

NTRU Challenge

Parameter Sets and Public Keys

Private keys are of the form $f = 1 + pF$, $F = f_1 * f_2 + f_3$, where f_1 , f_2 and f_3 have d_1 , d_2 , d_3 +1s and -1s respectively. Any vector in the lattice with L2 norm less than the Gaussian heuristic for the lattice will be considered equivalent to the actual private key. For an NTRU lattice with ring parameters N and q , the Gaussian heuristic estimates the length of a shortest vector to be $\sqrt{N * q / (\pi * e)}$. The zero and "all ones" vectors are not valid solutions.

The NTRU algorithm is available at <https://github.com/NTRUOpenSourceProject/ntru-crypto>

Challenge #1 (N = 107)

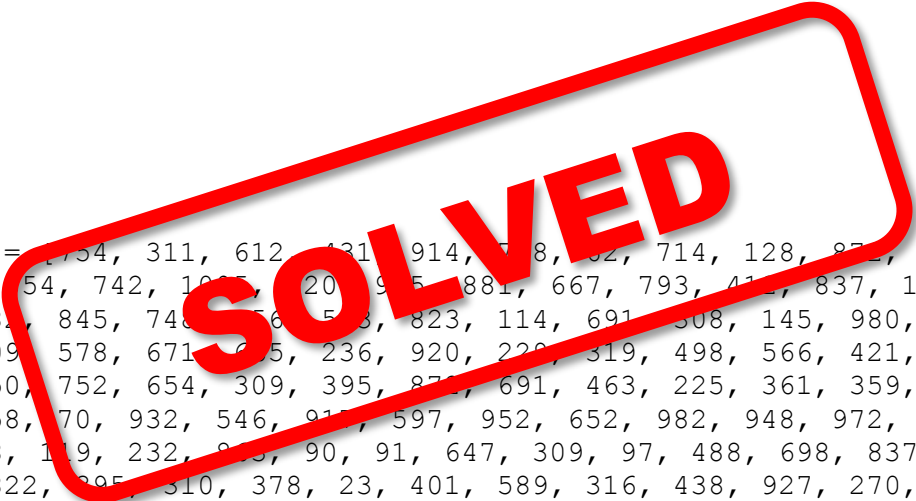
```
chl-107r1
N = 107
q = 512
d1 = 4
d2 = 4
d3 = 4
dg = 36
public_key = [378, 46, 408, 75, 205, 73, 86, 72, 469, 105, 396, 15,
178, 412, 108, 127, 145, 10, 338, 321, 200, 483, 399, 234, 227, 409,
15, 459, 334, 395, 162, 324, 164, 225, 79, 304, 133, 117, 165, 353,
129, 251, 488, 28, 453, 140, 150, 230, 103, 446, 260, 50, 284, 298,
458, 293, 38, 362, 314, 104, 242, 230, 26, 84, 213, 19, 229, 177, 211,
166, 201, 323, 309, 490, 46, 278, 154, 367, 299, 419, 329, 280, 456,
143, 459, 406, 275, 282, 172, 458, 229, 499, 286, 207, 94, 160, 131,
173, 188, 284, 509, 228, 493, 70, 300, 94, 304]
```

Challenge #2 (N = 113)

```
chl-113r1
N = 113
q = 1024
d1 = 5
d2 = 4
d3 = 3
dg = 38
public_key = [1021, 544, 107, 401, 91, 17, 980, 271, 512, 11, 957,
736, 920, 275, 807, 210, 41, 65, 80, 5, 333, 561, 312, 252, 472,
158, 999, 93, 906, 519, 40, 4, 285, 970, 1015, 234, 334, 512, 47,
899, 630, 634, 548, 11, 11, 338, 908, 758, 442, 44, 690, 380, 672,
143, 732, 14, 191, 120, 7, 606, 993, 944, 399, 138, 260, 745, 561,
428, 813, 459, 853, 604, 990, 813, 533, 37, 334, 143, 601, 389, 473,
713, 770, 7, 341, 246, 417, 789, 731, 562, 908, 789, 285, 320, 534,
271, 676, 1, 813, 788, 422, 169, 634, 986, 592, 168, 110, 648, 310,
502, 946, 1001, 778]
```

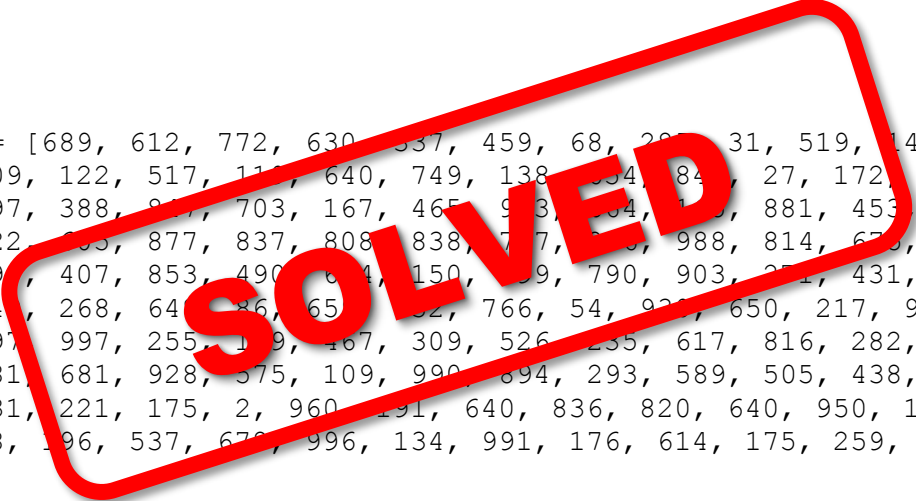
Challenge #3 (N = 131)

```
chl-131r1
N = 131
q = 1024
d1 = 5
d2 = 4
d3 = 4
dg = 44
public_key = [1754, 311, 612, 131, 914, 118, 32, 714, 128, 872, 349,
1021, 700, 54, 742, 1025, 20, 95, 881, 667, 793, 417, 837, 114,
411, 29, 181, 845, 748, 56, 53, 823, 114, 691, 308, 145, 980, 962,
45, 907, 309, 578, 671, 65, 236, 920, 228, 319, 498, 566, 421, 329,
728, 943, 50, 752, 654, 309, 395, 872, 691, 463, 225, 361, 359, 635,
47, 271, 958, 70, 932, 546, 917, 597, 952, 652, 982, 948, 972, 901,
551, 418, 8, 119, 232, 833, 90, 91, 647, 309, 97, 488, 698, 837, 574,
891, 944, 822, 895, 310, 378, 23, 401, 589, 316, 438, 927, 270, 363,
781, 948, 616, 515, 878, 372, 701, 556, 605, 514, 528, 228, 83, 469,
200, 405, 641, 892, 203, 220, 465, 70]
```



Challenge #4 (N = 139)

```
chl-139r1
N = 139
q = 1024
d1 = 5
d2 = 5
d3 = 3
dg = 46
public_key = [689, 612, 772, 630, 337, 459, 68, 287, 31, 519, 148,
804, 575, 609, 122, 517, 117, 640, 749, 138, 334, 84, 27, 172, 1,
488, 394, 597, 388, 817, 703, 167, 465, 93, 304, 113, 881, 453, 591,
973, 911, 722, 835, 877, 837, 808, 838, 717, 33, 988, 814, 673, 1019,
455, 323, 29, 407, 853, 490, 64, 150, 39, 790, 903, 251, 431, 469,
128, 982, 64, 268, 64, 86, 65, 32, 766, 54, 92, 650, 217, 957,
733, 948, 897, 997, 255, 119, 167, 309, 526, 235, 617, 816, 282, 928,
730, 860, 481, 681, 928, 575, 109, 990, 894, 293, 589, 505, 438, 592,
330, 450, 231, 221, 175, 2, 960, 191, 640, 836, 820, 640, 950, 167,
710, 61, 498, 196, 537, 678, 996, 134, 991, 176, 614, 175, 259, 953,
321, 1018]
```



Challenge #5 (N = 149)

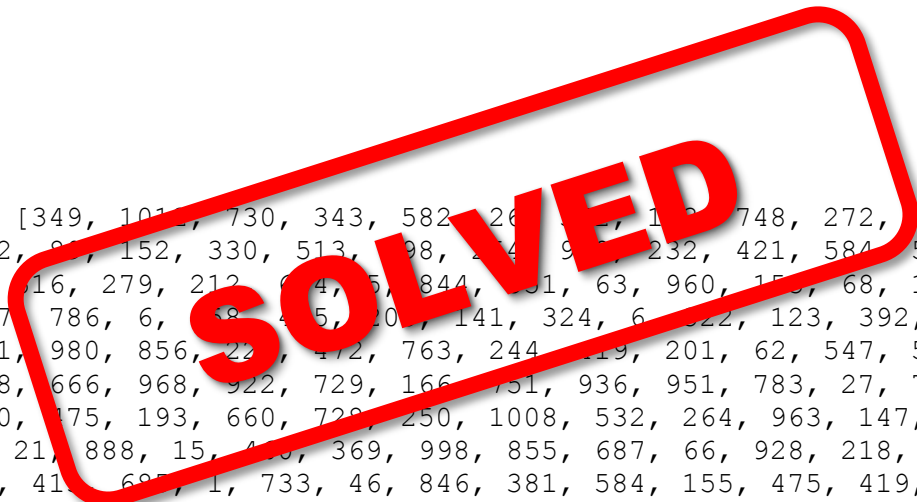
```
chl-149r1
N = 149
q = 1024
d1 = 5
d2 = 5
d3 = 3
dg = 50
public_key = [571, 837, 462, 662, 107, 11, 60, 164, 163, 980, 674,
720, 95, 17, 101, 456, 686, 808, 90, 78, 905, 749, 278, 414, 406,
651, 566, 838, 698, 724, 751, 50, 69, 652, 370, 222, 172, 212,
502, 422, 745, 439, 833, 103, 71, 288, 1005, 867, 221, 601, 223, 984,
917, 895, 869, 511, 22, 180, 22, 472, 253, 389, 170, 937, 9, 25,
933, 185, 117, 444, 140, 697, 274, 636, 188, 628, 350, 580, 853, 204,
747, 408, 604, 251, 844, 659, 572, 519, 130, 238, 771, 218, 661, 964,
507, 195, 313, 975, 588, 828, 312, 252, 405, 467, 997, 508, 24, 480,
356, 756, 13, 4, 370, 277, 981, 550, 188, 407, 896, 699, 966, 804,
202, 415, 839, 624, 782, 225, 565, 237, 790, 530, 27, 1018, 278, 450,
131, 366, 597, 170, 563, 319, 653, 204, 496, 373, 319]
```

Challenge #6 (N = 163)

```
chl-163r1
N = 163
q = 1024
d1 = 5
d2 = 5
d3 = 4
dg = 54
public_key = [391, 858, 742, 459, 973, 358, 532, 799, 233, 936, 523,
614, 304, 481, 978, 513, 356, 727, 593, 43, 944, 67, 273, 66, 979,
150, 302, 898, 826, 141, 652, 203, 281, 494, 595, 7, 839, 945, 805,
21, 481, 504, 20, 459, 596, 465, 22, 577, 1, 2, 169, 226, 2, 380,
61, 736, 735, 633, 91, 488, 51, 28, 738, 61, 331, 325, 459, 140, 860,
316, 504, 77, 934, 277, 555, 1, 7, 920, 312, 771, 753, 312, 347, 758,
328, 49, 216, 466, 826, 810, 52, 36, 815, 693, 158, 867, 543, 557,
359, 199, 72, 445, 209, 12, 460, 741, 619, 777, 612, 209, 574, 419,
440, 9, 225, 113, 388, 836, 341, 933, 324, 144, 372, 977, 908, 600,
866, 232, 133, 240, 552, 134, 453, 158, 371, 465, 503, 932, 385, 829,
838, 389, 249, 624, 207, 828, 621, 539, 863, 664, 32, 77, 1008, 215,
401, 297, 1011, 1001, 571, 436, 340, 968, 951, 868]
```

Challenge #7 (N = 173)

```
chl-173r1
N = 173
q = 1024
d1 = 6
d2 = 5
d3 = 4
dg = 58
public_key = [349, 101, 730, 343, 582, 26, 1, 1, 748, 272, 510,
490, 926, 792, 8, 152, 330, 513, 98, 24, 9, 232, 421, 584, 590,
96, 735, 81, 16, 279, 212, 84, 5, 844, 31, 63, 960, 15, 68, 109,
586, 422, 497, 786, 6, 58, 45, 10, 141, 324, 6, 22, 123, 392, 235,
440, 737, 881, 980, 856, 22, 172, 763, 244, 19, 201, 62, 547, 575,
660, 516, 788, 666, 968, 922, 729, 166, 751, 936, 951, 783, 27, 704,
654, 883, 970, 175, 193, 660, 728, 250, 1008, 532, 264, 963, 147, 659,
9, 607, 415, 21, 888, 15, 43, 369, 998, 855, 687, 66, 928, 218, 235,
266, 429, 74, 41, 687, 1, 733, 46, 846, 381, 584, 155, 475, 419, 252,
1012, 1018, 265, 892, 118, 65, 354, 600, 213, 793, 600, 7, 413, 671,
103, 515, 342, 643, 878, 579, 398, 895, 297, 719, 174, 462, 71, 71,
319, 744, 632, 571, 731, 573, 793, 255, 290, 380, 471, 1006, 544, 975,
81, 13, 204, 646]
```



Challenge #8 (N = 181)

```
chl-181r1
N = 181
q = 1024
d1 = 6
d2 = 5
d3 = 4
dg = 60
public_key = [955, 826, 662, 668, 264, 927, 771, 509, 929, 97, 533,
401, 845, 896, 53, 426, 127, 413, 253, 614, 948, 376, 273, 264, 901,
701, 539, 331, 225, 390, 206, 668, 287, 977, 100, 185, 683, 638, 792,
904, 944, 311, 984, 558, 404, 983, 269, 362, 812, 88, 484, 760, 827,
820, 554, 881, 900, 290, 315, 821, 735, 881, 374, 542, 679, 1020, 562,
661, 233, 239, 872, 465, 646, 507, 221, 125, 416, 78, 32, 180, 819,
946, 753, 961, 1015, 326, 3, 774, 564, 404, 785, 786, 394, 624, 258,
90, 256, 578, 302, 580, 610, 245, 200, 165, 213, 225, 975, 799, 302,
393, 116, 717, 942, 566, 384, 240, 623, 556, 600, 869, 771, 225, 692,
1019, 949, 8, 693, 400, 379, 698, 77, 369, 22, 644, 955, 828, 174,
640, 211, 119, 720, 926, 907, 32, 832, 232, 1018, 106, 65, 841, 273,
295, 921, 984, 64, 147, 373, 990, 761, 922, 628, 581, 994, 594, 718,
529, 600, 125, 352, 953, 231, 274, 557, 151, 827, 309, 835, 654, 884,
339, 514]
```

Challenge #9 (N = 191)

```
chl-191r1
N = 191
q = 1024
d1 = 6
d2 = 5
d3 = 4
dg = 64
public_key = [831, 940, 283, 1019, 98, 927, 499, 173, 774, 789, 412,
316, 1020, 530, 380, 138, 178, 245, 557, 307, 805, 159, 856, 400, 604,
695, 873, 935, 376, 553, 598, 602, 13, 766, 425, 100, 376, 234, 635,
879, 425, 47, 191, 700, 338, 998, 428, 918, 151, 619, 248, 163, 432,
982, 869, 222, 793, 793, 689, 351, 46, 975, 81, 839, 538, 147, 272,
768, 992, 469, 861, 76, 475, 824, 998, 236, 631, 589, 910, 152, 0,
641, 159, 64, 844, 246, 554, 88, 264, 111, 593, 872, 2, 77, 154, 798,
58, 796, 77, 372, 68, 443, 253, 346, 421, 782, 167, 694, 594, 8, 946,
421, 652, 119, 155, 604, 541, 561, 126, 850, 235, 248, 94, 71, 779,
526, 81, 137, 597, 658, 852, 978, 695, 681, 957, 447, 220, 921, 26,
753, 359, 444, 798, 278, 107, 282, 619, 683, 408, 712, 101, 222, 340,
47, 226, 910, 237, 345, 76, 1022, 231, 451, 816, 85, 997, 693, 530,
684, 19, 884, 854, 499, 936, 830, 224, 693, 757, 979, 53, 776, 543,
170, 279, 780, 488, 628, 35, 150, 1006, 294, 592]
```

Challenge #10 (N = 199)

```
chl-199r1
N = 199
q = 1024
d1 = 6
d2 = 5
d3 = 6
dg = 66
public_key = [884, 325, 227, 20, 231, 862, 755, 984, 601, 647, 654,
252, 434, 286, 264, 150, 489, 554, 437, 245, 967, 157, 602, 288, 904,
294, 520, 163, 523, 44, 548, 416, 127, 156, 988, 978, 758, 977, 756,
705, 528, 796, 411, 696, 310, 516, 435, 215, 607, 249, 340, 90, 998,
387, 97, 350, 996, 173, 451, 63, 263, 431, 422, 1017, 536, 1015, 866,
464, 209, 174, 645, 969, 524, 423, 966, 712, 940, 777, 155, 403, 138,
885, 834, 874, 135, 253, 414, 424, 728, 30, 317, 15, 52, 534, 940,
850, 620, 127, 342, 1008, 717, 265, 43, 60, 237, 41, 581, 254, 923,
538, 185, 625, 756, 617, 853, 366, 1012, 5, 663, 409, 384, 902, 914,
633, 437, 130, 8, 297, 853, 779, 656, 329, 151, 800, 752, 799, 62,
415, 43, 417, 400, 340, 640, 40, 371, 596, 317, 360, 601, 253, 334, 0,
87, 410, 385, 351, 481, 396, 114, 334, 762, 977, 573, 698, 610, 801,
398, 43, 516, 265, 506, 431, 570, 353, 499, 602, 63, 941, 305, 813,
585, 207, 149, 306, 223, 401, 15, 243, 708, 21, 273, 147, 46, 303,
478, 50, 996, 891, 385]
```

Challenge #11 (N = 211)

```
chl-211r1
N = 211
q = 1024
d1 = 6
d2 = 6
d3 = 4
dg = 70
public_key = [575, 500, 387, 728, 791, 515, 293, 768, 208, 284, 701,
623, 673, 944, 723, 616, 271, 676, 172, 410, 646, 979, 376, 933, 449,
820, 838, 164, 217, 688, 161, 531, 623, 146, 221, 866, 684, 679, 476,
668, 940, 14, 284, 664, 638, 618, 206, 969, 547, 839, 597, 111, 249,
923, 535, 635, 391, 811, 547, 389, 622, 507, 615, 720, 9, 499, 168,
476, 57, 822, 330, 880, 333, 915, 315, 364, 956, 557, 512, 386, 595,
770, 136, 214, 913, 376, 198, 1005, 687, 28, 431, 254, 991, 196, 266,
572, 628, 1021, 244, 355, 97, 551, 288, 462, 272, 282, 1019, 983, 997,
34, 123, 693, 404, 129, 382, 915, 271, 476, 99, 522, 530, 625, 113,
678, 554, 670, 705, 515, 662, 625, 285, 379, 337, 68, 756, 962, 615,
192, 979, 888, 164, 582, 101, 332, 492, 608, 957, 550, 157, 825, 149,
910, 546, 889, 513, 589, 686, 50, 273, 881, 630, 472, 927, 727, 732,
97, 500, 355, 530, 448, 974, 26, 964, 847, 210, 360, 50, 237, 312,
582, 328, 1011, 123, 565, 1011, 73, 88, 650, 799, 676, 986, 810, 733,
6, 876, 726, 388, 862, 14, 386, 407, 694, 405, 733, 121, 673, 833,
280, 688, 941, 483]
```

Challenge #12 (N = 227)

```
chl-227r1
N = 227
q = 1024
d1 = 6
d2 = 6
d3 = 4
dg = 76
public_key = [694, 734, 588, 304, 661, 505, 707, 678, 942, 616, 912,
980, 363, 426, 243, 503, 33, 578, 798, 189, 894, 214, 490, 399, 588,
351, 669, 312, 732, 788, 283, 827, 583, 646, 129, 879, 95, 161, 965,
304, 519, 930, 166, 922, 1022, 870, 788, 157, 328, 770, 577, 200, 599,
904, 681, 222, 35, 492, 295, 573, 189, 553, 806, 922, 344, 120, 1022,
743, 810, 1021, 181, 51, 943, 333, 118, 810, 150, 352, 725, 118, 914,
933, 572, 773, 467, 14, 241, 180, 698, 799, 230, 461, 380, 256, 544,
839, 342, 927, 1021, 941, 382, 552, 426, 60, 241, 685, 460, 871, 1007,
841, 239, 27, 120, 979, 748, 860, 547, 922, 622, 214, 250, 237, 389,
67, 313, 634, 755, 153, 666, 332, 320, 599, 553, 140, 1018, 962, 110,
12, 203, 455, 190, 204, 434, 493, 428, 617, 826, 214, 711, 853, 824,
34, 419, 237, 861, 437, 352, 967, 43, 597, 125, 153, 441, 193, 801, 5,
131, 106, 365, 55, 204, 529, 236, 433, 821, 323, 368, 404, 320, 250,
963, 285, 316, 1004, 443, 904, 362, 98, 252, 744, 606, 623, 461, 468,
259, 586, 790, 434, 526, 998, 193, 92, 552, 687, 944, 592, 608, 289,
979, 34, 11, 970, 796, 307, 855, 371, 688, 601, 714, 741, 654, 255,
104, 277, 595, 931, 96]
```

Challenge #13 (N = 239)

chl-239r1

N = 239

q = 1024

d1 = 7

d2 = 6

d3 = 4

dg = 80

```
public_key = [69, 356, 421, 1000, 853, 878, 377, 230, 696, 446, 1005,
295, 359, 663, 156, 111, 288, 677, 855, 103, 954, 381, 226, 249, 756,
441, 797, 204, 486, 896, 487, 891, 232, 189, 659, 80, 814, 836, 659,
246, 503, 473, 541, 66, 575, 715, 194, 127, 700, 314, 343, 11, 154,
837, 229, 430, 400, 1002, 299, 535, 57, 584, 1008, 340, 648, 573, 409,
897, 539, 672, 670, 653, 490, 933, 859, 52, 159, 1001, 547, 119, 1007,
608, 595, 276, 667, 821, 880, 164, 716, 363, 634, 747, 137, 257, 692,
608, 193, 863, 917, 95, 685, 832, 12, 977, 770, 660, 372, 417, 849,
59, 20, 286, 266, 776, 533, 458, 389, 785, 233, 514, 183, 813, 616,
530, 506, 678, 557, 364, 99, 13, 517, 316, 143, 373, 755, 912, 503,
72, 334, 640, 314, 603, 430, 807, 68, 99, 701, 317, 222, 195, 200,
586, 571, 272, 712, 128, 1016, 995, 928, 488, 180, 322, 130, 810, 357,
197, 823, 403, 514, 798, 353, 715, 714, 658, 385, 212, 214, 604, 982,
805, 168, 645, 590, 330, 29, 671, 189, 89, 152, 585, 160, 17, 969,
952, 673, 716, 394, 973, 546, 926, 894, 455, 21, 639, 155, 77, 89,
397, 694, 339, 955, 754, 943, 168, 629, 439, 265, 143, 315, 798, 384,
937, 488, 471, 991, 277, 818, 999, 911, 957, 585, 861, 572, 78, 468,
274, 884, 179, 892]
```

Challenge #14 (N = 251)

chl-251r1

N = 251

q = 1024

d1 = 7

d2 = 6

d3 = 4

dg = 84

```
public_key = [397, 334, 448, 719, 551, 657, 780, 985, 552, 725, 644,
328, 695, 1015, 43, 504, 988, 154, 312, 233, 582, 146, 917, 1013, 555,
136, 821, 798, 366, 992, 488, 54, 633, 794, 692, 982, 8, 181, 75, 637,
361, 969, 395, 857, 49, 608, 809, 444, 295, 152, 652, 411, 807, 840,
921, 81, 562, 365, 174, 117, 201, 744, 310, 551, 986, 245, 453, 614,
673, 422, 845, 867, 755, 753, 89, 556, 836, 987, 494, 1013, 277, 505,
459, 360, 726, 357, 778, 249, 241, 469, 254, 219, 845, 971, 464, 657,
228, 340, 1020, 938, 211, 633, 673, 407, 391, 126, 919, 532, 608, 937,
70, 319, 24, 340, 85, 140, 1018, 518, 416, 575, 968, 499, 774, 803,
22, 599, 693, 940, 7, 872, 768, 906, 274, 334, 691, 844, 94, 595, 310,
209, 355, 598, 56, 42, 328, 385, 450, 999, 357, 104, 257, 761, 691,
932, 523, 281, 405, 967, 334, 107, 697, 294, 541, 240, 731, 127, 180,
772, 127, 704, 865, 180, 38, 785, 779, 431, 800, 149, 754, 105, 543,
752, 272, 380, 811, 129, 856, 587, 718, 56, 985, 822, 302, 200, 690,
103, 364, 349, 346, 455, 651, 964, 178, 132, 846, 728, 20, 433, 160,
85, 319, 703, 140, 32, 3, 290, 872, 395, 539, 567, 801, 278, 301, 323,
801, 254, 237, 748, 969, 732, 134, 351, 804, 644, 323, 171, 452, 44,
82, 160, 603, 122, 923, 627, 733, 674, 82, 16, 948, 105, 781]
```


Challenge #15 (N = 263)

chl-263r1

N = 263

q = 1024

d1 = 7

d2 = 6

d3 = 4

dg = 88

```
public_key = [366, 698, 960, 64, 449, 422, 438, 591, 295, 877, 786,
883, 580, 507, 13, 584, 301, 848, 871, 956, 937, 143, 453, 23, 761,
583, 460, 717, 763, 741, 892, 756, 921, 372, 555, 386, 519, 623, 92,
579, 731, 3, 773, 329, 704, 829, 469, 702, 834, 368, 720, 592, 475,
954, 428, 885, 864, 678, 521, 157, 669, 753, 881, 728, 234, 1008, 753,
570, 452, 679, 77, 392, 800, 575, 638, 878, 955, 301, 912, 369, 6,
732, 406, 435, 162, 345, 35, 474, 548, 507, 390, 453, 512, 421, 124,
155, 847, 161, 794, 187, 806, 944, 327, 782, 703, 994, 420, 51, 903,
285, 537, 930, 825, 996, 1003, 252, 297, 1012, 195, 115, 84, 558, 37,
794, 985, 871, 549, 301, 1009, 502, 33, 424, 108, 990, 129, 748, 381,
673, 193, 361, 930, 481, 776, 843, 444, 657, 199, 885, 723, 379, 925,
591, 231, 351, 147, 134, 85, 923, 907, 4, 949, 716, 822, 818, 280, 34,
1010, 700, 589, 706, 164, 773, 249, 459, 269, 51, 690, 572, 806, 732,
736, 407, 186, 199, 311, 278, 267, 418, 96, 560, 99, 902, 721, 278,
722, 976, 1015, 482, 701, 1019, 738, 255, 599, 475, 569, 205, 928,
123, 42, 975, 1011, 257, 396, 448, 840, 450, 101, 31, 657, 959, 891,
865, 182, 150, 582, 1008, 529, 323, 594, 548, 373, 231, 917, 901, 263,
662, 22, 824, 28, 950, 122, 572, 653, 878, 682, 362, 306, 97, 251,
524, 938, 172, 598, 299, 488, 295, 365, 786, 319, 192, 664, 318, 947]
```

Challenge #16 (N = 271)

chl-271r1

N = 271

q = 1024

d1 = 7

d2 = 6

d3 = 6

dg = 90

```
public_key = [64, 875, 470, 863, 380, 607, 195, 401, 331, 542, 7, 413,
410, 403, 296, 253, 672, 551, 794, 670, 516, 845, 296, 99, 61, 244,
142, 17, 369, 779, 546, 55, 641, 95, 205, 1, 727, 159, 113, 748, 918,
631, 858, 926, 1004, 252, 387, 152, 559, 304, 590, 695, 862, 378, 759,
242, 614, 75, 215, 615, 615, 82, 636, 846, 993, 480, 889, 906, 994,
256, 728, 42, 54, 517, 742, 889, 561, 893, 838, 395, 569, 740, 427,
800, 257, 715, 779, 960, 1020, 225, 716, 260, 943, 1015, 168, 640,
440, 69, 784, 834, 835, 171, 223, 196, 713, 594, 644, 832, 127, 344,
905, 896, 339, 958, 140, 199, 528, 767, 311, 280, 656, 132, 360, 364,
488, 52, 1023, 1003, 633, 464, 501, 728, 428, 612, 730, 671, 244, 151,
267, 97, 306, 629, 622, 331, 929, 1015, 608, 244, 734, 564, 426, 72,
746, 831, 515, 547, 126, 800, 510, 880, 414, 410, 997, 858, 861, 1005,
452, 722, 224, 990, 119, 944, 1013, 788, 715, 540, 751, 711, 498, 537,
179, 916, 17, 531, 240, 848, 987, 921, 845, 842, 499, 169, 96, 734,
971, 605, 288, 848, 894, 831, 284, 931, 622, 5, 390, 367, 936, 54,
927, 246, 107, 696, 727, 593, 162, 199, 916, 691, 389, 206, 733, 606,
617, 879, 433, 402, 757, 108, 1004, 777, 141, 621, 423, 332, 941, 932,
863, 708, 229, 868, 969, 701, 529, 48, 882, 370, 8, 205, 347, 214,
724, 954, 990, 250, 1, 597, 881, 10, 323, 507, 352, 639, 275, 383,
449, 779, 157, 222, 138, 433, 767]
```

Challenge #17 (N = 281)

chl-281r1

N = 281

q = 2048

d1 = 7

d2 = 7

d3 = 4

dg = 94

```
public_key = [1290, 1668, 1482, 1229, 219, 1313, 1633, 646, 336, 716,
41, 918, 1161, 1369, 469, 1195, 1732, 798, 1953, 551, 1178, 516, 492,
1014, 1502, 1522, 646, 63, 1663, 59, 1254, 1299, 1738, 700, 152, 1201,
880, 1378, 1967, 1383, 720, 1504, 1044, 1682, 1425, 755, 687, 1189,
1001, 978, 1352, 1933, 1108, 448, 1659, 843, 260, 1401, 1504, 1262,
435, 592, 1591, 365, 1846, 539, 347, 1368, 16, 1053, 1062, 1095, 68,
1482, 1400, 684, 814, 1911, 1931, 117, 416, 1458, 1965, 1972, 0, 11,
151, 525, 1942, 1756, 1511, 1889, 1954, 1994, 1105, 1376, 819, 1624,
1640, 364, 234, 555, 1975, 150, 1684, 890, 239, 746, 75, 1131, 2041,
1382, 1843, 975, 390, 1074, 1872, 770, 569, 1300, 1776, 1047, 1762,
418, 264, 1513, 451, 1068, 658, 35, 1305, 1406, 811, 488, 817, 2001,
1519, 1568, 89, 545, 1947, 96, 442, 865, 1452, 0, 1860, 1389, 1158,
1840, 1750, 498, 1138, 1633, 1950, 987, 629, 829, 1246, 1134, 1211,
1626, 901, 1127, 989, 1956, 1136, 429, 92, 1238, 947, 37, 1807, 669,
210, 246, 1049, 1363, 581, 1935, 695, 514, 146, 662, 1887, 1552, 1013,
55, 466, 169, 1070, 2002, 304, 560, 947, 389, 1116, 1297, 1344, 365,
1507, 687, 1601, 1324, 762, 2021, 119, 1883, 1430, 1142, 475, 620,
631, 856, 467, 1780, 1919, 1520, 1004, 1596, 1158, 1322, 1306, 67,
1784, 1342, 1488, 931, 172, 676, 1355, 1941, 39, 153, 1181, 824, 404,
589, 332, 1792, 736, 1627, 1497, 1265, 1249, 1690, 1868, 909, 1473,
219, 882, 859, 21, 982, 910, 1248, 1235, 1918, 77, 1749, 1162, 2046,
968, 210, 1050, 1727, 709, 213, 503, 795, 1037, 1195, 465, 233, 736,
928, 1404, 404, 180, 763, 1777]
```

Challenge #18 (N = 293)

chl-293r1

N = 293

q = 2048

d1 = 7

d2 = 7

d3 = 4

dg = 98

```
public_key = [1014, 136, 120, 1978, 63, 1075, 994, 1653, 877, 1282,
631, 731, 246, 1544, 1990, 1092, 506, 1187, 1273, 1785, 1268, 1051,
761, 1387, 1538, 1648, 1364, 1056, 261, 803, 340, 766, 206, 739, 387,
1250, 1501, 1589, 230, 1562, 1362, 1979, 986, 1988, 1845, 2023, 1136,
567, 1302, 298, 128, 32, 438, 1769, 1666, 1003, 1884, 1297, 158, 1125,
683, 504, 945, 1319, 1364, 929, 1697, 1809, 636, 198, 1885, 1427, 795,
948, 543, 546, 869, 950, 1540, 1182, 1872, 591, 1904, 1893, 407, 1136,
1733, 1864, 2027, 830, 1645, 158, 1736, 642, 165, 2041, 975, 1237,
467, 1240, 1765, 1808, 1454, 1736, 1624, 1143, 797, 872, 1458, 62,
558, 1125, 1923, 323, 714, 1510, 552, 297, 912, 668, 1898, 772, 1398,
928, 644, 380, 1199, 1187, 1656, 60, 623, 1920, 1485, 851, 1353, 934,
316, 456, 1761, 9, 468, 564, 1761, 1722, 116, 217, 188, 1695, 983,
1194, 1003, 157, 377, 1007, 712, 1709, 1398, 1881, 1259, 1528, 1902,
1836, 535, 989, 1119, 1230, 1182, 1259, 1720, 479, 389, 909, 902, 190,
1014, 129, 664, 792, 1400, 1103, 1046, 1652, 1469, 567, 119, 159, 315,
853, 1559, 141, 889, 1877, 1425, 1196, 1655, 1343, 711, 1154, 1123,
1057, 557, 1254, 549, 377, 80, 317, 286, 72, 410, 1271, 949, 350,
1801, 1259, 1265, 1403, 1959, 1254, 236, 1397, 1547, 707, 1662, 1013,
1638, 1891, 1948, 1983, 1430, 360, 801, 1128, 1624, 1364, 662, 1272,
339, 198, 464, 1198, 1236, 664, 249, 737, 1096, 1134, 1361, 537, 1906,
210, 1190, 1606, 263, 460, 318, 1915, 1979, 412, 414, 83, 610, 841,
1040, 1496, 240, 944, 1268, 1182, 856, 142, 1612, 955, 769, 1812,
1010, 1181, 1485, 1337, 211, 421, 126, 1182, 1596, 970, 48, 1623, 305,
1827, 1116, 38, 344, 495, 509]
```

Challenge #19 (N = 307)

chl-307r1

N = 307

q = 2048

d1 = 7

d2 = 7

d3 = 4

dg = 102

```
public_key = [1018, 803, 1724, 1338, 1786, 1718, 1979, 485, 1878, 130,
824, 366, 1546, 325, 119, 865, 1108, 887, 1836, 1471, 688, 49, 580,
1620, 85, 506, 1079, 424, 1265, 615, 1703, 1421, 1894, 1802, 1908,
1693, 2031, 2009, 650, 35, 757, 583, 269, 931, 320, 1614, 1243, 1040,
200, 1466, 67, 556, 1525, 444, 1701, 2008, 1405, 463, 424, 584, 979,
1662, 1761, 1938, 1875, 1538, 1309, 1928, 712, 331, 1131, 1177, 1838,
991, 1623, 1758, 197, 334, 1397, 830, 600, 802, 1142, 154, 1841, 1476,
1014, 763, 842, 611, 1379, 827, 629, 371, 893, 796, 625, 611, 1813,
1218, 1106, 848, 1025, 1916, 443, 1334, 339, 700, 354, 1625, 500, 423,
122, 964, 1591, 780, 1655, 1308, 1352, 1032, 1225, 1904, 1205, 87,
1021, 428, 1557, 1623, 1659, 767, 1484, 1794, 806, 1456, 1678, 1081,
644, 1642, 1302, 790, 511, 814, 202, 1083, 503, 185, 650, 815, 477,
208, 1761, 936, 1565, 1524, 896, 1615, 1969, 838, 1599, 896, 1503,
1641, 1354, 1278, 1213, 668, 1116, 1800, 1192, 1474, 89, 1207, 362,
1776, 106, 1921, 961, 660, 332, 1275, 1849, 1647, 982, 1755, 1567,
1846, 514, 1843, 390, 1557, 1389, 454, 257, 1571, 760, 576, 1824,
1908, 848, 1591, 1610, 73, 630, 1118, 1160, 1734, 1760, 1688, 644,
608, 327, 1539, 201, 1079, 131, 1316, 55, 1394, 686, 445, 942, 1738,
247, 2014, 874, 66, 1880, 1037, 1701, 1360, 989, 948, 344, 1670, 881,
1211, 1598, 366, 948, 592, 831, 390, 128, 1153, 1364, 6, 782, 1974,
742, 1804, 860, 643, 1539, 1224, 169, 420, 199, 1767, 1941, 1572, 67,
195, 803, 828, 1924, 1843, 58, 49, 146, 579, 1709, 1043, 1300, 973,
1646, 394, 1530, 2020, 667, 511, 935, 84, 1797, 1225, 1548, 1177, 755,
1413, 304, 1898, 1879, 159, 0, 48, 737, 1559, 1895, 801, 424, 1509,
1324, 1918, 227, 863, 1099, 509, 753]
```

Challenge #20 (N = 317)

chl-317r1

N = 317

q = 2048

d1 = 8

d2 = 7

d3 = 5

dg = 106

```
public_key = [1275, 1442, 1239, 1507, 1647, 391, 827, 1620, 1925,
1161, 1310, 621, 239, 1683, 781, 958, 64, 58, 487, 1508, 367, 1087,
1858, 1203, 180, 1512, 1206, 1558, 123, 756, 1940, 1842, 1864, 94,
1713, 933, 335, 1247, 1396, 1043, 1338, 902, 1264, 1835, 844, 1753,
253, 2044, 762, 607, 686, 1581, 1380, 542, 1070, 1568, 1524, 1461,
1018, 1492, 1745, 175, 1270, 952, 1055, 469, 1608, 882, 23, 696, 1281,
1524, 1414, 684, 646, 800, 1957, 552, 213, 130, 1206, 848, 1151, 562,
958, 1353, 339, 198, 1984, 168, 868, 1799, 285, 256, 1702, 952, 521,
1715, 858, 1454, 1736, 195, 1033, 745, 2029, 1596, 293, 1270, 1784,
321, 360, 851, 92, 425, 676, 1254, 827, 493, 413, 1675, 1764, 168,
202, 243, 1465, 663, 1613, 70, 419, 207, 1004, 2003, 252, 806, 1876,
7, 1897, 258, 300, 79, 349, 1334, 224, 1027, 195, 1249, 1960, 1333,
729, 1041, 693, 721, 889, 1894, 275, 712, 310, 638, 741, 954, 230,
1947, 796, 1291, 1908, 284, 1549, 737, 1339, 1102, 889, 1605, 408, 90,
648, 123, 102, 1844, 1293, 1507, 379, 550, 553, 1739, 510, 250, 410,
836, 1606, 77, 1144, 1076, 96, 794, 987, 483, 1289, 1619, 1650, 498,
1985, 578, 661, 1527, 1853, 1224, 700, 1625, 945, 1899, 546, 1447,
1637, 1326, 1538, 1780, 1345, 64, 546, 1844, 1287, 49, 1700, 1421,
817, 314, 955, 798, 1619, 1762, 1479, 259, 661, 707, 645, 1450, 552,
1355, 1187, 247, 1399, 685, 498, 1763, 1, 595, 459, 1860, 267, 498,
648, 1162, 1354, 39, 987, 1322, 703, 1859, 260, 1849, 1342, 1629,
1104, 1113, 709, 1355, 1089, 161, 1963, 246, 854, 607, 1041, 925,
1350, 1543, 1866, 1213, 1591, 426, 265, 1723, 1244, 1858, 187, 1687,
335, 247, 1969, 1175, 111, 2002, 1391, 1982, 1002, 1887, 1920, 1462,
995, 226, 343, 1946, 1931, 557, 1862, 721, 1500, 1567, 1677, 1650,
1528, 925, 128, 1603, 79, 702, 1386]
```

Challenge #21 (N = 331)

chl-331r1

N = 331

q = 2048

d1 = 8

d2 = 7

d3 = 5

dg = 110

```
public_key = [664, 1170, 1317, 1741, 1784, 244, 934, 1204, 855, 1526,
988, 1221, 951, 1806, 866, 667, 871, 791, 1074, 182, 1653, 2033, 1430,
1065, 1659, 1895, 50, 329, 1814, 570, 1108, 302, 730, 1382, 1493,
1790, 1635, 1816, 375, 1130, 412, 901, 762, 875, 1043, 6, 362, 1492,
646, 1721, 1808, 1093, 1786, 1793, 64, 1764, 2026, 1712, 733, 1561,
1810, 1330, 1620, 1878, 1233, 659, 1572, 1333, 830, 1710, 1033, 51,
149, 1081, 414, 9, 1246, 1255, 1524, 1155, 886, 1991, 1320, 1340,
1010, 882, 248, 1817, 1124, 829, 1285, 1785, 1572, 430, 1787, 340,
1976, 1791, 1043, 261, 1541, 138, 106, 711, 668, 510, 1078, 115, 1927,
859, 1852, 1983, 1225, 1548, 1894, 1046, 1, 65, 1905, 339, 726, 359,
438, 1325, 1598, 1417, 1611, 647, 1780, 325, 1862, 310, 1529, 1544,
1432, 649, 535, 1608, 504, 639, 1421, 894, 232, 318, 1919, 1807, 1635,
1917, 615, 75, 502, 199, 1438, 2036, 1386, 1093, 657, 1698, 1379,
1061, 2042, 961, 2037, 583, 111, 1569, 1589, 1820, 83, 86, 535, 1624,
84, 1661, 1383, 1207, 662, 1592, 869, 2039, 593, 667, 1018, 193, 398,
244, 834, 590, 2003, 2010, 639, 892, 1698, 552, 614, 68, 1570, 1379,
587, 286, 649, 1452, 958, 1909, 73, 1657, 1618, 1511, 825, 130, 382,
1046, 1990, 498, 1763, 442, 1230, 1887, 200, 1788, 1840, 132, 1249,
757, 1106, 1919, 901, 1223, 764, 181, 1653, 1966, 1223, 1194, 1673,
1897, 372, 1912, 639, 1493, 1780, 1357, 1316, 1080, 1491, 1862, 821,
1791, 1283, 550, 115, 569, 1463, 1140, 358, 1981, 1400, 966, 1246,
1220, 1656, 180, 1510, 67, 1369, 853, 564, 109, 1755, 71, 361, 615,
692, 1855, 923, 95, 1267, 845, 309, 1139, 124, 1024, 338, 1551, 1145,
521, 790, 360, 1523, 832, 1845, 426, 1554, 1637, 1001, 41, 1436, 1704,
1144, 1693, 517, 539, 272, 1246, 2004, 370, 318, 803, 280, 16, 1857,
27, 1229, 1628, 460, 922, 1332, 567, 1479, 635, 893, 270, 267, 1241,
1894, 510, 1811, 894, 1955, 735, 1136]
```

Challenge #22 (N = 347)

chl-347r1

N = 347

q = 2048

d1 = 8

d2 = 7

d3 = 5

dg = 116

```
public_key = [932, 1481, 210, 566, 1333, 740, 1474, 624, 635, 27,
1759, 1158, 1740, 73, 1429, 863, 712, 1061, 1074, 1821, 1038, 22,
1215, 187, 1429, 1313, 1404, 134, 1019, 297, 1801, 1537, 1355, 1737,
1941, 1292, 770, 1842, 150, 1345, 315, 876, 1455, 626, 298, 1254,
2007, 1331, 1852, 755, 1722, 1815, 940, 368, 785, 1387, 1919, 462,
634, 535, 85, 347, 779, 1412, 2047, 1523, 1595, 1106, 476, 115, 449,
127, 1753, 736, 1871, 1531, 1910, 829, 1520, 1042, 1184, 1420, 718,
750, 1820, 1830, 46, 10, 1279, 158, 1427, 669, 969, 894, 1969, 1781,
1233, 1403, 1957, 1306, 813, 1985, 1504, 1965, 1491, 1080, 909, 1030,
1495, 1659, 10, 1969, 560, 1710, 1587, 1973, 600, 850, 492, 403, 1413,
1393, 795, 1, 1794, 695, 256, 1703, 1503, 833, 468, 301, 394, 1828,
38, 739, 197, 960, 760, 761, 1866, 17, 1452, 1018, 1566, 682, 1115,
1823, 1171, 1681, 1054, 1245, 1947, 1075, 1201, 461, 1961, 286, 997,
2024, 1704, 100, 402, 586, 861, 826, 1022, 1666, 1765, 406, 1915, 567,
2029, 1163, 236, 456, 1128, 817, 1072, 749, 196, 609, 615, 420, 45,
43, 1678, 926, 1175, 624, 620, 592, 805, 808, 526, 986, 1149, 1299,
1345, 1346, 1078, 534, 546, 1448, 1916, 1449, 186, 1289, 1873, 1844,
1788, 1301, 1326, 1813, 859, 281, 295, 1963, 1113, 111, 705, 1408,
1151, 1584, 550, 1998, 176, 998, 757, 1918, 110, 509, 1404, 1356,
1361, 1976, 902, 567, 259, 1370, 1407, 1712, 1297, 1150, 1182, 1496,
1611, 994, 121, 296, 160, 44, 968, 1494, 1089, 375, 334, 692, 1153,
1967, 1655, 152, 588, 750, 100, 1217, 764, 435, 846, 682, 319, 1211,
510, 65, 1071, 1502, 1128, 312, 1114, 1414, 1188, 291, 524, 532, 1915,
294, 1766, 958, 1601, 852, 1716, 812, 269, 1874, 476, 602, 554, 874,
52, 1800, 1172, 162, 950, 643, 1493, 863, 1819, 1669, 1499, 1752, 397,
1197, 537, 1526, 1094, 27, 174, 47, 1147, 1130, 1874, 1301, 131, 1090,
1527, 516, 1022, 624, 293, 384, 1611, 871, 425, 37, 874, 609, 375,
1810, 282, 1054, 703, 1487, 1676, 1554, 1604, 1088, 1950]
```


Challenge #23 (N = 359)

chl-359r1

N = 359

q = 2048

d1 = 8

d2 = 7

d3 = 8

dg = 120

```
public_key = [414, 762, 1867, 1861, 117, 1570, 1462, 1413, 203, 750,
1824, 1652, 1618, 529, 755, 142, 860, 1959, 956, 502, 502, 343, 650,
421, 1318, 1382, 579, 1197, 63, 494, 1661, 1796, 1447, 1475, 831, 145,
2023, 330, 866, 33, 340, 1982, 1204, 1622, 415, 1109, 2003, 1936, 316,
691, 1301, 542, 449, 332, 207, 81, 1712, 221, 344, 145, 52, 1593,
1004, 1176, 700, 344, 1500, 2021, 1643, 24, 398, 561, 1508, 271, 1622,
283, 1289, 786, 1552, 514, 876, 1875, 1510, 74, 705, 472, 647, 931,
199, 1597, 1086, 1404, 198, 1796, 647, 265, 1577, 1124, 1000, 1449,
745, 1202, 147, 1192, 1601, 668, 820, 265, 1416, 409, 1620, 165, 73,
1710, 1180, 410, 1950, 213, 587, 394, 766, 249, 1703, 1406, 188, 1174,
177, 1374, 1647, 2014, 569, 1644, 1756, 177, 739, 959, 1731, 1986,
1815, 1459, 793, 1364, 1113, 1766, 824, 1713, 530, 775, 574, 404, 452,
1179, 664, 1882, 189, 220, 911, 797, 17, 301, 182, 1263, 1891, 798,
1691, 1994, 723, 1480, 156, 1744, 1657, 331, 258, 1772, 1371, 1725,
972, 1567, 86, 1559, 63, 931, 561, 1248, 1039, 737, 612, 1844, 485,
761, 1749, 1260, 1221, 989, 1216, 963, 659, 427, 1348, 628, 117, 697,
1647, 271, 1739, 1657, 1851, 1994, 45, 41, 1988, 1398, 1649, 1767,
1324, 1839, 1978, 1468, 1737, 361, 281, 1566, 1102, 1417, 817, 649,
1410, 1367, 1438, 1034, 937, 221, 571, 92, 1554, 1193, 1116, 195,
1385, 1231, 665, 1226, 341, 683, 22, 1311, 1419, 1724, 1305, 1060,
137, 704, 501, 649, 1194, 57, 1653, 535, 1089, 80, 297, 1926, 1220,
649, 1491, 149, 1371, 208, 159, 1726, 364, 1349, 1051, 1809, 1954,
1555, 940, 1208, 1017, 154, 974, 1788, 1160, 1219, 1609, 863, 77, 760,
667, 729, 1102, 1023, 890, 130, 1706, 1953, 1646, 150, 543, 925, 877,
1352, 803, 1635, 550, 1245, 1143, 1685, 118, 1824, 1616, 1192, 1817,
1868, 577, 764, 1243, 1961, 1475, 1706, 845, 280, 3, 1315, 1577, 2007,
1316, 822, 710, 780, 1271, 630, 400, 1373, 1469, 1427, 287, 974, 1251,
1681, 1385, 463, 1992, 1210, 1456, 1434, 1910, 643, 340, 54, 1955,
1843, 12, 1515, 1297, 1244, 1926, 90, 1123]
```

Challenge #24 (N = 367)

chl-367r1

N = 367

q = 2048

d1 = 8

d2 = 8

d3 = 5

dg = 122

```
public_key = [685, 23, 538, 687, 446, 1930, 554, 1513, 115, 1751,
1391, 735, 1537, 140, 334, 1745, 1437, 1916, 1408, 408, 157, 1666, 92,
61, 1085, 629, 1777, 1974, 1012, 1662, 317, 1215, 328, 1004, 661, 132,
429, 85, 860, 1410, 1943, 195, 1201, 1880, 1891, 183, 492, 1994, 1170,
1364, 524, 796, 1905, 403, 1607, 1597, 1384, 854, 2027, 13, 2002,
1960, 609, 1820, 40, 1833, 1763, 1241, 863, 563, 1654, 1895, 320, 719,
1061, 41, 1440, 1515, 761, 866, 383, 1833, 163, 334, 1116, 1669, 1075,
1904, 1794, 132, 323, 2003, 1241, 624, 1513, 1895, 182, 1627, 53,
1700, 1977, 922, 433, 815, 1397, 786, 170, 1912, 1071, 908, 231, 1427,
1566, 1924, 683, 1121, 542, 81, 264, 1546, 381, 1665, 1162, 1895,
1466, 1533, 632, 714, 1979, 1873, 593, 1113, 1828, 1612, 1298, 1320,
634, 677, 1376, 578, 1154, 539, 197, 455, 1378, 1875, 621, 712, 1189,
192, 1254, 1597, 1792, 254, 764, 1861, 905, 606, 1220, 610, 1205,
1284, 1399, 1157, 525, 1823, 760, 141, 834, 758, 429, 1257, 1066, 155,
213, 623, 1755, 281, 1354, 191, 1074, 827, 1265, 666, 1040, 224, 894,
966, 333, 1995, 508, 106, 1284, 1049, 1861, 255, 260, 169, 1956, 1490,
146, 1949, 1544, 315, 935, 592, 1647, 1861, 576, 1463, 2002, 173, 735,
2009, 841, 853, 977, 1587, 1829, 1809, 533, 210, 1700, 1138, 1482,
646, 1041, 688, 321, 364, 1100, 887, 475, 73, 1370, 395, 1321, 385,
1275, 1487, 122, 1189, 852, 1876, 153, 1982, 623, 664, 1205, 1593,
1035, 1315, 1889, 463, 1267, 613, 1581, 403, 1208, 1128, 423, 1995,
106, 649, 747, 656, 1364, 168, 842, 1723, 334, 1346, 858, 1111, 607,
842, 923, 903, 1985, 768, 953, 1715, 1217, 1181, 93, 249, 240, 788,
1285, 557, 1106, 298, 2028, 349, 1338, 770, 63, 1845, 1169, 623, 450,
816, 1018, 1746, 536, 807, 348, 388, 1050, 946, 2017, 1580, 1243,
1626, 1531, 565, 139, 2047, 1561, 1372, 1299, 1620, 987, 1630, 865,
919, 1851, 779, 47, 1746, 1784, 218, 638, 292, 1446, 1885, 705, 1452,
543, 689, 100, 1736, 1933, 336, 969, 1221, 483, 1432, 1193, 1111,
1306, 1103, 1768, 1330, 1535, 858, 134, 1279, 1759, 260, 1083, 462,
1589, 618, 848, 715, 1769]
```

Challenge #25 (N = 379)

chl-379r1

N = 379

q = 2048

d1 = 8

d2 = 8

d3 = 5

dg = 126

```
public_key = [873, 220, 339, 1781, 1081, 1004, 965, 789, 828, 1592,
33, 275, 1410, 1874, 1502, 524, 1944, 1886, 318, 1112, 1039, 1734,
1088, 1909, 1990, 1545, 1187, 1887, 823, 181, 873, 640, 528, 1855,
2030, 1961, 399, 2002, 29, 2040, 1517, 486, 1634, 709, 200, 606, 1307,
488, 939, 1731, 808, 108, 692, 465, 1066, 490, 1802, 1086, 822, 1160,
977, 1901, 205, 384, 81, 748, 1573, 455, 1873, 838, 713, 851, 1853,
1452, 1525, 1007, 757, 1882, 708, 1665, 27, 998, 1055, 1596, 287,
1751, 1020, 221, 938, 1804, 899, 2034, 1859, 599, 1028, 789, 1036,
1426, 1793, 1830, 1902, 1040, 223, 984, 978, 1685, 1726, 1022, 1491,
1922, 255, 443, 385, 782, 728, 720, 1614, 1757, 1250, 1921, 21, 1639,
623, 943, 591, 1797, 1618, 1291, 1770, 379, 1364, 62, 1829, 907, 1402,
112, 712, 951, 1575, 1316, 584, 703, 1544, 77, 1820, 201, 1882, 1844,
1660, 2021, 381, 636, 1468, 1295, 728, 968, 1101, 64, 607, 973, 729,
830, 603, 330, 1479, 989, 1164, 1403, 461, 1977, 2029, 967, 1956,
1022, 972, 560, 905, 1821, 1274, 1824, 1072, 1342, 628, 1082, 78, 72,
750, 770, 10, 1832, 1510, 1039, 424, 694, 576, 1179, 598, 1877, 207,
835, 699, 974, 1704, 1564, 1526, 1828, 281, 207, 614, 1713, 1545,
1624, 438, 1708, 1887, 341, 726, 947, 375, 2037, 1274, 239, 395, 1025,
1613, 413, 1377, 959, 1981, 392, 242, 1233, 1617, 375, 1242, 638, 940,
534, 576, 1814, 1373, 186, 741, 415, 176, 1868, 649, 1933, 1494, 536,
1823, 938, 658, 1841, 2031, 217, 1749, 1660, 1934, 1670, 1463, 620,
2037, 1629, 509, 1083, 1819, 1058, 1568, 1552, 1635, 1134, 1781, 165,
916, 5, 1698, 919, 1784, 154, 1672, 1279, 1045, 347, 1769, 1787, 414,
1235, 977, 1045, 213, 819, 382, 305, 1205, 1547, 1944, 744, 16, 2003,
176, 1230, 777, 232, 1054, 170, 1189, 1180, 1382, 1603, 1110, 1095,
1217, 1819, 959, 1673, 1016, 633, 1865, 1216, 1995, 1075, 1330, 1135,
116, 1354, 1259, 1401, 107, 1196, 527, 925, 1189, 160, 1894, 117, 569,
524, 418, 165, 1117, 1717, 423, 1967, 1769, 153, 49, 1180, 388, 1229,
1076, 239, 954, 525, 681, 1481, 1848, 769, 31, 1653, 360, 1306, 1500,
345, 1716, 1818, 1774, 934, 582, 925, 785, 1120, 762, 1508, 1035, 559,
899, 1964, 629]
```

Challenge #26 (N = 389)

chl-389r1

N = 389

q = 2048

d1 = 8

d2 = 8

d3 = 5

dg = 130

```
public_key = [2019, 1829, 555, 1365, 979, 1011, 408, 302, 1028, 440,
874, 685, 266, 1075, 916, 534, 303, 1042, 334, 1290, 972, 762, 1134,
470, 1901, 1582, 599, 35, 1780, 1202, 1976, 1113, 1650, 1337, 674,
1888, 1524, 270, 912, 844, 1761, 1602, 723, 1068, 1612, 1193, 1056,
1371, 1338, 556, 1137, 370, 901, 1686, 1932, 227, 1249, 198, 1712,
753, 1568, 751, 332, 1858, 1155, 343, 1537, 1631, 763, 1028, 627, 613,
1090, 1637, 1710, 1184, 1915, 1722, 1999, 1723, 1834, 659, 352, 1034,
1782, 1520, 772, 1922, 1704, 1602, 1702, 1458, 1267, 1183, 1833, 1039,
447, 730, 40, 1724, 1165, 1214, 450, 1841, 824, 89, 1865, 210, 532,
113, 691, 1878, 133, 959, 457, 1168, 44, 39, 32, 588, 1382, 1095,
1776, 969, 647, 2009, 731, 788, 671, 309, 293, 213, 1467, 495, 1824,
1737, 1352, 1046, 188, 1351, 1228, 1715, 82, 908, 211, 264, 430, 1714,
351, 994, 740, 113, 290, 1484, 1276, 1642, 283, 1175, 1133, 554, 613,
633, 1616, 2003, 121, 1544, 617, 930, 1490, 738, 78, 776, 1635, 1790,
94, 78, 694, 1701, 1047, 1249, 1281, 1900, 92, 635, 37, 770, 337,
1596, 543, 1969, 1990, 1789, 1878, 2015, 709, 1901, 1727, 1982, 771,
715, 731, 1756, 688, 1892, 1925, 662, 1732, 1584, 1227, 1459, 1788,
1670, 558, 1113, 626, 1347, 1394, 307, 215, 376, 523, 623, 1753, 137,
764, 189, 2047, 1082, 1017, 1695, 467, 1147, 1889, 1292, 1606, 962,
674, 896, 1993, 1010, 744, 1332, 19, 1195, 1443, 1227, 316, 1814, 207,
648, 1711, 1531, 417, 932, 1364, 333, 1322, 1777, 1195, 473, 1208,
310, 675, 421, 1768, 1275, 1213, 764, 1946, 1609, 834, 410, 13, 1187,
386, 381, 1821, 1888, 495, 1783, 912, 422, 19, 1829, 1170, 146, 332,
1597, 1529, 236, 1770, 90, 791, 824, 1877, 1076, 1467, 1464, 279,
1284, 62, 522, 2010, 349, 706, 1971, 1107, 1265, 1089, 384, 439, 1209,
883, 1972, 1246, 274, 1845, 430, 472, 1401, 983, 1931, 1743, 377, 717,
1920, 1595, 816, 763, 312, 1783, 1317, 573, 1930, 943, 842, 170, 1155,
360, 1849, 1164, 803, 230, 1037, 649, 1719, 1788, 1667, 634, 918,
1451, 1289, 496, 379, 198, 1756, 359, 292, 1829, 1579, 1667, 648,
1790, 1739, 777, 312, 1826, 1709, 1938, 1251, 389, 1792, 768, 1838,
1723, 947, 137, 587, 1692, 1074, 654, 1833, 1183, 1397, 1645, 1258,
1935, 1154, 248]
```

Challenge #27 (N = 401)

chl-401r1

N = 401

q = 2048

d1 = 8

d2 = 8

d3 = 6

dg = 134

```
public_key = [85, 1720, 1358, 1315, 885, 1201, 942, 1310, 1354, 1881,
1304, 1560, 608, 954, 1555, 530, 1593, 698, 1576, 1326, 1368, 961,
1356, 1160, 348, 1089, 166, 1306, 1018, 1839, 478, 1586, 847, 1860,
1584, 281, 1079, 1058, 1704, 1762, 146, 226, 393, 147, 986, 655, 541,
760, 635, 1684, 1377, 1857, 911, 1853, 1609, 425, 1909, 28, 1512, 785,
1384, 877, 290, 535, 416, 1321, 837, 674, 1900, 1323, 1448, 165, 312,
1156, 1427, 672, 582, 398, 456, 1792, 367, 1399, 732, 1978, 546, 993,
1374, 1182, 1960, 973, 522, 1850, 1167, 276, 785, 1522, 1413, 1617,
331, 655, 1120, 1292, 520, 135, 77, 562, 748, 1874, 1529, 1507, 1447,
222, 1395, 1423, 1848, 1742, 501, 1146, 815, 787, 1368, 966, 145,
1225, 1478, 1976, 1124, 824, 290, 1647, 1411, 38, 600, 1430, 1747,
1652, 737, 640, 11, 69, 1304, 2038, 1529, 995, 1142, 1932, 1355, 681,
1916, 133, 679, 1608, 750, 1112, 1211, 1352, 1484, 679, 631, 1371,
1709, 24, 198, 1029, 1775, 943, 1464, 1533, 1581, 84, 1284, 1095,
1694, 1887, 954, 874, 211, 43, 1852, 1031, 1092, 1432, 1952, 1174,
810, 1124, 1868, 345, 379, 1917, 1454, 1458, 950, 1564, 1883, 1004,
804, 1609, 2018, 424, 370, 1715, 956, 2016, 2028, 421, 871, 1094,
1478, 1418, 1684, 306, 901, 296, 2047, 254, 1696, 972, 1337, 1713,
1498, 333, 414, 31, 1966, 1449, 355, 457, 435, 1664, 592, 1151, 545,
1472, 360, 335, 1616, 405, 630, 832, 222, 1890, 223, 1174, 1476, 806,
1714, 994, 337, 1811, 1509, 689, 909, 525, 750, 1584, 573, 1775, 1295,
1308, 1693, 1496, 1273, 436, 1238, 318, 164, 1435, 925, 1417, 1722,
653, 1850, 1686, 294, 896, 1485, 954, 1285, 1965, 1112, 872, 1433,
1207, 76, 1633, 1722, 938, 165, 1114, 1035, 1592, 245, 387, 1149,
1680, 1217, 564, 342, 1064, 165, 1952, 494, 1898, 1204, 1528, 274,
1841, 628, 222, 15, 576, 1678, 1978, 211, 1195, 1751, 496, 613, 1622,
1929, 666, 1214, 798, 1285, 57, 274, 519, 1876, 1923, 1569, 543, 1367,
693, 1802, 348, 491, 584, 1607, 1897, 1301, 1583, 932, 984, 887, 749,
1305, 938, 1496, 825, 1345, 714, 1614, 1854, 1548, 292, 617, 1467,
637, 9, 1013, 742, 908, 120, 1969, 110, 1069, 1831, 1262, 1999, 846,
1563, 1936, 1336, 77, 1574, 954, 1880, 858, 1124, 1616, 1612, 458,
944, 1534, 1406, 474, 635, 996, 1376, 404, 1717, 1241, 892, 25, 1000,
596, 953, 828, 134, 1537]
```

Cash Prizes

The first correct and complete submission for each NTRU Challenge will receive the following prizes (see contest rules for details and submission formats).

Challenge	Prize (US Dollars)
Challenge #1 (N = 107)	\$1,000
Challenge #2 (N = 113)	\$1,000
Challenge #3 (N = 131)	\$1,000
Challenge #4 (N = 139)	\$1,000
Challenge #5 (N = 149)	\$1,000
Challenge #6 (N = 163)	\$1,000
Challenge #7 (N = 173)	\$1,000
Challenge #8 (N = 181)	\$1,000
Challenge #9 (N = 191)	\$1,000
Challenge #10 (N = 199)	\$1,000
Challenge #11 (N = 211)	\$1,000
Challenge #12 (N = 227)	\$5,000
Challenge #13 (N = 239)	\$5,000
Challenge #14 (N = 251)	\$5,000
Challenge #15 (N = 263)	\$5,000
Challenge #16 (N = 271)	\$5,000
Challenge #17 (N = 281)	\$5,000
Challenge #18 (N = 293)	\$5,000
Challenge #19 (N = 307)	\$5,000
Challenge #20 (N = 317)	\$5,000
Challenge #21 (N = 331)	\$5,000
Challenge #22 (N = 347)	\$5,000
Challenge #23 (N = 359)	\$5,000
Challenge #24 (N = 367)	\$5,000
Challenge #25 (N = 379)	\$5,000
Challenge #26 (N = 389)	\$5,000
Challenge #27 (N = 401)	\$5,000