04. Kryptografia z kluczem publicznym

**Kryptografia z kluczem** publicznym jest to kryptografia **asymetryczna**. Kryptografię dzielimy na symetryczną i asymetryczną.

**Kryptografia Symetryczna** - służy np. do szyfrowania symetrycznego. Szyfrowanie to opiera się o wykorzystanie pojedynczego klucza. Klucz ten służy do szyfrowania oraz do deszyfrowania wiadomości. Do obu tych czynności używa się tego samego klucza, dlatego powinien być znany tylko uczestnikom. Np. szyfr cezara

**Kryptografia Asymetryczna** - służy do:

* szyfrowania asymetrycznego
* podpisów cyfrowych

Kryptografia asymetryczna zakłada istnienie dwóch zależnych od siebie kluczy. Jeden z kluczy jest kluczem publicznym(można go publicznie pokazywać), drugi kluczem prywatnym(jeśli nieporządana osoba pozna ten klucz wówczas może np. odszyfrować wiadomość).

Klucz publiczny używany jest do zaszyfrowania informacji, klucz prywatny do jej odczytu. Ponieważ klucz prywatny jest w wyłącznym posiadaniu adresata informacji, tylko on może ją odczytać. Natomiast klucz publiczny jest udostępniony każdemu, kto zechce zaszyfrować wiadomość.

Scenariusz szyfrowania wiadomości:

Użytownik B chce wysłać użytkownikowi A zaszyfrowaną wiadomość. Użytkownik A udostępnia klucz publiczny użytkownikowi B. Użytkownik B szyfruje wiadomość kluczem publicznym użytkownika A i wysyła wiadomość. Uzytkownik A odbiera wiadomość i deszyfruje ją swoim kluczem prywatnym.

Najpopularniejszym algorytmem szyfrującym za pomocą kryptografii asymetrycznej jest **RSA:**

Wybierzmy dwie różne i duże (2512) liczby pierwsze *p* i *q* i niech *n = pq*. Wybierzmy ponadto liczbę *e* **względnie pierwszą** [[1]](#footnote-1)z iloczynem *(p − 1)(q − 1).* Para *(n, e)* tworzy tak zwany klucz publiczny kryptosystemu: możemy taką parę ogłosić publicznie. Każdy zainteresowany może teraz przekazać nam zaszyfrowaną wiadomość, którą jedynie my będziemy w stanie odczytać. Załóżmy, że wiadomości będą resztami modulo n. Szyfrowanie wiadomości *a* za pomocą klucza *(n,e)* polega na obliczeniu

*s = ae mod n.*

Aby odszyfrować taką wiadomość, musimy przygotować sobie tak zwany klucz prywatny. Ponieważ

***NWD(****e, (p − 1)(q − 1)****)*** *= 1*, więc istnieją liczby naturalne *d* i *k*, dla których

*ed − k(p − 1)(q − 1) = 1.*

Co więcej, liczby te możemy efektywnie obliczyć, stosując rozszerzony algorytm Euklidesa. Klucz tajny stanowi para *(n,d)*, a odszyfrowanie polega na obliczeniu

*sd mod n.*

Dlaczego prowadzi to do odtworzenia wiadomości a? Zauważmy najpierw, że

*sd ≡ (ae)d = aed = a1+k(p-1)(q-1 ) = a,*

gdzie ≡ oznacza kongruencję modulo n.  
**Stwierdzenie**. Jeżeli p i q są różnymi liczbami pierwszymi i *n = pq*, to dla dowolnych *a ∈ Z* i *k ∈ N* zachodzi

*a1+k(p-1)(q-1) ≡ a (mod n)*

Dowód. Załóżmy na razie, że liczba a jest niepodzielna przez p. Wówczas z  
małego twierdzenia Fermata

*ap-1 ≡ 1 (mod p).*

Podnosząc kongruencję stronami do potęgi o wykładniku k(q − 1), a następnie przemnażając przez a, otrzymujemy

*a1+k(p-1)(q-1)  ≡ a (mod p).*

Jeżli liczba a jest podzielna przez p, to po obu stronach kongruencji mamy liczbę podzielną przez p, a więc kongruencja zachodzi w rzeczywistości dla wszystkich liczb całkowitych a. Tak samo możemy dowieźć analogicznej kongruencji modulo q. Ponieważ p i q jako różne liczby pierwsze są względnie pierwsze, więc  
przystawanie modulo p i q implikuje przystawanie modulo n = pq.

Warto wspomnieć, że pomiędzy kluczem prywatnym i kluczem publicznym nie ma róznicy – jeśli wyślemy klucz prywatny komuś to wówczas używamy publicznego jako prywatny. Czyli prywatnym możemy zaszyfrować a publicznym odszyfrować. Wynika to z przemienności możenia aed = ade.

Warto również wspomnieć, że trudność w rozszyfrowaniu wiadomości przez osoby nieporządane polega na odnalezieniu liczb p oraz q które są na ogół bardzo dużymi liczbami pierwszmi a jak wiemy nie ma wzoru na liczby pierwsze. Istnieją jedynie algorytmy, które w nieefektywnym czasie wyznaczają kolejne liczby pierwsze (np. sito erastotenesa).

**Podpisy cyfrowe:**

Strona uwierzytelniająca (nadawca) wylicza skrót (hash) podpisywanej wiadomości. Następnie szyfruje ten skrót swoim kluczem prywatnym i jako podpis cyfrowy dołącza do oryginalnej wiadomości. Dowolna osoba posiadająca klucz publiczny może sprawdzić autentyczność podpisu, poprzez odszyfrowanie skrótu za pomocą klucza publicznego nadawcy i porównanie go z własnoręcznie wyliczonym na podstawie wiadomości.

Natomiast podpis elektoroniczny to: Podpis elektroniczny obejmuje wszelkie metody w postaci elektronicznej służące potwierdzeniu tożsamości osoby dokonującej czynności prawnej, np.: PIN-y, hasła dostępu, numery kart kredytowych, zeskanowany podpis własnoręczny, „podpis klawiaturowy” pod e-mailem. Taki podpis elektroniczny nie gwarantuje pewnej identyfikacji osoby z uwagi na łatwość jego „podrobienia”, np. „wycięcia” zeskanowanego podpisu własnoręcznego z jednego dokumentu i przeniesienie go na inny dokument.

1. Związane z rozszerzonym twierdzeniem Euklidesa. e musi być względnie pierwsze z (p-1)(q-1) po to aby zawsze istniało jakieś d i k takie, że *ed − k(p − 1)(q − 1) = 1. A z rozszerzonego Eukl. wiemy że wtedy istnieją.* [↑](#footnote-ref-1)