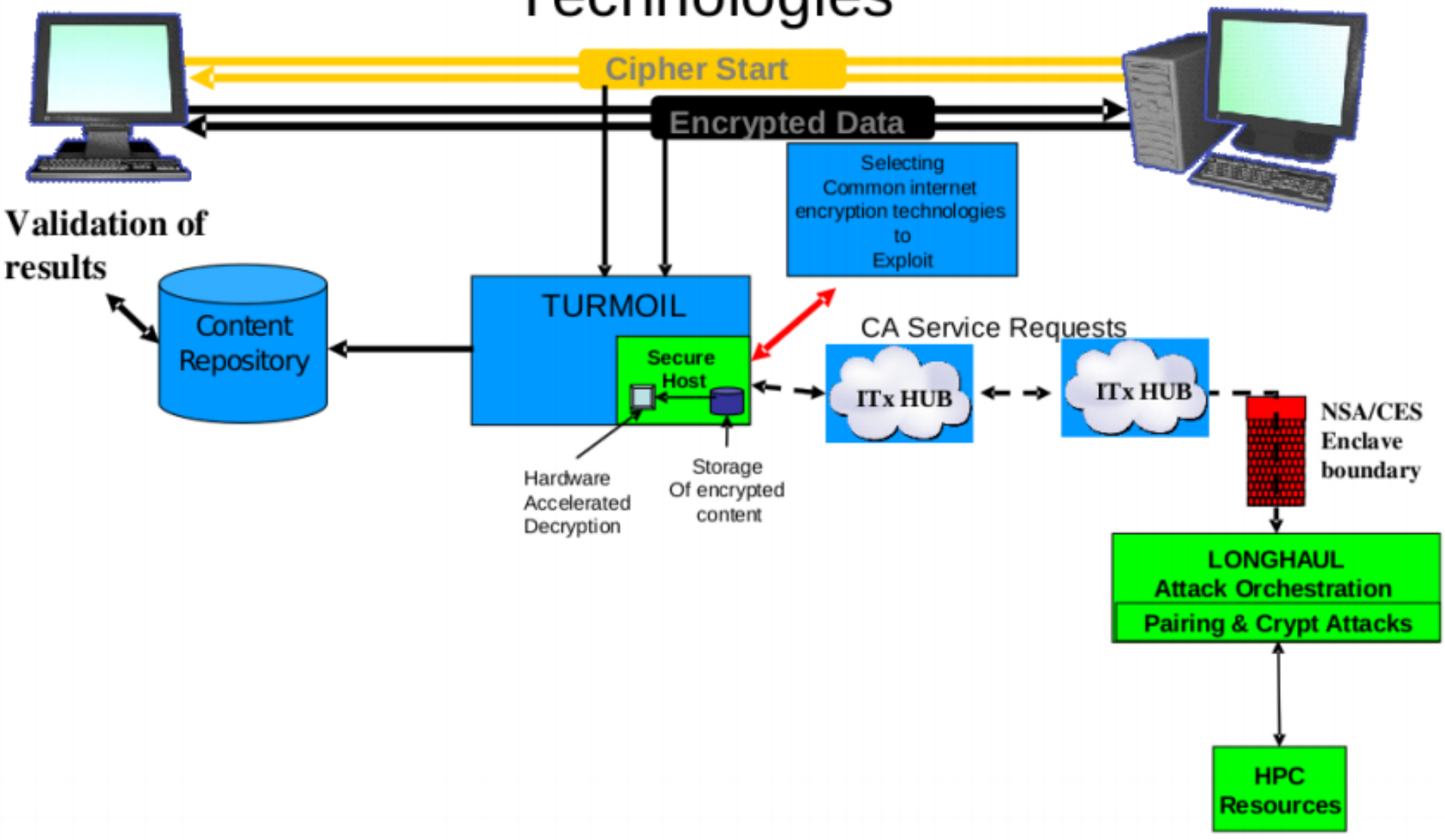
INDISCREET TWEETS

J. Alex Halderman and Nadia Heninger

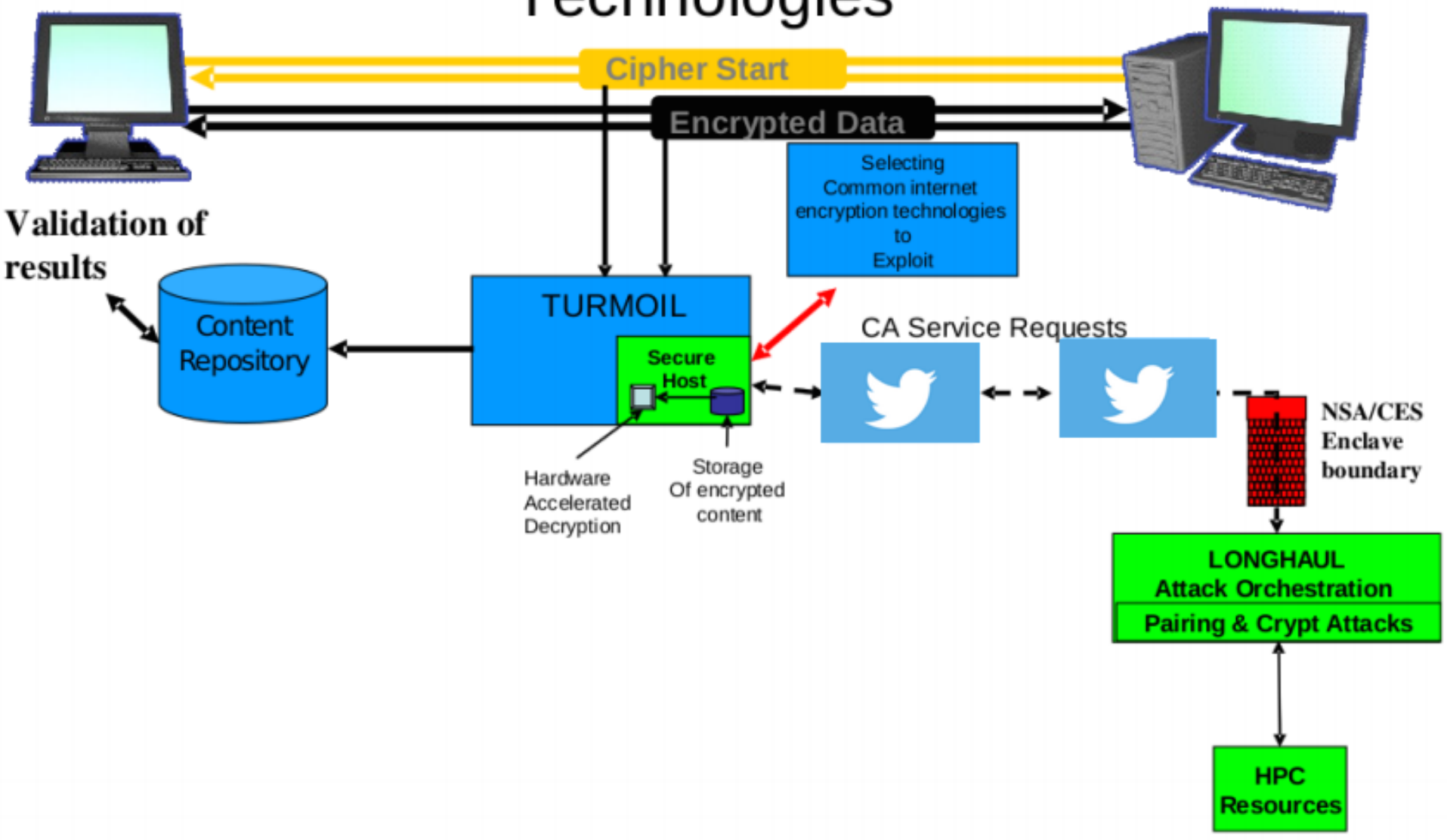

NSA
ILLEGAL SPYING BELOW
StandAgainstSpying.org
GREENPEACE

Exploitation of Common Internet Encryption Technologies



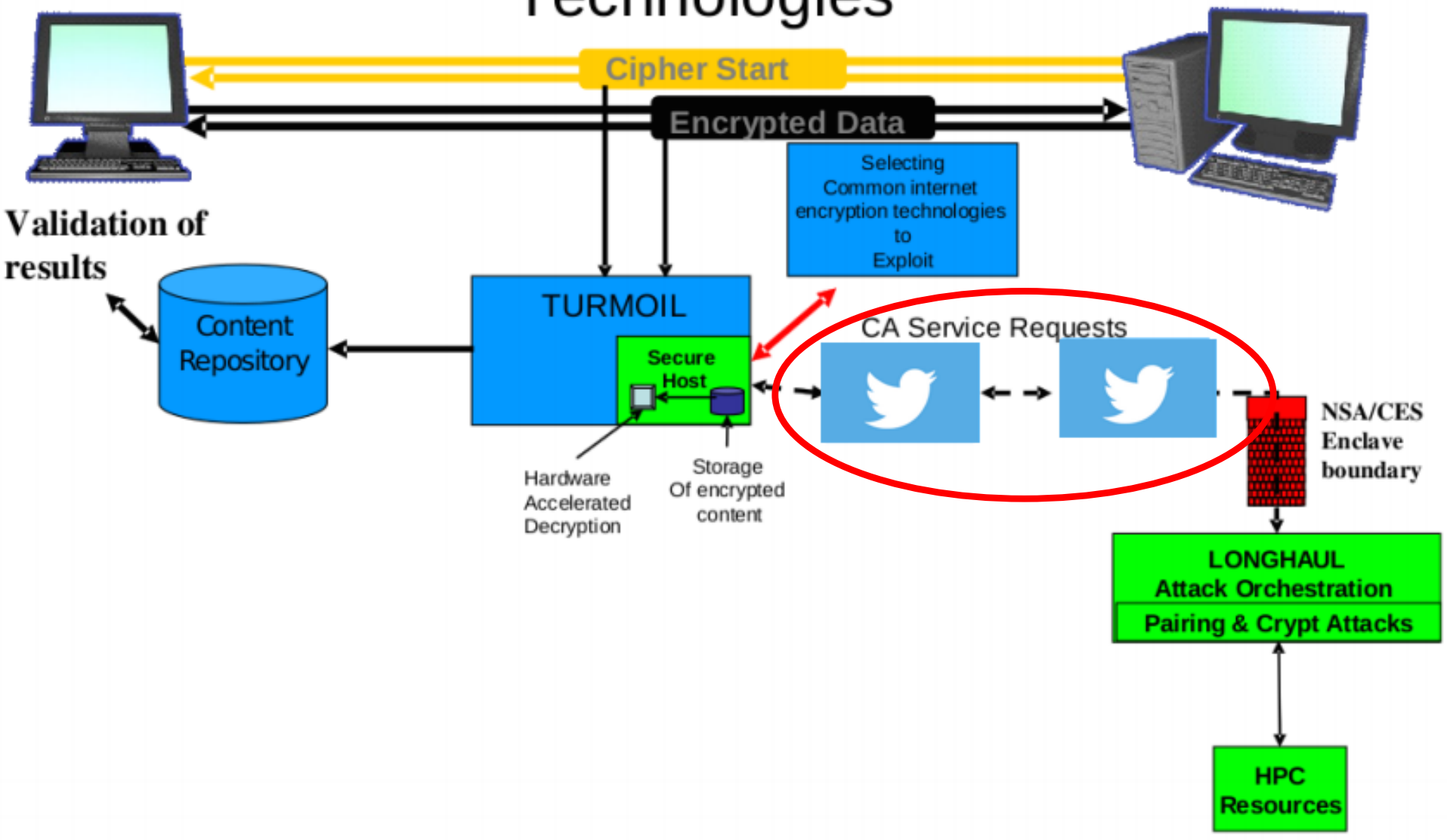
NEW SNOWDEN DOCS PUBLISHED TODAY...

Exploitation of Common Internet Encryption Technologies



TOP SECRET//SI//REL TO USA, FVEY//20320108

Exploitation of Common Internet Encryption Technologies



LOVELY HORSE

@lovelyhorse OUTER SPACE

Unstructured open source content for CDO

- 0xcharlie
- alexsotirov
- anonops
- anonymousirc
- anon_central
- anon_operations
- bradarkin
- CeRTFi
- danchodanchev
- daveaitel
- dinodaizovi
- diocyde
- DLogBot
- egyp7
- GoVCeRT_NL
- halvarflake
- hdmoore
- hernano
- JaNeTCSiRT
- kevinmitnick

- lennyzeltser
- lulzsec
- mdowd
- mikko
- msftsecresponse
- operationleaks
- owasp
- pusscat
- Shadowserver
- snowfl0w
- taosecurity
- taviso
- teamcymru
- thegrugq
- TheHackersNews
- tinman2k
- VuPeN
- WTFuzz

LOVELY HORSE

@lovelyhorse OUTER SPACE

Unstructured open source content for CDO

- 0xcharlie
- alexsotirov
- anonops
- anonymousirc
- anon_central
- anon_operations
- bradarkin
- CeRTFi
- danchodanchev
- daveaitel
- dinodaizovi
- [illegible]
- DLogBot
- [illegible]
- GoVCeRT_NL
- halvarflake
- hdmoore
- hernano
- JaNeTCSiRT
- kevinmitnick

- lennyzeltser
- lulzsec
- mdowd
- mikko
- msftsecresponse
- operationleaks
- owasp
- pusscat
- Shadowserver
- snowfl0w
- taosecurity
- taviso
- teamcymru
- thegrugq
- TheHackersNews
- tinman2k
- VuPeN
- WTFuzz

CA Services Test @CAServicesBot · 8s

@DLogBot What's up bot?

1

CA Services

@DLogBot

Following

@CAServicesBot Thank you for using the CA Services discrete logarithm bot. Your request should be <group (a/m/o)> <ephemeral key in hex>

3:58 PM - 12 Aug 2015

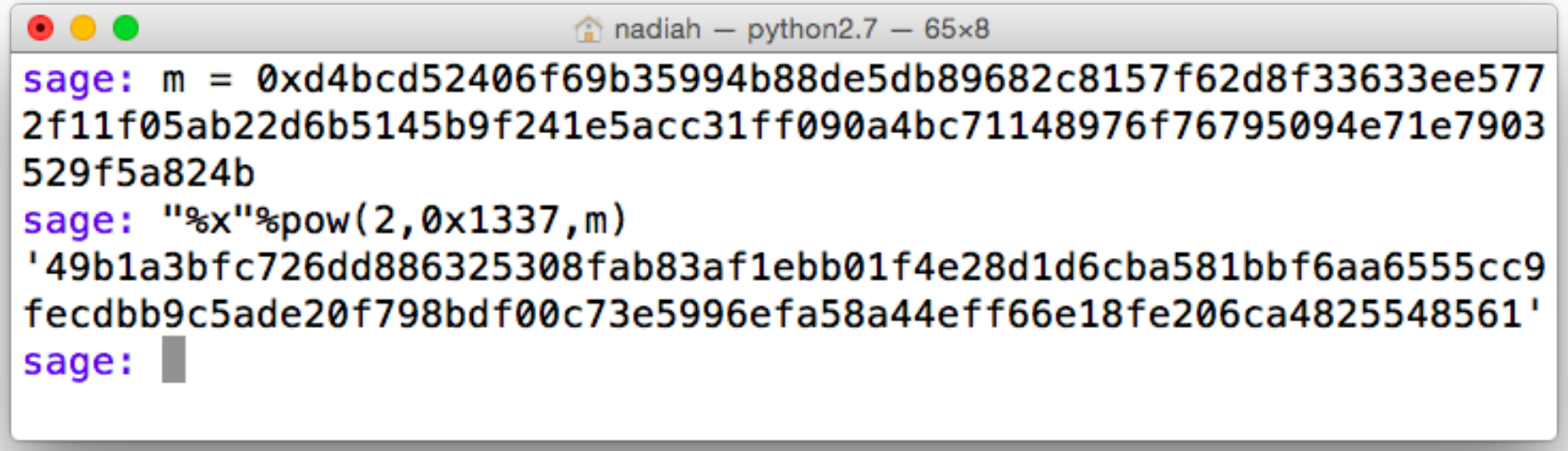
Reply to @DLogBot

g = 2

apache:
9fdb8b8a004544f0045f1737d0ba2e0b274cdf1a9f588218fb43
5316a16e374171fd19d8d8f37c39bf863fd60e3e300680a3030c
6e4c3757d08f70e6aa871033

openssl:
da583c16d9852289d0e4af756f4cca92dd4be533b804fb0fed94e
f9c8a4403ed574650d36999db29d776276ba2d3d412e218f4dd1e
084cf6d8003e7c4774e833

mod_ssl:
d4bcd52406f69b35994b88de5db89682c8157f62d8f33633ee577
2f11f05ab22d6b5145b9f241e5acc31ff090a4bc71148976f7679
5094e71e7903529f5a824b


nadiah — python2.7 — 65×8
sage: m = 0xd4bcd52406f69b35994b88de5db89682c8157f62d8f33633ee5772f11f05ab22d6b5145b9f241e5acc31ff090a4bc71148976f76795094e71e7903529f5a824b
sage: "%x"%pow(2,0x1337,m)
'49b1a3bfc726dd886325308fab83af1ebb01f4e28d1d6cba581bbf6aa6555cc9fecdbb9c5ade20f798bdf00c73e5996efa58a44eff66e18fe206ca4825548561'
sage:

Tweet to CA Services

@DLogBot m
49b1a3bfc726dd886325308fab83af1ebb01f4e28d1d6cba581bbf6aa6555cc9fecdbb9c5ade2
0f798bdf00c73e5996efa58a44eff66e18fe206ca4825548561

Add photo Location disabled 1 Tweet

View conversation

CA Services @DLogBot · 5m
@CAServicesBot
9fa918b3beea9b3a1d564d5656b0f2f20d4f05062eed6a9eecf48bc2119
e0d41be1bd418b29e4feff5600645f5fd80bcd71190bbe6cf6e592be513
9219414

View conversation

Who to follow

Joe Fi

Maryl

Kevin

Find friends

Trends · Chang

```
900755693880224784181826846280507 89
Wed Aug 12 18:45:33 2015 Deduced log of (470366623, 338113733, 1) from rel: 13237548435244169244143100182094873380360838654192799064225833828132022218196575848107253557044684872978237019555315126021801420268766874662578866567740811
Wed Aug 12 18:45:33 2015 Deduced log of (25962401291, 20249792848, 0) from rel: 505633307374159604150495753286374600982496989595759740618770110704480701624053426981957192559057945796090106755289534153710885079574744434237737252424012
Wed Aug 12 18:45:33 2015 Deduced log of (152250701, 93107759, 0) from rel: 368622813850158283152826798929907412284902377185469178829870371289144771591876492349659700969350065276910486022078530561941461460445126822792313541759652 2
Wed Aug 12 18:45:33 2015 Deduced log of (143560981, 107192704, 1) from rel: 307860298231873673521041039296250709974237070003579136705638665216739899169781455078181073498093656533016603801659935296931860439561657504329645695298987 5
Wed Aug 12 18:45:33 2015 Deduced log of (278147959, 4410170, 1) from rel: 250568495748563924992223084465769388412691186709473708889010485389673852742627612820328323174655027075651009937568594328296740001105522457321813526033020 8
Wed Aug 12 18:45:33 2015 Deduced log of (577776097, 143348514, 1) from rel: 442338900520785256843955526485021247124215862664804946530253545141243702700937987405857426583528963422304799351630803791913894065413730465443510800769091 6
Wed Aug 12 18:45:33 2015 Deduced log of (418914989, 316721060, 0) from rel: 367207948543056444750000809717878390413543347607219059542512916467040252344925831757084814255582491568962667272894312894745432354830030222594946416351771128
Wed Aug 12 18:45:33 2015 Deduced log of (338071753, 301777175, 1) from rel: 107520094080132598180876691823882310946126491164966924787589553472432468656483029744406591626920263170944975959228432814632855732906875574159648657015326 9
Wed Aug 12 18:45:33 2015 Deduced log of (334373141, 196775704, 0) from rel: 295924098567118682024550377212916862876453441769461426617303202625502622200306437293865652865355209952938669043254101956488326928215586243832945368451306 8
Wed Aug 12 18:45:33 2015 Deduced log of (85126349747, 78086389814, 1) from rel: 272008891507334686458442924203233155691323232288533240018774772348710672437432344405421003034049598156144493564929239372773533486332215126820403976503407
Wed Aug 12 18:45:33 2015 Deduced log of (61692766831901, 45737121448216, 0) from rel: 950385701946810568492835855519755175335271777937141287749717580863420767092852870952282318514359529666745662554115535892794666946074238694583128167593602 3
Wed Aug 12 18:45:33 2015 Deduced log of (206206811, 193918773, 1) from rel: 150129281584625653670608607473569366162828241135446571302979567882130921962371540905953102043599924796633201952837388941979655233459332812014626766068665 66
Wed Aug 12 18:45:33 2015 Deduced log of (226880903, 205068533, 1) from rel: 536845220976247216070823275266198080149544131379113941538069691920397796698875020561335789576215785486392872542467451478977409964811844057396299029579 51
Wed Aug 12 18:45:33 2015 Deduced log of (292902821, 134190188, 1) from rel: 439445138364582159970955146631236342487943352438465485528919566060271737879221218557114979606253028169269932103194756547132565957464751660244704990870 5083
Wed Aug 12 18:45:33 2015 Deduced log of (1307702399, 951504975, 0) from rel: 388412984539454708054236165551175352347925108926611462668495683292715649026161881839025602408585455677091772199785578032896317573836498043317135746913601 0
Wed Aug 12 18:45:33 2015 Deduced log of (202009439, 132696313, 1) from rel: 586746728022223145407986515759301518747360666540921337722240732928530330678243336945997816779047558926178822228470304876293629942892685459127281244685422
Wed Aug 12 18:45:33 2015 Deduced log of (277410803, 9791152, 1) from rel: 225900191667372239717508053757873005106976563413582561173459642209893512269377176143983896388166851314560890572508498540819037064719778284596654350279821 3
Wed Aug 12 18:45:33 2015 Deduced log of (5077939123, 4652063990, 1) from rel: 4700476107471785387546249836018003783883820730918635794744673497035689116025731296286088760225494958896998096151611592457429278405080150250145357601977064
Wed Aug 12 18:45:33 2015 Deduced log of (570419228219, 397375869245, 0) from rel: 3255654853015642854084419126761488294889128335840284315033305299124899394204172237584087433608546207517017017002433773924631799147022786959354304587524964
Wed Aug 12 18:45:33 2015 Deduced log of (149460671, 53992188, 1) from rel: 2651811832073407132611177858759137310517057082625851781864665609907080436715896016549107955625430256337426585266782281625402584417872997921002003028988191
Wed Aug 12 18:45:33 2015 Deduced log of (1004549233, 320473819, 1) from rel: 4364592475872277799643025982830330362613984403493365342236185699223330907782331434167819646594219292852478453423087536704765635181511493534233116851018079
Wed Aug 12 18:45:33 2015 Deduced log of (500400001, 21453686, 0) from rel: 1824485543248714996126611031082238658686942161900511996641160312138508104939395699652788432709468236780128943689748040801275264279266440000948459876830721
Wed Aug 12 18:45:33 2015 # p=111419736167993051826721259538215396217898638646520821894844183837557977265003942122273143385094102252406211275129135279721296280500639181169859831840446 19
Wed Aug 12 18:45:33 2015 # ell=557098680839965259133606297691076981089493193232604109474220919187789886325019710611365716925470511262031056375645676398606481402503195905849299159202230 9
Wed Aug 12 18:45:33 2015 log(2)=47197552632340568686371246544797334661553247954679670451641942805650991309645074077087810506576181574948593419547569918183935151167199904147667669979273 05
Wed Aug 12 18:45:33 2015 log(3)=20495757144121934877222047902663003624011491743961240029434474987370825650259443439987285179799353725777366586067257147915224641099414699956801923466367 33
Wed Aug 12 18:45:33 2015 log(7)=56085170553927017859636655668265525368994714302698459590550178723216657331070298461703411206941866056867006913261115179252433760356477128350339490874729626
Wed Aug 12 18:45:33 2015 # target=385966297662854851100984432444339538413671929321908207345189346625768237659353266583704409102443785749659034063226219416703000988881604865261883330006358 5
Wed Aug 12 18:45:33 2015 log(target)=21741092469733887286417505986311180188613069043166533718859635445180620508405973438845639004675124283789839022943072247456208168374594534974308988474516 92
Wed Aug 12 18:45:33 2015 Final consistency check ok!
```

CA Services Test @CAServicesBot · 3m

@DLogBot m
49b1a3bfc726dd886325308fab83af1ebb01f4e28d1d6cba581bbf6aa6555cc9fe
cdbb9c5ade20f798bdf00c73e5996efa58a44eff66e18fe206ca4825548561

1

CA Services
@DLogBot

Following

@CAServicesBot 1337

:45 PM - 12 Aug 2015

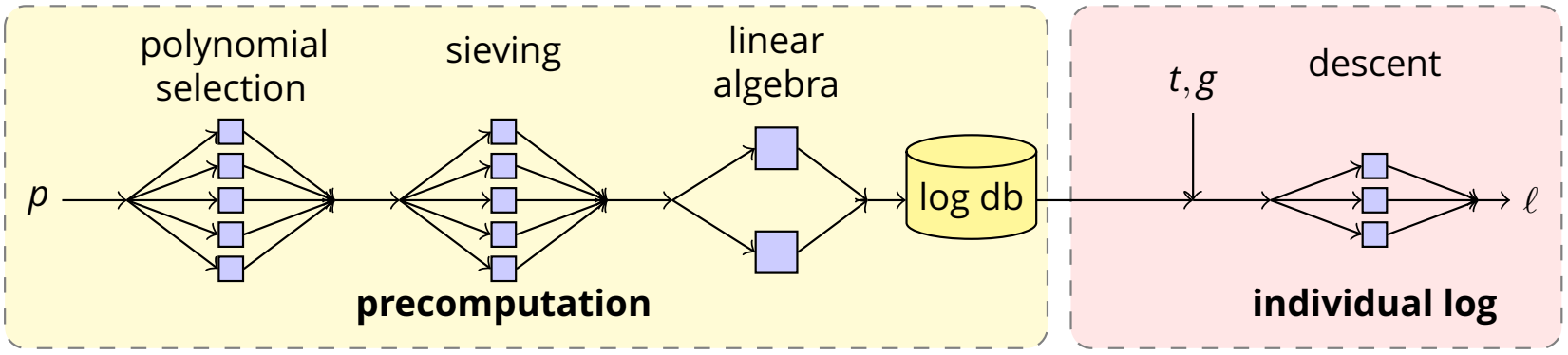
Reply to @DLogBot

PARALLEL CONSTRUCTION TIME

Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Barack Obama, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann

To appear in *CCS 2015* `https://weakdh.org`

STEP 1: RUN SOME 512-BIT NFS DL COMPUTATIONS



$L(1/3, 1.923)$

$L(1/3, 1.232)$

Times for cluster computation:

	polysel	sieving	linalg	descent
	2000-3000 cores		288 cores	36 cores
DH-512	3 hours	15 hours	120 hours	70 seconds

STEP 2: EXTRAPOLATE TO BIGGER SIZES

"Also, we are investing in groundbreaking cryptanalytic capabilities to defeat adversarial cryptography and exploit internet traffic." – 2013 NSA Black Budget

	Vulnerable servers, if the attacker can precompute for . . .			
	all 512-bit *p*	all 768-bit *p*	one 1024-bit *p*	ten 1024-bit *p*
HTTPS Top 1M MITM	45K (8.4%)	45K (8.4%)	205K (37.1%)	309K (56.1%)
HTTPS Top 1M	118 (0.0%)	407 (0.1%)	98.5K (17.9%)	132K (24.0%)
HTTPS Trusted MITM	489K (3.4%)	556K (3.9%)	1.84M (12.8%)	3.41M (23.8%)
HTTPS Trusted	1K (0.0%)	46.7K (0.3%)	939K (6.56%)	1.43M (10.0%)
IKEv1 IPv4	–	64K (2.6%)	1.69M (66.1%)	1.69M (66.1%)
IKEv2 IPv4	–	66K (5.8%)	726K (63.9%)	726K (63.9%)
SSH IPv4	–	–	3.6M (25.7%)	3.6M (25.7%)

weakdh.org

@DLogBot