
Podstawienie/wybór
32
Permutacja
32
XOR
L_i
R_i
C_i
D_i