Technologia informacyjna

Ochrona danych

Janusz Uriasz

Kryptologia

Kryptologia, jako nauka ścisła, bazuje na zdobyczach matematyki, a w szczególności teorii liczb i matematyki dyskretnej.

Kryptologia (z gr. κρυπτός – *kryptos* – "ukryty" i λόγος – *logos* – "słowo") – nauka o przekazywaniu informacji w sposób zabezpieczony przed niepowołanym dostępem. Podstawowe pojęcia:

- *tekst jawny*
- *tekst zaszyfrowany*
- *szyfr* - opis przekształceń szyfrujących i deszyfrujących, podawany najczęściej w postaci funkcji matematycznej (występujące w nich odwzorowania parametryczne nazywane są *kluczami)*

Kryptologię dzieli się na:

Kryptografia – nauka, która zajmuje się utajnianiem informacji

Kryptoanaliza – poszukuje dróg jej odzyskiwania z postaci utajnionej

Kryptografia

- **Kryptografia symetryczna** to taki rodzaj szyfrowania, w którym tekst jawny ulega przekształceniu na tekst zaszyfrowany za pomocą pewnego klucza, a do odszyfrowania jest niezbędna znajomość tego samego klucza.
- Bezpieczeństwo takiego szyfrowania zależy od:
- ilości możliwych kluczy, czyli długości klucza

Wszystkie tradycyjne szyfry miały charakter symetryczny.

Popularne szyfry symetryczne to m.in.:

AES (*Advanced Encryption Standard*,)

DES (*Data Encryption Standard*)

ENIGMA – maszyna szyfrująca oparta na w swej pracy na zasadzie obracających się wirników.

Kryptologia

Szyfrowanie – proces zamiany tekstu jawnego w szyfr

Deszyfrowanie – proces odwrotny

Szyfr - jest parą algorytmów służących do przeprowadzenia obu procesów.

Klucz – jest uzupełnieniem algorytmów parametrów (niezbędny parametr), od którego zależy wynik obu procesów. Inaczej: znajomość algorytmu i szyfrogramu bez dostępu do klucza nie pozwoli na odtworzenie tekstu jawnego.

Historia szyfrów

- Szyfry ***przestawieniowe*** - zmiana kolejności znaków tekstu jawnego
- Szyfry ***podstawieniowe*** - zamienniki dla poszczególnych części składowych tekstu (posługiwał się już J.Cezar)
- Odwzorowania ***kaskadowe -*** złożenie *n* kolejnych przekształceń $F_1,...,F_n$, z których każde F_i może być podstawieniem lub przestawieniem. Do połowy lat siedemdziesiątych szyfry kaskadowe uważane były za najlepsze
- Odwzorowania ***homofoniczne*** (jednemu znakowi tekstu jawnego przyporządkowuje się jeden z wielu znaków, tzw. *homofonów*) - stosowany, aby ograniczyć podatność nierównomiernego występowania liter języka naturalnego na kryptoanalizę

DES (Data Encryption Standard)

- Opracował IBM (konkurs na potrzeby rządu amerykańskiego)
- Zalety: trudny do złamania, możliwość wyprodukowania bardzo szybkich sprzętowych układów szyfrująco-deszyfrujących
- Wady algorytmu:
  - mała długość klucza (oryginalne rozwiązanie o nazwie Lucypher miało 112 bitów, ale na życzenie agencji nadzorującej konkurs długość klucza zmniejszono o połowę)
  - używa klucza symetrycznego
- 3DES - polega na trzykrotnym użyciu trzech różnych kluczy o długości 56 bitów. Wskutek tego zabiegu czas potrzebny na złamanie tak zakodowanej wiadomości wydłuża się z dnia do bilionów lat

Konkursy

- RSA Data Security - ogłasza serię konkursów na złamanie DES
- Wyniki: 1997 – 96 dni, 1998 – 56 godz., 1999 – 22 godz.
- Wygrywa distributed.net (superkomputer Deep Crack oraz około stu tysięcy komputerów PC połączonych za pośrednictwem Internetu)
- W 1997 r. RSA ogłosiło roku serię dwunastu zawodów dotyczących łamania algorytmu RC5. Trzy najłatwiejsze zadania (dla kluczy 40-, 48- i 56-bitowych) zostały rozwiązane, ale trwają próby odczytania pozostałych zakodowanych informacji
- distributed.net - specjalny program, który umożliwia każdej osobie podłączonej do Internetu wykonanie części obliczeń potrzebnych do otrzymania nagrody (współudział w nagrodzie)
- Udział w konkursie biorą także Polacy (RC5 Polish Official Team – PWr)

RSA

- 1978 r. - szyfrowanie z wykorzystaniem operacji potęgowania
- Na tej idei oparto algorytm ***RSA*** (Rivesta, Shamira i Adlemana)
- Odwzorowanie RSA umożliwia stosowanie metod szyfrowania z ***kluczem jawnym*** (publicznym) i ***kluczem niejawnym*** (prywatnym)
- Algorytm RSA ma również poważną wadę - jest bardzo wolny. Zaszyfrowanie takiej samej wiadomości za pomocą DES-a trwa ponad 1000 razy krócej (niekiedy wiadomość szyfruje się DES-em, a RSA kodowany jest klucz używany w DES-ie)
- Metody te znalazły zastosowanie nie tylko w systemach utajniania informacji, lecz również w systemach uwierzytelniania i w podpisach cyfrowych

Jakość szyfrów

- Jakość szyfru zależy od własności matematycznych użytego odwzorowania
- Szyfr ***przełamywalny*** – jeżeli istnieje możliwość odtworzenia tekstu jawnego lub klucza na podstawie tekstu zaszyfrowanego
- Szyfr ***bezwarunkowo bezpieczny*** - jeżeli niezależnie od ilości przechwyconego tekstu zaszyfrowanego nie można jednoznacznie określić tekstu jawnego (w praktyce można mówić co najwyżej o szyfrach ***obliczeniowo bezpiecznych)***
- Utrzymywaniu w tajemnicy przekształceń szyfrujących i deszyfrujących nie świadczy o jakości ochrony
- Długości klucza nie powodują istotnego zwiększenia poziomu ochrony przed atakami kryptoanalitycznymi

Podpis elektroniczny i cyfrowy certyfikat

- Podpis elektroniczny - zabezpiecza elektroniczny obrót dokumentów. Wykorzystują go powszechnie banki, co pozwala błyskawicznie dokonać przelewów i innych operacji finansowych oraz ZUS (system Płatnik). Urzędy muszą być przygotowane na elektroniczny obieg dokumentów

- Certyfikat cyfrowy - poświadcza tożsamość właściciela narzędzi, które umożliwiają składanie podpisu. Urzędy wydające certyfikaty, jednocześnie udostępniają je wszystkim chętnym, chcącym sprawdzić prawdziwość podpisu

- Cechy podpisu i certyfikatu:
  - *Integralność* – czyli pewność, że podpisany dokument nie został zmodyfikowany
  - *Wiarygodność* – czyli pewność, że dokument pochodzi od osoby, która ją wysłała
  - *Niezaprzeczalność* -czyli brak możliwości zaprzeczenie faktu złożenia podpisu
  - *Poufność* - dane nie zostaną odczytanie przez osoby nieuprawnione
  - *Korzyści ekonomiczne* – czas, finanse

Podpis cyfrowy

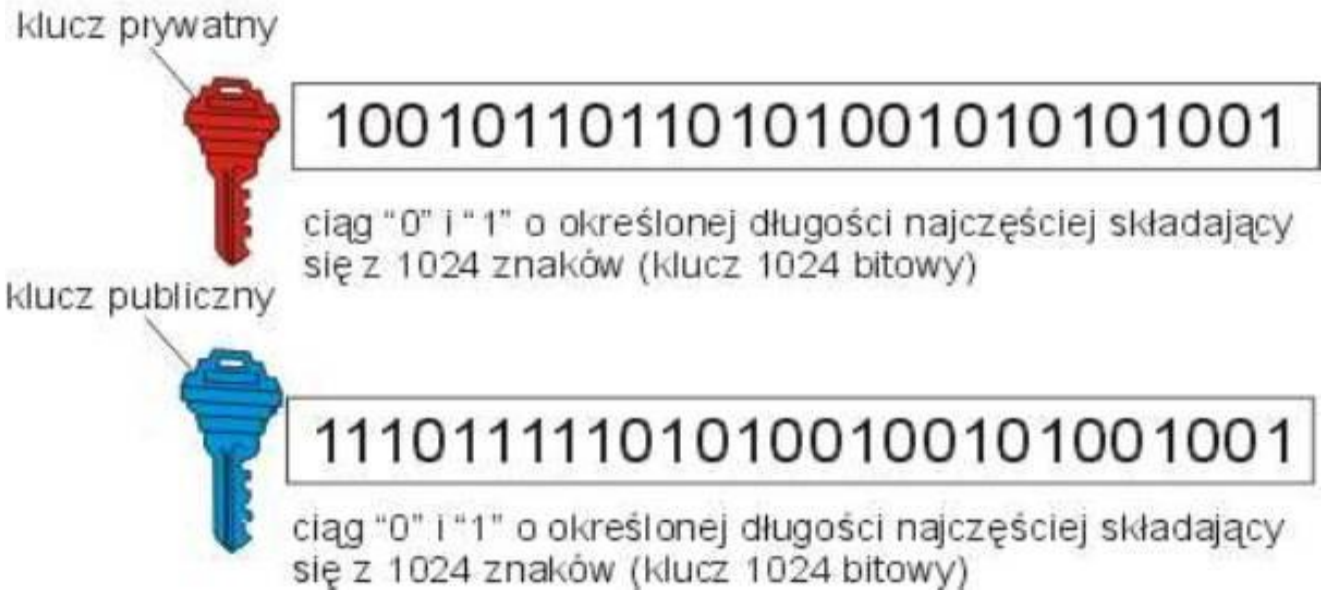
Podpis elektroniczny – pojęcie normatywne zdefiniowane w ustawie z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2001 r. Nr 130, poz. 1450 z późn. zm). Zgodnie z art.3 pkt 1 ustawy podpis elektroniczny stanowią dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny.

Podpis cyfrowy

- jest przyporządkowany wyłącznie do osoby składającej ten podpis,
- jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,
- jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.

Podpis elektroniczny i cyfrowy certyfikat

klucz prywatny jest znany i używany tylko przez jedną osobę
klucz publiczny jest ogólnie dostępny



Certyfikat


CERTYFIKAT
klucz publiczny
klucz prywatny
Certyfikat Klucza Publicznego
dane osoby
posługującej
się certyfikatem
Jan Kowalski
FIRMA
ważny do
2004-06-01
data ważności certyfikatu
podpis Centrum Certyfikacji
wydającego certyfikat

Szyfrowanie i deszyfrowanie