2550 Intro to cybersecurity

L4: Crypto, OWF

abhi shelat

A Network is a public resource.

Goal: add privacy to a public resource.

Perfect secrecy

$(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathcal{M}, \mathcal{K})$

is said to be PERFECTLY SECRET if

$$\forall m_1, m_2 \in \mathcal{M}, \forall c$$

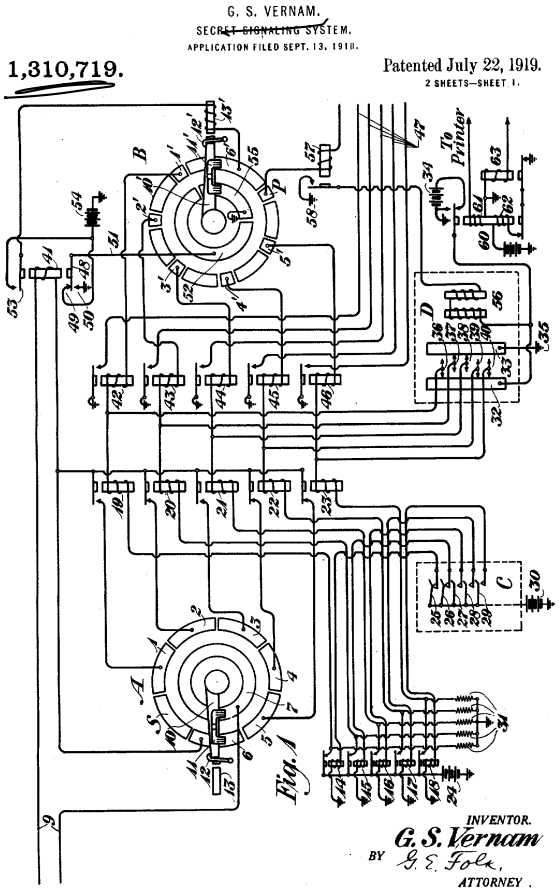
$$\Pr[k \leftarrow \mathsf{Gen} \ : \ \mathsf{Enc}_k(m_1) = c]$$

$$=$$

$$\Pr[k \leftarrow \mathsf{Gen} \ : \ \mathsf{Enc}_k(m_2) = c]$$

One-time pad (Vernam 1917)

$$
\begin{aligned}
\mathcal{M} &= \{0,1\}^n \\
\mathcal{K} &= \{0,1\}^n \\
\mathsf{Gen} &= k = k_1 k_2 \ldots k_n \leftarrow \{0,1\}^n \\
Enc_k(m_1 m_2 \ldots m_n) &= c_1 c_2 \ldots c_n \text{ where } c_i = m_i \oplus k_i \\
Dec_k(c_1 c_2 \ldots c_n) &= m_1 m_2 \ldots m_n \text{ where } m_i = c_i \oplus k_i
\end{aligned}
$$



ABCDEFGHIJKLMNOPQRSTUVWXYZ
01234567890123456789012345

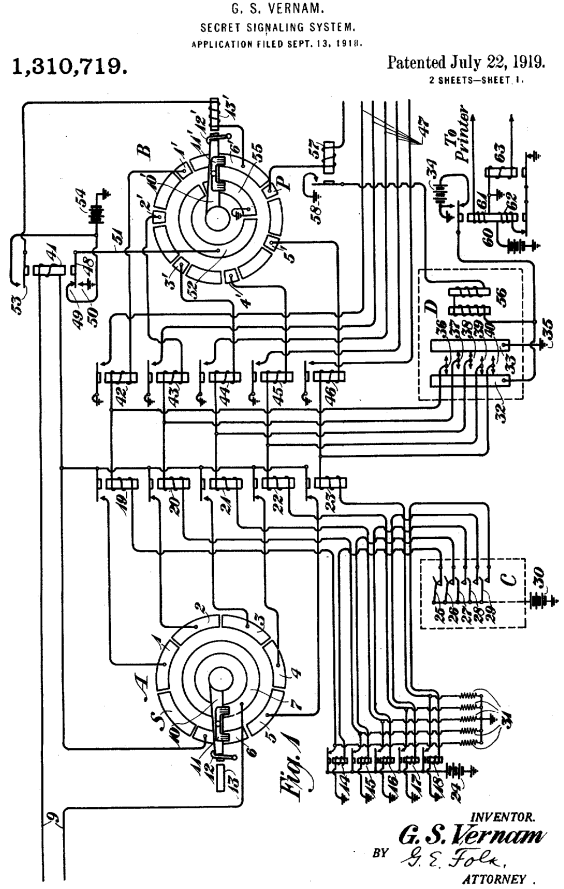
8 19 22

M = ITWASTHEBESTOFTIMES

14 18 13

K = OSNEKHRJFUTGXMGALEQ

WLJ...



ABCDEFGHIJKLMNOPQRSTUVWXYZ
0123456789012345678901234 5

ITWASTHEBESTOFTIMES

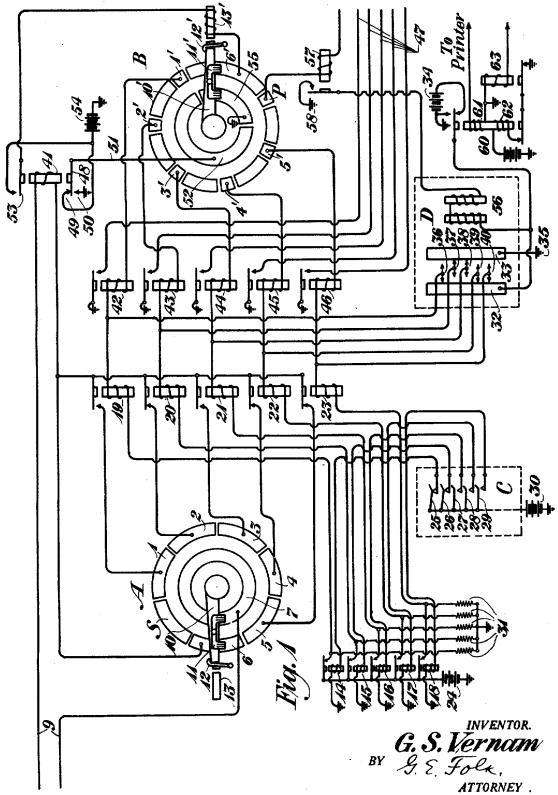
OSNEKHRJFUTGXMGALEQ

WLJECAYNGYLZLRZIXII

G. S. VERNAM.
SECRET SIGNALING SYSTEM.
APPLICATION FILED SEPT. 13, 1918.

1,310,719. Patented July 22, 1919.

2 SHEETS—SHEET 1.



INVENTOR.
G. S. Vernam
BY G. E. Folk,
ATTORNEY.

ABCDEFGHIJKLMNOPQRSTUVWXYZ
0123456789012345678901234 5

12 1 6
C = MBGZBWSNDHCVCGFN

K MVCLWOFLMDZBRYMP~~DVEE~~

M = AGE...

One-time pad (Vernam 1917)

- key size has to be equal to msg length
- hard to implement key mgmt.

$$
\begin{aligned}
\mathcal{M} &= \{0,1\}^n \\
\mathcal{K} &= \{0,1\}^n \\
\mathsf{Gen} &= k = k_1 k_2 \ldots k_n \leftarrow \{0,1\}^n \\
Enc_k(m_1 m_2 \ldots m_n) &= c_1 c_2 \ldots c_n \text{ where } c_i = m_i \oplus k_i \\
Dec_k(c_1 c_2 \ldots c_n) &= m_1 m_2 \ldots m_n \text{ where } m_i = c_i \oplus k_i
\end{aligned}
$$

- Shannon shows this is unavoidable for perfect security.

FAILURE CASES: ① key runs out. what to do??
⇒ key reuse, which breaks security

Uniform distribution on strings of len n

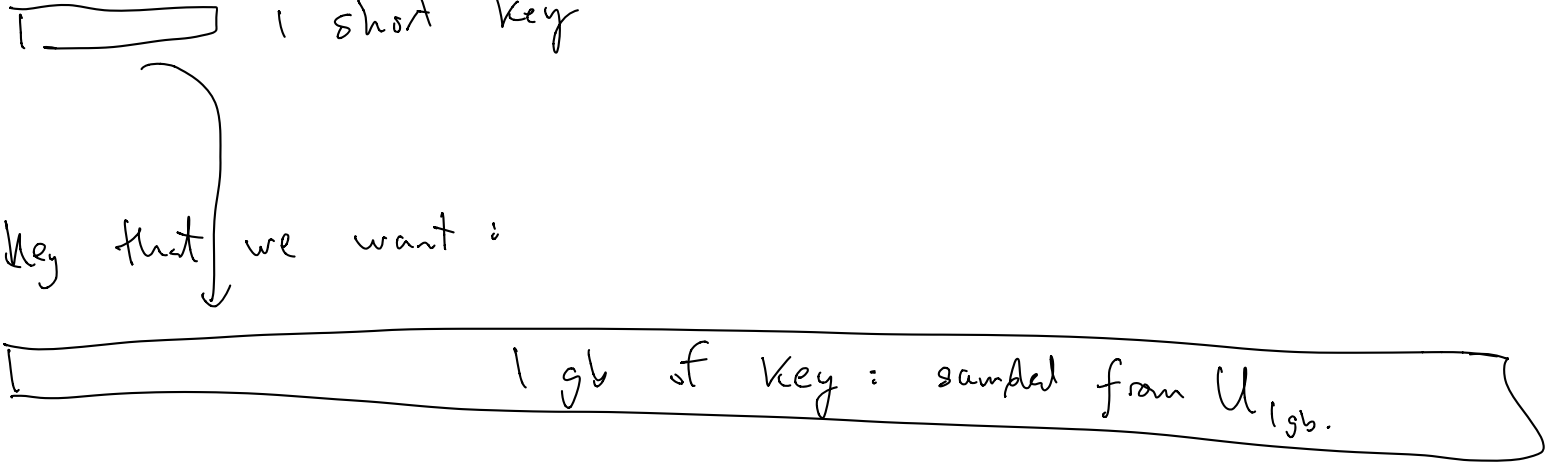
$$K = U_n = \{t \leftarrow \{0,1\}^n\}$$

random strings of length n.

- the keys in the onetime pad are drawn from U_n.

Goal: 1 key to many keys

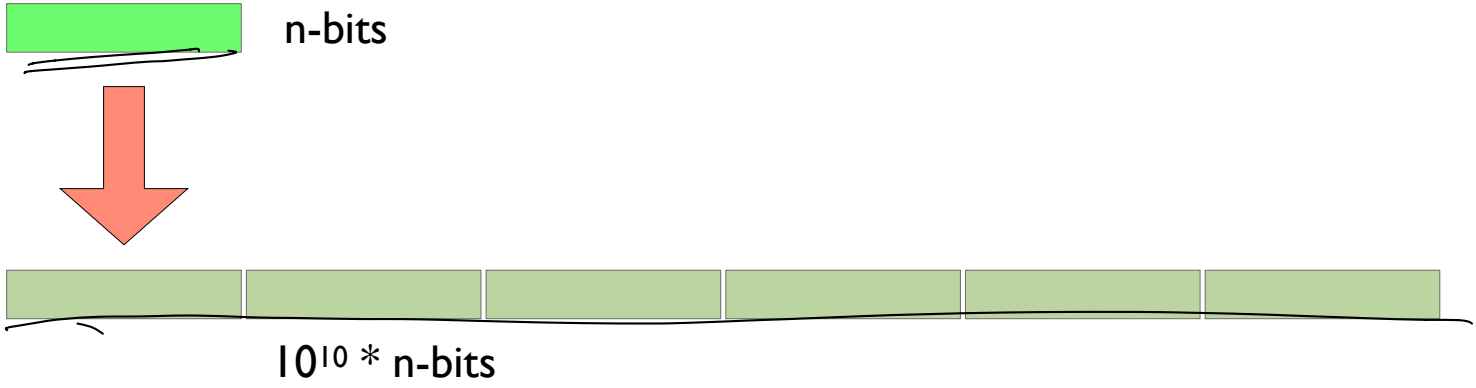
1 short key ⇒ produce many long keys.



Goal: 1 key to many keys

10^{10} * n-bits

τ should look like U_n.



This is the idea behind a stream cipher.

Stream cipher

Gen: pick an n-bit binary string k

Enc(k,m): Output G(k) + m

Dec(k,m): Output G(k) + m

what security properties are needed for this to work?

① the output of our generator should appear uniformly random...

Vigenere cipher

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
01234567890123456789012345
```

MSG: THEMODERNSTUDYOF ...

$\oplus$

KEY: ABHIABHIABHIABHIABHIABHI

ciphertext: TILUOELZNTACDZVN...

Insecure b/c key is not random !!

10^{10} * n-bits

Key

G

Pseudo-random generator.

stream

10^{10} * n-bits

should appear to be the same as a random string $\{0,1\}^{10^{10}n}$

$$U_{10^{10}n}$$

what does it mean for a process $\{X\}$ to be pseudo-random?

$$\{X_n\}_{n \in \mathbb{N}}$$

$$x \leftarrow X_n$$

$$\{X_n\}_{n\in\mathbb{N}}$$

$$x \leftarrow X_n$$

$\{U_n\}_{n\in\mathbb{N}}$

random process

roughly same # of 0s and 1s $\rightarrow$ 0101010101 ..

same # of 00 and 11, 01, 10 $\rightarrow$ 00100111|0010

# of 000, 001, 010 ... , 111

$$\{X_n\}_{n \in \mathbb{N}}$$

$$x \leftarrow X_n$$

roughly same # of 0s and 1s

roughly same # of 00s and 11s

$$\{X_n\}_{n \in \mathbb{N}}$$

$$x \leftarrow X_n$$

roughly same # of 0s and 1s

roughly same # of 00s and 11s

roughly same # of any pattern

"any efficient statistical test should pass on both $\{U_n\}$ and $\{X_n\}$"

$$\{X_n\}_{n\in\mathbb{N}} \quad \text{and} \quad \{U_n\}$$

$$x \leftarrow X_n$$

ARE

INDISTINGUISHABLE

TO THE

ADVERSARY.

roughly same # of 0s and 1s

roughly same # of 00s and 11s

roughly same # of any pattern

given any prefix, hard to guess next bit

{ Computational

"Indistinguishability" }

provides a precise way of formulating pseudo-randomness

next slide has 2 pics

are they the same
or different?

same or different?

twice the time.

same or different?

same or different?

twice the time.

same or different?

same or different?

twice the time.

same or different?

lesson:

Ability to answer correctly...

Depends on the amount of computational power that you have

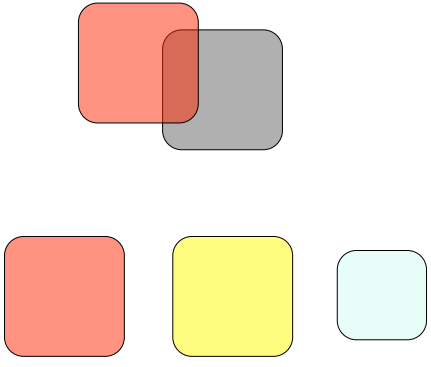
http://i.telegraph.co.uk/telegraph/multimedia/archive/01553/toss_1553792c.jpg

NEW PROBLEM:

consider all drawings consisting of boxes.

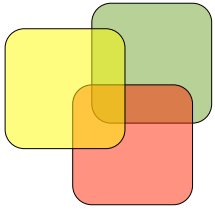
evens

# of boxes that overlap another box is even



odds

of ... is odd

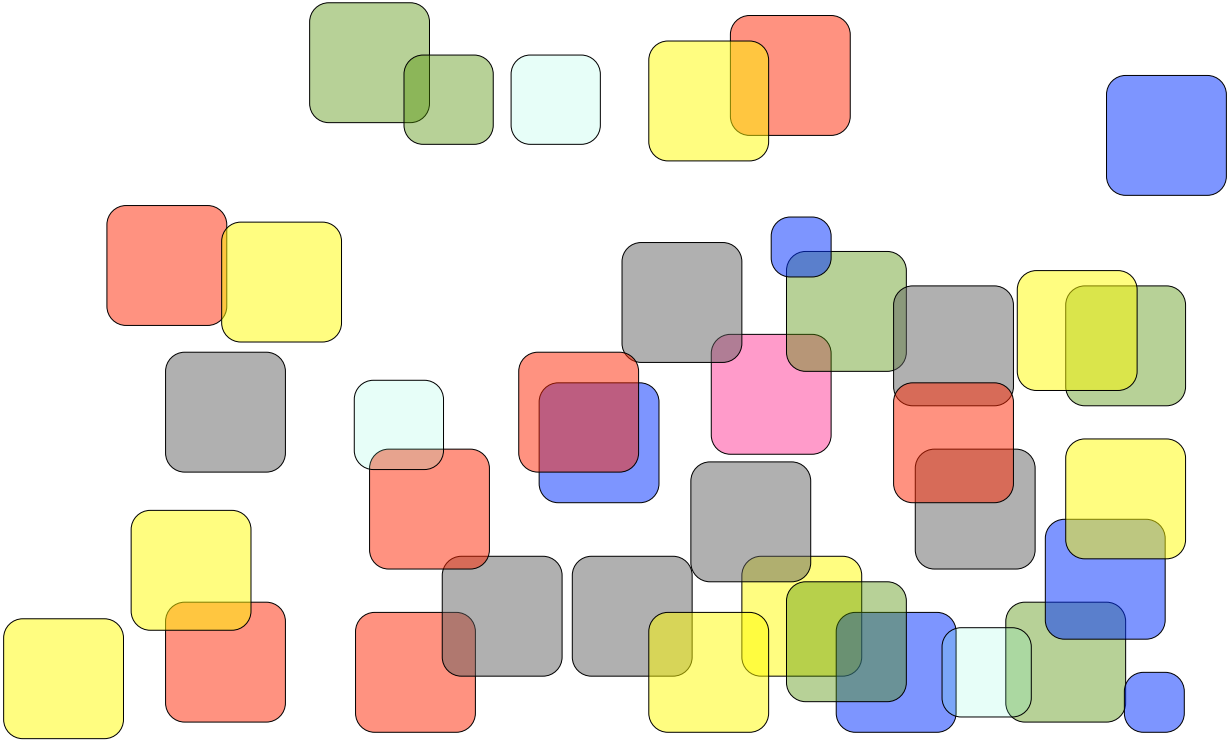


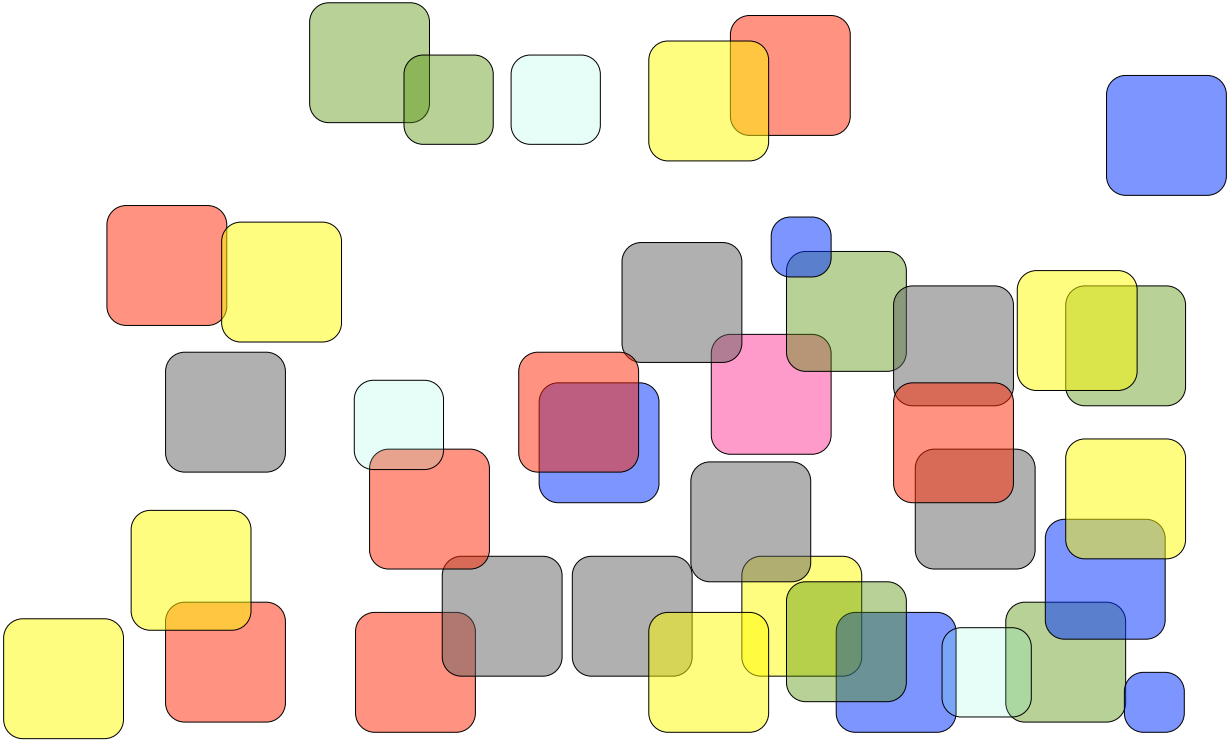
GAME:

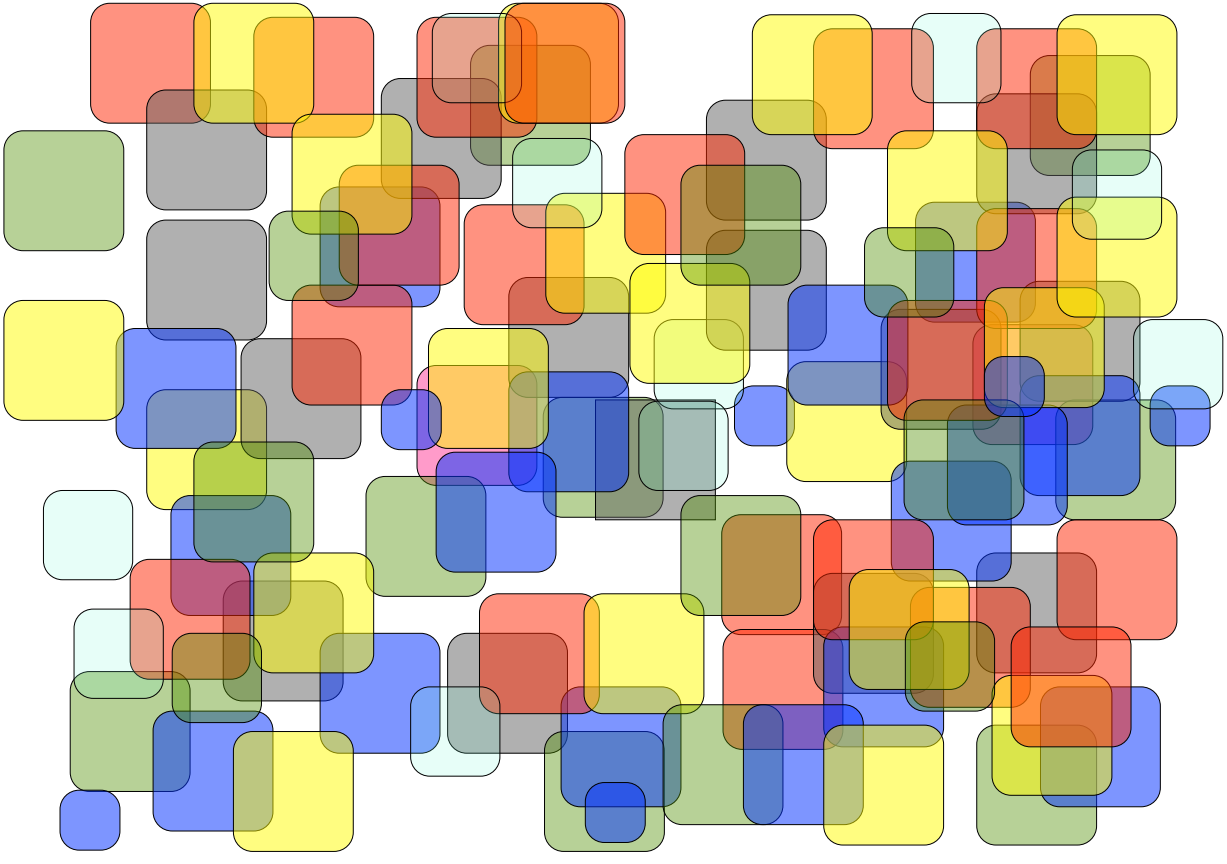
I will pick a sample from either evens or odds, and you will have to guess which one.

READY?

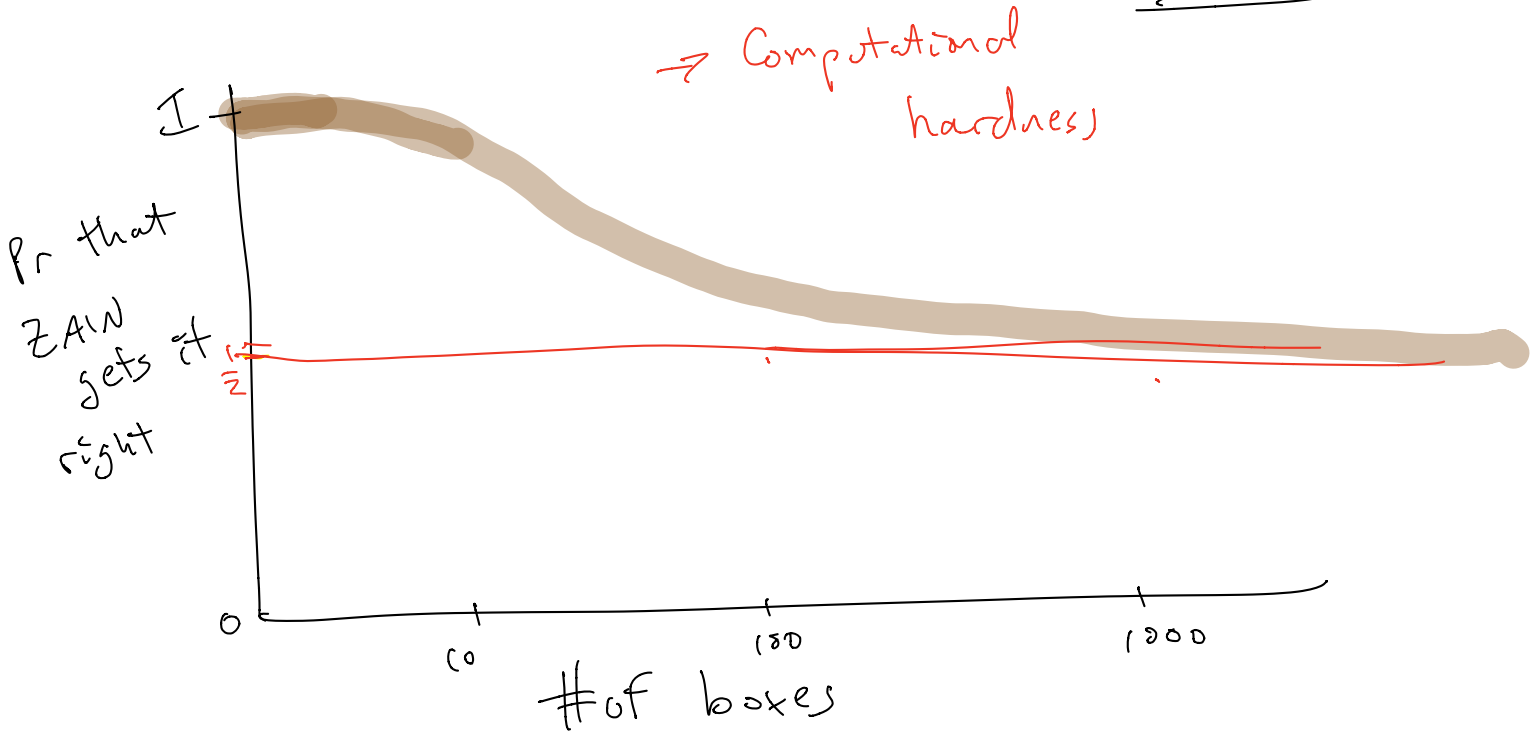
READY?







This game is parameterized by its size: i.e, # of boxes.



This game is parameterized by its size: i.e, # of boxes.

evens_n odds_n

As the game size increases, it becomes intractable to distinguish b/w evens and odd

parameterized experiment

$$\underbrace{\{X_n\}_{n\in\mathbb{N}}}$$

a sequence of probability distributions
where X_n is a distribution over strings of length
$\ell(n)$

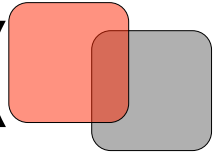
ensembles

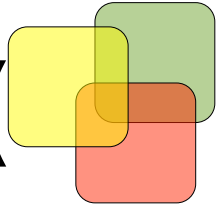
Computational Indistinguishability

"let there be two parameterized experiments, *X* and *Y*. as the experiment size increases, no p.p.t. algorithm *D* succeeds in distinguishing *X* from *Y*."

probabilistic polynomial time } "efficient"

what does it mean
for an algorithm D to
distinguish a sample?

D()= “evens”

D()= “odds”

Two ensembles are comp. indistinguishable

Two ensembles are comp. indistinguishable

$$\{X_n\}_{n \in N} \approx \{Y_n\}_{n \in N}$$

Two ensembles are comp. indistinguishable

$$\{X_n\}_{n \in N} \approx \{Y_n\}_{n \in N}$$

if for all non-uniform p.p.t. alg D,
there exists a negligible function $\epsilon(n)$
such that for all n

Two ensembles are comp. indistinguishable

formally

$$\{X_n\}_{n\in N} \approx \{Y_n\}_{n\in N}$$

if for all non-uniform p.p.t. alg D,
there exists a negligible function $\epsilon(n)$
such that for all n

$$|\Pr[t \leftarrow X_n, D(t) = 1] - \Pr[t \leftarrow Y_n, D(t) = 1]| \leq \epsilon(n).$$

what does it mean
for a process $\{x\}$ to be
pseudo-random?

$$\{X_n\}_{n \in \mathbb{N}}$$

$$x \leftarrow X_n$$

$$\{X_n\}_{n \in \mathbb{N}}$$

$$x \leftarrow X_n$$

roughly same # of 0s and 1s

$$\{X_n\}_{n \in \mathbb{N}}$$

$$x \leftarrow X_n$$

roughly same # of 0s and 1s

roughly same # of 00s and 11s

$$\{X_n\}_{n \in \mathbb{N}}$$

$$x \leftarrow X_n$$

roughly same # of 0s and 1s

roughly same # of 00s and 11s

roughly same # of any pattern

$$\{X_n\}_{n \in \mathbb{N}}$$

$$x \leftarrow X_n$$

roughly same # of 0s and 1s

roughly same # of 00s and 11s

roughly same # of any pattern

given any prefix, hard to guess next bit

indistinguishability provides a precise way of formulating pseudo-randomness

pseudo-random

An ensemble {X} is said to be

pseudo-random

pseudo-random

if

$$\{X\}_{n\in\mathbb{N}} \approx \{U_n\}_{n\in\mathbb{N}}$$

An ensemble {X} is said to be

pseudo-random

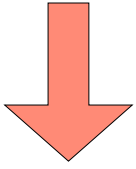
if

$$\{X\}_{n\in\mathbb{N}} \approx \{U_n\}_{n\in\mathbb{N}}$$

Original goal

small key

n-bits



large one-time pad.

10^{10} * n-bits

indistinguishable from a random key.

Pseudo-random generator

A function $G : \{0,1\}^* \to \{0,1\}^*$

is a pseudo-random generator if

G can be computed in p.p.t.

$|G(x)| > \ell(|x|)$ for some $\ell(y) > y$

$\{x \leftarrow U_n \ : \ G(x)\}_{n \in \mathbb{N}}$ is pseudo-random

How can we build pseudo-random generators?

7

$$7 * 7 =$$

49

$$\underbrace{7 \cdot 7 \cdots 7}_{x \text{ times}}$$

$$7^x$$

7^{1000}

1253256639965718318107554832382734206164985075080986171463495007520970596317381164324488390543515207631986159195515940766858289
8946726302276179083827085457983001511124666120398462435892983257161571801470409630566809750761327366302322689525054138592715842
6088684494082416768617708189592286936039922311125683719215046689156738352590137241554510185855964549927575493247391132548534378
4979788060849510858742020118363623157274201095547829887915300882897118445505002304856384131899471321422439473341992593007356224
9293741945365006149030210512792031443040163685567754913633748132181134967842707609143734504539933734861126116805592935540299282
3192491190360027036112283180935872775214517464013178274657100736321564606838252739601156414628445543663144696050650160812621814
3270626661951727017802002866450238230831859280613713103008292840711412077312806000001

7^{10000}

95587288567444097027721621933777274477156508800837670232809747736882802688984737969351872846915678176303391547032418309440558367061778809896056537787
80399681208530465536899923872083728356691350372430337696619926639213646136205780780799564658253882535717364116449482061428736198739029989324013720616
22798495221711362842179827842727414295003904969814698887647607489396731788861520661760706501004653662221061702731812881848142381806779161139684997815
33857229583655468142483727845972893261563186914448396106549374910394408496075970728927209606377135009929343770889544886395210196985248511900291396723
34581096971834261761008159149534484118177736597236191071022784445587105969769066773943151852497146078670876701272357547133220831824869952253405695472
24637119563739118489076548828690529780180285781790200709105216646950073585170470697772749289033207716010189419921643140458588853251039197496070544889
71652559170240935385129592437066664987443935314310318787709572181947687110460396215414209965523374474058355202693094219280954613682387054722403565561
68312930388055119358800784517897136666191879774303837940606358829794421599264636917853403624967743494135245600686835446913717210276536426354058103443
91477855285718310897324368748177703731383290606646196241766322273949789427186494573916220387132050170812874260685993980785991365062484904774284092738
45322293948595250418133360588306541097125781628428197968967708785261936745801584142161171842336306061944607580316035087158545049258220657354157171176
42951641517044516126295875685241125426213156539867646429188235196051228173319647034882976905185935972581124925543404862657129745082863682768217744513
28996893631934434841791210613977737646500169926470060725939192900341372098057933793890328524106945011721530158679597549366961544323520396108216845856
60293442216332255507058075007157057934008407572852685095108138875038783467527808394272833031297114865113153007797888201808406197212237152401786723674
96637042272860292245006757733008463731247340730605827559431458687544786940933264980621447456906707991547128831033370293831198789730566529222267250464
94001644377943743452783533866658332825699115526102481808742271316354083188217216735072401255075831638502315154196349830971547344213153150365567385039
52579851113060316168285064441232537103590182621079377832843019727603226096866723988722891001182616180230977331759604555319089344641568797218346060486
91762387934893989942083292678611416543611768850763424813437908028375226699829575967165231253786105772454128891004817031720210914641548363847541833079
22685257765508608568562975782300697197204032540698594430286977219892762377295441285181042879127802999024719080613210271422102554740752710289946806735
37259392939342492022814681786038589505372793746046900629086230630259659924116133599305462808406201633629428637101656936527502479985898768332184004335
96639923643807793537485122586379078832995205363197648627390047750400245522036935578273297419752227419104359783605213749942580361012317260930722582974
40735657687656653417040524326319232166510843949286941183532589457466149344002398542045031768982820134480807533788305522366049120476884093493951048644
07345150328046921038566652090310866567690216457225948387309395598104621188922299520026018146333402349443994282604600758932366539153393090504007103991
18863480174135729126354272327526198931847020456672879532506696333611778066210820579248916858197102905558561073173654738527663802764255064566025275401
17971724098601448357463139833373628747458351815403543341999906781590500386735380120235572414794413580542733270524897365599418650411306114136782193558
93476567393224303909082190781300190833131836924007165565422712251679628183801808697438471248270896656566801392106045976601094176105501078995413630627
05900288745023359281714958359096826397307447904564333619769407450980366639836081278482723694195682833281497420595461768778209208730309972518514909989
34287793587314012691376625709193571373268588370102514439184276312405197068399204828411850218556413588259632958205256693710041664679094714984459699883
10316737367710893103311537634234857638996253794816827403174591340923560355044325962134721789323355449602766761015911412461491615405576309511983254641
61885467428416604670527897561905627890990303514190544175156737750586986075245694893976422852835685633907883822672296964630492690390472027126075506211
74274970352102351832642427284726879688473896768703167609747279566439557849880039271927498105906302920460627895414166402998481514856889679663643426632
59247454948386361302515198028514970927235946532045204096515486837699846692599719887881781588315175577292901153095490566264727752914630463195487187579
81842193591589605589369634076907345944834305812025808883916881139977347406610415831245496265129664629242501811263830170572918809855757043839746107727
51107669799661841774127735327529629987980135495274197751725763357367533317639259538639631812862500262581861604130322932796068961074378772900122619610
95075078523249740107441649074205707503339857610479405501354002538172669003503829435619181066724693520857662065505547119775673157892582974345012851224
03345550857364422106089400098097980710060066914254172300542199332763840179799715395210417981973291905376852621563340366608473882951965177128199303553
97583590688781450433887737655547586394649717798423766234759515768872575211201196790591177321395066955978185826696587614884398699723936600276791352446
68433614093303498345026183151219733115820351724151015788117079632416971637874342694800810920986588090282101606161109083273544569683892703076884385369
76695229421549667227488553970025901787267380707303012994912546555721617521680092662101142028491284877797981483652170709353747182682111023619809685273
30949883894783925818255430850346483797946697754305745787159147586676699909367391555177886905439435498431811636138145965247047741495066940582775786312
52301110003288825754780655518167212766883031211722120463766886341101457050139738519752913754699466098465402702788083305676643164175653164229195638479
75365991386486427417012635420756335784238406846840625370460253690959084071991825552481499175959058377594905342179223414288460633222644816783912057037
07075354557112511918073873731274143941499679321050883552677572347377971057431359097681006230800441905433405184408400167924093651739070513667007673993
24486401863133453523692216106044837426872832723526396728877036669789154090875467323512305194341580241450118168534722412097353945900003375105188790288
35718109216677544706167532779894334539341149484795033723281521701291803170133581206157279751790372163062541903141120263356260078563881028828158044322
566790345244428893261896452335957448388704292410919276051488657556172485434602528126371477338338731272695247871214853134420858804219624769529530849648
24305461165483344052069705969562416904959592823688304857706697333346755997888475028602837035242143266422559083501581674445876349033308556314401236564
30541941576610331943099851040885295757540282534806827228478629743216744688778020961699159280663882846234689310077081736602436416683820654352128761662
53949114415001240168660248112047077862925289611603281589332853085867183258825475535891673425352359526353307011017102021845622963926668929672265589093
26151385289475138108952342727756434000169914627664682562543427367805737384621907606506084956620139938655220574272932080283397508049767236316047819413
05576510837522255187398122932575970203218521158723210423508984903210022531681471604161527283425018665371038789874350824128553133183897478964095512132
10937623745552392107065182174128788308985231038174181837246685831115344213967160913112271567741324804620469079393138672209754183205957678245976901221
45557246628826166559252644534293178263695795467108877595954276881268091161226599431968684120556631276490437760589000224109022110256760502207506663688
18628742451124407441779463590967479146039988804969207182365365846712087804226663296973642180785685584316325681616712576674198500848437376727048109601
05239453347719567200067141961335872126244003706089402421142339549257662158399796716927732769103582352343826936693477382089998797977999286844063504765
61759956702127474423874275294409773813374583525458136888505635396193029768685508418714596477252230715588593206795794876020845605080470098683651949698
87758274490615795726597857727249417216377578462655704874289400476685655266879736209501456715267417789381173273996244782286259433553292793669397502330
94318083024928950873135211011911245462183122413017132231172152100517301924058849195801312549213512806000001

WolframAlpha computational knowledge engine

7^100000000000000000

Examples Random

Input:

$$7^{100\,000\,000\,000\,000\,000}$$

Power of 10 representation:

$$10^{10^{10^{1.228577610529823}}}$$

Number length:

84 509 804 001 425 684 decimal digits

$\approx 8.45098 \times 10^{16}$ digits

Last few digits:

...0000000001

Computed by Wolfram *Mathematica*

Download page

Inverse problem is EASY:

Given: 1231928

Find X such that $7^X = 1231928$

logarithm, base 7 of

7.206957107766616386323701465694329662925565456980879196705 1

```
64831936445514484296737132458433022652098303334461251908514292315298512553903416621859592276076307799482097609958723358451791109978182289700786364863824648810145249985430601341479277669793832705651025815006255478759889873655454905090873063026581370116536275858702975014847204915700862860231833061
33455366592617835140131175611703893193429363165940695562319050607564687650319875859174000596171732116770104906655824875711731473680512360650469242685034259493290610884210138780183226197185982894639421900458669356734662773831558233635540572813236439369823939340502167087409590468011658820785778842
5868781748252365441466382277808813375660826088134041920001745915925179241690870852680759157014233254542183107477030640733571427076098557819329420982592997983577907943780894626667865215271095869971954642244073426179861834829928832200978239295797035084901220602367581404038998227763576977761855874
52277612961264061642537298318897323647352110247384346412108452265480755693154187956891149899825423642578017562975309655874765173766031742650101882593893037888231049036311592110401415054556297880680171667665383315898910824641434154543538600064351880165329257476831340356876666480479640466010157544
31884995701176096109574526173071495255143752351273096705370154719516955717243671362145664896007341931979420412942179132897157805583968725684928623686473418412333882769351338654757154430219495028393172415151723654090303590460463772947681359500334701565844945500525444903486768035692093326479688326
68291230987183536497490561045507737873655901049744409453177731644143965005961634875713289798641117535951475456729275590255698241577146690348309111990384362657633791910511801036453226923683401841628270865973153618310223959934456438388117885899480187854272770038034395422960510755045423709788584393
53108101890024887085210098472410484762660474113306337722659930715614663254696251755366961417019745364475814665752558651803635970627347334594531204720387332655352536968266297007278814066785763286686115088722021745763589065117966918221608219615889405412126658274259710708070043145517984831056822309
690192021794687796903333283369960635163252895203992640192671539071795689146403934802263878958477434807932559712738319551622023618836261903131834335266179590335515821669040302655533196031984852929774133989376723398202957122132498953725688362253386242489803030468186681118297113965053261054359806912
15777941268987258727860128126394037547045978570055011055338601677093422767716133888283378409820484220412949171117130638145241854536687292077522794372714827492955814059985113525113360666843209287910220166020934253919858638173260254765515190857996091876378401353053545110883123532400916406286413505
074757508178438472874735046634389596025530905134043562531464815136843759331085489079837769713111694092738570097841132412969773986438301314533546108361471934371282675948602416743706140297027465391346008597764909918122517251006223721329281306890029616961061433068257217371625110812356472475303420382
56310738643027014754938251536821341728639744418048908883980913711265710232997945552840814484237021554489466356335551238877754222823997822129081574027518056175016907536157252781437046987916810083794981337260518057489431738676661601564128200416186766055505062989829792030723902089824791141018090432
456567775910808153793753695189678184551823614421873013559375615580437185972823148829576047998707729784242728129465584374410112095202076370518778332840706646930468905139573766074448961239349408731807891817705247846619350244388467010087958233325673533355165424456811269729842981465285467841850640264
57008366691943029828692750803725634127806645988392987627783104362368417055949052999642344680534402129937746123183776164699408405419292159726895047811312909304479594186975112988187367137608032227832010660844543238232139091211743250866950961840720232753518733600672269258223622965326751665631587302
1305753781877466751434462285146541939978805120825442059217196855226324326648884995914339908757240134867052380361480665176861093660211161192929260778426113247559651259385314122895090572695332777928624667423419509485789507555508869973017282594580749537108503541235270480676116717339941833898243257
12258707335623319681724277021714513832885838400471357784138270315022714258886941806955561600610864075114018138239586124321554499179247445640040473940382330821976934816191285724845735014253759066405944511524445876297610125331845735820827599471093712131563818949295084201428822981430389615409883516
20208812082006794359867149157447572488936132332308339843744928897141473588594873097582926966883461552687570558999484891500751774286854746530916405004428404895237737559635256276742020859875572361611017272956597191853194826421651024586055198835788132828607421305117998244628271079481205148167786459
65204295377461723336941317907494267696155042684961457605434704954181061725176455725138995550123113045771256648006647247603329049383967794276727850246674341938497944769068120377762980746623483509321262984763547446896193290413770282464240809947925718810583152274558974681306196286546804183804584553
05795128833591914182460028544977040428025105228944383874814021276166660128640575086164105278321130387122760287279544635948975403883307474155540907004313577088323593539963859609557862498338673092345998088836686049771026003385672722262967093236798377448940924839830808532494232147183697713785313077
39846400872102419461411773960992788225962961276798183602539736495950862607780460384480382948355869368810561991104203026962331635707138610345717316559886595000024317612449956191815186989221266458656196131885947777084260437740608257107693246362823904952178486988631783620107188686080192136003873988
65613052964702437785578269141885747072965483773127395837821777702594544312140548413774254512401957383549522683760816306365030810445726373376801902196318563868898847905733582434685680781043387650705820872142306274905439408371119472432107321503659500504357718506020906855730855001837446324448979842
930335730538154793176264078478844462739936940334810560889013869204145574034266286787043034989156716230523870386271790786096882961363775089001613960113660994095958303179676334555153558652177937380986079841290773871994381802737922334326772669394183184652473429000853385154532488238441170239696462589
59854985634130188764032779803081984098976611696707697626870621068376359963144394043357765756425186145710178172230042886456701583796343518437764968250258055751902500461839723468309825997023753563446753091643566803879438011879903461649391646698316532760048063253096420226296824720632486180094231751
98183331056899448782970422756660111093548528263532416730214942527058934533659951138490044209179107867200964290111252096590104000133033612503552752294290955972846689933068098770411723440734978146662559599031654832797386666390645754581259819501899321430453254867288133021340475260965914664242166415
18356278389826914767288770146001042347297614475769345245332134644639670718838026224119393759899076423347006353317625195430902080005284149925627328221489858821438967133970914096381740189938499366460494128093949813096106697470393853061378820362931096688075146630078598162051374556260111694602216820
514343399891398597828367182143220898512744684099603984916555943795280017377613922566781108587109989093225893068338802161528096436603404391151045438992354279604151682826619507962698058042214226923606217761361312699697861222041925800931269315295640484942849888925321099956767251464335487255605472200
26479495010912935540642369304589061191772304256718499779219984174090262346814983203361192587923345466447636910276095146322855458502244389261979613140184891562146538344374108125455020687825490584605794292138838411157234429639597090657398883578272038585024757044198839872259196282933685141723227600
9392395494018277199166577633206376839068887464904411933925593848530164127335085843789180071309366754943402383766758661276167840347665893156585762152695049295995349041178429347183891252849721947240776889305910341107515260088494687370065986561790224088999012095853686396150899868624834046281291358
69011127192551641423043727042272076921109589594976528596935835810310750451212145342497200433761532477892798903246410450926639179315774753209706625970940878501155503060756926739281588980071084347240786740043672632803649159256110668229619807489682833935795697286944679547675750329503168335789873705
024196445254643969214982242521636934713748798425211381479115784785395342684674853315330749842622783307603886313622956730400615360583334397249503183451943104226584737453450390450798022483277788674126298747675876345393606741620938541197365215575432025820333470273799396168578491375370983872399951588
41977646846105258720517244932151581477866949075594930925228341512692916336127471885268052836575524215177823481205502471309859891643607482415745192874501976689194929667481306216093865748373238208141429952384567058799653894516369842792777905572130754433677198867431690451889716377928449630370037174
87996613260272036001766473704506604043145582657970224083505409405499092528206378604424270909393512465798326444278217846167012399192706457137211311171935400435139353143065219113887532244839722576298884785217917791166772724475831941750581121085705249180429060741302399334148930326718858268024738960
79852286523506185290389810048320424693044975103022867136385283306789589158285913398707409780615181100465882933583141507047817317219119206956447257366867693972402438740251804585080677002477231703781247399324100337614268218647337718048918704839016328165477633445278459142785358654995112470905661888
80849556271016016984158825879161568932520313935124499355400846353394263283622244587157922863303533776699384876927857878196482125681152981506326865509844502253732625677770676691715755168652833817369559610210046108830260829521506234984986564630346306191814740076122484667898234510659486796037288425
78069124892245805141512012017290266132835577283546865674058048242585418628737612873777073372265587527808307362797988062069931457747743500650070084328696662500695613859159862644528052826285725905787115554094963334500579072217063752804668061837312340592706954447061371268546850304405298657506877564
23169698675377107272802634467492589187780171581335161612072721776186231822517627434567666576849016051762537456273936721182197801642724422852697347308908149337102239221961682375774568173610057548962262075626740070369207155397821065714765948287601001037451620415449103013646184564599007915392663194
35358883397084905809163265045342340254886912164943307144337503949209888956593359708937170707357988193124911456210998933744900879521875306133929142569727046304921666158451125695711968324707102674925899289308359742475119679959250891310832394948039936537049352320788403707364322240152475901090139728
62308294650697900050457608654759906580173511522229530657023187721922630301422529860424558767607424597472675000432597969456958807775819574311326732913195921274613254595843155475867829953344050385290183297744037906669807126760114758081795036995481684472643157848556426654608300524936031655559659896
37470850591271992552720976247833236621130747843023337416452503253293593962974212267349091949706426202736453437823261130147782955425756904301025185889649104121532675204359864961342082684556133679649530962401491440173068635693596440599749074363170301305300965811724879837743637855794114563593785674
14586299684134282105439022338900274518958296029656207908379429244806882827997898118912647666450814357715958080807323264885235129121628886552818126829812464242329271514999777868680563019687631290929157767171601459409854696548319064924198599452562048979071186228203400764072957507445950201585462177
14240325085825178716228311469390083984278252337299391318540374381356351358174392077152708782780135515852493475668359969684351468855697181165887512870435422979507579009750836141703799088068420554219056391663044644838126137015896881979903861334378439317525580445976095237933836697129755381755178216
30610322835283537989564358453128920197111227664008052360454885288717454734639983317980511832868813836794287849711315136654781699811080896024693527815084965843274585768146912408724830461507161529354900003824985462563426151311902383569112945625317286967350656657522790338730115188066035990864549151
96726977203341118221927021014855502309466572949965697465661312898975802738212775033687972481414373496219236340256381570376610486610376501889801291043236445944675060145957458529401013804886564939448209138270688699316334913534956740595794875905992569616464767973525223310325429117795240815921761883
53820358359299397467667536678905981292822357738009400209629984616746150592420772076091678994330262729562951396616935557235141958583906591756938108095820670344619573220846204432365001211267716152817791049874309698013928369153808978615606958122980810976786754095847961288658345621242286327200431198
87187185890072281288470509250639399416082901297648803134823082962539418274394401721518689425840029763324560176966940752294313238839758260172967852270818477582459478461653047851345368457408589727461964355422258719755722841332087768660567739852514523608936387860951891855816162176938421041699480909
22877269282879720510325205676879543635610936273131752018678759008785136459531835310675469620001275656700789244345571870702262346872352609532767534276778820167198133345549614561854847183524765708892952008308936692551348960685325174316902425963938295358159794641086873040225758611527806648907908035
7335524645515263825448615357595248766183956935456116972223637475376469138658585561310065566229305236394545616623249793391180590980002634387864800293220238602110585992049223546353863801218698714349613177849901610057055208519132212782653469683758219785472716242072291170544514040610610652593609468520
10763136992839157744676167257144679203101264443770725806755566305998140969972919864345460338795790315043417761545200226994252583096086787010251056986151341912373937481633264284463282979097305736353453648700821548220873079921845934988250743870655335719101453120721144800793609022581324203172179137
47747485630525866432941602334253520948659363728118339836725412709177498353534793968565080845280029785714033646572862308168339893559254593533584410519868394770171921032316982737575470745953493709629785261970477309783611595641408283980814965268138125081918935647135211796798632036790599400949886536
15871531662063127821501524918844407099064758151063901408418098257666814634781254497212605142889282057502742566242165633041340338122501931231910632586110228418015048026889814608767926294374040886029220056863122800223540523252301692415392342298741201751672640933861164288084642653286074443309506352
78358965716530968540131707806249382703964140772291651531365245260108651959004205791754042668098962443907535001162287719334021967637481619783768948768370393657780006002502678507641810526014260651666094632359605538230721144002301904079258177508824303204837770919490933025853592858630340719725863004
47011944323441942658284826395476187697354850211273322220021346592018048044207302190084811057882073812132102008038436356113103725306622408704339956014615182065369269457821299092164144325424679336760195747040900507886028285463765837565755281780038569751020514346177862450815213554473200381480013925
45285090395787288551056503347087143533012586871389703766959802630252097433885018168863471740613901205851547506642729879806816030794702391970090692876771203403300388565212167700525785129853280191867453875442738513943052148664044211275191876852856032773158861627319330477774338085063926714997721386
74359710863604952510921005891701623732689896530911942046611079903770417889010720192480286794174238554395881795503729796045503381998735763344099378724410447405418301277878716344750315322688298617968796452958680180045054137549395720318019933837538361458664658770270876564334930693460369756382500409
79450055265281628417625438601188553058588513181137091824452428069216107299746443122272343943636835106119218944689813973429773373121110085663209462368825908788660630170497925170116383953449289832156934707759421689662420131530602669222053349635528097836303799440927049162182945885279665682433077451
72761011522340662297402744750029300507441476468990213931184155485168582273085340524305765767861460879023313682916310995540434466614213860686150793200690365314330310604147127288027730344588409965057799722337497437003066254872956874302737349247127430873663261002661636227797992554157911565603939816
20939298804989512791777703999420967673837590999433391838124126051054245248462117101466446897110547648459477072078078431794784389089474658865177442001474362992843685823308636078603252824775949649163477789362801062619592679110844074329784248624601932467176434431257323456950386355542040974763127428
2837530293580094584406733057318967924249582916555085715142973714301595241092301050009749001187742813303707637694815456081175737429935539751370210374784131558875556551657889931054167665426361280606397731811510324258366325483225471695199190226810279887670883645945278455254575728291583007618652346
48428739126523579088961606988709999337646307585416542318910349001412792947801679784982502028497161790354771015519121630739107837135227100950386145810612067983385976485054552921568454767904747954996098279282441198695878974790898043897488413752133288282158049995649074982923255375827943254106858769
47833437970093823018846516250274284730266582560120791278267840544221664443725969035049857276130258897085271041316639212114445429390321680215148623958902450395312754442921124077159174016690970787789118201558301328159451164302232726778668019604867033258676631161848206102198740931031433567872020225
60655476278364447625502997964131972773930165020870255525021118542282926383876262364193939300732051144870300324473946980782109321157837251510157240639821558111798207577102413442692391646769498492855666094356618401823688696829143815773484083518852915062875737929159300698933601896412609941693308053
82148298356991564853531877243033226215805404902776694590616820357857636275908452534419885321299909700331871077711307245188283185622582584774781093743148499626670320308338538363969012207863096576755761315442492837926891249944094786431955042489192395148450505590640278731615331176327525632093074952
14186477194417948432251833153434027680358625675385569029721917730620377025274858684718981193142241982947259557558826863746260938086662475791346427440039894294012434822956077625394907852392163046887519874543353985846179284416703155183058228538684309143887843892878396080883035691487079141373521429
00795157240433007313722486859370462382596690547611375463323672447814729656250090749498903564319195950164954910976751939991777350709368222665402248619925535331926584461295130174148808258980923055371375243641254416739525915194565078793637177046335453005901032143773182922338906723599463637291957557
58397887644107471900432202511367819686937736631233689565059243386931261151872215756698734483539633791369738003428362218539143868806121460512386198753614680453176676043232155708649066139530106434952273271227928797937847208245573672136014330817641610259366081845326003033895054364410167882676726568
28136560890533032491572696595522163274962773145155338222102950736977026644866487696713465794875416848212438929556683152068947948031513872617293902437619133748543137265971885491798177005088464119393136057321914703656061599593016715996032980189538151219758809793561308328681669139710807435736119626
65359616220647422975813809585865183580162618071296061518145594203361716105066235850478737554000285593950965907349160434336489473339465391673636632757868347576989393114904771592720715317725618703509518219930446121542729426843365614587984789864924305684439396905385213168436963391579012245350009801
33645078925874818662651956911227386032468938982083788785432866087405632792037155814498966340592131006627194688623512809473829028598582426871030045725895771256052347283230219390841390316451012320908615045751382388694750449282211183378528772798836725834489915631992602593060104535992583049434682245
22689980460286489745199547766321711921976739109818730209772268949342097824262046591456734755597646452421192766995078402137825114000192147664571979763487235549944352486721655436674977946331170059821736704695667834928870342771376064139786755188152063063717908584759827701277079896930471979658270674
39861090351882945741400407418524167258979428464867490233757440378859634442201261866239655655815918593831995366931703989192247248813968410233870608631812708677837269209227859998881690913910976766622022562281532000268563382734443181258968713194215289345210819775008222880215781539306836202283008384
90269263146708339214426392939524208892427434239490648393167072142415435805590678061223217787530043845837872294097971868852441885090738120718953678333109705638200661470040653875974682649868970486997503184394617269174954692469232649404677206264761386297164469820377921008311465079538615897606515290
93165942933662120863576730345979089273847936366910572183711437946275862357965900591372051061271031111490583828472267826809564835692643476767327364804242632424017916261231438072541499474173607968577789791623336832846344843889797500202472877896455127802833918090355053193585813030671946616260155740
95136536942102116754509323941552674372311218436130371523490636475090641252030913634253996436591272917544810811625063828805085991231004847928538116413442113861262777328572591736760593442592715731583682279758427567424236031056582101954627346869186286479408477369072830712779146543823787469169987293
94598684997171429150125025804080163244249539359767116284760855384269271087049492875751034557821802017815457542877164940361678577433423209649604527114484279465030730492310119623615590581974726719103758305891688166885246416800010878023062423058402530227839874394422995062453106763469447254688830036
34956472410955903557592275728435303449109626897195470035587178642925543905599847657356030978743446114150514884977248044559651208023639961425220001653694407971844057751655739659880862038337184976685985435930570489022507987008286055267100351084175139860293750455821743272346097401736282917091219506
79145657628402020109598010671769462167993092535113179138805655966444956263493864980212393529397704558729435226240708314662774878456426310771985461180278665568593977417029521373609018058131781391491759411553540945789604854600942957684548562205809872644807960125214456901258625326582373989770625579
75135075203394646435118330672087335416178903184894923829664432640487963271274021831488524194682111423324044202255697622503545025826471506264823412735458206324134600126381320789166720445778318182227033538538064098665364374459254597750085992853576034192086109686839823513154287019280614355388545827
27630293654546617518134855197673128285382476014050720927662757930949078883456665384901799977783548417747027426334146884568255163407549368244716331716852407925421651154471351895838436834488629983274643052234159645940143820348309117746301353495895205060709472035322652515266805056988311351719577657
25885193852225027887541691387196876435029576983736103574280896861243580062399650250765056706721968127811688670790833407245968537880718219031335243193059072546167696746601212080526588588986707417907829870337811206055002668507190583715719566005421196581969073343761462326936373167536072708300163060
77161848158587502186760366333969558668963983003788420972748764413391700548198665270070837912968338205038468744936453130537931763179013928709714805152038994070850963782000356145791452343751358814049237961385712931578647876093856870272917440950550132189892607760888610404504221340178154247878591931
09872352647462740051332834605369178895526138491792163654990546695596366586463172566100097875436805839471854776099838763353975864145057593907668041031063102589953037867257034191300511722398662464721073430033747747337898770181478590915059965325845560347386120771324407116858463868277341987856095087
94288701668322550915040882084312819176048059542961355281670198621566596343971361430369279120748290551566205181193556685531037788771844143606445798920321039355957817691674020822900530402916153423221733021807006819446190224965322295568296562828657258607176517001955824274474326460047986044510377515
89490964379182252120684959377219350828210980685950530619255249792894511373996829091646680566841906914328706900485827882435571455280939915008861869586387008247643058156017916244667591053799470169488165124172849367434925045270858613906645932272815182297306868580842349749762435357382224755791800900
50464117053519759163150201375829498743899079257668435828972296930550737236279882629852150829408797296129393672472906682534883252714994695597319832163654949903114314215750590826404782057913709785118360510832962935327742530856494053211914263771171812918225340159592328711719843135096017670815387493
156721296597065124949995939514699203071222430133433126017923518786157066778317533952506581383481973786643975987585213814866397223492928792756260239616941932390160207191212886371511936194266870415793966044917419504985161701085382538814230445955182637728355283096635593948186964521054695316997330155
07040449870825396265246527498432866237932736995429113720613979603015659112002786522510756198998699116260714428938958075981046064384957533712647721676131951717230671711126648479570192338948178778301926588342774327212769444173732431404262596450119522348100807247511465397611266558931110803344848441
530946421053322489329018611244042452524793927980618250149676231153119539301216991848490370825053955586391715447980139944119053476893037243069223787988187766860288187141095444581477812551397178820901210706772761656654573550743381757626262650846787393583315446698197370321444728901428951047836757405
3127730977210647258721325466365761340167854254394152204960813051611687176440364890100719185706930366332976153072830958163346881230542635670793278668451747508371521473377454323652243159734514559074675280702015299941442327232511329565350758476832849
```

$$f(x) = 7^x$$

Easy

$$X \qquad\qquad Y$$

Also easy

$$f^{-1}(Y)$$

log base 7

$$7^x$$

$$\underbrace{7 \cdot 7 \cdots 7}_{x \text{ times}}$$

$$f(x) = 7^x \bmod p$$

$$7^2 = \underbrace{7 \cdot 7}_{49} \mod \underline{131}$$

$49 \mod 131 = 49$

$$7^2 = 7 \cdot 7 \mod 131$$

$$= 49$$

$$7^3 = \underbrace{49 \cdot 7}_{} \bmod 131$$

$$131 \overline{)343} \bmod 131$$

2, r. 81

262

81

$$7^3 = 49 \cdot 7 \mod 131$$

$$\begin{array}{r|l} & 2 \\ \hline 131 & 343 \\ & 262 \\ \hline & 81 \end{array} \mod 131$$

$$7^3 = 49 \cdot 7 \mod 131$$

$$\begin{array}{r|l} & 2 \\ \hline 131 & 343 \\ & 262 \\ \hline & 81 \end{array} \mod 131$$

$7^4 = 81 \cdot 7$

$$= 81 \mod 131$$

Pick a large prime number, ~200 digits long

p=

```
52061717268811022582985085340962890043057948799610254543088975844032721944045806199348262783479007502882378061899682808553821447440104558871825720697952817636569237467061923678480735550795549941664404569955484 99
```

$$(7, x, p) \rightarrow 7^x \bmod p$$

Remarkably easy

Assailing U.S. and Kiev, Putin Keeps Open Option of Force, By STEVEN LEE MYERS, ELLEN BARRY and ALAN COWELL 56 minutes ago, President Vladimir V. Putin of Russia on Tuesday described events in Ukraine as an unconstitutional coup, expressed contempt toward the United States and said that any potential use of military force would be a last resort.

$7^x \bmod p$

```
sage:
power_mod(7,661615980609061103328546834632981100327606021844328118170610327602021315328013021032801317061210331202327112150001443267213283846986697832766969327789698283443269767669783266658282893298110032657665783267798769767632535433100611181702153298041144328115021606010211163287089801061006143286463281181706103312023283181616059733121032851802160098213301021600150599020033021902111715330610328608149806110132981532981033181100121116170617181706121098083300121812443302211315021616020033001211170210131633171219981500331705013286110617020032841698170215329811003315980600331704981632981121331312170211170598083318160133120233100609061698152133031215000133201218090032990132973308981616331502161215164 6,p)

497929711688584217527863332300629329098654983269423357729595289026203941126793387158661751180509701235256633429962635553676002083869590769727522267027725835398089223356845936769316025070772103626851899346393242 9
```

$Y = 12345$

$$(7, p, Y) \rightarrow x$$

such that $7^x \bmod p = Y$

discrete logarithm

Incredibly hard!

World record in discrete logarithms in GF(p)

232 digits (768 bits)

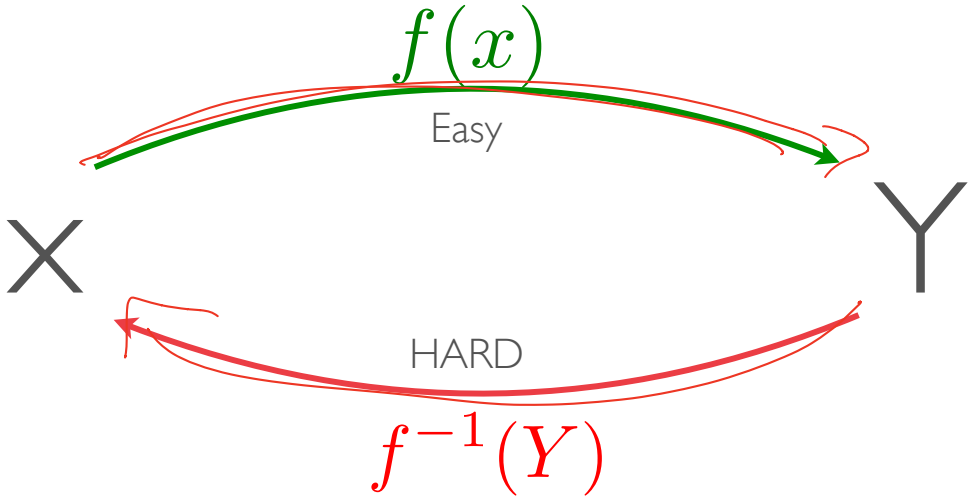
6600yrs of CPU time

Intel Xeon E5-2660 at 2.2 GHz

2016

Thorsten Kleinjung, Claus Diem, Arjen K. Lenstra, Christine Priplata, and Colin Stahlke

$$X \xrightarrow[7^x \bmod p = Y]{f(x)} Y$$



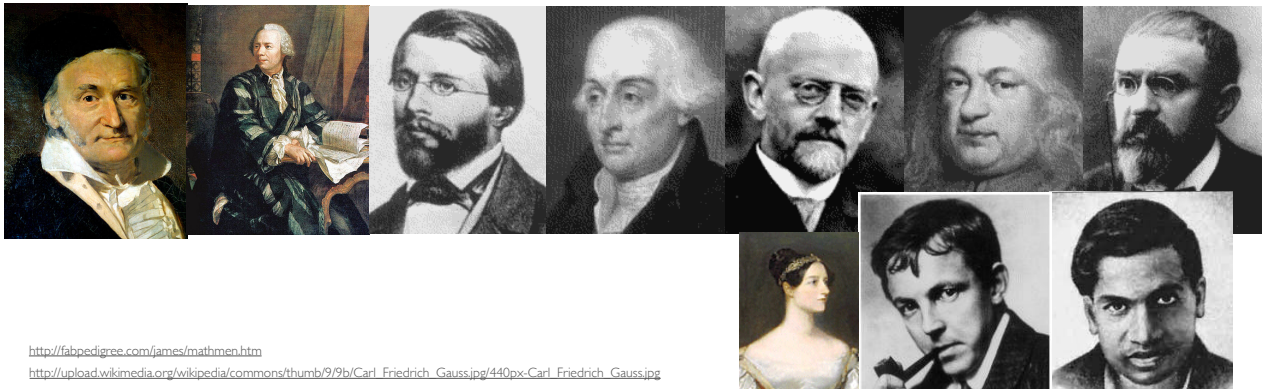
compute an x such that $7^x = Y \bmod p$

http://www.fitzmuseum.cam.ac.uk/gallery/chinesevases/sortingfragments.html

$7^x \bmod p.$

$$X \xrightarrow[\text{Easy}]{f(x)} Y$$

$$X \xleftarrow[\text{HARD}]{f^{-1}(Y)} Y$$



http://fabpedigree.com/james/mathmen.htm

http://upload.wikimedia.org/wikipedia/commons/thumb/9/9b/Carl_Friedrich_Gauss.jpg/440px-Carl_Friedrich_Gauss.jpg