ZAKRES MATERIAŁU

I. System kryptograficzny RSA

[Algorytm] (Kryptosystem RSA (Rivest, Shamir, Adleman)) (system kryptograficzny z kluczem publicznym)
Niech $n = pq$, gdzie p, q są liczbami pierwszymi oraz niech $P = C = Z_n$.
$K = \{(n,p,q,a,b) : n = pq, p, q \text{ pierwsze}, ab \equiv 1 \pmod{\varphi(n)}\}$
Dla $K = (n,p,q,a,b)$ definiujemy

- regułę szyfrowania $e_K(x) = x^b \bmod n$
- regułę deszyfrowania $d_K(y) = y^a \bmod n$

gdzie $x, y \in Z_n$. Wartości n, b są znane publicznie, a liczby p, q, a są tajne.

(A) Generowanie kluczy (publicznego i prywatnego)

[Algorytm] (generowania kluczy)
(1) Wybierz losowo dwie duże liczby pierwsze p, q>2,
(2) Oblicz wartości $n = pq$ i $\varphi(n) = (p-1)(q-1)$,
(3) Wybierz losowo liczbę $b \in \{2,...,\varphi(n)-1\}$ spełniającą warunek $NWD(b, \varphi(n)) = 1$,
(4) Oblicz wartość $a = b^{-1} \bmod \varphi(n)$ (skorzystaj z rozszerzonego algorytmu Euklidesa),
(5) Opublikuj **klucz publiczny** (n,b). **Kluczem prywatnym** jest liczba a.
b - wykładnik szyfrowania, a - wykładnik deszyfrowania, n – moduł RSA.

[Uwaga]
- (Wybór p i q) Przy obecnym stanie wiedzy, dla utrudnienia złamania szyfru, powinny to być losowe liczby pierwsze o podobnej długości (co najmniej 512 bitowe).
- (Wybór b) W celu zwiększenia efektywności szyfrowania należy wybrać możliwie najmniejszy wykładnik szyfrowania b.

[Przykład 01] Wygeneruj klucze (prywatny i publiczny) i niezbędne parametry dla systemu RSA.
Niech p = 17 i q = 23. Wtedy $n = 17 * 23 = 391$ i $\varphi(391) = 16*22 = 352$.
Najmniejszą możliwą liczbą b jest b = 3 (NWD(3,352)=1). Wówczas $a = 3^{-1} \pmod{352} = 235$.
p = 17, q = 23, n = 391, a = 235, b = 3, $\varphi(391) = 352$

(B) Szyfrowanie

[Algorytm] (RSA - szyfrowanie liczb)
Przestrzeń tekstów otwartych – zbiór wszystkich liczb naturalnych m, takich że $0 \le m < n$ ($\Sigma = \{0,1,...,n-1\}$)

- Korzystając z klucza publicznego (n,b) szyfrujemy tekst otwarty na podstawie wzoru $c = m^b \bmod n$.
  c - kryptogram
- Efektywność obliczeń poprawimy stosując algorytm szybkiego potęgowania.

[Przykład 02] Kontynuacja przykładu 01. Dla klucza publicznego (391,3) przestrzenią tekstów otwartych jest zbiór $\Sigma = \{0,1,...,390\}$. Niech tekstem otwartym będzie m = 168. Wówczas kryptogram $c = 168^3 \pmod{391} = 366$.

[Algorytm] (System RSA jako szyfr blokowy)

- $\Sigma = Z_N = \{0,1,...,N-1\}$ - alfabet (N – ustalona liczba naturalna (ilość znaków alfabetu))
- $k = \lfloor \log_N n \rfloor$ - długość bloków tekstu jawnego
- szyfrowanie bloków tekstu jawnego (szyfr RSA przekształca różnowartościowo bloki długości k na bloki długości k+1)
  (1) dla bloku $(m_1...m_k \in \Sigma^k)$ tekstu jawnego znajdujemy liczbę całkowitą $m = \sum_{i=1}^{k} m_i N^{k-i}$ $(0 \le m < n)$,
  (2) blok m szyfrujemy obliczając $c = m^b \bmod n$,
  (3) liczbę c zapisujemy w systemie pozycyjnym o podstawie N ($c = \sum_{i=0}^{k} c_i N^{k-i}$, $c_i \in \Sigma$, $0 \le i \le k$).
  Rozwinięcie liczby c w tym systemie pozycyjnym może mieć długość co najwyżej k+1,
  (4) Zaszyfrowany blok to $c = c_0 c_1 ... c_k \in \Sigma^{k+1}$.

[Przykład] Kontynuacja przykładu 01. Niech $\Sigma = \{a,b,c,d,e\}$. Zaszyfruj blok jawny abc.

- Przyjmujemy odpowiedniość znaków i liczb

a	b	c	d	e
0	1	2	3	4

- $k = \lfloor \log_5 391 \rfloor = 3$ - długość bloków tekstu jawnego
- k+1=4 - długość bloków szyfrogramu

(1) dopasowujemy do bloku tekstu jawnego abc (który identyfikujemy z blokiem 012) liczbę całkowitą
$m = 0*5^2 + 1*5^1 + 2*5^0 = 7$
(2) szyfrujemy liczbę m jako $c = 7^3 \pmod{391} = 343$
(3) zapisujemy c w systemie pozycyjnym o podstawie N=5
$c = 2*5^3 + 3*5^2 + 3*5^1 + 3*1$,
(4) zaszyfrowany blok to $c=(2333)_5$. Stąd blok kryptogramu to cddd.

(C) Deszyfrowanie

[TW01] Dla dowolnej liczby całkowitej m, takiej że $0 \le m < n$
kongruencja $(m^b)^a \equiv m \pmod n$ ma rozwiązanie wtw $ab \equiv 1 \pmod{\varphi(n)}$.

[Algorytm] (RSA - deszyfrowanie liczb)

- Na podstawie [TW01] kryptogram zaszyfrowany za pomocą wzoru $c = m^b \bmod n$ może być rozszyfrowany za pomocą wzoru $m = c^a \bmod n$

[Przykład] Kontynuacja przykładu 02. Deszyfrowanie kryptogramu 366. $m = 366^{235} \bmod 391 = 168$
168 – tekst otwarty; Do wyznaczenia wartości m potrzebny jest szybki algorytm potęgowania (mod n)

[Algorytm] (RSA - deszyfrowanie bloków)

- deszyfrowanie bloków kryptogramu (przekształcamy bloki długości k+1 na bloki długości k)

(1) dopasowujemy do bloku (słowa $c_0c_1...c_k \in \Sigma^{k+1}$) kryptogramu liczbę całkowitą $c = \sum_{i=0}^{k} c_i N^{k-i}$,

(2) dla liczby c obliczamy $m = c^a \bmod n$,

(4) liczbę m zapisujemy w systemie pozycyjnym o podstawie N. Rozwinięcie tej liczby w tym systemie pozycyjnym może mieć długość co najwyżej k,

(4) Stąd blok tekstu jawnego to $m = m_1...m_k \in \Sigma^k$.

[Przykład] Kontynuacja przykładu 01. $\Sigma = \{a, b, c, d, e\}$. Deszyfrowanie kryptogramu cddd.

- Przyjmujemy identyfikację

a	b	c	d	e
0	1	2	3	4

(1) dopasowujemy do bloku kryptogramu cddd (który identyfikujemy z blokiem 2333) liczbę całkowitą
$c = 2*5^3 + 3*5^2 + 3*5^1 + 3*5^0 = 250 + 75 + 15 + 3 = 343$

(2) dla liczby c wyznaczamy wartość $m = 343^{235} (\bmod 391) = 7$

(3) zapisujemy m w systemie pozycyjnym o podstawie N=5
$m = 0*5^2 + 1*5^1 + 2*1$,

(4) zaszyfrowany blok $m=(012)_5$. Stąd blok tekstu jawnego to abc.

II. Sito Eratostenesa

[TW02] Liczba złożona n, taka że n>1, ma dzielnik pierwszy p spełniający nierówność $p \le \sqrt{n}$.

[Algorytm] (Sito Eratostenesa) – służy do wyznaczania wszystkich liczb pierwszych <= od liczby n

(1) Tworzymy tablicę t wartości int o rozmiarze n+1. W pozycje od 2 do n wpisujemy wartość 1.

(2) W kolejnych iteracjach dla i=2,..., $\lfloor\sqrt{n}\rfloor$,

- jeśli t[i]==1, to zerujemy wszystkie pozycje tablicy t o indeksach będących wielokrotnością i,

(3) tablica zawiera wartości równe 1 tylko na pozycjach o indeksach będących liczbami pierwszymi.

[Przykład 03] Wyznacz metodą sita Eratostenesa wszystkie liczby pierwsze mniejsze od 24.

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

$p = \lfloor\sqrt{24}\rfloor = \lfloor 4{,}898979486\rfloor = 4$

i=2	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	0	0	1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0

i=3	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	0	0	1	1	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0

i=4 nie wykreślamy, ponieważ t[4]==0
Liczby pierwsze mniejsze lub równe od 24 to {2,3,5,7,11,13,17,19,23}

III. Szybki algorytm potęgowania $a^c \pmod n$

[Algorytm] (Szybki algorytm potęgowania $a^c \pmod n$)

(1) znajdujemy postać binarną wykładnika e. ($e=e_k*2^k+...+e_1*2+e_0$, gdzie $e_i \in \{0,1\}$),

(2) zmiennej x (używanej do przechowywania wyników częściowych) przypisujemy wartość początkową 1,

(3) w kolejnych iteracjach dla i=0,...,k wykonujemy podstawienia: $x = x * a^{e_i} \pmod n$ i $a = a^2$,

(4) zwracany wynik to wartość x,

[Przykład] Wyznacz $7^{13} \bmod 9$
$e = 1 * 2^3 + 1 * 2^2 + 0 * 2^1 + 1 * 2^0 = (1101)_2$,

	x=1	a=7
$e_0=1$	$x=1*7^1$	$a=7^2=49\equiv4(\bmod9)$
$e_1=0$	$x=7*4^0$	$a=4^2=16\equiv7(\bmod9)$
$e_2=1$	$x=7*7^1=49\equiv4(\bmod9)$	$a=7^2=49\equiv4(\bmod9)$
$e_3=1$	$x=4*4^1=16\equiv7(\bmod9)$	$a=4^2=16\equiv7(\bmod9)$

Wynik x=7

[Zadanie 01] Zaimplementuj
(a) algorytm szybkiego potęgowania (mod a).
(b) algorytm sprawdzania, czy p jest liczbą pierwszą (metodą sita Eratostenesa)
(c) algorytm szyfrowania i deszyfrowania RSA.

[Zadanie 02] Wyznacz metodą sita Eratostenesa wszystkie liczby pierwsze mniejsze bądź równe od podanych niżej wartości.
(a) n=101
(b) n=333
(c) n=781

[Odp.]
(a) n==101
$p = \lfloor\sqrt{101}\rfloor = \lfloor 10{,}04987562\rfloor = 10$
liczby pierwsze
{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,101}

(b) n=333
$p = \lfloor\sqrt{333}\rfloor = \lfloor 4{,}898979486\rfloor = 4$
liczby pierwsze
{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,101,
103,107,109,113,127,131,137,139,149,151,157,163,167,173,179,181,191,193,197,
199,211,223,227,229,233,239,241,251,257,263,269,271,277,281,283,293,307,311,

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

313,317,331}

(c) n=781

$p = \lfloor\sqrt{781}\rfloor = \lfloor 27{,}94637723\rfloor = 27$

liczby pierwsze:

{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,101,
103,107,109,113,127,131,137,139,149,151,157,163,167,173,179,181,191,193,197,
199,211,223,227,229,233,239,241,251,257,263,269,271,277,281,283,293,307,311,
313,317,331,337,347,349,353,359,367,373,379,383,389,397,401,409,419,421,431,
433,439,443,449,457,461,463,467,479,487,491,499,503,509,521,523,541,547,557,
563,569,571,577,587,593,599,601,607,613,617,619,631,641,643,647,653,659,661,
673,677,683,691,701,709,719,727,733,739,743,751,757,761,769,773}

[Zadanie 03] Wykonaj podane niżej operacje potęgowania mod a. Skorzystaj z algorytmu szybkiego potęgowania.

(a) $m = 111^{235} \pmod{391}$
(b) $m = 27^{235} \pmod{391}$
(c) $m = 78^{235} \pmod{391}$

$m = c^a \pmod{n}$

(a) $m = 111^{235} \pmod{391} = 66$, ponieważ

$a = 235 = (11101011)_2$,

	x=1	c=111
$a_0 = 1$	$x=1*111^1 \equiv 111 \pmod{391}$	$c=(111)^2=12321 \equiv 200 \pmod{391}$
$a_1 = 1$	$x=111*200^1=22200 \equiv 304 \pmod{391}$	$c=(200)^2=40000 \equiv 118 \pmod{391}$
$a_2 = 0$	$x=304*118^0 \equiv 304 \pmod{391}$	$c=(118)^2=13924 \equiv 239 \pmod{391}$
$a_3 = 1$	$x=304*239^1=72656 \equiv 321 \pmod{391}$	$c=(239)^2=57121 \equiv 35 \pmod{391}$
$a_4 = 0$	$x=321*35^0 \equiv 321 \pmod{391}$	$c=(35)^2=1225 \equiv 52 \pmod{391}$
$a_5 = 1$	$x=321*52^1=16692 \equiv 270 \pmod{391}$	$c=(52)^2=2704 \equiv 358 \pmod{391}$
$a_6 = 1$	$x=270*358^1=96660 \equiv 83 \pmod{391}$	$c=(358)^2=128164 \equiv 307 \pmod{391}$
$a_7 = 1$	$x=83*307^1=25481 \equiv \mathbf{66} \pmod{391}$	

(b) $m = 27^{235} \pmod{391} = 3$, ponieważ

$a = 235 = (11101011)_2$,

	x=1	c=27
$a_0 = 1$	$x=1*27^1 \equiv 27 \pmod{391}$	$c=(27)^2=729 \equiv 338 \pmod{391}$
$a_1 = 1$	$x=27*338^1=9126 \equiv 133 \pmod{391}$	$c=(338)^2=114244 \equiv 72 \pmod{391}$
$a_2 = 0$	$x=133*101^0 \equiv 133 \pmod{391}$	$c=(72)^2=5184 \equiv 101 \pmod{391}$
$a_3 = 1$	$x=133*101^1=13433 \equiv 139 \pmod{391}$	$c=(101)^2=10201 \equiv 35 \pmod{391}$
$a_4 = 0$	$x=139*35^0 \equiv 139 \pmod{391}$	$c=(35)^2=1225 \equiv 52 \pmod{391}$
$a_5 = 1$	$x=139*52^1=7228 \equiv 190 \pmod{391}$	$c=(52)^2=2704 \equiv 358 \pmod{391}$
$a_6 = 1$	$x=190*358^1=68020 \equiv 377 \pmod{391}$	$c=(358)^2=128164 \equiv 307 \pmod{391}$
$a_7 = 1$	$x=377*307^1=115739 \equiv \mathbf{3} \pmod{391}$	

(c) $m = 78^{235} \pmod{391} = 3$, ponieważ

$a = 235 = (11101011)_2$,

	x=1	c=78
$a_0 = 1$	$x=1*78^1 \equiv 78 \pmod{391}$	$c=(78)^2=6084 \equiv 219 \pmod{391}$
$a_1 = 1$	$x=78*219^1=17082 \equiv 269 \pmod{391}$	$c=(219)^2=47961 \equiv 259 \pmod{391}$
$a_2 = 0$	$x=269*259^0 \equiv 269 \pmod{391}$	$c=(259)^2=67081 \equiv 220 \pmod{391}$
$a_3 = 1$	$x=269*220^1=59180 \equiv 139 \pmod{391}$	$c=(220)^2=48400 \equiv 307 \pmod{391}$
$a_4 = 0$	$x=139*307^0 \equiv 139 \pmod{391}$	$c=(307)^2=94249 \equiv 18 \pmod{391}$
$a_5 = 1$	$x=139*18^1=2502 \equiv 156 \pmod{391}$	$c=(18)^2=324 \equiv 324 \pmod{391}$
$a_6 = 1$	$x=156*324^1=50544 \equiv 105 \pmod{391}$	$c=(324)^2=104076 \equiv 188 \pmod{391}$
$a_7 = 1$	$x=105*188^1=19740 \equiv \mathbf{190} \pmod{391}$	

[Zadanie 04] Przeanalizuj działanie szyfru RSA dla p=17, q=23, alfabetu Σ ={a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p} (16 znaków) i tekstu otwartego abecadlo.

[Odp.]

GENEROWANIE KLUCZY I PARAMETRÓW SZYFROWANIA

p=17, q=23, n=391, a=235, b=3, k=2, φ=352, N=16

Σ={a,b,c,d,e,f,g,h,i,j,k, l, m, n, o, p}, T="abecadlo"
0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15

SZYFROWANIE

Tekst jawny: "abecadlo"

♦ blok tekstu jawnego "ab" = $(0,1)_{16}$,

$m = 0*16^1 + 1*16^0 = 1$,

$c = 1^3 \pmod{391} = 1$,

$c = 0*16^2 + 0*16^1 + 1*16^0 = (0,0,1)_{16}$,

blok kryptogramu "aab"

♦ blok tekstu jawnego "ec" = $(4,2)_{16}$,

$m = 4*16^1 + 2*16^0 = 64 + 2 = 66$,

$c = 66^3 \pmod{391} = 111$,

$c = 0*16^2 + 6*16^1 + 15*16^0 = (0,6,15)_{16}$,

blok kryptogramu "agp"

♦ blok tekstu jawnego "ad" = $(0,3)_{16}$,

$m = 0*16^1 + 3*16^0 = 0 + 3 = 3$,

$c = 3^3 \pmod{391} = 27$,

$c = 0*16^2 + 1*16^1 + 11*16^0 = (0,1,11)_{16}$,

blok kryptogramu "abl"

♦ blok tekstu jawnego "lo" = $(11,14)_{16}$,

$m = 11*16^1 + 14*16^0 = 176 + 14 = 190$,

$c = 190^3 \pmod{391} = 78$

$c = 0*16^2 + 4*16^1 + 14*16^0 = (0,4,14)_{16}$,

blok kryptogramu "aeo"

Kryptoram: "aabagpablaeo"

DESZYFROWANIE (przy znajomości klucza prywatnego)

Kryptogram: "aabagpablaeo"

♦ blok kryptogramu "aab" = $(0,0,1)_{16}$,

$c = 0*16^2 + 0*16^1 + 1*16^0 = 1$,

$m = 1^{235} \pmod{391} = 1$,

$m = 0*16^1 + 1*16^0 = (0,1)_{16}$,

blok tekstu jawnego: "ab"

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

- blok kryptogramu ”agp” = $(0,6,15)_{16}$,

$c = 0*16^2 + 6*16^1 + 15*16^0 = 96 + 15 = 111$,
$m = 111^{235} \pmod{391} = 66$, (patrz zad02(a))
$m = 4*16^1 + 2*16^0 = 64 + 2 = (4,2)_{16}$,
blok tekstu jawnego: ”ec”

- blok kryptogramu ”abl” = $(0,1,11)_{16}$,

$c = 0*16^2 + 1*16^1 + 11*16^0 = 16 + 11 = 27$,
$m = 27^{235} \pmod{391} = 3$, (patrz zad02(b))
$m = 0*16^1 + 3*16^0 = (0,3)_{16}$,
blok tekstu jawnego: ”ad”

- blok kryptogramu ”aeo” = $(0,4,14)_{16}$,

$c = 0*16^2 + 4*16^1 + 14*16^0 = 64 + 14 = 78$,
$m = 78^{235} \pmod{391} = 190$, (patrz zad02(c))
$m = 11*16^1 + 14*16^0 = 176 + 14 = (11,14)_{16}$,
blok tekstu jawnego: ”lo”

---

tekst jawny: ”abecadlo”

---

to samo z pomocą programu

//----------

Realizacja:

//----------

```
RSAblok sys01 = new RSAblok("abcdefghijklmnop",17,23);
System.out.println(sys01);
System.out.println(sys01.szyfr("abecadlo"));
System.out.println(sys01.deszyfr("aabagpablaeo"));
```

//----------

```
//---WYNIKI
p=17, q=23, n=391, a=235, b=3, k=2
e=11
   x=1 a=1
e0 x=1 a=1
e1 x=1 a=1
m=1 c=1 aab
e=11
   x=1 a=66
e0 x=66 a=55
e1 x=111 a=288
m=66 c=111 agp
e=11
   x=1 a=3
e0 x=3 a=9
e1 x=27 a=81
m=3 c=27 abl
e=11
   x=1 a=190
e0 x=190 a=128
e1 x=78 a=353
m=190 c=78 aeo
aabagpablaeo
e=11101011
   x=1 a=1
e0 x=1 a=1
e1 x=1 a=1
e2 x=1 a=1
e3 x=1 a=1
e4 x=1 a=1
e5 x=1 a=1
e6 x=1 a=1
e7 x=1 a=1
c=1 m=1 ab
e=11101011
   x=1 a=111
e0 x=111 a=200
e1 x=304 a=118
e2 x=304 a=239
e3 x=321 a=35
e4 x=321 a=52
e5 x=270 a=358
e6 x=83 a=307
e7 x=66 a=18
c=111 m=66 ec
e=11101011
   x=1 a=27
e0 x=27 a=338
e1 x=133 a=72
e2 x=133 a=101
e3 x=139 a=35
e4 x=139 a=52
e5 x=190 a=358
e6 x=377 a=307
e7 x=3 a=18
c=27 m=3 ad
e=11101011
   x=1 a=78
e0 x=78 a=219
e1 x=269 a=259
e2 x=269 a=220
e3 x=139 a=307
e4 x=139 a=18
e5 x=156 a=324
e6 x=105 a=188
e7 x=190 a=154
c=78 m=190 lo
abecadlo
```


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