ZAKRES MATERIAŁU

I. Grupy. Niezbędne fakty i definicje

[DEF] (grupa)
Zbiór G, w którym określone jest działanie ° i spełnione następujące własności
(1) $\forall a,b,c\ (a°b)°c=a°(b°c)$ łączność działania °,
(2) $\exists e\ \forall a\ (e°a=a°e=a)$ istnienie w G elementu neutralnego działania °
(3) $\forall a\ \exists a^{-1}\ (a°a^{-1}=a^{-1}°a=e)$ dla każdego a∈G istnienie (dokładnie jednego) elementu odwrotnego
---

[Przykład 01] Każdy ze zbiorów Z (zbiór liczb całkowitych), Q (zbiór liczb wymiernych), R (zbiór liczb rzeczywistych) z działaniem + (dodawania) jest grupą. Elementem neutralnym jest liczba 0, a odwrotnym dla a – wartość -a. Są to grupy addytywne odpowiednio liczb całkowitych (Z,+), liczb wymiernych (Q,+) i liczb rzeczywistych (R,+).

[Przykład 02] Każdy ze zbiorów Q\{0}, R\{0} z działaniem * (mnożenia) jest grupą. Elementem neutralnym jest liczba 1, a odwrotnym dla a – wartość a^{-1}. Są to grupy multiplikatywne odpowiednio liczb wymiernych (Q\{0},*) i liczb rzeczywistych (R\{0},*).

[DEF] (rząd grupy)
Grupę składającą się ze skończonej liczby elementów nazywamy **grupą skończoną**, wówczas **rzędem grupy** nazywamy liczbę jej elementów.

[DEF] (grupa multiplikatywna reszt modulo m (ozn Z_m^*))

- Grupa odwracalnych klas reszt modulo m.
- Jej rząd (ozn. φ(m)) wyznaczamy korzystając z funkcji Eulera φ. φ(m) jest liczbą tych liczb całkowitych a∈{1,...,m}, dla których NWD(a,m)=1.

[Przykład 03] Z_{18}^* = {1,5,7,11,13,17} jest grupą multiplikatywną reszt modulo 18. Stąd rząd grupy Z_{18}^* jest równy φ(18)=6. Zauważmy, że dla a∈{1,5,7,11,13,17} NWD(a,18)=1, zatem dla każdego a istnieje element odwrotny (mod18).
1*1(mod 18)=1, a=1, a^{-1}=1,
5*11(mod 18)=1, a=5, a^{-1}=11,
7*13(mod 18)=1, a=7, a^{-1}=13,
11*5(mod 18)=1, a=11, a^{-1}=5,
13*7(mod 18)=1, a=13, a^{-1}=7,
17*17(mod 18)=1, a=17, a^{-1}=17.
---

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
φ(m)	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

Kilka wartości funkcji Eulera

[TW] Jeśli m jest liczbą pierwszą, to φ(m)=m-1 ponieważ dla każdego a∈{1,...,m-1} NWD(a,m)=1).

[Przykład 04] Z_{13}^* = {1,2,3,4,5,6,7,8,9,10,11,12} jest grupą multiplikatywną reszt modulo 13. Stąd rząd grupy Z_{13}^* jest równy φ(13)=12. Zauważmy, że dla a∈{1,2,3,4,5,6,7,8,9,10,11,12} NWD(a,13)=1, zatem dla każdego a istnieje element odwrotny (mod13).

[DEF] (grupa cykliczna)
Grupa G, w której istnieje element g o tej własności, że każdy element z G jest jego potęgą.

- Element g nazywamy wówczas **generatorem grupy cyklicznej** (ozn. G=<g>).
- Stąd G=<g> wtw $\exists g\in G\ \forall a\in G\ \exists n\in Z\ (g=a^n)$

[Przykład 05] Z_5^* = {1,2,3,4} jest grupą cykliczną. Jej generatorem jest liczba 2 i liczba 3.

Z_5^* =<2>={2^1=2, 2^2=4, 2^3=3, 2^4=1},

Z_5^* =<3>={3^1=3, 3^2=4, 3^3=2, 3^4=1}.

[DEF] (podgrupa H grupy G (ozn. H<G))
Podzbiór H grupy G, będący grupą względem działania w G, tj.
Jeśli G jest grupą i H niepustym podzbiorem, to [H<G] wtw $[(a,b\in H) \Rightarrow (a°b\in H \wedge a^{-1}\in H)]$

[Przykład 06] Grupa multiplikatywna liczb wymiernych jest podgrupą grupy multiplikatywnej liczb rzeczywistych.

[DEF] (rząd elementu g grupy G (ozn. $rząd_G g$))
Jeśli podgrupa <g> grupy G jest skończona i ma rząd n, to mówimy, że g jest elementem rzędu n.
Jeśli <g> jest grupą nieskończoną, to g jest elementem rzędu nieskończonego.

[Przykład 07] Weźmy grupę multiplikatywną reszt modulo 7 (Z_7^* ={1,2,3,4,5,6}).

rząd1=1, ponieważ <1>={1},
rząd2=3, ponieważ <2>={1, 2, 4}, ponieważ 2^1=2, 2^2=4, 2^3=1, 2^4=2, 2^5=4, 2^6=1,
rząd3=6, ponieważ <3>={1, 2, 3, 4, 5, 6}, ponieważ 3^1=3, 3^2=2, 3^3=6, 3^4=4, 3^5=5, 3^6=1,
rząd4=3, ponieważ <4>={1, 2, 4}, ponieważ 4^1=4, 4^2=2, 4^3=1, 4^4=4, 4^5=2, 4^6=1,
rząd5=6, ponieważ <5>={1, 2, 3, 4, 5, 6}, ponieważ 5^1=5, 5^2=4, 5^3=6, 5^4=2, 5^5=3, 5^6=1,
rząd6=2, ponieważ <6>={1, 6}, ponieważ 6^1=6, 6^2=1, 6^3=6, 6^4=1, 6^5=6, 6^6=1.

[TW] Rząd każdego elementu grupy G jest dzielnikiem rzędu grupy G.

[TW] Jeśli grupa G jest skończona i cykliczna, to G ma dokładnie φ(|G|) generatorów i jej wszystkie generatory mają rząd |G|.

[Przykład] Kontynuacja przykładu 05. Z_5^* = {1,2,3,4} jest grupą cykliczną, ma φ(| Z_5^* |)=φ(4)=2 generatory, tj. Z_5^* =<2> i Z_5^* =<3> oraz rząd2=4 i rząd3=4.

[TW] Jeśli p jest liczbą pierwszą, to grupa Z_p^* ma następujące własności

(a) Rząd grupy Z_p^* : $\varphi(p)=p-1$,

(b) Rząd każdego elementu grupy Z_p^* jest dzielnikiem liczby p-1,

(c) Z_p^* jest grupą cykliczną,

[TW] Niech p będzie liczbą pierwszą i Z_p^* grupą multiplikatywną reszt modulo p.

(a) Element α rzędu p-1 nazywamy **elementem pierwotnym** modulo p.

(b) Element α jest elementem pierwotnym wtw $\{\alpha^i : 0 \le i \le p-2\} = Z_p^*$.

(c) Niech α będzie elementem pierwotnym modulo p.

- Każdy element $\beta \in Z_p^*$ można jednoznacznie zapisać w postaci $\beta = \alpha^i$, gdzie $0 \le i \le p-2$.
- Rząd elementu β jest równy $(p-1)/NWD(p-1,i)$.

(d) β jest elementem pierwotnym wtw $NWD(p-1,i)=1$.

(e) Liczba elementów pierwotnych modulo p jest równa $\varphi(p-1)$.

[Przykład 08] Niech p=17. Wyznacz wszystkie elementy pierwotne modulo p.

$Z_p^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$,

- Niech $\alpha=2$ (czy 2 jest elementem pierwotnym (mod 17)?)
  $2^0=1$, $2^1=2$, $2^2=4$, $2^3=8$, $2^4=16$, $2^5=15$, $2^6=13$, $2^7=9$, $2^8=1$, więc
  $<2>=\{1, 2, 4, 8, 9, 13, 15, 16\}$, rząd2=8, więc 2 nie jest elementem pierwotnym modulo 17,
- Niech $\alpha=3$ (czy 3 jest elementem pierwotnym (mod 17)?)
  $3^0=1$, $3^1=3$, $3^2=9$, $3^3=10$, $3^4=13$, $3^5=5$, $3^6=15$, $3^7=11$, $3^8=16$, $3^9=14$, $3^{10}=8$, $3^{11}=7$, $3^{12}=4$, $3^{13}=12$, $3^{14}=2$, $3^{15}=6$,
  $<3>=\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\} = Z_p^*$, $\alpha=3$ jest elementem pierwotnym (mod 17).

Elementów pierwotnych modulo 17 jest $\varphi(16)=8$,
Pozostałe elementy pierwotne modulo 17 to
$\beta = 4 = 3^{12} \pmod{17}$ i $NWD(16,12)=4\neq1$, więc $\beta=4$ nie jest elementem pierwotnym modulo 17,
$\beta = 5 = 3^{5} \pmod{17}$ i $NWD(16,5)=1$, więc $\beta=5$ jest elementem pierwotnym modulo 17,
$\beta = 6 = 3^{15} \pmod{17}$ i $NWD(16,15)=1$, więc $\beta=6$ jest elementem pierwotnym modulo 17,
$\beta = 7 = 3^{11} \pmod{17}$ i $NWD(16,11)=1$, więc $\beta=7$ jest elementem pierwotnym modulo 17,
$\beta = 8 = 3^{10} \pmod{17}$ i $NWD(16,10)=2\neq1$, więc $\beta=8$ nie jest elementem pierwotnym modulo 17,
$\beta = 9 = 3^{2} \pmod{17}$ i $NWD(16,2)=2\neq1$, więc $\beta=9$ nie jest elementem pierwotnym modulo 17,
$\beta = 10 = 3^{3} \pmod{17}$ i $NWD(16,3)=1$, więc $\beta=10$ jest elementem pierwotnym modulo 17,
$\beta = 11 = 3^{7} \pmod{17}$ i $NWD(16,7)=1$, więc $\beta=11$ jest elementem pierwotnym modulo 17,
$\beta = 12 = 3^{13} \pmod{17}$ i $NWD(16,13)=1$, więc $\beta=12$ jest elementem pierwotnym modulo 17,
$\beta = 13 = 3^{4} \pmod{17}$ i $NWD(16,4)=4\neq1$, więc $\beta=13$ nie jest elementem pierwotnym modulo 17,
$\beta = 14 = 3^{9} \pmod{17}$ i $NWD(16,9)=1$, więc $\beta=14$ jest elementem pierwotnym modulo 17,
$\beta = 15 = 3^{6} \pmod{17}$ i $NWD(16,6)=2\neq1$, więc $\beta=15$ nie jest elementem pierwotnym modulo 17,
$\beta = 16 = 3^{8} \pmod{17}$ i $NWD(16,8)=8\neq1$, więc $\beta=16$ nie jest elementem pierwotnym modulo 17,
Elementy pierwotne modulo 17 {3, 5, 6, 7, 10, 11, 12, 14}

II. Problem logarytmu dyskretnego

[Problem] (logarytmu dyskretnego)
Niech p będzie ustaloną liczbą pierwszą, a α ustalonym elementem pierwotnym modulo p.

Należy znaleźć dla ustalonego elementu $\beta \in Z_p^*$ (jednoznacznie określony) wykładnik a, taki że $\alpha^a \equiv \beta \pmod p$ dla $0 \le a \le p-2$.

[Przykład 09] Niech p=17, α=3, β=14. Znajdź (metodą kolejnych prób) logarytm o podstawie α z wartości β w arytmetyce modulo p.

$3^0 = 1 \equiv 1 \pmod{17}$, $3^1 = 3 \equiv 3 \pmod{17}$, $3^2 = 9 \equiv 9 \pmod{17}$, $3^3 = 27 \equiv 10 \pmod{17}$,

$3^4 = 81 \equiv 13 \pmod{17}$, $3^5 = 243 \equiv 5 \pmod{17}$, $3^6 = 729 \equiv 15 \pmod{17}$, $3^7 = 2187 \equiv 11 \pmod{17}$,

$3^8 = 6561 \equiv 16 \pmod{17}$, $3^9 = 19683 \equiv 14 \pmod{17}$

wykładnik a=9.

III. Algorytm Shanksa

[Algorytm] (Shanksa dla problemu logarytmu dyskretnego)

Niech p będzie ustaloną liczbą pierwszą, α ustalonym elementem pierwotnym modulo p i niech $\beta \in Z_p^*$.

Algorytm wyznacza logarytm o podstawie α z wartości β w arytmetyce modulo p.

Niech $m = \left\lfloor \sqrt{p-1} \right\rfloor$.

(1) for(int j=0; j<m; j++) dodaj do listy L1 (uporządkowanej ze względu na II współrzędną) parę $(j, \alpha^{mj} \pmod p)$

(2) for(int i=0; i<m; i++) dodaj do listy L2 (uporządkowanej ze względu na II współrzędną) parę $(i, \beta\alpha^{-i} \pmod p)$

(3) znajdź dwie pary o tej samej drugiej współrzędnej, tj. parę $(j, y) \in L1$ i parę $(i, y) \in L2$,

(4) wyznacz $\log_\alpha \beta = mj + i \pmod{p-1}$.

[Przykład 10] Przeanalizuj algorytm Shanksa dla parametrów p=17, α=3 i β = 14.

$m = \left\lfloor \sqrt{17-1} \right\rfloor = \left\lfloor \sqrt{16} \right\rfloor = \lceil 4 \rceil = 4$, $\alpha^{-1} = 6$,

L1: $(0, 3^{(0*4)} \pmod{17}=1)$, $(3, 3^{(3*4)} \pmod{17}=4)$, $(1, 3^{(1*4)} \pmod{17}=13)$, $(2, 3^{(2*4)} \pmod{17}=16)$,
L2: $(2, 14*6^2 \pmod{17}=11)$, $(0, 14*6^0 \pmod{17}=14)$, $(3, 14*6^3 \pmod{17}=15)$, $(1, 14*6^1 \pmod{17}=16)$,
Dwie pary o tej samej drugiej współrzędnej to (2, 16) i (1, 16),

$\log_\alpha \beta = 4*2+1 \pmod{16} = 9$,

wykładnik a=9

IV. Protokół wymiany klucza Diffiego-Hellmana

Uzgadnianie kluczy – protokół ustalania tajnego klucza przez osoby komunikujące się. Komunikacja protokołu odbywa się kanałem publicznym.

[Algorytm] (Protokół wymiany kluczy Diffiego-Hellmana)

Zakładamy, że p jest liczbą pierwszą, a α - elementem pierwotnym w Z_p^*. Para (p, α) jest znana publicznie.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

(1) Osoba U losuje wartość a_U ze zbioru {0,...,p-2},

(2) U wyznacza wartość $\alpha^{a_U} \pmod p$ i przekazuje ją osobie V,

(3) Osoba V losuje wartość a_V ze zbioru {0,...,p-2},

(4) V wyznacza wartość $\alpha^{a_V} \pmod p$ i przekazuje ją osobie U,

(5) U wyznacza klucz $K = (\alpha^{a_V})^{a_U} \bmod p$,

(6) U wyznacza klucz $K = (\alpha^{a_U})^{a_V} \bmod p$,

Po zakończeniu protokołu obaj użytkownicy U i V mają ten sam klucz $K = \alpha^{a_U a_V} \pmod p$.

Zaletą protokołu jest nowy klucz po każdorazowym uruchomieniu protokołu (za każdym razem losowane są nowe wartości a_U i a_V).

[Przykład 11] Wygeneruj klucz zgodnie z protokołem wymiany kluczy Diffiego-Hellmana dla parametrów p=17, α=10.

Osoba U: Niech $a_U = 13$, $\alpha^{a_U} \pmod p = 10^{13} \pmod{17} = 11$, $K = (\alpha^{a_V})^{a_U} \bmod p = 14^{13} \pmod{17} = 5$

Osoba V: Niech $a_V = 19$, $\alpha^{a_V} \pmod p = 10^{19} \pmod{17} = 14$, $K = (\alpha^{a_U})^{a_V} \bmod p = 11^{19} \pmod{17} = 5$

V. Schematy podpisów

- **Wiarygodny czynnik** (ozn. TA) – czynnik odpowiedzialny m.in. za ustalenie tożsamości użytkownika, wybór klucza, przekazanie go użytkownikom.

- Schematy podpisów (podpisy cyfrowe).
- Stosowanie podpisów cyfrowych zapobiega możliwość fałszerstwa.
- Podpis cyfrowy może zweryfikować każdy (na podstawie publicznego algorytmu weryfikacji).
- Schemat podpisu składa się z **algorytmu podpisu** i **algorytmu weryfikacji**.
- B może podpisać wiadomość x za pomocą algorytmu podpisu sig, a następnie A może zweryfikować podpis sig(x) za pomocą publicznego algorytmu weryfikacji ver.

[Schemat] (podpisu cyfrowego)

Piątka uporządkowana $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ spełniająca warunki

(1) $\mathcal{P}$ - skończony zbiór możliwych wiadomości,

(2) $\mathcal{A}$ - skończony zbiór możliwych podpisów,

(3) $\mathcal{K}$ - skończony zbiór możliwych kluczy,

(4) Dla każdego $K \in \mathcal{K}$ istnieje tajny **algorytm podpisu** $sig_K \in \mathcal{S}$ oraz odpowiadający mu jawny **algorytm weryfikacji** $ver_K \in \mathcal{V}$.

Algorytmy $sig_K : \mathcal{P} \to \mathcal{A}$ oraz $ver_K : \mathcal{P} \times \mathcal{A} \to \{tak, nie\}$ to funkcje, takie że dla każdej wiadomości $x \in \mathcal{P}$ i każdego podpisu $y \in \mathcal{A}$ spełnione jest równanie

$$ver(x, y) = \begin{cases} tak, & \text{dla } y = sig(x) \\ nie, & \text{dla } y \neq sig(x) \end{cases}$$

VI. Schemat podpisu ElGamala

[Schemat] (podpisu ElGamala)

Niech p będzie liczbą pierwszą i niech $\alpha \in Z_p^*$ będzie elementem pierwotnym.

Niech $\mathcal{P} = Z_p^*$, $\mathcal{A} = Z_p^* \times Z_{p-1}^*$, $\mathcal{K} = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod p\}$ (Wartości p, α, β są publiczne, liczba a jest tajna).

(1) Dla $K = (p, \alpha, a, \beta)$ i tajnej losowej liczby $k \in Z_{p-1}$ definiujemy

$sig_K(x, k) = (\gamma, \delta)$, gdzie **algorytm podpisu**

$\gamma = \alpha^k \pmod p$ i

$\delta = (x - a\gamma)k^{-1} \pmod{(p-1)}$

(2) Dla $x, \gamma \in Z_p^*$ i $\delta \in Z_{p-1}^*$ definiujemy

$$ver_K(x, \gamma, \delta) = \begin{cases} tak, & \text{gdy } \beta^\gamma \gamma^\delta \equiv \alpha^x \pmod p \\ nie, & \text{w przeciwnym przypadku} \end{cases}$$ **algorytm weryfikacji**

[Przykład 12] Ustal schemat podpisu ElGamala dla p=17, α=3, β=14 (3, $14 \in Z_{17}^*$) i alfabetu alf={abcdefghijklmnopqrstuvwxyz}. Prześlij podpisaną wiadomość x="w" i zweryfikuj podpis.

- Z przykładów 09 i 10 wiadomo, że a=9.
- Kluczem jest K=(p=17, α=3, a=9, β=14), (a - wartość tajną). Literze "w" odpowiada wartość 22.
- losujemy wartość k=11,
- $sig_K = (22,11) = (\gamma, \delta)$,

  $\gamma = 3^{11} \pmod{17} = 7$,

  $\delta = (22 - 9*7)11^{-1} \pmod{16} = (-41*3) \pmod{16} = 5$

- $$ver_K(x = 22, \gamma = 7, \delta = 5) = \begin{cases} tak, & \text{gdy } 14^7 7^5 \equiv 3^{22} \pmod{17} \\ nie, & \text{w przeciwnym przypadku} \end{cases}$$

  Odp. tak, ponieważ $14^7 7^5 \pmod{17} = 6*11 \pmod{17} = 15$, $3^{22} \pmod{17} = 15$

[Zadanie 01] Zaimplementuj
(a) Algorytm Shanksa dla problemu logarytmu dyskretnego
(b) Protokół wymiany kluczy Diffiego-Hellmana
(c) Schemat podpisu ElGamala

[Zadanie 02] Przeanalizuj algorytm Shanksa dla parametrów p=17, α=11 i β = 13.

[Zadanie 03] Wygeneruj klucz zgodnie z protokołem wymiany kluczy Diffiego-Hellmana dla parametrów p=17, α=7.

[Zadanie 04] Ustal schemat podpisu ElGamala dla p=17, α=11, β=13 (11, $13 \in Z_{17}^*$) i alfabetu alf={abcdefghijklmnopqrstuvwxyz}. Prześlij podpisaną wiadomość x="v" i zweryfikuj podpis.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

[Zadanie 02] p=17, α=11, β = 13.

$m = \left|\sqrt{17-1}\right| = \left|\sqrt{16}\right| = \lceil 4 \rceil = 4$, $\alpha^{-1} = 14$.

L1: $(0, 11^{(4*0)}(\text{mod}17)=1)$, $(1, 11^{(4*1)}(\text{mod}17)=4)$, $(3, 11^{(4*3)}(\text{mod}17)=13)$, $(2, 11^{(4*2)}(\text{mod}17)=16)$,
L2: $(3, 13*14^{3}(\text{mod}17)=6)$, $(1, 13*14^{1}(\text{mod}17)=12)$, $(0, 13*14^{0}(\text{mod}17)=13)$, $(2, 13*14^{2}(\text{mod}17)=15)$,

Dwie pary o tej samej drugiej współrzędnej to (3, 13) i (0, 13),
$\log_{11} 13 = 4*3+0(\text{mod } 16) = 12$,
wykładnik a=12

[Zadanie 03] p=17, α=7.

Osoba U: Niech $a_U = 13$, $\alpha^{a_U} (\text{mod p}) = 10^{13} (\text{mod } 17) = 11$, $K = (\alpha^{a_V})^{a_U} \text{ mod p} = 14^{13} (\text{mod} 17) = 5$

Osoba V: Niech $a_V = 19$, $\alpha^{a_V} (\text{mod p}) = 10^{19} (\text{mod } 17) = 14$, $K = (\alpha^{a_U})^{a_V} \text{ mod p} = 11^{19} (\text{mod} 17) = 5$

[Zadanie 04] p=17, α=11, β=13 (11, 13$\in Z_{17}^{*}$), alf={abcdefghijklmnopqrstuvwxyz}, x="v". Niech k=3.

$\gamma = \alpha^{k} (\text{mod p}) = 11^{3} (\text{mod} 17) = 5$

$\delta = (x - a\gamma)k^{-1} (\text{mod}(p-1)) = (21 - 12*5)3^{-1} (\text{mod} 16) = 9*11 (\text{mod } 16) = 3$

$\text{sig}_K(x, k) = (\gamma, \delta) = (5, 3)$

$\beta^{\gamma}\gamma^{\delta} = 13^{5}*5^{3} (\text{mod } 17) = 10$ $\alpha^{x} (\text{mod p}) = 11^{21} (\text{mod } 17) = 10$

$\text{ver}_K(x, \gamma, \delta) = \text{ver}_K(21,5,3) = \text{tak}$

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego