

Crypto challenge - Untwist Me

deuterium — 2021-07-25

Canonical HTML: <https://deut-erium.github.io/2021/07/25/untwist-me.html>

Abstract

Crypto challenge - Untwist Me, published in deuterium's blog.

One can guess all the future outputs of a random number generator once they recover the state, but how feasible is it to recover the past state of pseudo random number generator given its present state?

Mersenne Twister is a pseudorandom number used ubiquitously in so many pseudo random number generation libraries across programming languages and softwares alike. It uses a state of 624 32-bit integers. Each 32-bit word contributes to to unique output, once the index reaches the end of the array, this array is “twisted” to generate a new array of state. Now, given this state, can you recover back the original state?

```
from secret import flag
import os
import random

state_len = 624*4
right_pad = random.randint(0,state_len-len(flag))
left_pad = state_len-len(flag)-right_pad
state_bytes = os.urandom(left_pad)+flag+os.urandom(right_pad)
state = tuple( int.from_bytes(state_bytes[i:i+4],'big') for i in range(0,state_len,4)
)
random.setstate((3,state+(624,),None))
outputs = [random.getrandbits(32) for i in range(624)]
print(outputs)

# outputs
#[3010212863, 1638790982, 2153727997, 800741962, 1300126498, 1008035836,
# 1757095206, 1670433536, 3087496760, 1747385781, 2120399163, 1134629113,
# 919775231, 3379878969, 3743636691, 4037703354, 809158834, 2188423766,
# 895667276, 3377213573, 3894587783, 346471012, 3945760625, 1014890401,
# 3489634126, 2274362888, 3566959444, 381269327, 3621452664, 1760615420,
# 2482052829, 1842093601, 3135000809, 889501115, 1870391126, 721464471,
# 1146162062, 3157702100, 1067328755, 3362963308, 2290029991, 2055264656,
# 2800137102, 252553871, 1631088230, 58620923, 1016025333, 2676322857,
# 4030931310, 3783089217, 2821383676, 1395746047, 1917600767, 2278459122,
# 1434446925, 4074687527, 2498110773, 3316902826, 2958570141, 5147159,
# 2277916584, 1311785024, 2808116680, 3897795015, 1091778004, 4044893667,
# 3442360193, 2471121578, 3266124707, 945709239, 4254600747, 269780363,
# 1687521986, 728060741, 3239438658, 1275400802, 3976720484, 542928488,
# 1591685538, 801156258, 2997864916, 1334519032, 3054095657, 1519771487,
# 1744098263, 1926575149, 3509052482, 1155668294, 948649192, 3728061600,
# 2546291029, 834854025, 1130467450, 2269145652, 462981709, 2095530900,
# 2829210433, 2033516625, 2094545879, 4032850882, 1534276992, 2245901424,
# 2298906123, 2692400842, 1832625190, 1401500215, 2247699783, 2688167016,
# 1815564529, 134150505, 1022130290, 810101229, 4102800158, 203439793,
```

1563110047, 4122501009, 897838871, 2839458623, 4235007515, 2805467536,
3669331231, 4213272249, 334116894, 1720279917, 3768575383, 3712492986,
492673800, 2448994557, 2136407709, 1007047910, 2856006838, 1451254580,
3752603100, 1353653315, 22030732, 1162510422, 1861605544, 52494704,
4264490153, 962746860, 3803153407, 3865003091, 1963762549, 1166411853,
4085109678, 1720009340, 3149090189, 997456656, 377660043, 1392682564,
4111511899, 1589429762, 4189913787, 3956043196, 2524895159, 1150952959,
3230524959, 1922940535, 3161766763, 1498062044, 1193570808, 3609861632,
1166059038, 4013944388, 1321750226, 4270860030, 3020259258, 1888279874,
3509465770, 1132931626, 3981029460, 225835700, 2398674556, 1037771691,
1183027818, 3062062705, 2201412587, 4027219272, 2656813603, 2238798992,
2321355543, 770644701, 3644674099, 3924455525, 599621572, 2865872023,
547681040, 2504523252, 1595600675, 2770244206, 4207940231, 1034385830,
3646850280, 2354492616, 1547726173, 2144551580, 3310312279, 4079068944,
1052121020, 1167730938, 1859530296, 3935988096, 653145852, 3190034909,
306014083, 3112209831, 1319990284, 2366174046, 2873692054, 3612521192,
3474355729, 2078348431, 3093619143, 767721911, 1799487931, 3769008967,
2510379156, 3997118470, 1858256570, 2511138610, 3119850305, 4123020796,
1467948580, 2169662247, 1042659524, 706459993, 1279903660, 161481894,
3047758921, 2128081746, 1481302067, 3572046415, 130443674, 1882613027,
1949012711, 786180871, 1401546008, 3025028339, 2109417076, 2415110785,
1333312666, 2808997450, 92196701, 35189050, 1628124503, 919909324,
3735308735, 1672915082, 848573625, 3900913677, 4067446247, 3045201457,
4262710543, 407360835, 914980841, 1201056276, 2367451149, 4012096496,
3644273047, 2793106080, 4059628962, 956823679, 504646522, 1577066976,
3103848478, 281560705, 3654634065, 1200837960, 2469148835, 1515087929,
986675230, 1014717995, 3626085805, 3427299665, 3199504838, 1499632928,
864019141, 3092221246, 3432793142, 961906091, 4087241347, 1501385695,
1869078181, 1432754296, 1929269813, 20545849, 79773598, 2225667827,
2803991524, 3271497, 2000244219, 2235945517, 198649159, 3130926875,
2061536635, 4127935142, 2509945885, 2800177774, 122281515, 1483335934,
517228772, 687237830, 699903391, 1270471004, 3950520968, 3878199844,
2604191970, 1471453307, 612589164, 1337743243, 488061378, 1083836576,
2385268945, 981256534, 1592250232, 3753674057, 1249785337, 176131676,
1547866758, 3387578645, 1918971958, 3149508022, 225736357, 2820091446,
1309599295, 801349594, 1443931329, 4141370827, 486328175, 303404609,
2740073709, 1241722868, 1085359414, 4250625563, 53936008, 1526883658,
81508000, 3394245176, 3523129205, 1065188556, 495179175, 1610340591,
1173947008, 2581378909, 345913430, 1811845756, 299708365, 274267008,
1155972508, 3069794235, 2406176022, 275597450, 1254348890, 395814304,
4153790237, 3099560409, 3533186000, 2135638402, 510811973, 1415172809,
451611225, 4168777378, 990982351, 3349791003, 2296538215, 2315312562,
1414386168, 428503045, 3351836071, 405842630, 809372501, 3967844511,
3746788355, 4102787435, 1511139290, 717968187, 1555067606, 1588912940,
843054791, 3824649799, 3018771508, 3905102930, 4045409252, 3653536948,
4111211541, 3524774589, 3822695255, 2242439159, 863036773, 787822092,
3858607605, 2697827303, 84884878, 3116656440, 351049518, 318784403,
553018425, 1265079730, 1277921250, 2775298261, 3472975923, 317887667,
4272975757, 738903299, 1868393449, 475826860, 2198737207, 1785005722,
3868235178, 3857360992, 1533904162, 394948937, 334461989, 2723127934,
3356703544, 2541615860, 4061593776, 4252987627, 3734936262, 2164663823,
3615908783, 708670146, 2725980744, 1752233272, 2043945199, 2132585334,
389187774, 3190948655, 1188340687, 1824879665, 4127459778, 3493838393,
2358471830, 516747657, 3944247696, 2367031994, 3819176400, 1020231474,
1295927899, 1557493532, 2504559554, 355169608, 2068224633, 2158052129,
3853591734, 48976763, 437527498, 200103512, 478262500, 2889753391,
1580502604, 2959449602, 1157521586, 4002445978, 3347949331, 2997248270,
2299459163, 1175224056, 2543436468, 2446001038, 2412693662, 1807105817,
1113873459, 3747132011, 3790216955, 543944458, 1256685827, 3101958425,
2408556173, 1777559571, 1594278081, 1036622339, 2667517584, 1802664264,

```
# 2395732937, 2465933464, 3521205735, 2803861899, 3746620807, 706899206,  
# 1143296823, 3128028140, 2716694130, 2420134119, 3649408943, 3806142051,  
# 2412349072, 2575408306, 1642100358, 1783271826, 2674421352, 2653988508,  
# 2643495441, 1842848679, 4220332304, 4168164191, 2619268737, 2661380897,  
# 3743142783, 1663838902, 4070629703, 3371465149, 4072450405, 1381310429,  
# 3337325442, 959691182, 2249789821, 2349309328, 3918167103, 926837360,  
# 2116928637, 3831738553, 4189427640, 3449232305, 3257706763, 3116333625,  
# 7526877, 4276590659, 4238805869, 2592717756, 3374263699, 1977523723,  
# 3519377356, 4233779985, 2905650247, 1713286703, 1679927293, 2319165794,  
# 3765526325, 3518105912, 1963471116, 4210271043, 112289569, 1200491141,  
# 4054218896, 1510045663, 4221937409, 1533659251, 1746527391, 1627955838,  
# 2852075184, 3539991984, 1601441271, 3299595676, 739020629, 3508463551,  
# 1543596798, 2192302007, 4063098133, 766518400, 2933103841, 2737391081,  
# 3014416175, 3067006685, 43083155, 1955768112, 2013953097, 625393267,  
# 3754403452, 3162101151, 1158861805, 621313486, 2900452280, 708979785,  
# 1757275009, 3677576137, 3714338118, 3533758422, 1512551802, 2746196950,  
# 2024585134, 612115745, 1058450417, 3090795349, 2068644030, 3186840221,  
# 1889899349, 3527732807, 1973474012, 2217193389, 3059044320, 1341979563,  
# 440406938, 3114173896, 4244113771, 2649834470, 1123591556, 629408126,  
# 596756734, 51416208, 1914543972, 1383958459, 2273526307, 25072794,  
# 71325945, 3466520611, 3572779967, 3335604477, 3831987682, 2076185615,  
# 1715359843, 71359213, 2625736992, 3006341223, 2092810088, 716083061,  
# 772294292, 2395463157, 1777066971, 2719722784, 3668605324, 3583574126,  
# 1238971203, 1536994984, 309161525, 2444639752, 1974758564, 2344173080,  
# 2925231177, 3095359598, 742425414, 741710625, 2806953195, 3410696260]
```

Enter the flag

The local SHA-256 checker requires JavaScript. The challenge itself does not.

Interactive controls are omitted from this PDF. See the canonical HTML version.