

Untwisting the Mersenne Twister

KILLING PRNGS



WHOAMI

UNTWISTING THE MERSENNE TWISTER

Bishop Fox

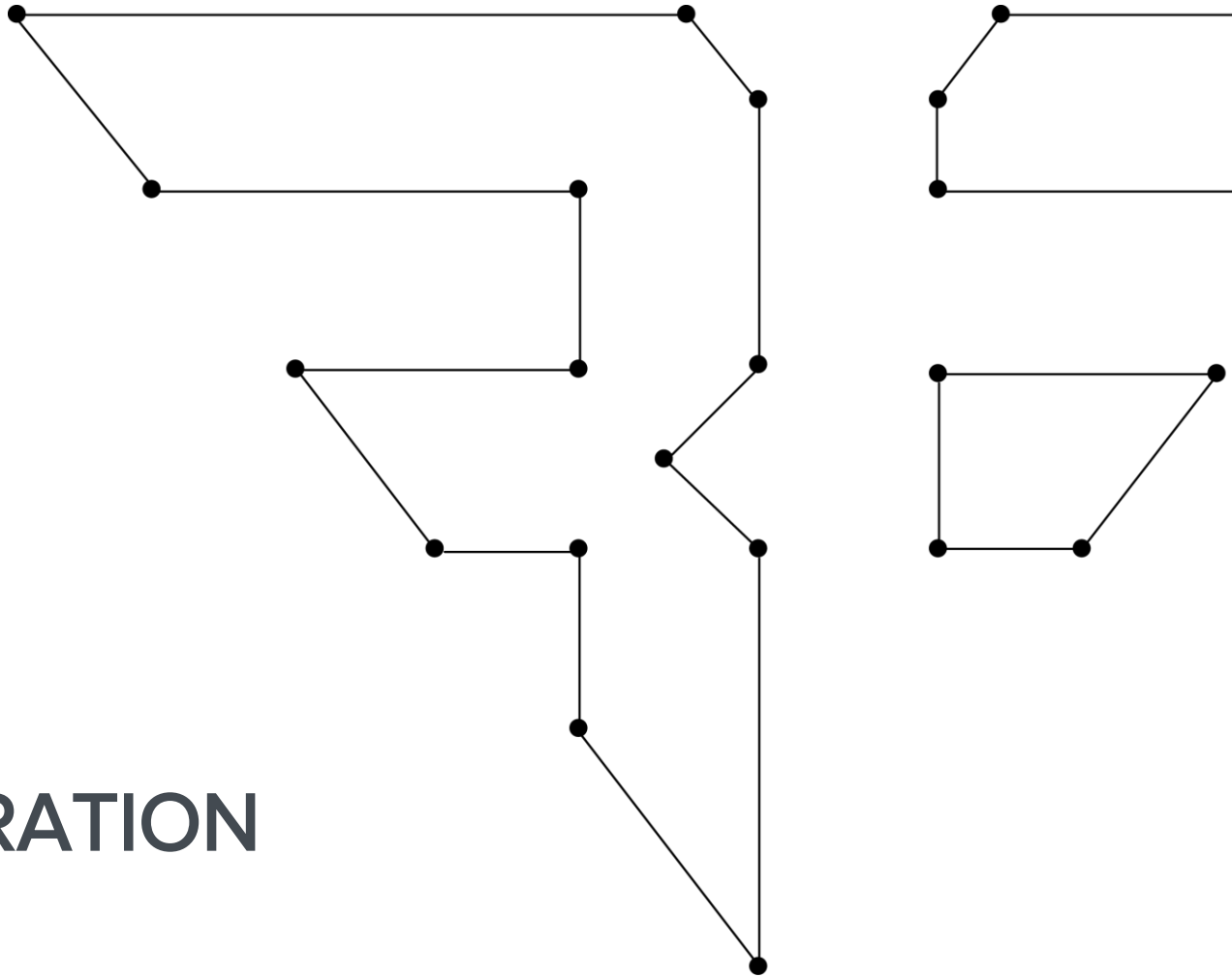


- Dan Petro
Sr. Security Analyst
 - *PHX 2600*
 - *Nova / Honeyd*
 - *Rickmote*
- Moloch
Security Associate
 - *Root the Box*
 - *[buffer]overflow*
 - *iSpy*



DEMONSTRATION

CROSS FINGERS



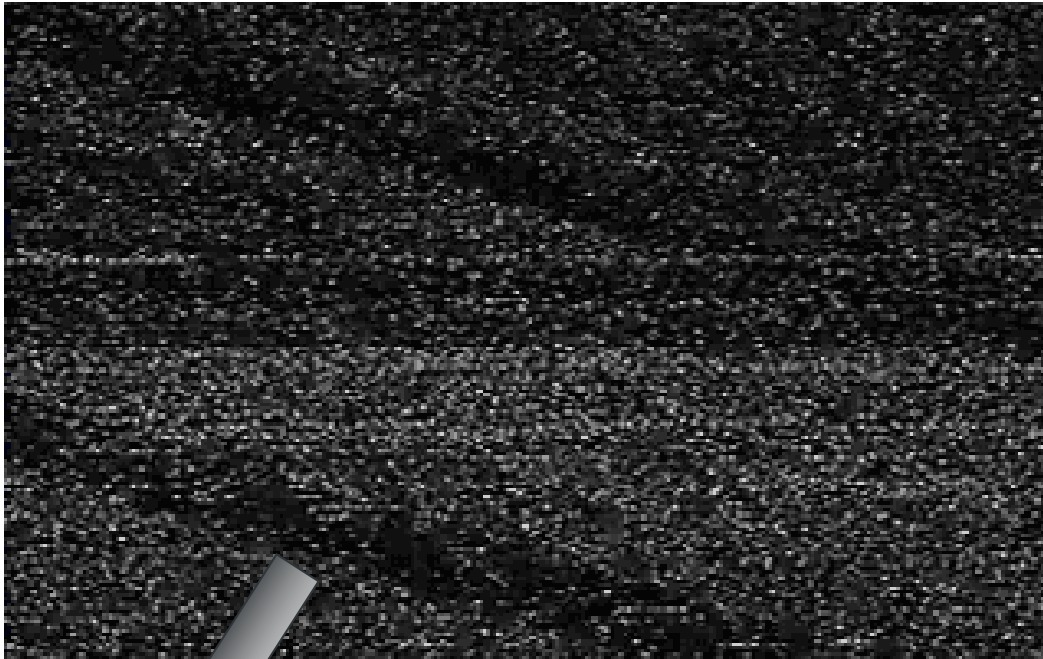
WHAT IS PSEUDORANDOM

A QUICK HISTORY LESSON



Nature

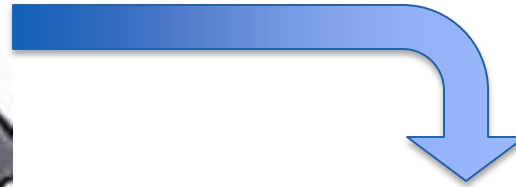
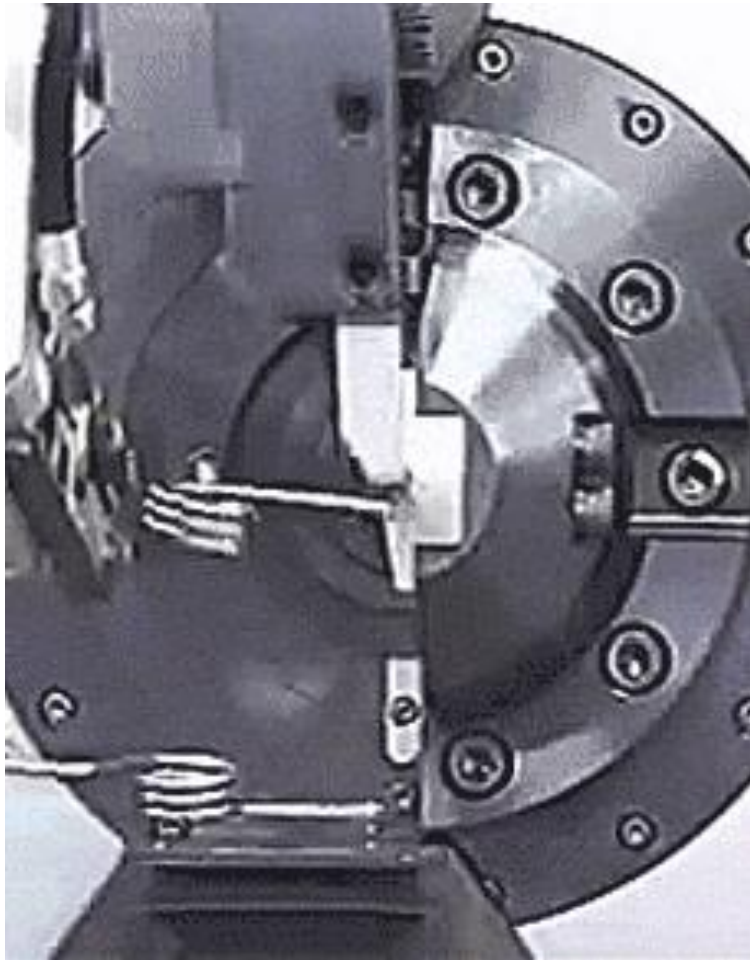
BY THE NUMBERS



579834279173498173984179871938247981

Machines

DETERMINISTIC



57983420

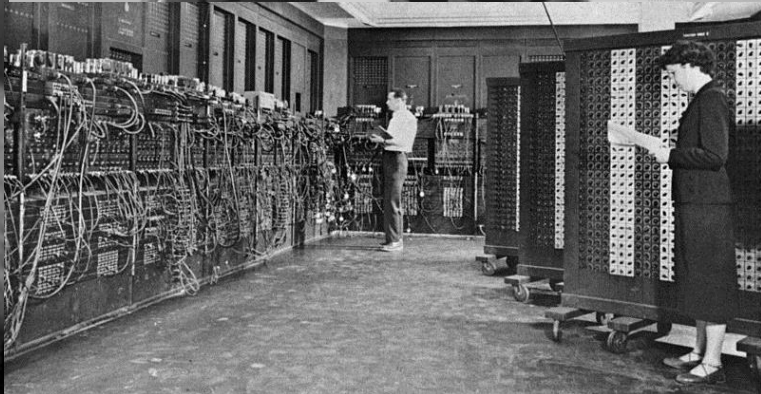
57983420

57983420

...

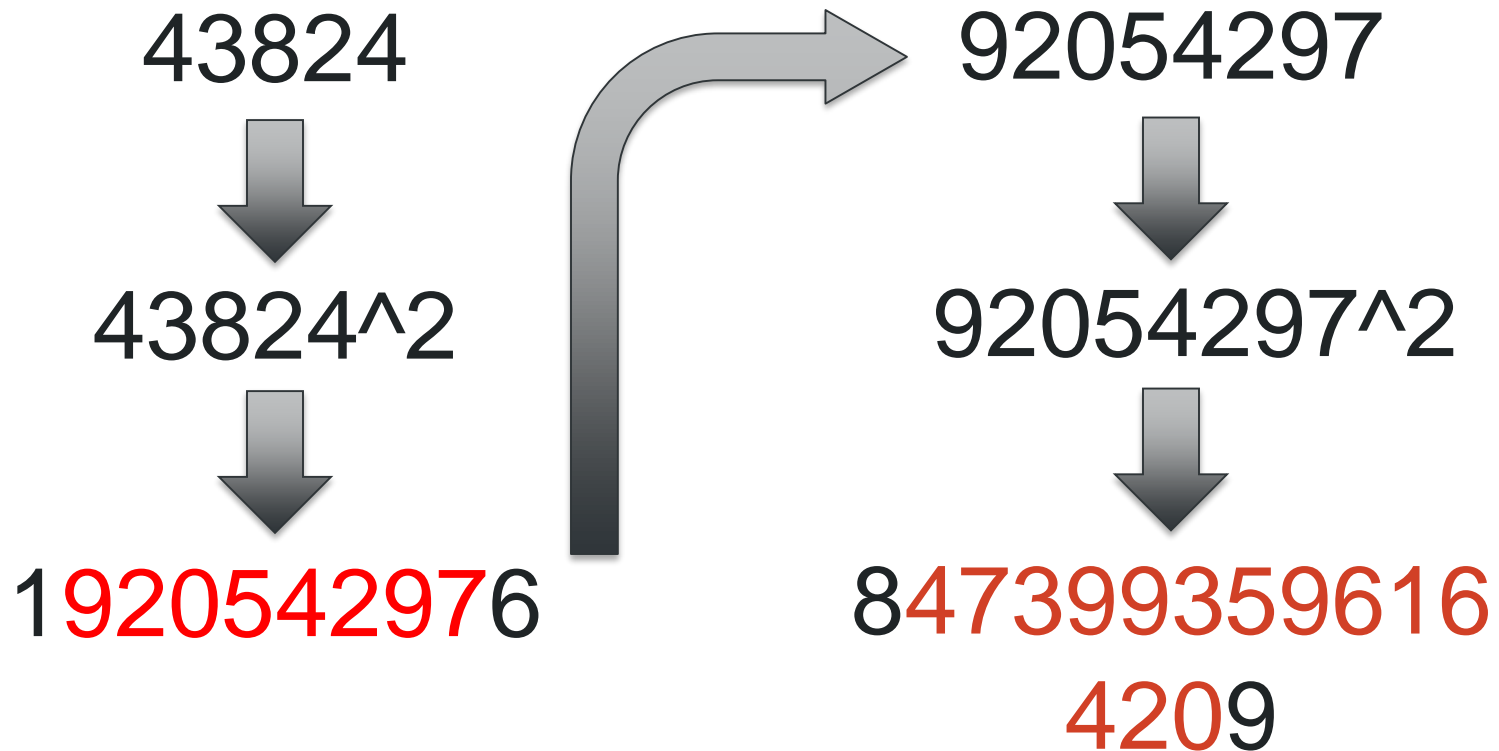
Early Pseudorandom Generators

JOHN VON NEUMAN



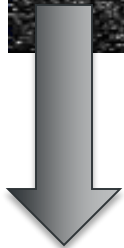
Middle Squares Method

PRNG

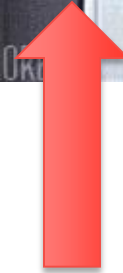
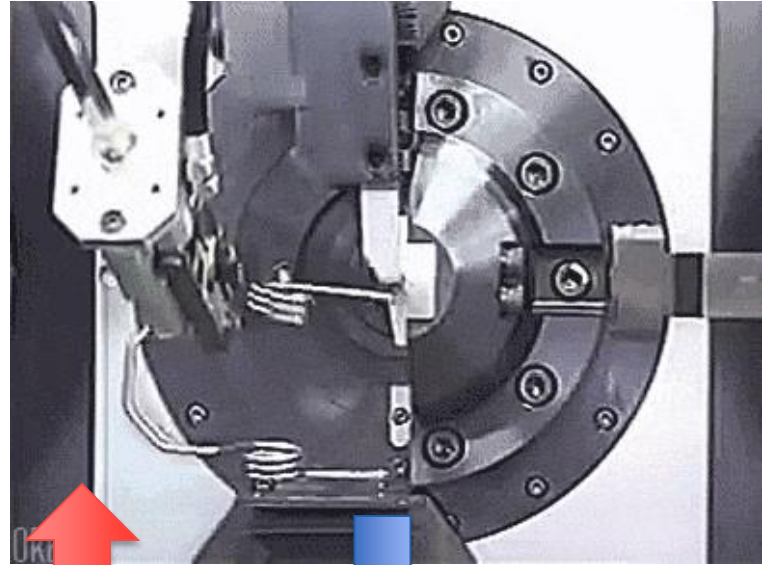


Random vs. Pseudorandom

DETERMINISTIC RANDOMNESS



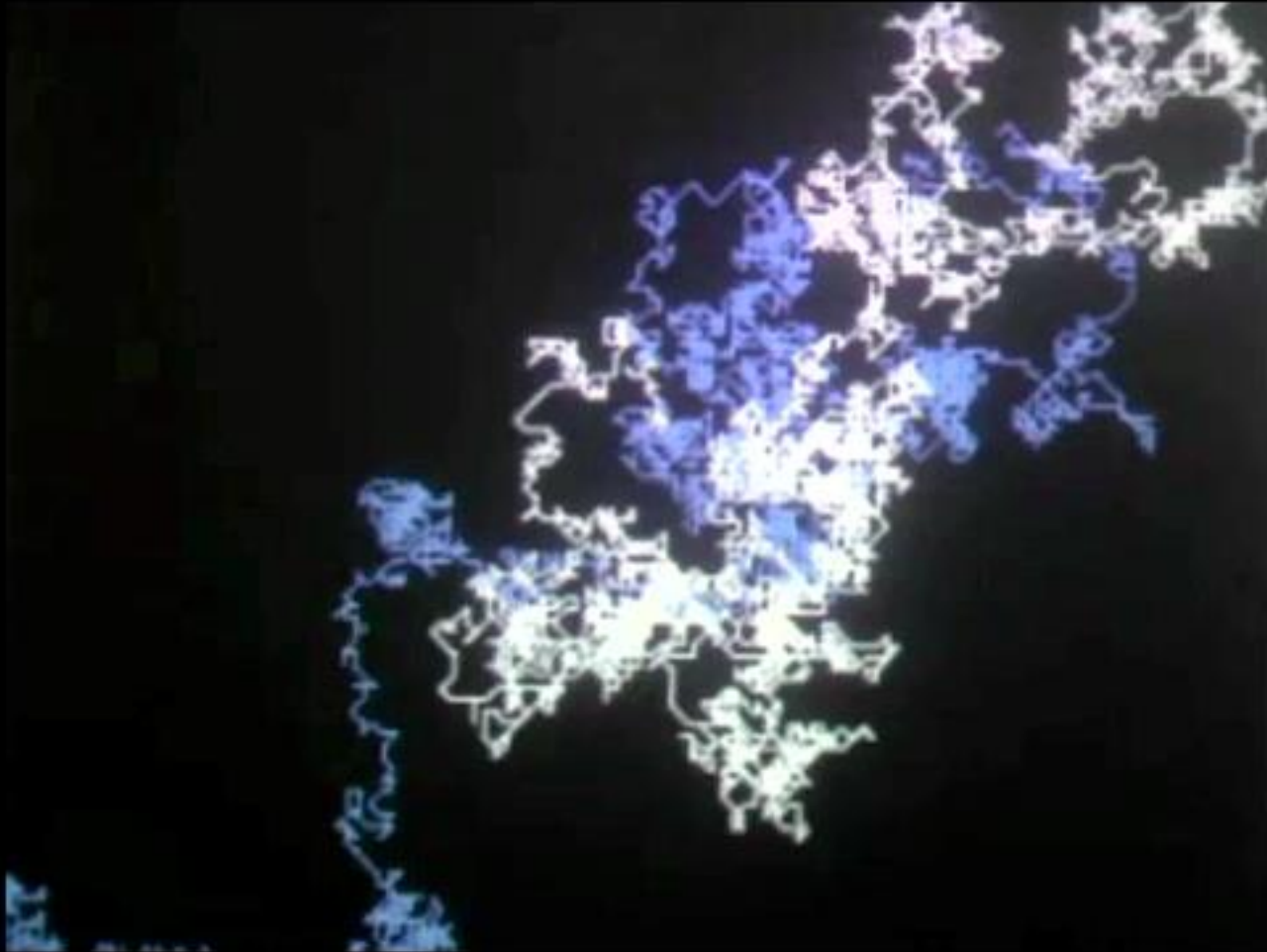
983427917349817...



5480



7983349817...



PRNG Period Size

THE MERSENNE TWISTER

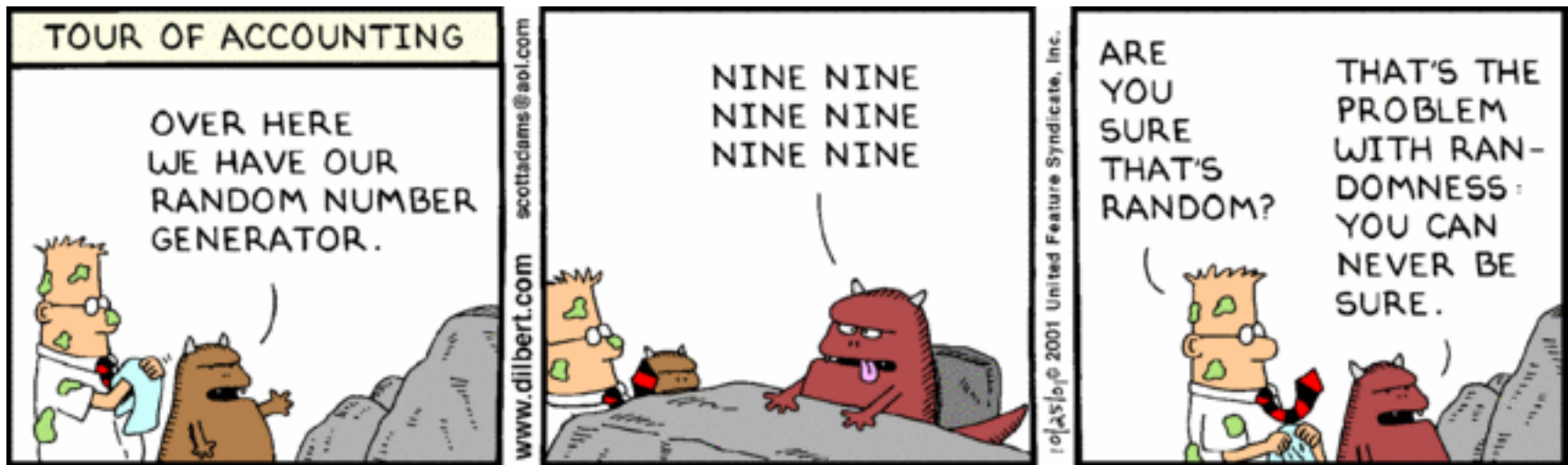
$$(2^{19937})-1 =$$

43154247973881626480552355163379198390539350432267115051652505414033306801376580911304513629318584665545269938257648835317902217334584413
9095282691546091680190078753437413962968019201144864809026614131844327698030006672810498409545158817607713296984376213462179039639134128
52056276196005131066463766486159942366754865374802419643502959351686623639090479483476923139783013778207857124190544743328445291831729732
4231088826508132162646945107707812282829444775022680488057820028764659399164766265200900561495800344054353690389862894061792872011120833
61480844748291354732836727787956564830784690911694586623016970240126024018702874665003344577457031543129299602518778079011937590286317108
4149642473378986267503308961374905766340905289572290016038000571630875191373979550474681543332534749910462481325045163417965514705754814
59200859472614836213875557116864445789750886277996487304308450484223420629266518556024339339190844368921018424844677042727664601852914925
27728092269753842677025733392895440120546589561034765885538663390254628996213264328242574803578623358060815469654693256383323767076989943
9774888526682785274510029630591469638757154257355344759797344631006783673933274021499309687782967413915145996023742136298987206114314104
02147238998090962818915890645693934483330994169632295877995848993366747014871763494805549996163051541225403465297007721146231355704081493
0986630657336771911728539870957481678162560842128233801686253345864312540346708061352735432707144788768618619833207728064480669112571319
72625817631513135964295477635763678370193498351784621424949607571909180546251141436663841894338525764522893476524546315357404687862289458
85654608562058042468987372436921445092315377698407168198376538237748614196207041548106379365123192817999006621766467167113471632715481795
87700538269439340040306170045769113534918787488892342934934014517057171618112579588888927749542697714991454962391639401482298502533165151
14312788020090568084565068188772666098316368838849056218222629339865486456690806721917047404088913498356856624280632311985204368263294152
9075297279834342944650999220636878136715409170265577272739132942427752934982600585884766523150957417077831910016168475685658673192860882
0701797603072698499873548360423717346602576943472355063017441188741412924389581415491006097522168822308876114319964723084238013711092744
94835578150375868496445857499177728699267442183696211376751010832785437940817490940910430840967741447084363242794768920562004272279616386
69149805489831121244676399931955371484012886360748706479568669048574782855217054740113945929622177502575565811067452201448981991968635965
36155168127398274076013889963882031877630366876273015758464004279888069186264026861268618088387493957381812502227968993026744625577395954
2469831637863000171279227151406034129902181570659650532600775823677398182129087394449859182749999007223592423345678506711865688391867477
049600162775406253314406190191299837899147125153652003360579935086016788078568562377857095255541304902927192220184172502357124449911870
21064269456506138491937347432450396626779903840238678168680996201587909058654942350469919074351955104372254451574096782908433602593822578
07308802738552615519720440756203267806244488034909982321612316877947156134057932495455095280525180101230872587789741158170482455889714385
96754408081313438375502988726739523375296641615501406091607983229239827240614783252892479716519936989519187808681221191641747710902480633
4910917048274412282811866324459071457871383512348422613800746219140048181523866660431334487506790358283828356268808326357548206847963954
638381953217452250268237244136327576587560919783653298312066708217149316773364340379289724393986744139891855416612295739356686126582712
34696438377120838998040199739078061443675415671078463304673702403777653478173367084844734702056866636158138003692253382209909466469591930
161626097925087421175670306055139542860750806159835357541032147095084278461056701367739794932024202998707713017692508204621070221251412042
93225304317896162670477761151235979354041470848709854654265027720573009003338479053342506041195030300017040028878929414046033458699263675
01355094942750552591581639980523190679610784993580896683299297681262442314008657033421868094551740506448829039207316711307695131892296593
509018623094810557519560305240787163809219164433754514863301009915916985856242171656362477132898167854824629737624953025136036341276836645
61750770319774575349128064331765399959943433081184701471587128161493944212766142282629099500557469810532066100015602957846566161932522694
1202683115950894967151384519588321714798274887926185141781997903441728559860772220866677680426090308754823803345446566305619241308374452
7546681430154877108772801108600432589226225941396828528349704557106275770142176156526272515340740762540514993198949445910641466053430537
85767098625200498648809611448692586034737143636591940139627063668513892996928694918051725568185082988249549548157966631695176657414201597
98754273428026723452481263569157307213153739781041627653715078598504154797287663122946711348158529418816432825044466692781137474494898385
06437578750737649634514862530638339155514569008789195531599446294449323524881759990711913575593338212170619147718505493663221115722292033
11485024875633031180188056850735698415805181187107786539535712960143729408652704070219243831672903232315679122894194862405940390744523216
78019381871219092155460768444573578559513613304242206151356457513937270939009707237827101245853837678338161023397586854894230696091540249
98790745346131192396385295075475805820562595660081774300719174681265595502174767092246086674774452087560785906233475062709832859348006778
9456169602494392813763495657599847485773553990957557313200809040830036446492219409934096948730547494301216165686750735749558823403039898
74672975455060957736921559195480815514035915707129930057027117286252843197413312307617886797506784260195436760305990340708481464607278955
495487742140753570621217198252192978869786916734625618430175454903864111585429504569920905636741539030968041741



Can you be sure?

EVALUATING RANDOMNESS



The Die Hard Tests

TESTING RANDOMNESS



Die Hard Randomness Tests

999999999999 ...

- Birthday attacks
- “Craps” tests
- Count the 1s
- Monkey tests
- Parking lot tests
- Squeeze tests
- Etc.



SEEDS

HOW DO THEY WORK?



Do You Want Vulns?

CHOOSING A “SECURE” SEED

- Time
- PIDs
- Stack memory
- Hardcoded “random” seed
- Combinations of any of the above

Vulns.

THAT'S HOW YOU GET THEM



Sony's ECC Random

EVALUATING RANDOMNESS

```
int getRandomNumber()  
{  
    return 4; // chosen by fair dice roll.  
             // guaranteed to be random.  
}
```

ATTACKING PRNGS

UNTWISTING THE TWISTER



Bruteforce

EVEN CHOOSING A SEED WELL CAN'T SAVE YOU

- **32 bit seeds on most algorithms**
 - 4,294,967,296 values
 - Enumerable
- **Offline attack**
 - Limited only by CPU power
- **Timestamp based seeds**
 - 31,557,600 values

Algorithm

USED IN UNTIWSTER

- **Given set of observed numbers**
 - 42, 61, 27, 75, 89, 34, 12
- **Calculate random numbers**
 - One by one
 - Compare to head of observed list
 - If it matches, look for the next observed #
 - Continue until match is found
- **Allows for missing values**
 - Don't have to be sequential

Algorithm

USED IN UNTIWSTER

↓ ↓ ↓ ↓ ↓ ↓ ↓
42, 61, 27, 75, 89, 34, 12

45, 33, 42, 97, 61, 27, 75, 49, 51, 89, 34, 12,

,

Problem of Depth

WHERE TO HALT

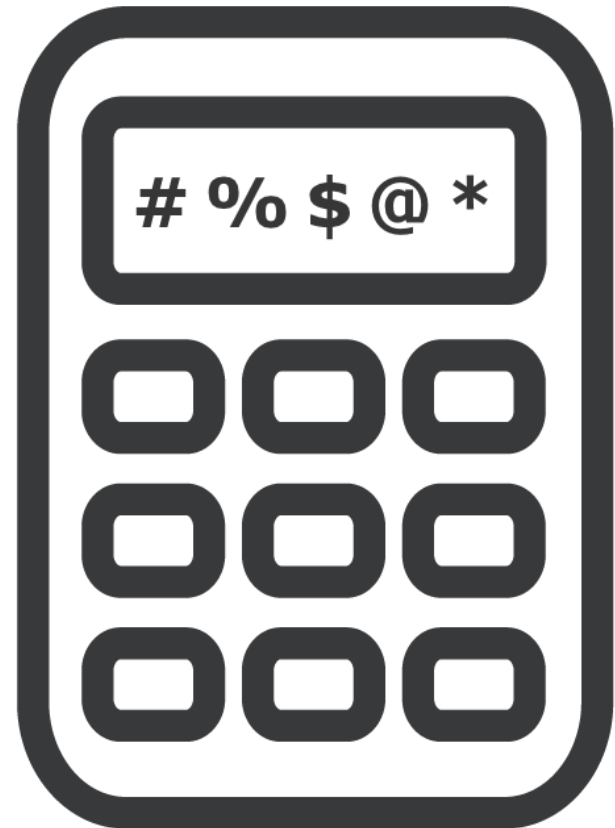
- **How do you know you're deep enough?**
 - Maybe the correct numbers are just about to appear
 - Haven't yet
- **Halting problem**
 - Depth is given as input
 - Give up after depth is explored
- **Efficiency vs Completeness Tradeoff**



State Inference

MATH IS HARD

- **Crack RNG state**
 - Predict future and past values
 - Without knowing the seed!
- **Much easier with sequential numbers**
 - Current implementation requires it*
- **Small state size helps, too**



glibc rand()

MATH IS HARD

- **Very simple algorithm**
 - $r[i] = r[i-3] + r[i-31]$
 - With the LSB chopped off
- **Produces 31 bit numbers**
 - Internal state has 32 bit numbers
- **Observe 32 sequential numbers**
 - This IS the internal state
 - Missing the LSBs

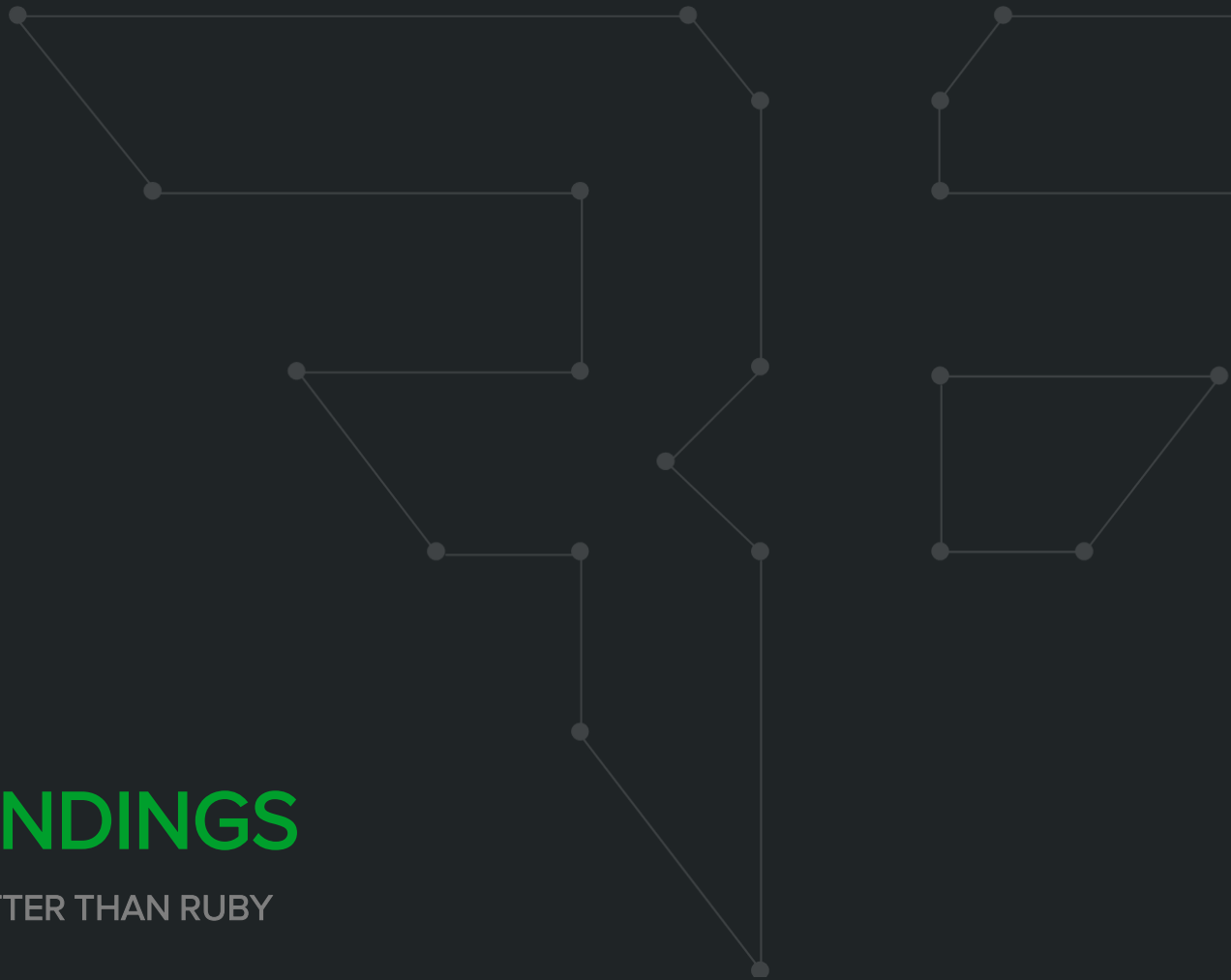
glibc rand()

MATH IS HARD

- **LSB reconstruction**
- **Guess-and-check**
 - Use state to predict random numbers
 - Measure how well it predicts
 - Try with 0 and 1 LSB
 - Go with the better guess!
- **Boolean Algebra**
 - Really long Boolean equation
 - Only guaranteed for ~ 132 consecutive outputs

PYTHON BINDINGS

BECAUSE PYTHON IS BETTER THAN RUBY



The Python GIL

THREADING ISSUES IN PYTHON

- Bytes codes do not execute concurrently
- The GIL is not going anywhere
- Threads are still useful for certain tasks, but not performance



Code Sample

THE C++ // PYTHON BRIDGE

```
/* Suspend Python's thread, so we can use native C++ threads */  
  
PyThreadState* pyThreadState = PyEval_SaveThread() ;  
  
StartBruteForce(threads, answers, (double) minimumConfidence,  
lowerBoundSeed, upperBoundSeed, depth, rng);  
  
/* Clean up and restore Python thread state */  
  
PyEval_RestoreThread(pyThreadState) ;  
  
pyThreadState = NULL;
```

Distributed Computing

REMOTE PYTHON CALL

```
tomere@hollywood: ~
File Edit View Search Terminal Help
tomere@hollywood:~> rpyc_classic.py
INFO:SLAVE/18812:server started on [0.0.0.0]:18812
INFO:SLAVE/18812:accepted [redacted]:58779
INFO:SLAVE/18812:welcome [redacted]:58779
hello world

C:\Windows\system32\cmd.exe - python
>>> import sys
>>> sys.platform
'win32'
>>>
>>> import rpyc
>>> c = rpyc.classic.connect("redacted")
>>> c.modules.sys
<module 'sys' (built-in)>
>>> c.modules.sys.platform
'linux2'
>>>
>>> rsys = c.modules.sys
>>> type(rsys)
<netref class '__builtin__.module'>
>>> rsys.stdout.write("hello world\n")
>>>
>>> f = c.builtin.open("/etc/motd")
>>> for line in f:
...     print line,
...
Welcome to Ubuntu 11.04 (GNU/Linux 2.6.38-8-generic i686)

x Documentation: https://help.ubuntu.com/

System information as of Fri Jun 3 00:24:30 IDT 2011
```

Contact Us

 bishopfox.com

 [@bishopfox](https://twitter.com/bishopfox)



BishopFox
AltF4
Moloch--

Thank You



BISHOP FOX

We're Hiring

bishopfox.com

careers@bishopfox.com

Especially if you know how to make final slides...immediate hire.