Wstęp

Kryptografia lub kryptologia, jest praktyką i badaniem technik bezpiecznej komunikacji w obecności wrogiego zachowania. Mówiąc bardziej ogólnie, kryptografia polega na konstruowaniu i analizowaniu protokołów, które uniemożliwiają osobom trzecim lub opinii publicznej odczytywanie prywatnych wiadomości; różne aspekty bezpieczeństwa informacji, takie jak poufność danych, integralność danych, uwierzytelnianie i niezaprzeczalność są kluczowe dla nowoczesna kryptografia.

Historia

Kryptografia sprzed ery nowożytnej była praktycznie synonimem szyfrowania, przekształcania informacji ze stanu czytelnego w niezrozumiały nonsens w celu wykluczenia jej odczytania przez osoby niemające klucza do odszyfrowania, a które mogłyby tę wiadomość przechwycić lub podsłuchać. Jednym z najwcześniejszych szyfrów podstawieniowych był szyfr Cezara, w którym każda litera tekstu jawnego zastępowana była literą oddaloną o pewną ustaloną liczbę pozycji w alfabecie. Szyfr ten został nazwany na cześć Juliusza Cezara, który używał go (z przesunięciem o 3) do komunikacji podczas kampanii wojskowych.

Szyfrowanie z kluczem symetrycznym

Termin kryptografia symetryczna odnosi się do metod, w których nadawca i odbiorca wiadomości używają tego samego klucza (rzadziej: różnych kluczy, ale łatwych do wyliczenia jeden na podstawie drugiego). Szyfry z kluczem symetrycznym są zaimplementowane jako szyfry blokowe lub strumieniowe.

Szyfr blokowy polega na szyfrowaniu bloku wejściowego (np. fragmentu pliku) na podstawie zadanego klucza, przekształcając go na blok wyjściowy o takiej samej długości w taki sposób, że niemożliwe jest odwrócenie tego przekształcenia bez posiadania klucza.

Szyfr strumieniowy (także: algorytm strumieniowy, algorytm potokowy) – algorytm symetryczny, który szyfruje oddzielnie każdy bit wiadomości. Algorytm ten składa się z generatora strumienia bitowego, będącego kluczem szyfrującym oraz elementu dodającego (na przykład operacji XOR).

Kryptografia klucza publicznego

Kryptografia klucza publicznego (kryptografia asymetryczna) – rodzaj kryptografii, w którym jeden z używanych kluczy jest udostępniony publicznie. Każdy użytkownik może użyć tego klucza do zaszyfrowania wiadomości, ale tylko posiadacz drugiego, tajnego klucza może odszyfrować taką wiadomość. Istnieją również bardziej zaawansowane algorytmy wykorzystujące więcej kluczy i inne zależności między kluczami.

Kryptografia asymetryczna opiera się na funkcjach jednokierunkowych – takich, które da się łatwo wyliczyć w jedną stronę, ale bardzo trudno w drugą. Np. mnożenie jest łatwe, a rozkład na czynniki (z ang. faktoryzacja) trudny (na czym przykładowo opiera się RSA).

Algorytm RSA

W celu wygenerowania pary kluczy (prywatnego i publicznego) należy posłużyć się algorytmem:

Wybieramy dwie duże liczby pierwsze {p, q}(>200cyfr)

Obliczamy iloczyn n = p\*q

Losujemy liczby 1 < e < (p-1)(q-1)

e jest względnie piewszą liczbą: (p-1)(q-1)

e jest kluczem szyfrującym

wyliczamy liczby d o własności e\*d = 1(mod(p-1)(q-1)), tzn d jest odwrotnością modulo liczby e

liczby d i e oraz d i n są względnie pierwsze

d jest kluczem deszyfrującym

{e, n} są ujawnionym kluczem publicznym

{d, n} są tajnym kluczem prywatnym

Ciągły wzrost mocy obliczeniowej komputerów zwiększa długość klucza, przy której atak typu brute-force może się powieść. Przedmiotem troski niektórych kryptografów są ewentualne efekty potencjalnego rozwoju obliczeń przy pomocy komputerów kwantowych.

Liczby pierwsze

Liczba pierwsza – liczba naturalna większa od 1, która ma dokładnie dwa dzielniki naturalne: jedynkę i siebie samą.

Aby znaleźć wszystkie liczby pierwsze w zadanym przedziale liczbowym, można posłużyć się algorytmem zwanym sitem Eratostenesa: jeśli liczba naturalna N N {\displaystyle N} większa od 1 nie jest podzielna przez żadną z liczb pierwszych nie większych od pierwiastka z N , {\displaystyle N,} N to N N {\displaystyle N} jest liczbą pierwszą

ηξζξβζγεΑδ