Podstawy Kryptologii

Kamil Król

20 stycznia 2018

Politechnika Śląska, Wydział Matematyki Stosowanej

Spis treści

Wprowadzenie

Kryptologia

Kryptologia – dziedzina wiedzy o przekazywaniu informacji w sposób zabezpieczony przed niepowołanym dostępem.
Współcześnie kryptologia jest uznawana za gałąź zarówno matematyki, jak i informatyki.
Kryptologię dzieli się na:

- kryptografię - czyli gałąź wiedzy o utajnianiu wiadomości;
- kryptoanalizę - czyli gałąź wiedzy o przełamywaniu zabezpieczeń

Terminologia

Istotnym elementem technik kryptograficznych jest proces zamiany tekstu jawnego w szyfrogram (inaczej kryptogram); proces ten nazywany jest **szyfrowaniem**, a proces odwrotny, czyli zamiany tekstu zaszyfrowanego na powrót w możliwy do odczytania, **deszyfrowaniem**.

Przez **szyfr** rozumiana jest para algorytmów służących do przeprowadzenia obu procesów. Wraz z algorytmami dodatkowo używa się **kluczy**, czyli pewnych niezbędnych parametrów, od których zależy wynik obu procesów. Innymi słowy: znajomość algorytmu i szyfrogramu bez dostępu do klucza nie pozwoli na odtworzenie tekstu jawnego.

Terminologia

Kryptografia nie zajmuje się jednak wyłącznie szyfrowaniem i deszyfrowaniem tekstów. Po pierwsze, dane przekazywane są najczęściej w postaci binarnej, co umożliwia również obróbkę takich danych jak dźwięk czy obraz; po drugie, równie ważne jak zapewnianie poufności danych jest ich **integralność** (niezmienność danych w czasie procesu), **uwierzytelnianie** (pewność co do ich pochodzenia) oraz **niezaprzeczalność** (nadawca nie może wyprzeć się faktu, że był nadawcą wiadomości).

Ważnym terminem używanym w kryptografii jest **kryptosystem**, a więc system obejmujący zastosowane w danym wypadku szyfry, metody generowania kluczy, urządzenia wraz z oprogramowaniem oraz procedury ich użycia. Istotnym aspektem kryptosystemu jest jego bezpieczeństwo – odporność na ataki kryptologiczne.

Szyfr Cezara

Opis szyfru

Szyfr Cezara (zwany też szyfrem przesuwającym, kodem Cezara lub przesunięciem Cezariańskim) – jedna z najprostszych technik szyfrowania.

Jest to rodzaj szyfru podstawieniowego, w którym każda litera tekstu jawnego (niezaszyfrowanego) zastępowana jest inną, oddaloną od niej o stałą liczbę pozycji w alfabecie, literą (szyfr monoalfabetyczny), przy czym kierunek zamiany musi być zachowany.

Nie rozróżnia się przy tym liter dużych i małych. Nazwa szyfru pochodzi od Juliusza Cezara, który prawdopodobnie używał tej techniki do komunikacji ze swymi przyjaciółmi.

Przykład

Sposób szyfrowania może być przedstawiony za pomocą diagramu dwóch ciągów z odpowiadającymi sobie kolejnymi literami alfabetu. Te same litery drugiego ciągu są przesunięte względem ciągu pierwszego o określoną liczbę pozycji, zwaną parametrem przesunięcia (tutaj 3) i pełniącą funkcję klucza szyfru:

Dane: AĄBCĆDEĘFGHIJKLŁMNŃOÓPRSŚTUWYZŹŻ

Szyfr: CĆDEĘFGHIJKLŁMNŃOÓPRSŚTUWYZŹŻAĄB

Przykład

Należy przy tym zauważyć, że ostatnim literom alfabetu w górnym ciągu odpowiadają początkowe litery w ciągu dolnym (alfabet został „zawinięty").

Chcąc zaszyfrować wiadomość, należy każdą jej literę zastąpić odpowiednikiem z szyfru (wiadomość w przykładzie jest zapisana wersalikami, aczkolwiek szyfr jest niewrażliwy na wielkość liter):

Tekst jawny: MĘŻNY BĄDŹ, CHROŃ PUŁK TWÓJ

Tekst szyfr: OHBÓŻ DĆFĄ, EKTRP ŚZŃM YŹSŁ

Ujęcie matematyczne

Operację szyfrowania i deszyfrowania można wyrazić w języku arytmetyki modularnej.

W tym celu wystarczy każdej literze alfabetu jednoznacznie przypisać jej numer według schematu A-0, Ą-1, B-2, . . . , Ż-31.

Wygodnie jest też przyjąć, że klucz n jest pewną liczbą z zakresu 0...31 (jest to numer zaszyfrowanej litery A).

Ujęcie matematyczne

Szyfrowanie i Deszyfrowanie:

x - numer litery tekstu jawnego w alfabecie

n - liczba pozycji do przesuniecia litery tekstu jawnego

s - zaszyfrowany znak

Szyfrowanie:

$s = x + (n(mod 32))$

Deszyfrowanie:

$x = s - (n(mod 32))$

Algorytm Szyfrowania RSA

Podstawowe Informacje

RSA – jeden z pierwszych i obecnie najpopularniejszych asymetrycznych algorytmów kryptograficznych z kluczem publicznym, zaprojektowany w 1977 przez Rona Rivesta, Adi Shamira oraz Leonarda Adlemana.

Pierwszy algorytm, który może być stosowany zarówno do szyfrowania jak i do podpisów cyfrowych.

Bezpieczeństwo szyfrowania opiera się na trudności faktoryzacji dużych liczb złożonych.

Jego nazwa pochodzi od pierwszych liter nazwisk jego twórców

Kryptosystem RSA

Aytmetyka modulo i właściwości liczb pierwszych są podstawą szyfru RSA - techniki szyfrowania asymetrycznego z kluczem publicznym.

Proces szyfrowania wyglądają następująco: Uzytkownik X wybiera dwie dowolne, duże liczby pierwsze p i q (im są większe, tym lepiej, gdyż od ich wielkosci zalezy bezpieczeństwo szyfru). Aby uprościc obliczenia, w poniższym przykładzie wybrane zostały liczby 11 i 17.

Następnie X oblicza liczę n będącą iloczynem tych dwóch liczb ($n = 187$). Trzeba jeszcze wybrać liczbę e, która wspólnie z iloczynem n stanowić będzie klucz szyfrujacy.

Liczby e oraz (p-1)*(q-1) powinnym być względnie pierwsze. Załóżmy, że $e = 7$.

Kryptosystem RSA

Obie te liczby (n i e) podawane są do wiadomości wszystkkich, którzy chcieliby wysłac zaszyfrowaną wiadomość do danego użytkownika. Aby to zrobić, należy w pierwszej kolejności przekształcić wysłaną wiadomość do postali liczbowej.

Stosowany jest tu standard ASCII. Niech przesłanym znakiem będzie litera A. W kodzie ASCII symbolowi temu odpowiada kombinacja 01000001. Po przeliczeniu na system dziesiętny przyjmuje ona wartośc 65.

Tekst jawny wynosi więc $J = 65$.

Kryptosystem RSA

Wartość tekstu tajnego obliczana jest według wzoru:

$S = J^e (mod n)$

a zatem

$S = 65^7 (mod 187) = [65^4 (mod 187) * 65^2 (mod 187) * 65 (mod 187)] mod 187$

W celu usprawnienia obliczeń korzysta się tu z własności potęgowania:

$a^{n+m} = a^n * a^m$

oraz z własności arytmetyki modulo:

$(a * b) mod n = ((a mod n) * (b mod n)) mod n$

czyli:

$[17850625 (mod 187) * 4225 (mod 187) * 65] mod 187 =$
$(166 * 111 * 65) mod 187 = [7215 (mod 187) * 166 (mod 187)] mod 187 =$
$109 * 166 (mod 187) = 142$

Wiadomość po zaszyfrowaniu ma zatem postać $S = 142$.

Kryptosystem RSA

Warto zauważyć, że dla kogoś, kto posiada tylko publiczne klucze, odwrócenie działania funkcji jest niemożliwe.

Nawet jeśli zna on algorytm szyfrowania, nie jest w stanie powiedzieć, jakie były dane wejściowe, ponieważ $142 = 329(\text{mod}187)$ lub $471(\text{mod}187)$ lub $163(\text{mod}187)$ itd. Dopiero wartość $65^7(\text{mod}187)$ jest poprawna.

Aby sprawdzić całą przestrzeń kluczy i dojść aż do tej wartości w rozsądnym czasie potrzeba ogromnej mocy obliczeniowej.

Kryptosystem RSA

Aby odwrócić działanie funkcji szyfrującej, należy uruchomic jej "zapadkę", czyli klucz deszyfrujący. Użytkownik X oblicza go ze wzoru:

$ke = 1 mod (p-1)(q-1)$

Tak więc:

$7k = 10 * 16 + 1 = 161$

stąd :

$k = 161/7 = 23$

Teraz użytkownik X używa swojego tajnego klucza, aby odczytać wiadomość.Dekryptaż odbywa się według poniższego wzoru:

$j = S^k (mod n)$

Kryptosystem RSA

Wstępne obliczenia wyglądają nastepująco:

$J = 142^{23}(mod 187) = [142^{16}(mod 187) * 142^{4}(mod 187) * 142^{2}(mod 187) * 142^{1}(mod 187)]mod(187)$

$142^{1}(mod 187) = 142$

$142^{2}(mod 187) = 155$

$142^{4} mod 187 = (142^{2} mod 187)^{2} mod 187 = 155^{2} mod 187 = 89$

$142^{8} mod 187 = (142^{4} mod 187)^{2} mod 187 = 89^{2} mod 187 = 67$

$142^{16} mod 187 = (142^{8} mod 187)^{2} mod 187 = 67^{2} mod 187 = 1$

Kryptosystem RSA

Ósma potęga liczby 142 nie wystepuje we wzorze obliczającym wartość tekstu jawnego, jej wyznaczenie ułatwia jednak obliczenie wartości $142^{16} mod 187$.

Wstawiamy teraz obliczone reszty modulo kolejnych potęg do wzoru głównego:

$$142^{23}(mod187) = (1 * 89 * 155 * 142) mod 187 = [(89 * 155 mod 187) *$$

$$(142 mod 187)] mod 187 = (144 * 142) mod 187 = 20448 mod 187 = 65$$

Długość i zastosowanie kluczy szyfrujących

Dłygośc klucza	Zastosnowanie
$512b < 2048b$	brak
$2048b < 4096b$	dla cywilów
$4096b+$	wojskowe

MD5

Podstawowe informacje

MD5 (z ang. Message-Digest algorithm 5) – algorytm kryptograficzny, opracowany przez Rona Rivesta (współtwórcę RSA) w 1991 roku, będący popularną kryptograficzna funkcją skrótu, która z ciągu danych o dowolnej długości generuje 128-bitowy skrót.

Funkcja skrótu, funkcja mieszająca lub funkcja haszująca – funkcja przyporządkowująca dowolnie dużej liczbie krótką, zawsze posiadającą stały rozmiar, niespecyficzną, quasi-losową wartość, tzw. skrót nieodwracalny.

W informatyce funkcje skrótu pozwalają na ustalenie krótkich i łatwych do weryfikacji sygnatur dla dowolnie dużych zbiorów danych.

Przykład

Skrót obliczony dla krótkiego tekstu:

MD5("Ala ma kota") = 91162629d258a876ee994e9233b2ad87

Nawet niewielka zmiana w tekście (w tym przypadku zamiana a na y) powoduje (z bardzo dużym prawdopodobieństwem) powstanie zupełnie innego skrótu MD5

MD5("Ala ma koty") = 6a645004f620c691731b5a292c25d37f

Przykład

Dość powszechnym zastosowaniem MD5 jest generowanie skrótów wszelkiego rodzaju plików udostępnianych publicznie (najczęściej w Internecie), dzięki czemu osoba, która pobrała dany plik z sieci może od razu zweryfikować (generując skrót MD5 na swojej kopii i porównując wyniki) czy jest to ten sam plik, który został zamieszczony przez jego autora lub czy nie nastąpiły przekłamania podczas samego procesu pobierania danych.

Publikowana w takim przypadku wartość ma postać 32-znakowej liczby w zapisie szesnastkowym.

Wynik MD5 dla archiwum "linux-2.6.10.tar.bz2" o wielkości 35 MB: cffcd2919d9c8ef793ce1ac07a440eda

Bibliografia

Witryny internetowe:

https://pl.wikipedia.org/wiki/Kryptologia Kryptologia

https://pl.wikipedia.org/wiki/Szyfr_Cezara Szyfr Cezara

https://pl.wikipedia.org/wiki/RSA_(kryptografia) RSA

https://pl.wikipedia.org/wiki/MD5 MD5

Literatura:

Podstawy kryptografii. Wydanie III - Marcin Karbowski

Dziękuję za uwagę