

Blog Entry © Friday, August 21, 2026, by James Pate Williams, Jr. NIST FIPS 203 C/C++ Implementations

== Main Menu ==

0 - Small Vector Test NTT, NTT^{-1}
 1 - Test BitRev, NTT, NTT^{-1}
 2 - Test SHA-3
 3 - Exit

Option = 0

forward NTT of f

f[0] =	1	fHat[0] =	10
f[1] =	2	fHat[1] =	913
f[2] =	3	fHat[2] =	7679
f[3] =	4	fHat[3] =	6764

inverse NTT of f

f[0] =	1	fHat[0] =	10
f[1] =	2	fHat[1] =	913
f[2] =	3	fHat[2] =	7679
f[3] =	4	fHat[3] =	6764

forward NTT of g

g[0] =	5	gHat[0] =	26
g[1] =	6	gHat[1] =	913
g[2] =	7	gHat[2] =	7679
g[3] =	8	gHat[3] =	6764

the positive-wrapped convolution of f and g is:

h[0] =	66	hHat[0] =	260
h[1] =	68	hHat[1] =	4021
h[2] =	66	hHat[2] =	4
h[3] =	60	hHat[3] =	3660

== Main Menu ==

0 - Small Vector Test NTT, NTT^{-1}
 1 - Test BitRev, NTT, NTT^{-1}
 2 - Test SHA-3
 3 - Exit

Option = 1

Testing NIST BitRev Etc.
 BitReversal NTT and NTT⁻¹
 See NIST FIPS 203 Appendix A

BitRev(0) =	0	1	17
BitRev(1) =	64	1729	3312
BitRev(2) =	32	2580	2761
BitRev(3) =	96	3289	568
BitRev(4) =	16	2642	583
BitRev(5) =	80	630	2746
BitRev(6) =	48	1897	2649
BitRev(7) =	112	848	680
BitRev(8) =	8	1062	1637
BitRev(9) =	72	1919	1692
BitRev(10) =	40	193	723
BitRev(11) =	104	797	2606
BitRev(12) =	24	2786	2288
BitRev(13) =	88	3260	1041
BitRev(14) =	56	569	1100
BitRev(15) =	120	1746	2229
BitRev(16) =	4	296	1409
BitRev(17) =	68	2447	1920
BitRev(18) =	36	1339	2662
BitRev(19) =	100	1476	667
BitRev(20) =	20	3046	3281
BitRev(21) =	84	56	48
BitRev(22) =	52	2240	233
BitRev(23) =	116	1333	3096
BitRev(24) =	12	1426	756
BitRev(25) =	76	2094	2573
BitRev(26) =	44	535	2156
BitRev(27) =	108	2882	1173
BitRev(28) =	28	2393	3015
BitRev(29) =	92	2879	314
BitRev(30) =	60	1974	3050
BitRev(31) =	124	821	279
BitRev(32) =	2	289	1703
BitRev(33) =	66	331	1626
BitRev(34) =	34	3253	1651
BitRev(35) =	98	1756	1678
BitRev(36) =	18	1197	2789
BitRev(37) =	82	2304	540
BitRev(38) =	50	2277	1789
BitRev(39) =	114	2055	1540
BitRev(40) =	10	650	1847
BitRev(41) =	74	1977	1482
BitRev(42) =	42	2513	952

BitRev(43) =	106	632	2377
BitRev(44) =	26	2865	1461
BitRev(45) =	90	33	1868
BitRev(46) =	58	1320	2687
BitRev(47) =	122	1915	642
BitRev(48) =	6	2319	939
BitRev(49) =	70	1435	2390
BitRev(50) =	38	807	2308
BitRev(51) =	102	452	1021
BitRev(52) =	22	1438	2437
BitRev(53) =	86	2868	892
BitRev(54) =	54	1534	2388
BitRev(55) =	118	2402	941
BitRev(56) =	14	2647	733
BitRev(57) =	78	2617	2596
BitRev(58) =	46	1481	2337
BitRev(59) =	110	648	992
BitRev(60) =	30	2474	268
BitRev(61) =	94	3110	3061
BitRev(62) =	62	1227	641
BitRev(63) =	126	910	2688
BitRev(64) =	1	17	1584
BitRev(65) =	65	2761	1745
BitRev(66) =	33	583	2298
BitRev(67) =	97	2649	1031
BitRev(68) =	17	1637	2037
BitRev(69) =	81	723	1292
BitRev(70) =	49	2288	3220
BitRev(71) =	113	1100	109
BitRev(72) =	9	1409	375
BitRev(73) =	73	2662	2954
BitRev(74) =	41	3281	2549
BitRev(75) =	105	233	780
BitRev(76) =	25	756	2090
BitRev(77) =	89	2156	1239
BitRev(78) =	57	3015	1645
BitRev(79) =	121	3050	1684
BitRev(80) =	5	1703	1063
BitRev(81) =	69	1651	2266
BitRev(82) =	37	2789	319
BitRev(83) =	101	1789	3010
BitRev(84) =	21	1847	2773
BitRev(85) =	85	952	556
BitRev(86) =	53	1461	757
BitRev(87) =	117	2687	2572
BitRev(88) =	13	939	2099
BitRev(89) =	77	2308	1230

BitRev(90) =	45	2437	561
BitRev(91) =	109	2388	2768
BitRev(92) =	29	733	2466
BitRev(93) =	93	2337	863
BitRev(94) =	61	268	2594
BitRev(95) =	125	641	735
BitRev(96) =	3	1584	2804
BitRev(97) =	67	2298	525
BitRev(98) =	35	2037	1092
BitRev(99) =	99	3220	2237
BitRev(100) =	19	375	403
BitRev(101) =	83	2549	2926
BitRev(102) =	51	2090	1026
BitRev(103) =	115	1645	2303
BitRev(104) =	11	1063	1143
BitRev(105) =	75	319	2186
BitRev(106) =	43	2773	2150
BitRev(107) =	107	757	1179
BitRev(108) =	27	2099	2775
BitRev(109) =	91	561	554
BitRev(110) =	59	2466	886
BitRev(111) =	123	2594	2443
BitRev(112) =	7	2804	1722
BitRev(113) =	71	1092	1607
BitRev(114) =	39	403	1212
BitRev(115) =	103	1026	2117
BitRev(116) =	23	1143	1874
BitRev(117) =	87	2150	1455
BitRev(118) =	55	2775	1029
BitRev(119) =	119	886	2300
BitRev(120) =	15	1722	2110
BitRev(121) =	79	1212	1219
BitRev(122) =	47	1874	2935
BitRev(123) =	111	1029	394
BitRev(124) =	31	2110	885
BitRev(125) =	95	2935	2444
BitRev(126) =	63	885	2154
BitRev(127) =	127	2154	1175

Testing NIST NTT

f[0] =	41	fHat[0] =	63
f[1] =	3005	fHat[1] =	989
f[2] =	2524	fHat[2] =	2586
f[3] =	1491	fHat[3] =	2084
f[4] =	330	fHat[4] =	1135
f[5] =	2376	fHat[5] =	1013

f[6] = 3307	fHat[6] = 0
f[7] = 3303	fHat[7] = 822
f[8] = 2995	fHat[8] = 887
f[9] = 1498	fHat[9] = 2602
f[10] = 2430	fHat[10] = 1196
f[11] = 573	fHat[11] = 1453
f[12] = 292	fHat[12] = 2287
f[13] = 776	fHat[13] = 2338
f[14] = 3073	fHat[14] = 2640
f[15] = 2118	fHat[15] = 230
f[16] = 1455	fHat[16] = 1759
f[17] = 1869	fHat[17] = 1058
f[18] = 2364	fHat[18] = 2830
f[19] = 390	fHat[19] = 981
f[20] = 2071	fHat[20] = 794
f[21] = 1361	fHat[21] = 343
f[22] = 1028	fHat[22] = 3201
f[23] = 1825	fHat[23] = 287
f[24] = 1621	fHat[24] = 2938
f[25] = 2244	fHat[25] = 2922
f[26] = 2701	fHat[26] = 267
f[27] = 63	fHat[27] = 3029
f[28] = 2065	fHat[28] = 2080
f[29] = 897	fHat[29] = 2019
f[30] = 2329	fHat[30] = 2032
f[31] = 2216	fHat[31] = 1743
f[32] = 288	fHat[32] = 3322
f[33] = 2382	fHat[33] = 2683
f[34] = 2619	fHat[34] = 1757
f[35] = 814	fHat[35] = 2546
f[36] = 2574	fHat[36] = 1965
f[37] = 1067	fHat[37] = 1092
f[38] = 1690	fHat[38] = 1838
f[39] = 1090	fHat[39] = 3304
f[40] = 2984	fHat[40] = 1159
f[41] = 781	fHat[41] = 2092
f[42] = 2111	fHat[42] = 1863
f[43] = 1637	fHat[43] = 3070
f[44] = 615	fHat[44] = 1897
f[45] = 299	fHat[45] = 938
f[46] = 1323	fHat[46] = 2093
f[47] = 2208	fHat[47] = 1994
f[48] = 2802	fHat[48] = 314
f[49] = 2955	fHat[49] = 1857
f[50] = 1504	fHat[50] = 2225
f[51] = 1310	fHat[51] = 3293
f[52] = 2730	fHat[52] = 1373

f[53] = 661	fHat[53] = 2197
f[54] = 1712	fHat[54] = 50
f[55] = 1692	fHat[55] = 1162
f[56] = 292	fHat[56] = 3287
f[57] = 2941	fHat[57] = 3091
f[58] = 145	fHat[58] = 1634
f[59] = 1768	fHat[59] = 3246
f[60] = 683	fHat[60] = 2669
f[61] = 2503	fHat[61] = 2933
f[62] = 2381	fHat[62] = 2764
f[63] = 352	fHat[63] = 2738
f[64] = 702	fHat[64] = 999
f[65] = 718	fHat[65] = 572
f[66] = 296	fHat[66] = 2285
f[67] = 650	fHat[67] = 1809
f[68] = 1146	fHat[68] = 263
f[69] = 1362	fHat[69] = 1367
f[70] = 2141	fHat[70] = 1158
f[71] = 1121	fHat[71] = 964
f[72] = 1629	fHat[72] = 731
f[73] = 2248	fHat[73] = 478
f[74] = 918	fHat[74] = 2932
f[75] = 3093	fHat[75] = 2079
f[76] = 874	fHat[76] = 407
f[77] = 3097	fHat[77] = 361
f[78] = 900	fHat[78] = 1169
f[79] = 2117	fHat[79] = 399
f[80] = 765	fHat[80] = 671
f[81] = 992	fHat[81] = 466
f[82] = 1574	fHat[82] = 1255
f[83] = 963	fHat[83] = 2389
f[84] = 273	fHat[84] = 302
f[85] = 304	fHat[85] = 1862
f[86] = 2716	fHat[86] = 1983
f[87] = 1267	fHat[87] = 1841
f[88] = 716	fHat[88] = 3178
f[89] = 3023	fHat[89] = 9
f[90] = 1623	fHat[90] = 1054
f[91] = 53	fHat[91] = 2886
f[92] = 3115	fHat[92] = 607
f[93] = 242	fHat[93] = 321
f[94] = 1482	fHat[94] = 1263
f[95] = 399	fHat[95] = 672
f[96] = 1345	fHat[96] = 3069
f[97] = 1162	fHat[97] = 1159
f[98] = 994	fHat[98] = 2618
f[99] = 2839	fHat[99] = 279

f[100]	=	993	fHat[100]	=	888
f[101]	=	2290	fHat[101]	=	1544
f[102]	=	626	fHat[102]	=	462
f[103]	=	3203	fHat[103]	=	1011
f[104]	=	2824	fHat[104]	=	1027
f[105]	=	2895	fHat[105]	=	603
f[106]	=	2515	fHat[106]	=	325
f[107]	=	1673	fHat[107]	=	695
f[108]	=	3195	fHat[108]	=	2301
f[109]	=	3093	fHat[109]	=	2819
f[110]	=	562	fHat[110]	=	2030
f[111]	=	2682	fHat[111]	=	3235
f[112]	=	790	fHat[112]	=	22
f[113]	=	142	fHat[113]	=	2264
f[114]	=	606	fHat[114]	=	1521
f[115]	=	1482	fHat[115]	=	815
f[116]	=	2944	fHat[116]	=	2527
f[117]	=	1377	fHat[117]	=	3240
f[118]	=	498	fHat[118]	=	331
f[119]	=	1893	fHat[119]	=	1758
f[120]	=	2709	fHat[120]	=	1709
f[121]	=	1545	fHat[121]	=	827
f[122]	=	1300	fHat[122]	=	671
f[123]	=	3170	fHat[123]	=	2125
f[124]	=	2511	fHat[124]	=	56
f[125]	=	2886	fHat[125]	=	1325
f[126]	=	969	fHat[126]	=	3101
f[127]	=	354	fHat[127]	=	2198

Testing NIST NTT⁻¹

fHat[0]	=	63	f[0]	=	41
fHat[1]	=	989	f[1]	=	3005
fHat[2]	=	2586	f[2]	=	2524
fHat[3]	=	2084	f[3]	=	1491
fHat[4]	=	1135	f[4]	=	330
fHat[5]	=	1013	f[5]	=	2376
fHat[6]	=	0	f[6]	=	3307
fHat[7]	=	822	f[7]	=	3303
fHat[8]	=	887	f[8]	=	2995
fHat[9]	=	2602	f[9]	=	1498
fHat[10]	=	1196	f[10]	=	2430
fHat[11]	=	1453	f[11]	=	573
fHat[12]	=	2287	f[12]	=	292
fHat[13]	=	2338	f[13]	=	776
fHat[14]	=	2640	f[14]	=	3073
fHat[15]	=	230	f[15]	=	2118

fHat[16] = 1759	f[16] = 1455
fHat[17] = 1058	f[17] = 1869
fHat[18] = 2830	f[18] = 2364
fHat[19] = 981	f[19] = 390
fHat[20] = 794	f[20] = 2071
fHat[21] = 343	f[21] = 1361
fHat[22] = 3201	f[22] = 1028
fHat[23] = 287	f[23] = 1825
fHat[24] = 2938	f[24] = 1621
fHat[25] = 2922	f[25] = 2244
fHat[26] = 267	f[26] = 2701
fHat[27] = 3029	f[27] = 63
fHat[28] = 2080	f[28] = 2065
fHat[29] = 2019	f[29] = 897
fHat[30] = 2032	f[30] = 2329
fHat[31] = 1743	f[31] = 2216
fHat[32] = 3322	f[32] = 288
fHat[33] = 2683	f[33] = 2382
fHat[34] = 1757	f[34] = 2619
fHat[35] = 2546	f[35] = 814
fHat[36] = 1965	f[36] = 2574
fHat[37] = 1092	f[37] = 1067
fHat[38] = 1838	f[38] = 1690
fHat[39] = 3304	f[39] = 1090
fHat[40] = 1159	f[40] = 2984
fHat[41] = 2092	f[41] = 781
fHat[42] = 1863	f[42] = 2111
fHat[43] = 3070	f[43] = 1637
fHat[44] = 1897	f[44] = 615
fHat[45] = 938	f[45] = 299
fHat[46] = 2093	f[46] = 1323
fHat[47] = 1994	f[47] = 2208
fHat[48] = 314	f[48] = 2802
fHat[49] = 1857	f[49] = 2955
fHat[50] = 2225	f[50] = 1504
fHat[51] = 3293	f[51] = 1310
fHat[52] = 1373	f[52] = 2730
fHat[53] = 2197	f[53] = 661
fHat[54] = 50	f[54] = 1712
fHat[55] = 1162	f[55] = 1692
fHat[56] = 3287	f[56] = 292
fHat[57] = 3091	f[57] = 2941
fHat[58] = 1634	f[58] = 145
fHat[59] = 3246	f[59] = 1768
fHat[60] = 2669	f[60] = 683
fHat[61] = 2933	f[61] = 2503
fHat[62] = 2764	f[62] = 2381

fHat[63] = 2738	f[63] = 352
fHat[64] = 999	f[64] = 702
fHat[65] = 572	f[65] = 718
fHat[66] = 2285	f[66] = 296
fHat[67] = 1809	f[67] = 650
fHat[68] = 263	f[68] = 1146
fHat[69] = 1367	f[69] = 1362
fHat[70] = 1158	f[70] = 2141
fHat[71] = 964	f[71] = 1121
fHat[72] = 731	f[72] = 1629
fHat[73] = 478	f[73] = 2248
fHat[74] = 2932	f[74] = 918
fHat[75] = 2079	f[75] = 3093
fHat[76] = 407	f[76] = 874
fHat[77] = 361	f[77] = 3097
fHat[78] = 1169	f[78] = 900
fHat[79] = 399	f[79] = 2117
fHat[80] = 671	f[80] = 765
fHat[81] = 466	f[81] = 992
fHat[82] = 1255	f[82] = 1574
fHat[83] = 2389	f[83] = 963
fHat[84] = 302	f[84] = 273
fHat[85] = 1862	f[85] = 304
fHat[86] = 1983	f[86] = 2716
fHat[87] = 1841	f[87] = 1267
fHat[88] = 3178	f[88] = 716
fHat[89] = 9	f[89] = 3023
fHat[90] = 1054	f[90] = 1623
fHat[91] = 2886	f[91] = 53
fHat[92] = 607	f[92] = 3115
fHat[93] = 321	f[93] = 242
fHat[94] = 1263	f[94] = 1482
fHat[95] = 672	f[95] = 399
fHat[96] = 3069	f[96] = 1345
fHat[97] = 1159	f[97] = 1162
fHat[98] = 2618	f[98] = 994
fHat[99] = 279	f[99] = 2839
fHat[100] = 888	f[100] = 993
fHat[101] = 1544	f[101] = 2290
fHat[102] = 462	f[102] = 626
fHat[103] = 1011	f[103] = 3203
fHat[104] = 1027	f[104] = 2824
fHat[105] = 603	f[105] = 2895
fHat[106] = 325	f[106] = 2515
fHat[107] = 695	f[107] = 1673
fHat[108] = 2301	f[108] = 3195
fHat[109] = 2819	f[109] = 3093

fHat[110] = 2030	f[110] = 562
fHat[111] = 3235	f[111] = 2682
fHat[112] = 22	f[112] = 790
fHat[113] = 2264	f[113] = 142
fHat[114] = 1521	f[114] = 606
fHat[115] = 815	f[115] = 1482
fHat[116] = 2527	f[116] = 2944
fHat[117] = 3240	f[117] = 1377
fHat[118] = 331	f[118] = 498
fHat[119] = 1758	f[119] = 1893
fHat[120] = 1709	f[120] = 2709
fHat[121] = 827	f[121] = 1545
fHat[122] = 671	f[122] = 1300
fHat[123] = 2125	f[123] = 3170
fHat[124] = 56	f[124] = 2511
fHat[125] = 1325	f[125] = 2886
fHat[126] = 3101	f[126] = 969
fHat[127] = 2198	f[127] = 354

Testing NIST NTT Multiplication

f[0] = 41	fHat[0] = 63	g[0] = 1822	gHat[
0] = 2489			
f[1] = 3005	fHat[1] = 989	g[1] = 3197	gHat[
1] = 1236			
f[2] = 2524	fHat[2] = 2586	g[2] = 2408	gHat[
2] = 2689			
f[3] = 1491	fHat[3] = 2084	g[3] = 2726	gHat[
3] = 875			
f[4] = 330	fHat[4] = 1135	g[4] = 1161	gHat[
4] = 1893			
f[5] = 2376	fHat[5] = 1013	g[5] = 1513	gHat[
5] = 2738			
f[6] = 3307	fHat[6] = 0	g[6] = 182	gHat[
6] = 1563			
f[7] = 3303	fHat[7] = 822	g[7] = 491	gHat[
7] = 1254			
f[8] = 2995	fHat[8] = 887	g[8] = 1955	gHat[
8] = 3032			
f[9] = 1498	fHat[9] = 2602	g[9] = 2107	gHat[
9] = 816			
f[10] = 2430	fHat[10] = 1196	g[10] = 1288	gHat[
10] = 2796			
f[11] = 573	fHat[11] = 1453	g[11] = 153	gHat[
11] = 1136			
f[12] = 292	fHat[12] = 2287	g[12] = 2395	gHat[
12] = 360			

f[13] = 776	fHat[13] = 2338	g[13] = 2071	gHat[
13] = 1214			
f[14] = 3073	fHat[14] = 2640	g[14] = 3250	gHat[
14] = 1760			
f[15] = 2118	fHat[15] = 230	g[15] = 1752	gHat[
15] = 3229			
f[16] = 1455	fHat[16] = 1759	g[16] = 1551	gHat[
16] = 2334			
f[17] = 1869	fHat[17] = 1058	g[17] = 3267	gHat[
17] = 3029			
f[18] = 2364	fHat[18] = 2830	g[18] = 2996	gHat[
18] = 2486			
f[19] = 390	fHat[19] = 981	g[19] = 3236	gHat[
19] = 3204			
f[20] = 2071	fHat[20] = 794	g[20] = 508	gHat[
20] = 2297			
f[21] = 1361	fHat[21] = 343	g[21] = 372	gHat[
21] = 1852			
f[22] = 1028	fHat[22] = 3201	g[22] = 1335	gHat[
22] = 3185			
f[23] = 1825	fHat[23] = 287	g[23] = 1053	gHat[
23] = 1541			
f[24] = 1621	fHat[24] = 2938	g[24] = 210	gHat[
24] = 2041			
f[25] = 2244	fHat[25] = 2922	g[25] = 1012	gHat[
25] = 2053			
f[26] = 2701	fHat[26] = 267	g[26] = 2796	gHat[
26] = 1887			
f[27] = 63	fHat[27] = 3029	g[27] = 2872	gHat[
27] = 608			
f[28] = 2065	fHat[28] = 2080	g[28] = 3083	gHat[
28] = 852			
f[29] = 897	fHat[29] = 2019	g[29] = 778	gHat[
29] = 356			
f[30] = 2329	fHat[30] = 2032	g[30] = 3035	gHat[
30] = 681			
f[31] = 2216	fHat[31] = 1743	g[31] = 1842	gHat[
31] = 376			
f[32] = 288	fHat[32] = 3322	g[32] = 145	gHat[
32] = 557			
f[33] = 2382	fHat[33] = 2683	g[33] = 2284	gHat[
33] = 1306			
f[34] = 2619	fHat[34] = 1757	g[34] = 2674	gHat[
34] = 2742			
f[35] = 814	fHat[35] = 2546	g[35] = 502	gHat[
35] = 463			

f[36] = 2574	fHat[36] = 1965	g[36] = 71	gHat[
36] = 2109			
f[37] = 1067	fHat[37] = 1092	g[37] = 2034	gHat[
37] = 2226			
f[38] = 1690	fHat[38] = 1838	g[38] = 1140	gHat[
38] = 3081			
f[39] = 1090	fHat[39] = 3304	g[39] = 219	gHat[
39] = 2671			
f[40] = 2984	fHat[40] = 1159	g[40] = 2636	gHat[
40] = 597			
f[41] = 781	fHat[41] = 2092	g[41] = 3309	gHat[
41] = 781			
f[42] = 2111	fHat[42] = 1863	g[42] = 1853	gHat[
42] = 1349			
f[43] = 1637	fHat[43] = 3070	g[43] = 718	gHat[
43] = 3220			
f[44] = 615	fHat[44] = 1897	g[44] = 3005	gHat[
44] = 1545			
f[45] = 299	fHat[45] = 938	g[45] = 2478	gHat[
45] = 1479			
f[46] = 1323	fHat[46] = 2093	g[46] = 1336	gHat[
46] = 638			
f[47] = 2208	fHat[47] = 1994	g[47] = 1564	gHat[
47] = 2459			
f[48] = 2802	fHat[48] = 314	g[48] = 2082	gHat[
48] = 11			
f[49] = 2955	fHat[49] = 1857	g[49] = 3225	gHat[
49] = 3053			
f[50] = 1504	fHat[50] = 2225	g[50] = 1154	gHat[
50] = 429			
f[51] = 1310	fHat[51] = 3293	g[51] = 3026	gHat[
51] = 28			
f[52] = 2730	fHat[52] = 1373	g[52] = 3272	gHat[
52] = 353			
f[53] = 661	fHat[53] = 2197	g[53] = 2306	gHat[
53] = 1000			
f[54] = 1712	fHat[54] = 50	g[54] = 2412	gHat[
54] = 2569			
f[55] = 1692	fHat[55] = 1162	g[55] = 2113	gHat[
55] = 156			
f[56] = 292	fHat[56] = 3287	g[56] = 2427	gHat[
56] = 2530			
f[57] = 2941	fHat[57] = 3091	g[57] = 2500	gHat[
57] = 2530			
f[58] = 145	fHat[58] = 1634	g[58] = 2257	gHat[
58] = 1159			

f[59] = 1768	fHat[59] = 3246	g[59] = 3196	gHat[
59] = 601			
f[60] = 683	fHat[60] = 2669	g[60] = 3303	gHat[
60] = 1637			
f[61] = 2503	fHat[61] = 2933	g[61] = 1991	gHat[
61] = 117			
f[62] = 2381	fHat[62] = 2764	g[62] = 1464	gHat[
62] = 1436			
f[63] = 352	fHat[63] = 2738	g[63] = 2258	gHat[
63] = 517			
f[64] = 702	fHat[64] = 999	g[64] = 2065	gHat[
64] = 450			
f[65] = 718	fHat[65] = 572	g[65] = 1150	gHat[
65] = 2983			
f[66] = 296	fHat[66] = 2285	g[66] = 1750	gHat[
66] = 3168			
f[67] = 650	fHat[67] = 1809	g[67] = 101	gHat[
67] = 1155			
f[68] = 1146	fHat[68] = 263	g[68] = 230	gHat[
68] = 3302			
f[69] = 1362	fHat[69] = 1367	g[69] = 1350	gHat[
69] = 2182			
f[70] = 2141	fHat[70] = 1158	g[70] = 2300	gHat[
70] = 2251			
f[71] = 1121	fHat[71] = 964	g[71] = 396	gHat[
71] = 2823			
f[72] = 1629	fHat[72] = 731	g[72] = 2251	gHat[
72] = 137			
f[73] = 2248	fHat[73] = 478	g[73] = 3100	gHat[
73] = 1429			
f[74] = 918	fHat[74] = 2932	g[74] = 1943	gHat[
74] = 1402			
f[75] = 3093	fHat[75] = 2079	g[75] = 1643	gHat[
75] = 3311			
f[76] = 874	fHat[76] = 407	g[76] = 3043	gHat[
76] = 2999			
f[77] = 3097	fHat[77] = 361	g[77] = 2536	gHat[
77] = 2963			
f[78] = 900	fHat[78] = 1169	g[78] = 2630	gHat[
78] = 958			
f[79] = 2117	fHat[79] = 399	g[79] = 1655	gHat[
79] = 953			
f[80] = 765	fHat[80] = 671	g[80] = 3030	gHat[
80] = 1587			
f[81] = 992	fHat[81] = 466	g[81] = 563	gHat[
81] = 537			

f[82] = 1574	fHat[82] = 1255	g[82] = 3154	gHat[
82] = 1553			
f[83] = 963	fHat[83] = 2389	g[83] = 712	gHat[
83] = 3242			
f[84] = 273	fHat[84] = 302	g[84] = 1047	gHat[
84] = 850			
f[85] = 304	fHat[85] = 1862	g[85] = 875	gHat[
85] = 1863			
f[86] = 2716	fHat[86] = 1983	g[86] = 1033	gHat[
86] = 2378			
f[87] = 1267	fHat[87] = 1841	g[87] = 718	gHat[
87] = 1594			
f[88] = 716	fHat[88] = 3178	g[88] = 3225	gHat[
88] = 1833			
f[89] = 3023	fHat[89] = 9	g[89] = 1181	gHat[
89] = 741			
f[90] = 1623	fHat[90] = 1054	g[90] = 1405	gHat[
90] = 1764			
f[91] = 53	fHat[91] = 2886	g[91] = 1999	gHat[
91] = 3288			
f[92] = 3115	fHat[92] = 607	g[92] = 1306	gHat[
92] = 2806			
f[93] = 242	fHat[93] = 321	g[93] = 459	gHat[
93] = 3227			
f[94] = 1482	fHat[94] = 1263	g[94] = 467	gHat[
94] = 2885			
f[95] = 399	fHat[95] = 672	g[95] = 1577	gHat[
95] = 2554			
f[96] = 1345	fHat[96] = 3069	g[96] = 2509	gHat[
96] = 990			
f[97] = 1162	fHat[97] = 1159	g[97] = 2421	gHat[
97] = 3036			
f[98] = 994	fHat[98] = 2618	g[98] = 3288	gHat[
98] = 2566			
f[99] = 2839	fHat[99] = 279	g[99] = 2856	gHat[
99] = 988			
f[100] = 993	fHat[100] = 888	g[100] = 958	
gHat[100] = 2026			
f[101] = 2290	fHat[101] = 1544	g[101] = 806	
gHat[101] = 1416			
f[102] = 626	fHat[102] = 462	g[102] = 1920	
gHat[102] = 2238			
f[103] = 3203	fHat[103] = 1011	g[103] = 1595	
gHat[103] = 1961			
f[104] = 2824	fHat[104] = 1027	g[104] = 342	
gHat[104] = 308			

f[105] = 2895	fHat[105] = 603	g[105] = 1021
gHat[105] = 651		
f[106] = 2515	fHat[106] = 325	g[106] = 2648
gHat[106] = 2426		
f[107] = 1673	fHat[107] = 695	g[107] = 2741
gHat[107] = 2858		
f[108] = 3195	fHat[108] = 2301	g[108] = 511
gHat[108] = 3132		
f[109] = 3093	fHat[109] = 2819	g[109] = 1027
gHat[109] = 243		
f[110] = 562	fHat[110] = 2030	g[110] = 1587
gHat[110] = 1153		
f[111] = 2682	fHat[111] = 3235	g[111] = 2845
gHat[111] = 1035		
f[112] = 790	fHat[112] = 22	g[112] = 1897
gHat[112] = 3103		
f[113] = 142	fHat[113] = 2264	g[113] = 3289
gHat[113] = 1841		
f[114] = 606	fHat[114] = 1521	g[114] = 3151
gHat[114] = 3320		
f[115] = 1482	fHat[115] = 815	g[115] = 1965
gHat[115] = 919		
f[116] = 2944	fHat[116] = 2527	g[116] = 824
gHat[116] = 2724		
f[117] = 1377	fHat[117] = 3240	g[117] = 525
gHat[117] = 3011		
f[118] = 498	fHat[118] = 331	g[118] = 319
gHat[118] = 2165		
f[119] = 1893	fHat[119] = 1758	g[119] = 2305
gHat[119] = 1912		
f[120] = 2709	fHat[120] = 1709	g[120] = 876
gHat[120] = 1889		
f[121] = 1545	fHat[121] = 827	g[121] = 3025
gHat[121] = 1510		
f[122] = 1300	fHat[122] = 671	g[122] = 2862
gHat[122] = 279		
f[123] = 3170	fHat[123] = 2125	g[123] = 2914
gHat[123] = 3055		
f[124] = 2511	fHat[124] = 56	g[124] = 1524
gHat[124] = 1739		
f[125] = 2886	fHat[125] = 1325	g[125] = 2634
gHat[125] = 3112		
f[126] = 969	fHat[126] = 3101	g[126] = 81
gHat[126] = 137		
f[127] = 354	fHat[127] = 2198	g[127] = 2672
gHat[127] = 1750		

fHat[0] = 63	gHat[0] = 2489	hHat[0] = 1594
fHat[1] = 989	gHat[1] = 1236	hHat[1] = 2791
fHat[2] = 2586	gHat[2] = 2689	hHat[2] = 4926
fHat[3] = 2084	gHat[3] = 875	hHat[3] = 3528
fHat[4] = 1135	gHat[4] = 1893	hHat[4] = 3225
fHat[5] = 1013	gHat[5] = 2738	hHat[5] = 1778
fHat[6] = 0	gHat[6] = 1563	hHat[6] = 3038
fHat[7] = 822	gHat[7] = 1254	hHat[7] = 3121
fHat[8] = 887	gHat[8] = 3032	hHat[8] = 5093
fHat[9] = 2602	gHat[9] = 816	hHat[9] = 4262
fHat[10] = 1196	gHat[10] = 2796	hHat[10] = 3255
fHat[11] = 1453	gHat[11] = 1136	hHat[11] = 1632
fHat[12] = 2287	gHat[12] = 360	hHat[12] = 237
fHat[13] = 2338	gHat[13] = 1214	hHat[13] = 2804
fHat[14] = 2640	gHat[14] = 1760	hHat[14] = 5416
fHat[15] = 230	gHat[15] = 3229	hHat[15] = 4311
fHat[16] = 1759	gHat[16] = 2334	hHat[16] = 2687
fHat[17] = 1058	gHat[17] = 3029	hHat[17] = 4194
fHat[18] = 2830	gHat[18] = 2486	hHat[18] = 1604
fHat[19] = 981	gHat[19] = 3204	hHat[19] = 4391
fHat[20] = 794	gHat[20] = 2297	hHat[20] = 2985
fHat[21] = 343	gHat[21] = 1852	hHat[21] = 4626
fHat[22] = 3201	gHat[22] = 3185	hHat[22] = 3183
fHat[23] = 287	gHat[23] = 1541	hHat[23] = 4441
fHat[24] = 2938	gHat[24] = 2041	hHat[24] = 1858
fHat[25] = 2922	gHat[25] = 2053	hHat[25] = 4458
fHat[26] = 267	gHat[26] = 1887	hHat[26] = 2252
fHat[27] = 3029	gHat[27] = 608	hHat[27] = 5703
fHat[28] = 2080	gHat[28] = 852	hHat[28] = 4032
fHat[29] = 2019	gHat[29] = 356	hHat[29] = 3866
fHat[30] = 2032	gHat[30] = 681	hHat[30] = 2394
fHat[31] = 1743	gHat[31] = 376	hHat[31] = 3550
fHat[32] = 3322	gHat[32] = 557	hHat[32] = 4545
fHat[33] = 2683	gHat[33] = 1306	hHat[33] = 3884
fHat[34] = 1757	gHat[34] = 2742	hHat[34] = 879
fHat[35] = 2546	gHat[35] = 463	hHat[35] = 1434
fHat[36] = 1965	gHat[36] = 2109	hHat[36] = 1454
fHat[37] = 1092	gHat[37] = 2226	hHat[37] = 5802
fHat[38] = 1838	gHat[38] = 3081	hHat[38] = 1991
fHat[39] = 3304	gHat[39] = 2671	hHat[39] = 5223
fHat[40] = 1159	gHat[40] = 597	hHat[40] = 4482
fHat[41] = 2092	gHat[41] = 781	hHat[41] = 3569
fHat[42] = 1863	gHat[42] = 1349	hHat[42] = 3306
fHat[43] = 3070	gHat[43] = 3220	hHat[43] = 156
fHat[44] = 1897	gHat[44] = 1545	hHat[44] = 3469
fHat[45] = 938	gHat[45] = 1479	hHat[45] = 3740
fHat[46] = 2093	gHat[46] = 638	hHat[46] = 1540

fHat[47] = 1994	gHat[47] = 2459	hHat[47] = 547
fHat[48] = 314	gHat[48] = 11	hHat[48] = 206
fHat[49] = 1857	gHat[49] = 3053	hHat[49] = 3672
fHat[50] = 2225	gHat[50] = 429	hHat[50] = 5467
fHat[51] = 3293	gHat[51] = 28	hHat[51] = 3579
fHat[52] = 1373	gHat[52] = 353	hHat[52] = 5039
fHat[53] = 2197	gHat[53] = 1000	hHat[53] = 4665
fHat[54] = 50	gHat[54] = 2569	hHat[54] = 4116
fHat[55] = 1162	gHat[55] = 156	hHat[55] = 3536
fHat[56] = 3287	gHat[56] = 2530	hHat[56] = 1566
fHat[57] = 3091	gHat[57] = 2530	hHat[57] = 677
fHat[58] = 1634	gHat[58] = 1159	hHat[58] = 5946
fHat[59] = 3246	gHat[59] = 601	hHat[59] = 3652
fHat[60] = 2669	gHat[60] = 1637	hHat[60] = 1626
fHat[61] = 2933	gHat[61] = 117	hHat[61] = 3579
fHat[62] = 2764	gHat[62] = 1436	hHat[62] = 2355
fHat[63] = 2738	gHat[63] = 517	hHat[63] = 1066
fHat[64] = 999	gHat[64] = 450	hHat[64] = 2580
fHat[65] = 572	gHat[65] = 2983	hHat[65] = 1629
fHat[66] = 2285	gHat[66] = 3168	hHat[66] = 2194
fHat[67] = 1809	gHat[67] = 1155	hHat[67] = 4310
fHat[68] = 263	gHat[68] = 3302	hHat[68] = 4727
fHat[69] = 1367	gHat[69] = 2182	hHat[69] = 4317
fHat[70] = 1158	gHat[70] = 2251	hHat[70] = 1705
fHat[71] = 964	gHat[71] = 2823	hHat[71] = 6070
fHat[72] = 731	gHat[72] = 137	hHat[72] = 3326
fHat[73] = 478	gHat[73] = 1429	hHat[73] = 4857
fHat[74] = 2932	gHat[74] = 1402	hHat[74] = 475
fHat[75] = 2079	gHat[75] = 3311	hHat[75] = 2371
fHat[76] = 407	gHat[76] = 2999	hHat[76] = 4410
fHat[77] = 361	gHat[77] = 2963	hHat[77] = 1557
fHat[78] = 1169	gHat[78] = 958	hHat[78] = 3980
fHat[79] = 399	gHat[79] = 953	hHat[79] = 4907
fHat[80] = 671	gHat[80] = 1587	hHat[80] = 4869
fHat[81] = 466	gHat[81] = 537	hHat[81] = 1299
fHat[82] = 1255	gHat[82] = 1553	hHat[82] = 3206
fHat[83] = 2389	gHat[83] = 3242	hHat[83] = 2283
fHat[84] = 302	gHat[84] = 850	hHat[84] = 2894
fHat[85] = 1862	gHat[85] = 1863	hHat[85] = 1450
fHat[86] = 1983	gHat[86] = 2378	hHat[86] = 396
fHat[87] = 1841	gHat[87] = 1594	hHat[87] = 1944
fHat[88] = 3178	gHat[88] = 1833	hHat[88] = 5608
fHat[89] = 9	gHat[89] = 741	hHat[89] = 4476
fHat[90] = 1054	gHat[90] = 1764	hHat[90] = 2236
fHat[91] = 2886	gHat[91] = 3288	hHat[91] = 926
fHat[92] = 607	gHat[92] = 2806	hHat[92] = 1828
fHat[93] = 321	gHat[93] = 3227	hHat[93] = 3233

fHat[94] = 1263	gHat[94] = 2885	hHat[94] = 3002
fHat[95] = 672	gHat[95] = 2554	hHat[95] = 4472
fHat[96] = 3069	gHat[96] = 990	hHat[96] = 310
fHat[97] = 1159	gHat[97] = 3036	hHat[97] = 5176
fHat[98] = 2618	gHat[98] = 2566	hHat[98] = 5704
fHat[99] = 279	gHat[99] = 988	hHat[99] = 3459
fHat[100] = 888	gHat[100] = 2026	hHat[100] = 4693
fHat[101] = 1544	gHat[101] = 1416	hHat[101] = 4588
fHat[102] = 462	gHat[102] = 2238	hHat[102] = 5178
fHat[103] = 1011	gHat[103] = 1961	hHat[103] = 2721
fHat[104] = 1027	gHat[104] = 308	hHat[104] = 321
fHat[105] = 603	gHat[105] = 651	hHat[105] = 5406
fHat[106] = 325	gHat[106] = 2426	hHat[106] = 4314
fHat[107] = 695	gHat[107] = 2858	hHat[107] = 1655
fHat[108] = 2301	gHat[108] = 3132	hHat[108] = 6036
fHat[109] = 2819	gHat[109] = 243	hHat[109] = 3800
fHat[110] = 2030	gHat[110] = 1153	hHat[110] = 3218
fHat[111] = 3235	gHat[111] = 1035	hHat[111] = 1926
fHat[112] = 22	gHat[112] = 3103	hHat[112] = 2136
fHat[113] = 2264	gHat[113] = 1841	hHat[113] = 1556
fHat[114] = 1521	gHat[114] = 3320	hHat[114] = 5644
fHat[115] = 815	gHat[115] = 919	hHat[115] = 5600
fHat[116] = 2527	gHat[116] = 2724	hHat[116] = 3600
fHat[117] = 3240	gHat[117] = 3011	hHat[117] = 2613
fHat[118] = 331	gHat[118] = 2165	hHat[118] = 2192
fHat[119] = 1758	gHat[119] = 1912	hHat[119] = 1385
fHat[120] = 1709	gHat[120] = 1889	hHat[120] = 5161
fHat[121] = 827	gHat[121] = 1510	hHat[121] = 1517
fHat[122] = 671	gHat[122] = 279	hHat[122] = 132
fHat[123] = 2125	gHat[123] = 3055	hHat[123] = 2883
fHat[124] = 56	gHat[124] = 1739	hHat[124] = 2721
fHat[125] = 1325	gHat[125] = 3112	hHat[125] = 1671
fHat[126] = 3101	gHat[126] = 137	hHat[126] = 3382
fHat[127] = 2198	gHat[127] = 1750	hHat[127] = 1996

hHat[0] = 1594	h[0] = 2081
hHat[1] = 2791	h[1] = 1086
hHat[2] = 4926	h[2] = 3162
hHat[3] = 3528	h[3] = 2025
hHat[4] = 3225	h[4] = 3102
hHat[5] = 1778	h[5] = 968
hHat[6] = 3038	h[6] = 3299
hHat[7] = 3121	h[7] = 2744
hHat[8] = 5093	h[8] = 2406
hHat[9] = 4262	h[9] = 3085
hHat[10] = 3255	h[10] = 626
hHat[11] = 1632	h[11] = 2549

hHat[12]	=	237	h[12]	=	2988
hHat[13]	=	2804	h[13]	=	2892
hHat[14]	=	5416	h[14]	=	3026
hHat[15]	=	4311	h[15]	=	809
hHat[16]	=	2687	h[16]	=	1225
hHat[17]	=	4194	h[17]	=	1120
hHat[18]	=	1604	h[18]	=	3039
hHat[19]	=	4391	h[19]	=	40
hHat[20]	=	2985	h[20]	=	32
hHat[21]	=	4626	h[21]	=	3231
hHat[22]	=	3183	h[22]	=	2791
hHat[23]	=	4441	h[23]	=	1392
hHat[24]	=	1858	h[24]	=	2063
hHat[25]	=	4458	h[25]	=	1559
hHat[26]	=	2252	h[26]	=	2026
hHat[27]	=	5703	h[27]	=	3109
hHat[28]	=	4032	h[28]	=	3076
hHat[29]	=	3866	h[29]	=	2609
hHat[30]	=	2394	h[30]	=	2435
hHat[31]	=	3550	h[31]	=	309
hHat[32]	=	4545	h[32]	=	137
hHat[33]	=	3884	h[33]	=	3147
hHat[34]	=	879	h[34]	=	317
hHat[35]	=	1434	h[35]	=	733
hHat[36]	=	1454	h[36]	=	549
hHat[37]	=	5802	h[37]	=	683
hHat[38]	=	1991	h[38]	=	870
hHat[39]	=	5223	h[39]	=	2976
hHat[40]	=	4482	h[40]	=	361
hHat[41]	=	3569	h[41]	=	963
hHat[42]	=	3306	h[42]	=	2827
hHat[43]	=	156	h[43]	=	2515
hHat[44]	=	3469	h[44]	=	1754
hHat[45]	=	3740	h[45]	=	2905
hHat[46]	=	1540	h[46]	=	259
hHat[47]	=	547	h[47]	=	195
hHat[48]	=	206	h[48]	=	1434
hHat[49]	=	3672	h[49]	=	1653
hHat[50]	=	5467	h[50]	=	1765
hHat[51]	=	3579	h[51]	=	985
hHat[52]	=	5039	h[52]	=	2250
hHat[53]	=	4665	h[53]	=	1082
hHat[54]	=	4116	h[54]	=	2859
hHat[55]	=	3536	h[55]	=	366
hHat[56]	=	1566	h[56]	=	3150
hHat[57]	=	677	h[57]	=	2810
hHat[58]	=	5946	h[58]	=	764

hHat[59] = 3652	h[59] = 2183
hHat[60] = 1626	h[60] = 1233
hHat[61] = 3579	h[61] = 1214
hHat[62] = 2355	h[62] = 268
hHat[63] = 1066	h[63] = 1680
hHat[64] = 2580	h[64] = 1891
hHat[65] = 1629	h[65] = 2119
hHat[66] = 2194	h[66] = 1437
hHat[67] = 4310	h[67] = 25
hHat[68] = 4727	h[68] = 1346
hHat[69] = 4317	h[69] = 2481
hHat[70] = 1705	h[70] = 2239
hHat[71] = 6070	h[71] = 2866
hHat[72] = 3326	h[72] = 2292
hHat[73] = 4857	h[73] = 2995
hHat[74] = 475	h[74] = 2938
hHat[75] = 2371	h[75] = 2856
hHat[76] = 4410	h[76] = 842
hHat[77] = 1557	h[77] = 2032
hHat[78] = 3980	h[78] = 989
hHat[79] = 4907	h[79] = 2556
hHat[80] = 4869	h[80] = 1573
hHat[81] = 1299	h[81] = 2403
hHat[82] = 3206	h[82] = 2384
hHat[83] = 2283	h[83] = 1153
hHat[84] = 2894	h[84] = 3287
hHat[85] = 1450	h[85] = 511
hHat[86] = 396	h[86] = 1865
hHat[87] = 1944	h[87] = 2339
hHat[88] = 5608	h[88] = 1012
hHat[89] = 4476	h[89] = 2006
hHat[90] = 2236	h[90] = 2027
hHat[91] = 926	h[91] = 1422
hHat[92] = 1828	h[92] = 2672
hHat[93] = 3233	h[93] = 577
hHat[94] = 3002	h[94] = 527
hHat[95] = 4472	h[95] = 1109
hHat[96] = 310	h[96] = 2793
hHat[97] = 5176	h[97] = 651
hHat[98] = 5704	h[98] = 1309
hHat[99] = 3459	h[99] = 2715
hHat[100] = 4693	h[100] = 395
hHat[101] = 4588	h[101] = 651
hHat[102] = 5178	h[102] = 2305
hHat[103] = 2721	h[103] = 729
hHat[104] = 321	h[104] = 1150
hHat[105] = 5406	h[105] = 1955

hHat[106] = 4314	h[106] = 473
hHat[107] = 1655	h[107] = 905
hHat[108] = 6036	h[108] = 1724
hHat[109] = 3800	h[109] = 711
hHat[110] = 3218	h[110] = 118
hHat[111] = 1926	h[111] = 3255
hHat[112] = 2136	h[112] = 3236
hHat[113] = 1556	h[113] = 2296
hHat[114] = 5644	h[114] = 67
hHat[115] = 5600	h[115] = 1153
hHat[116] = 3600	h[116] = 2832
hHat[117] = 2613	h[117] = 1167
hHat[118] = 2192	h[118] = 89
hHat[119] = 1385	h[119] = 1340
hHat[120] = 5161	h[120] = 2669
hHat[121] = 1517	h[121] = 2858
hHat[122] = 132	h[122] = 1304
hHat[123] = 2883	h[123] = 1899
hHat[124] = 2721	h[124] = 3202
hHat[125] = 1671	h[125] = 925
hHat[126] = 3382	h[126] = 932
hHat[127] = 1996	h[127] = 2043

== Main Menu ==

- 0 - Small Vector Test NTT, NTT^{-1}
- 1 - Test BitRev, NTT, NTT^{-1}
- 2 - Test SHA-3
- 3 - Exit

Option = 3

D:\NISTFIPS203\x64\Release\NISTFIPS203.exe (process 8780) exited
with code 0 (0x0).

Press any key to close this window . . .