ZAKRES MATERIAŁU

I. Szyfr Rabina
II. Szyfr ElGamala

I. Szyfr Rabina

(A) Generowanie kluczy i szyfrowanie

generowanie kluczy
- wybieramy losowo dwie duże liczby pierwsze p i q spełniające warunek $p \equiv q \equiv 3 \pmod 4$,
- wyznaczamy wartość n=pq,
- (p,q) - klucz prywatny, n – klucz publiczny

szyfrowanie
- $\Sigma = \{0, 1, ..., n-1\}$ - przestrzeń tekstów otwartych
- $c = m^2 \pmod n$ - reguła szyfrowania $m \in \Sigma$

[Przykład 01]
Niech tekstem otwartym będzie wartość 141. Losujemy p=11 i q=23. n=11*23=253.
Szyfrujemy tekst otwarty $141^2 \pmod{253} = 147$.

(B) Deszyfrowanie

(a) Obliczamy pierwiastki kwadratowe liczby c (mod p) i liczby c (mod q). Tzn. obliczamy
$m_p = c^{(p+1)/4} \pmod p$, $m_q = c^{(q+1)/4} \pmod q$

(b) wyznaczamy 4 pierwiastki kwadratowe z c (mod n),
- obliczamy wartości $y_p, y_q \in Z$ spełniające warunek $y_p p + y_q q = 1$ (korzystamy z rozszerzonego algorytmu Euklidesa)
- liczymy $r = (y_p p m_q + y_q q m_p) \bmod n$ i $s = (y_p p m_q - y_q q m_p) \bmod n$
- $\pm r$, $\pm s$ są czterema pierwiastkami kwadratowymi z c (mod n) w zbiorze {0, 1, ..., n-1}.
- Jednym z tych pierwiastków jest zaszyfrowana wiadomość m.

[Przykład] Kontynuacja przykładu 01.
$m_p = 147^{(11+1)/4} \pmod{11} = 147^3 \pmod{11} = 9$
$m_q = 147^{(23+1)/4} \pmod{23} = 147^6 \pmod{23} = 3$
$y_p = -2$, $y_q = 1$, wtedy $-2*11+1*23 = 1$
$r = (-2*11*3+1*23*9) \bmod 253 = (-66+207) \bmod 253 = 141$
$s = (-2*11*3-1*23*9) \bmod 253 = (-66-207) \bmod 253 = 233$
Pierwiastkami kwadratowymi z liczby 147 (mod 253) należącymi do zbioru{1,...,252} są 20, 112, **141**, 233.
Jeden z nich (141) to zaszyfrowany tekst otwarty.

[Zadanie 01] Zaimplementuj
(a) szyfrowanie i deszyfrowanie w systemie Rabina.
(b) szyfr Rabina jako szyfr blokowy

II. Szyfr ElGamala

(A) Generowanie klucza i szyfrowanie

generowanie klucza
- wybieramy losowo liczbę pierwszą p taką, że (p-1)/2 jest liczbą pierwszą a następnie wybieramy pierwiastek pierwotny g (mod p),
- losujemy wykładnik $a \in \{0,..., p-2\}$ i obliczamy $A = g^a \pmod p$,
- kluczem publicznym jest (p, g, A), a kluczem prywatnym wartość a

---

szyfrowanie
- $\Sigma = \{0, 1, ..., n-1\}$ - przestrzeń tekstów otwartych
- wybieramy losowo liczbę $b \in \{0,..., p-2\}$ i obliczamy $B = g^b \pmod p$
- wyznaczamy $c = A^b m \pmod p$, gdzie $m \in \Sigma$
- kryptogramem jest para (B,c)

[Przykład 02]
Niech p=23, (23-1)/2=11, g=10, a=5, $A = 10^5 \pmod{23} = 19$
kluczem publicznym jest (p, g, A)=(23,10,19), kluczem prywatnym – wartość a=5
szyfrujemy m=6
wybieramy b=3 i obliczamy $B = 10^3 \pmod{23} = 11$
stąd $c = 19^3 * 6 \pmod{23} = 5*6 \pmod{23} = 7$
kryptogramem jest para (B,c)=(11,7).

Dla liczby pierwszej p postaci (p-1)=2q, gdzie q jest pierwsza, aby wykazać, że g jest pierwiastkiem pierwotnym (mod p), wystarczy sprawdzić, że $g^2 \not\equiv 1 \pmod p$ i $g^q \not\equiv 1 \pmod p$.

g	2	3	4	**5**	6	**7**	8	9	**10**	**11**	12	13	**14**	**15**	16	**17**	18	**19**
$g^2 \pmod{23}$	4	9	16	**2**	13	**3**	18	12	**8**	**6**	6	8	**12**	**18**	3	**13**	2	**16**
$g^{11} \pmod{23}$	1	1	1	**22**	1	**22**	1	1	**22**	**22**	1	1	**22**	**22**	1	**22**	1	**22**

Reszty mod 23 dla liczb między 2 i 19

Pierwiastki pierwotne (mod 23) są między innymi: 5, 7, 10, 11, 14, 15, 17, 19

(B) Deszyfrowanie

(a) dzielimy c przez $B^a \pmod p$
- obliczamy wykładnik x=p-1-a
- ponieważ $1 \le a \le p-2$, więc $1 \le x \le p-2$

- obliczamy $m = B^x c \pmod p$

[Przykład] Kontynuacja przykładu 02. Kryptogram (B, c) = (11, 7)

$m = B^{p-1-a} c \pmod p = 11^{23-1-5} * 7 \pmod{23} = 11^{17} * 7 \pmod{23} = 14 * 7 \pmod{23} = 6$

[Zadanie 02] Zaimplementuj szyfrowanie i deszyfrowanie w systemie ElGamala.

[Zadanie 03] Szyfr Rabina. Niech para (p, q) będzie ustalonym kluczem prywatnym. Określ klucz publiczny i kryptogram dla tekstu otwartego T.
(a) (11, 31), T=134
(b) (23, 31), T=234
Rozwiązanie
(a) p=11≡q=31≡3(mod 4), n=11*31=341.

Szyfrujemy tekst otwarty $134^2 \pmod{341} = 224$.

(b) p=23≡q=31≡3(mod 4), n=23*31=713.

Szyfrujemy tekst otwarty $234^2 \pmod{713} = 568$.

[Zadanie 04] Szyfr Rabina. Niech para (p, q) będzie ustalonym kluczem prywatnym. Określ klucz publiczny i wyznacz tekst jawny (cztery możliwości) dla kryptogramu X.
(a) (11, 31), X=224
(b) (23, 31), X=568

Rozwiązanie
(a) klucz publiczny n=341
Obliczamy pierwiastki kwadratowe liczby $224 \pmod{11}$ i liczby $224 \pmod{31}$

$m_p = 224^{(11+1)/4} \pmod{11} = 224^3 \pmod{11} = 9$

$m_q = 224^{(31+1)/4} \pmod{31} = 224^8 \pmod{31} = 10$

Obliczamy 4 pierwiastki kwadratowe z $224 \pmod{341}$

$11y_p + 31y_q = 1$

$y_p = 17$, $y_q = -6$, wtedy $11*17 - 31*6 = 1$

$r = (17*11*10 - 6*31*9) \bmod 341 = (1870 - 1674) \bmod 341 = 196$

$s = (17*11*10 + 6*31*9) \bmod 341 = (1870 + 1674) \bmod 341 = 134$

Pierwiastkami kwadratowymi z liczby $134 \pmod{341}$ należącymi do zbioru $\{1,...,340\}$ są 134, 145, 196, 207.
Jeden z nich (134) to zaszyfrowany tekst otwarty.

(b) klucz publiczny n=713
Obliczamy pierwiastki kwadratowe liczby $568 \pmod{23}$ i liczby $568 \pmod{31}$

$m_p = 568^{(23+1)/4} \pmod{23} = 568^6 \pmod{23} = 4$

$m_q = 568^{(31+1)/4} \pmod{31} = 568^8 \pmod{31} = 14$

Obliczamy 4 pierwiastki kwadratowe z $568 \pmod{713}$

$23y_p + 31y_q = 1$

$y_p = -4$, $y_q = 3$, wtedy $23*(-4) + 31*3 = 1$

$r = (-4*23*14 + 3*31*4) \bmod 713 = (-1288 + 372) \bmod 713 = 510$

$s = (-4*23*14 - 3*31*4) \bmod 713 = (-1288 - 372) \bmod 713 = 479$

Pierwiastkami kwadratowymi z liczby $568 \pmod{713}$ należącymi do zbioru $\{1,...,712\}$ są 203, 234, 479, 510.
Jeden z nich (234) to zaszyfrowany tekst otwarty.

[Zadanie 05] Szyfr ElGamala. Niech p będzie ustaloną liczbą pierwszą, g - pierwiastkiem pierwotnym mod p oraz niech $a \in \{0,...,p-2\}$ i $b \in \{0,...,p-2\}$ reprezentują wykładniki wykorzystywane odpowiednio do generowania klucza publicznego i kryptogramu. Określ klucz publiczny, prywatny i kryptogram dla tekstu otwartego T.
(a) p=11, g=6, a=5, b=3, T=9
(b) p=47, g=13, a=26, b=3, T=31

Rozwiązanie
(a) GENEROWANIE KLUCZY
p=11 (?), (11-1)/2 = 5 – liczba pierwsza (p - ok)
g=6 (?)

g	**2**	3	4	5	**6**	**7**	**8**	9	10
$g^2 \pmod{11}$	**4**	9	5	3	**3**	**5**	**9**	4	1
$g^5 \pmod{11}$	**10**	1	1	1	**10**	**10**	**10**	1	10

Reszty modulo 11 dla liczb między 2 i 10

Pierwiastki pierwotne (mod 11): 2, 6, 7, 8
więc g=6 jest pierwiastkiem pierwotnym mod 11 (g - ok)
$a = 5 \in \{0,...,11-2\}$ (a - ok)

$A = g^a \pmod p$, $A = 6^5 \pmod{11} = 10$

klucz publiczny (p, g, A)=(11, 6, 10), klucz prywatny a=5
SZYFROWANIE
T=9 (T - ok)
$b = 3 \in \{0,...,11-2\}$ (b - ok)

$B = g^b \pmod p$, $B = 6^3 \pmod{11} = 7$

$X = A^b T \pmod p$, $X = 10^3 9 \pmod{11} = 10*9 \pmod{11} = 2$

kryptogram (B, X) = (7, 2)

(b) GENEROWANIE KLUCZY
p=47 (?), (46-1)/2 = 23 – liczba pierwsza (p - ok)
g=13 (?)

g	2	3	4	**5**	6	7	8	9	**10**	**11**	12	**13**	14
$g^2 \pmod{47}$	4	9	16	**25**	36	2	17	34	**6**	**27**	3	**28**	8
$g^{23} \pmod{47}$	1	1	1	**46**	1	1	1	1	**46**	**46**	1	**46**	1

Reszty modulo 47 sdla liczb między 2 i 14

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

Pierwiastki pierwotne (mod 47) są między innymi: 5, 10, 11, 13, ...
więc g=13 jest pierwiastkiem pierwotnym mod 47 (g - ok)
$a = 26 \in \{0,...,47-2\}$ (a - ok)

$A = g^a \pmod p$, $A = 13^{26} \pmod{47} = 12$

klucz publiczny (p, g, A)=(47, 13, 12), klucz prywatny a=26
SZYFROWANIE
T=36 (T - ok)
$b = 3 \in \{0,...,47-2\}$ (b - ok)

$B = g^b \pmod p$, $B = 13^3 \pmod{47} = 35$

$X = A^b T \pmod p$, $X = 12^3 31 \pmod{47} = 36*31 \pmod{47} = 35$

kryptogram (B, X) = (35, 35)

[Zadanie 06] Szyfr ElGamala. Niech p będzie ustaloną liczbą pierwszą, g - pierwiastkiem pierwotnym mod p oraz niech $a \in \{0,..., p-2\}$ reprezentuje wykładnik wykorzystywany do generowania klucza publicznego. Określ klucz publiczny, prywatny i tekst otwarty dla kryptogramu (B, X).
(a) p=11, g=6, a=5, (B, X)=(7, 2)
(b) p=47, g=13, a=26, (B, X)=(35, 35)

Rozwiązanie
(a) klucz publiczny (p, g, A)=(11, 6, 10), klucz prywatny a=5
kryptogram (B, X)=(7, 2)
obliczam wykładnik x = p-1-a = 11-1-5=5

$T = B^x X \pmod p$, $T = 7^5 * 2 \pmod{11} = 9$

(b) klucz publiczny (p, g, A)=(47, 13, 12), klucz prywatny a=26
kryptogram (B, X)=(35, 35)
obliczam wykładnik x = p-1-a = 47-1-26=20

$T = B^x X \pmod p$, $T = 35^{20} * 35 \pmod{47} = 17 * 35 \pmod{47} = 31$

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