# Podstawy kryptografi - algorytm DSA

Adam Czerwonka 242374
Marcel Badek 242352
Wtorek 12.15-13.45

# Podpis Cyfrowy DSA

## Cel zadania

Celem zadania jest implementacja podpisu cyfrowego przy pomocy algorytmu DSA.

## Działanie algorytmu

W algorytmie możemy wyróżnić trzy części: generacja kluczy, podpis oraz weryfikacja.

### Generacja kluczy

1. Wybieramy losową liczbę $L$ taką, że

$$512 < L < 1024$$
$$L \bmod 64 = 0$$

2. Wybieramy liczbę pierwszą $q$ z 160 bitami w rozwinięciu dwójkowym
3. Wybieramy liczbę pierwszą $p$ z $L$ bitami w rozwinięciu dwójkowym taką żę $p-1$ jest wielokrotnością $q$
4. Wybieramy losową liczbę $h$ z zakresu $\{2 \dots p-2\}$
5. Obliczamy $g$. Jeżeli $g = 1$ to wybieramy inne $h$

$$g = h^{(p-1)/q} \bmod p$$

6. Wybieramy losową liczbę $x$ z zakresu $\{1 \dots q-1\}$
7. Obliczamy $y$

$$y = g^x \bmod p$$

Liczby $(p, q, g)$ są parametrami algorytmu i są publiczne.
Liczba $x$ to klucz prywatny.
Liczba $y$ to klucz publiczny.

### Podpis

W celu podpisania wiadomości $m$ musimy wykonać następujące kroki:

1. Wybieramy losową liczbę $k$ z zakresu $\{1 \dots q-1\}$
2. Obliczamy $r$. Jeżeli $r = 0$ wybieramy inne $k$

$$r = (g^k \bmod p) \bmod q$$

3. Obliczamy $s$. Jeżeli $s = 0$ wróć do kroku 1.

$$s = (k^{-1}(H(m) + xr)) \bmod q$$

Podpis to para liczb: $(r, s)$.

## Weryfikacja

W celu weryfikacji podpisu $(r, s)$ dla wiadomości $m$ musimy wykonać następujące kroki:

1. Sprawdzenie, że

$$0 < r < q$$

$$0 < s < q$$

2. Obliczamy $w$

$$w = s^{-1} \bmod q$$

3. Obliczmy $u_1$

$$u_1 = H(m) \cdot w \bmod q$$

4. Obliczamy $u_2$

$$u_2 = r \cdot w \bmod q$$

5. Obliczamy $v$

$$v = (g^{u_1} y^{u_2} \bmod q) \bmod q$$

Jeżeli $v = r$ to podpis jest zgodny z przekazaną wiadomością.