Блочные методы возведения в степень по модулю (методы окна)

Вариант 1: “традиционный” блочный метод

$$R = x^k \bmod N;$$

$$k = (k_{t-1}k_{t-2}\ldots k_1k_0)_2, k_{t-1} \neq 0;$$

$$k = (k_{d-1}k_{d-2}\ldots k_1k_0)_{2^w}, d = \left\lceil \frac{t}{w} \right\rceil, k_{d-1} \neq 0;$$

$$k = 2^{(d-1)w}k_{d-1} + 2^{(d-2)w}k_{d-2} + \ldots + 2^{2w}k_2 + 2^w k_1 + k_0;$$

$$x^k = x^{2^{(d-1)w}k_{d-1}} \times \ldots \times x^{2^{2w}k_2} \cdot x^{2^w k_1} \cdot x^{k_0} \bmod N;$$

$$k = \left(\left(\left(k_{d-1} \cdot 2^w + k_{d-2} \right) \cdot 2^w + \ldots + k_2 \right) \cdot 2^w + k_1 \right) \cdot 2^w + k_0;$$

$$x^k = \left(\left(\left(\left(x^{k_{d-1}} \right)^{2^w} \times x^{k_{d-2}} \right)^{2^w} \times \ldots \times x^{k_2} \right)^{2^w} \times x^{k_1} \right)^{2^w} \times x^{k_0}.$$

1. (*Предвычисления:* $x^0, x^1, x^2, \square, x^{2^w-1}$)

   1.1. $X[0] = 1; X[1] = x;$

   1.2. $\text{for}\,(i = 2;\ i <= \left(2^w - 1\right);\ i++)$

   $X[i] = X[i\text{-}1] \cdot x \bmod N;$

2. $R = 1;$

3. $\text{for}\,(i = d\text{-}1\ ;\ i >= 0\ ;\ i\text{--}\,)\,\{$

   3.1. $R = R^{2^w} \bmod N;$

   3.2. $R = R \cdot X[k_i] \bmod N;$ // $R\ *= x^{k_i}$

   }

1. (*Предвычисления:* $x^0, x^1, x^2, \boxtimes, x^{2^w-1}$)

   1.1. $X[0] = 1; X[1] = x;$

   1.2. $\text{for}\,(i = 2;\ i <= \left(2^w - 1\right);\ i++)$

   $X[i] = X[i\text{-}1] \cdot x \bmod N;$

2. $R = \boldsymbol{X[k_{d\text{-}1}]}$; // $x^{k_{d-1}}$
3. $\text{for}\,(i = \boldsymbol{d\text{-}2}\ ;\ i >= 0\ ;\ i\text{--})\ \{$

   3.1. $R = R^{2^w} \bmod N;$

   3.2. $R = R \cdot X[k_i] \bmod N;$ // $R\ *= x^{k_i}$

   }

Пример 1.

$k = 23_{<10>} = 17_{<16>} = (\underline{10}\ \underline{111})_2 = (k_1\, k_0) = (27)_8$;

$w = 3,\ b = 2^w = 8$; $\{[X[0], X[1],] X[2], \ldots, X[7]\} =$

$= \{[1, x,] \underline{x^2}, x^3, \underline{x^4}, x^5, \underline{x^6}, x^7\}$.

$23_{<10>} = ($ (10) (111) $)_2{}^3$

i		1	0	
R	3.1	x^2	$\left(x^2\right)^8 = x^{16}$	$(d\text{-}1)w = 3$
	3.2		$x^{16} \cdot X[7] = x^{16} \cdot x^7 = x^{23}$	$(d\text{-}1) = 1$

$I'_{block} = 1 \cdot I_M + 3 \cdot I_S$; $I_{block} = 4 \cdot I_M + 6 \cdot I_S$ ($I^{\cup}_{block} = 3 \cdot I_M + 3 \cdot I_S$);

$I_{bin} = (wt(\mathrm{k})\text{-}1) \cdot I_M + (t\text{-}1) \cdot I_S = 3 \cdot I_M + 4 \cdot I_S$.

Пример 2.

$k=283_{<10>}=11B_{<16>}=(1\,0001\,1011)_2=$

$=(\underline{100}\ \underline{011}\ \underline{011})_2=(k_2\ k_1\ k_0)=(433)_8;$

$w=3,\ b=2^w=8\ ;\ \{[X[0],X[1],]\ X[2],\ldots,X[7]\}=$

$=\{[1,x,]\ \underline{x^2},\ x^3,\ \underline{x^4},\ x^5,\ \underline{x^6},\ x^7\}\ .$

i		2	1	0	
k_i		4	3	3	
R	(3.1)	x^4	$\left(x^4\right)^8=x^{32}$	$\left(x^{35}\right)^8=x^{280}$	$(d\text{-}1)w=6$
	(3.2)		$x^{32}\cdot X[3]=$ $x^{32}\cdot x^3=x^{35}$	$x^{280}\cdot X[3]=$ $x^{280}\cdot x^3=x^{283}$	$d\text{-}1=2$

$t_{block}=2\cdot t_M+6\cdot t_S$, $t_{block}=3\cdot t_M+9\cdot t_S$ ($t_{block}=3\cdot t_M+3\cdot t_S$),

$l_{bin}=(wt(k)\text{-}1)\cdot l_M+(t\text{-}1)\cdot l_S=4\cdot l_M+8\cdot l_S$.

Оценки средней вычислительной сложности

Для этапа предвычислений:

$$I^0_{block} = \left(2^w - 2\right) \cdot I_M;$$

$$I^0_{block} = (2^{w-1} - 1)\left(I_M + I_S\right).$$

Для основного цикла алгоритма:

$$I^1_{block} = (d-1)\left(\frac{2^w - 1}{2^w} I_M + w \cdot I_S\right);$$

$$I^1_{block} = \left(\left\lceil \frac{t}{w} \right\rceil - 1\right)\frac{2^w - 1}{2^w} I_M + (t-w) I_S.$$

$$I^1_{block} \le \left(\left\lceil \frac{|N|_2}{w} \right\rceil - 1\right)\frac{2^w - 1}{2^w} I_M + (t-w) I_S.$$

$$\frac{2^{w-1}(t-1)}{\left(2^{w}-1\right)\left(\left\lceil \frac{t}{w} \right\rceil -1\right)};$$

$$\frac{2^{w-1}(t-1)}{\left(2^{w}-1\right)\left(\left\lceil \frac{t}{w} \right\rceil -1\right)+2^{w}\left(2^{w-1}-1\right)}.$$

w \ *t*	1024	2048
4	2,14 / 1,99	6,41 / 5,76
8	4,04 / 1,33	4,03 / 1,99

w \ *t*	512	1 024	2 048	4 096	8 192	16 384
1	255.5 511	511.5 1023	1023.5 2047	2047.5 4095	4095.5 8191	8191.5 16383
2	192.3 511	384.3 1023	768.3 2047	1536.3 4095	3072.3 8191	6144.3 16383
3	151.8 513	301.4 1026	599.8 2049	1197.4 4098	2391.8 8193	4781.4 16386
4	126.1 515	246.1 1027	486.1 2051	966.1 4099	1926.1 8195	3846.1 16387
5	113.8 525	212.6 1035	411.2 2060	808.4 4110	1601.8 8205	3188.6 16395
6	114.7 541	198.3 1051	366.7 2077	702.3 4123	1374.7 8221	2718.3 16411
7	135.4 574	207.9 1085	352.7 2107	643.4 4158	1223.9 8253	2384.7 16443
8	189.8 631	253.5 1143	381.0 2167	636.0 4215	1146.0 8311	2166.0 16503
9	310.9 759	367.8 1272	481.6 2298	709.1 4350	1163.2 8445	2071.4 16635
10	562.0 1021	612.9 1531	714.8 2551	919.6 4601	1329.2 8701	2147.4 16891

w \ t	512	1 024	2 048	4 096	8 192	16 384
1	335804672 392448	2685399552 1571328	21479023616 6288384	171815454720 25159680	1374456614912 100651008	10995384655872 402628608
2	302578688 360064	2418276352 1441024	19336785920 5765632	154656563200 23065600	1237101559808 92268544	9896208596992 369086464
3	282092544 340352	2249031424 1359232	17935208448 5424640	143358557184 21689856	1145956614144 86710272	9165684076544 346806272
4	269387584 328224	2134494848 1303616	16993656064 5195904	135620278784 20746496	1083646833664 82911744	8663914047488 331498496
5	266897472 327072	2076906240 1277568	16422183808 5061056	130605858048 20145792	1041128260608 80337408	8314154987520 320858112
6	273660848 335704	2072133824 1279328	16155356864 5004640	127373411072 19764608	1012249180928 78607744	8068102360064 313415168
7	297583544 363228	2145673440 1323888	16227149696 5037504	126277262784 19666656	995226879744 77634432	7901864082432 308473344
8	348606980 420226	2332865032 1430020	16842333200 5218312	127463069728 19869712	990615679040 77471776	7808596926592 305872960
9	462737040 547784	2775981628 1679134	18511093992 5692532	133315515280 20722120	1006418648640 78710560	7810983696640 306486400
10	697979597 810470.5	3698574644 2195354	22061676752 6688360	146699279160 22612380	1054473542864 82167400	7954853958464 311925152

методы

w \ t	512	1 024	2 048	4 096	8 192	16 384
1	336197120	2686970880	21485312000	171840614400	1374557265920	10995787284480
2	302938752	2419717376	19342551552	154679628800	1237193828352	9896577683456
3	282432896	2250390656	17940633088	143380247040	1146043324416	9166030882816
4	269715808	2135798464	16998851968	135641025280	1083729745408	8664245545984
5	267224544	2078183808	16427244864	130626003840	1041208598016	8314475845632
6	273996552	2073413152	16160361504	127393175680	1012327788672	8068415775232
7	297946772	2146997328	16232187200	126296929440	995304514176	7902172555776
8	349027206	2334295052	16847551512	127482939440	990693150816	7808902799552
9	463284824	2777660762	18516786524	133336237400	1006497359200	7811290183040
10	698790067	3700769998	22068365112	146721891540	1054555710264	7955165883616