Opracowanie przykładów zaszyfrowania i rozszyfrowania algorytmem RSA

Przykład 1

Lp.	Działanie	Przykład	Uwagi
1)	losujemy liczby pierwsze ***p*** i ***q***	***p = 3***, ***q = 19***	liczby ***p*** i ***q*** nie powinni być liczbami typu specjalistycznego, na przykład liczbami Fermata lub Mersenne'a:
• pierwsze liczby Fermata wyrażony są w postaci $2^r + 1$, gdzie r > 1 – liczba pierwsza; • pierwsze liczby Mersenne'a określane są ze wzoru $2^r - 1$, gdzie r > 1 – liczba pierwsza (na rok 1995 zostały znaleziony 33 wartości r, dla których $2^r - 1$ jest liczbą pierwszą, największą z nich r = 859433; pierwszą złożoną liczbą postaci $2^r - 1$ dla liczby pierwszej r jest $2^{11} - 1 = 23 * 89 = 2047$)			
2)	obliczamy ***n = p * q***	***n = 3 * 19 = 57***	***n*** i ***e*** – klucz publiczny
3)	wyliczamy funkcję Eulera ***φ(n) = (p –1)(q – 1)***	***φ(n) = (3 –1)(19 – 1) = 36***	
4)	losujemy liczbę ***e*** taką, że ***NWD(e, φ(n)) = 1***	np. ***e = 5, ponieważ NWD(5, 36) = 1***	
Liczby ***p*** i ***q*** wymazujemy z systemu !!!			
5)	określamy ***d*** z kongruencji ***d * e ≡ 1*** **mod** ***φ(n)***:		***d*** – klucz tajny (prywatny)

5.1) ww. kongruencję sprowadzamy do równania Diofantesa ***d * e - φ(n) * y = 1***, w którym spełnia się warunek ***e < φ(n);***

5.2) stosujemy rozszerzony algorytm Euklidesa do rozwiązania równania Diofantesa.

Rozszerzony algorytm Euklidesa:

- ***wersja klasyczna***

$$
\begin{array}{lcl}
 & & q_0 \\
 & & // \\
5 & = & 36 * 0 + 5 \\
 & & q_1 \\
 & & // \\
36 & = & 5 * 7 + 1 \\
 & & q_2 \rightarrow k = 2 \\
 & & // \\
5 & = & 1 * 5 + 0
\end{array}
$$

$W_i = q_i * W_{i-1} + W_{i-2}$; $U_i = q_i * U_{i-1} + U_{i-2}$;

($W_{-2} = U_{-1} = 0$; $W_{-1} = U_{-2} = 1 \rightarrow$ *zawsze!!!*)

$W_0 = 0 * 1 + 0 = 0$; $U_0 = 0 * 0 + 1 = 1$;

$W_1 = 7 * 0 + 1 = 1 \rightarrow W_{k-1}$; $U_{k-1} \leftarrow U_1 = 7 * 1 + 0 = 7$;

$W_2 = 5 * 1 + 0 = 5$; $U_2 = 5 * 7 + 1 = 36$;

i	-2	-1	0	1	2
q_i			0	7	5
W_i	0	1	0	1	5
U_i	1	0	1	7	36

U_{k-1} W_{k-1}

$$d = (-1)^{k-1} * U_{k-1} = (-1)^{2-1} * 7 = -7;$$
$$y = (-1)^{k-1} * W_{k-1} = (-1)^{2-1} * 1 = -1.$$

Ponieważ otrzymany klucz prywatny ***d*** jest liczba ujemna (a powinien być liczbą dodatnią), przeprowadzamy przetwarzania stosując kongruencje:

$d = -7 \equiv -7 \bmod 36 \equiv ((-1) * 36 + 29) \bmod 36 \equiv 29 \bmod 36 = 29$.

- ***wersja modyfikowana***

q_2 //

$36 = 5 * 7 + 1$

$q_3 \rightarrow k = 3$ //

$5 = 1 * 5 + 0$

$W_i = q_i * W_{i-1} + W_{i-2}$; $U_i = q_i * U_{i-1} + U_{i-2}$;

($W_0 = U_1 = 1$; $W_1 = U_0 = 0 \rightarrow$ *zawsze!!!*)

$W_2 = 7 * 0 + 1 = 1 \rightarrow W_{k-1}$; $U_{k-1} \leftarrow U_2 = 7 * 1 + 0 = 7$;

$W_3 = 5 * 1 + 0 = 5$; $U_3 = 5 * 7 + 1 = 36$;

i	0	1	2	3
q_i			7	5
W_i	1	0	1	5
U_i	0	1	7	36

U_{k-1} W_{k-1}

$$d = (-1)^{k-2} * U_{k-1} = (-1)^{3-2} * 7 = -7;$$
$$y = (-1)^{k-2} * W_{k-1} = (-1)^{3-2} * 1 = -1.$$

Ponieważ otrzymany klucz prywatny ***d*** jest liczba ujemna (a powinien być liczbą dodatnią), przeprowadzamy przetwarzania stosując kongruencje:

$$d = -7 \equiv -7 \bmod 36 \equiv ((-1) * 36 + 29) \bmod 36 \equiv 29 \bmod 36 = 29.$$

6)	zaszyfrowanie: $c = m^e \bmod n$	np. $m = 637$; $c_1 = 6^5 \bmod 57 = 24$, $c_2 = 37^5 \bmod 57 = 37$, $c = \{c_1 c_2\} = \{24;37\}$
	Ponieważ $m = 637 > n = 57$, dzielimy m tak, żeby $m_j < n$, np. $m_1 = 6$, $m_2 = 37$.	
7)	rozszyfrowanie: $m = c^d \bmod n$	$m_1 = 24^{29} \bmod 57 = 6$, $m_2 = 37^{29} \bmod 57 = 37$, $m = \{m_1 m_2\} = 637$.

Przykład 2

Lp.	Działanie	Przykład	Uwagi
1)	losujemy liczby pierwsze ***p*** i ***q***	***p = 7, q = 31***	Patrz. Przykład 1
2)	obliczamy ***n = p * q***	***n = 7 * 31 = 217***	***n*** i ***e*** – klucz publiczny
3)	wyliczamy funkcję Eulera ***φ(n) = (p –1)(q – 1)***	***φ(n) = (7 –1)(31 – 1)= 180***	
4)	losujemy liczbę ***e*** taką, że ***NWD(e, φ(n)) = 1***	np. ***e = 7, ponieważ NWD(7, 180) = 1***	
Liczby ***p*** i ***q*** wymazujemy z systemu !!!			
5)	określamy ***d*** z kongruencji ***d * e ≡ 1*** **mod** ***φ(n)***:		***d*** – klucz tajny (prywatny)

5.3) ww. kongruencję sprowadzamy do równania Diofantesa ***d * e - φ(n) * y = 1***, w którym spełnia się warunek ***e < φ(n);***

5.4) stosujemy rozszerzony algorytm Euklidesa do rozwiązania równania Diofantesa.

Rozszerzony algorytm Euklidesa:

- ***wersja klasyczna***

$$
\begin{array}{rcl}
 & & q_0 \\
 & & // \\
7 & = & 180 * 0 + 7 \\
 & & \dashrightarrow q_1 \\
 & & // \\
180 & = & 7 * 25 + 5 \\
 & & \dashrightarrow q_2 \\
 & & // \\
7 & = & 5 * 1 + 2 \\
 & & \dashrightarrow q_3 \\
 & & // \\
5 & = & 2 * 2 + 1 \\
 & & \dashrightarrow q_4 \rightarrow k = 4 \\
 & & // \\
2 & = & 1 * 2 + 0
\end{array}
$$

$W_i = q_i * W_{i-1} + W_{i-2}$; $\qquad$ $U_i = q_i * U_{i-1} + U_{i-2}$;

$(W_{-2} = U_{-1} = 0; \quad W_{-1} = U_{-2} = 1 \rightarrow$ *zawsze!!!*$)$

$W_0 = 0 * 1 + 0 = 0$;		$U_0 = 0 * 0 + 1 = 1$;
$W_1 = 25 * 0 + 1 = 1$;		$U_1 = 25 * 1 + 0 = 25$;
$W_2 = 1 * 1 + 0 = 1$;		$U_2 = 1 * 25 + 1 = 26$;
$W_3 = 2 * 1 + 1 = 3 \rightarrow W_{k-1}$;	$U_{k-1} \leftarrow$	$U_3 = 2 * 26 + 25 = 77$;
$W_4 = 2 * 3 + 1 = 7$;		$U_4 = 2 * 77 + 26 = 180$;

i	-2	-1	0	1	2	3	4
q_i			0	25	1	2	2
W_i	0	1	0	1	1	3	7
U_i	1	0	1	25	26	77	180

U_{k-1} W_{k-1}

$$d = (-1)^{k-1} * U_{k-1} = (-1)^{4-1} * 77 = -77;$$
$$y = (-1)^{k-1} * W_{k-1} = (-1)^{4-1} * 3 = -3.$$

Ponieważ otrzymany klucz prywatny ***d*** jest liczba ujemna (a powinien być liczbą dodatnią), przeprowadzamy przetwarzania stosując kongruencje:

$$d = -77 \equiv -77 \bmod 180 \equiv ((-1) * 180 + 103) \bmod 180 \equiv 103 \bmod 180 = 103.$$

- ***wersja modyfikowana***

q_2 //
$180 = 7 * 25 + 5$
q_3 //
$7 = 5 * 1 + 2$
q_4 //
$5 = 2 * 2 + 1$
$q_5 \rightarrow k = 5$ //
$2 = 1 * 2 + 0$

$W_i = q_i * W_{i-1} + W_{i-2}$; $U_i = q_i * U_{i-1} + U_{i-2}$;

($W_0 = U_1 = 1$; $W_1 = U_0 = 0 \rightarrow$ *zawsze!!!*)

$W_2 = 25 * 0 + 1 = 1$; $U_2 = 25 * 1 + 0 = 25$;
$W_3 = 1 * 1 + 0 = 1$; $U_3 = 1 * 25 + 1 = 26$;
$W_4 = 2 * 1 + 1 = 3 \rightarrow W_{k-1}$; $U_{k-1} \leftarrow$ $U_4 = 2 * 26 + 25 = 77$;
$W_5 = 2 * 3 + 1 = 7$; $U_5 = 2 * 77 + 26 = 180$;

i	0	1	2	3	4	5
q_i			25	1	2	2
W_i	1	0	1	1	3	7
U_i	0	1	25	26	77	180

U_{k-1} W_{k-1}

$$d = (-1)^{k-2} * U_{k-1} = (-1)^{5-2} * 77 = -77;$$
$$y = (-1)^{k-2} * W_{k-1} = (-1)^{5-2} * 3 = -3.$$

Ponieważ otrzymany klucz prywatny ***d*** jest liczba ujemna (a powinien być liczbą dodatnią), przeprowadzamy przetwarzania stosując kongruencje:

$$d = -77 \equiv -77 \bmod 180 \equiv ((-1) * 180 + 103) \bmod 180 \equiv 103 \bmod 180 = 103.$$

6)	zaszyfrowanie: $c = m^e \bmod n$	np. $m = 547$; $c_1 = 5^7 \bmod 217 = 5,$ $c_2 = 4^7 \bmod 217 = 109,$ $c_3 = 7^7 \bmod 217 = 28,$ $c = \{c_1 c_2 c_3\} = \{5;109;28\}$
	Ponieważ $m = 547 > n = 217,$ dzielimy m tak, żeby $m_j < n$, np. $m_1 = 5, m_2 = 4, m_3 = 7.$	
7)	rozszyfrowanie: $m = c^d \bmod n$	$m_1 = 5^{103} \bmod 217 = 5,$ $m_2 = 109^{103} \bmod 217 = 4,$ $m_2 = 28^{103} \bmod 217 = 7,$ $m = \{m_1 m_2 m_3\} = 547.$