Q1

https://www.mobilefish.com/services/rsa_key_generation/rsa_key_generation.php

s4010423January

s4010423February

s4010423March

1)

p=
fb9ddfe3e18439490359761969b6015ceacfae408eee0ed029bc375550550f25effb28812fe97
82ef6a8c4e8e43fba95d69782d628498ce5d042440a9b02869b

q=
dceeff6d1c6bff190218fe003b88c52581af11cd07778132f297a9198e6a635bc0f51188ebc8d0
3329779c734c4dcc60300e1cd4b5a7895a796d580c4a18bb55

n=p*q=
d926943b7bd5060612867cb578d6e21cf2e6ee1432aee6c7f50643dfb5b670a654c47f22370e
f8e10dddb075f0c260ffffed421c9a51917bd41e3cfb82d61a85bc8e6a831b9d21bb0b0846269
0c6812ebcb2e0a2c954d093bed09d702f1a5fbfc2a00d7b592fe55f68ef55e1340daa2583486f
c18366a248b4e43129bcb1ea77

n^2=
b8326d1d2f6cbc74b443b09d92f7d32372786b98079fbf57f0ec285f9258bd83651932b97cc7c
ad481c2b25c80d165d5786b8ef91773575af1903dd919dbdf78b0e9114f7eb4b3f50ddb96a3a
1cabb12f850667324a52ed4ae3fcb615bd45e4074fd5b2bc04687c01bcff28083f4d902fa2b12
111c25371f1615693c86e858fd426c221f0575da7881deaebff038d9e4e7f95a3d18bdf54b467
5c3fa8f82b7439314a87da193df8b82ff0bfd2527f65eb562c683391fe68ab22079f3f5f86ef0b91
6d427402a06e41898fb0ce2c4b2db942ee48b0f4ca9efb9f8b4eeaaf317af0401d2e5d06ad227
b5bf7d94222828bf6d4d58003ec9ce9b13cc7422d74bc351

g=n+1=
d926943b7bd5060612867cb578d6e21cf2e6ee1432aee6c7f50643dfb5b670a654c47f22370e
f8e10dddb075f0c260ffffed421c9a51917bd41e3cfb82d61a85bc8e6a831b9d21bb0b0846269
0c6812ebcb2e0a2c954d093bed09d702f1a5fbfc2a00d7b592fe55f68ef55e1340daa2583486f
c18366a248b4e43129bcb1ea78

The public key is (n,g) and the private key is (p,q).

2) Encryption

R1 =
ff6d3e6b05cc05ae35c1fcf96b9290d023424741b0e3488779a7f37069ead092a151fc4c106c2
446ab5dd4b5f67ee72008e169bf4ab7833a8e1a182a87eb8eaf

R2 =
b160e82b6d0f61b645534379f5adb18f969b609ef81295bf22e78b40ecc8251aa1714f1e9c7aa
c98d8d124a2c122f82c211d01b0dcdd01957291992cb5307c6d

R3 =
c4922d9b4ae1bec47f459fdfab61ca79d712e725a9d3d56121c986dc39eb939600c6fc405c75
84706c7a2f781ce8d457dfa52b8f6ce848e159993c25ff25c959

s4010423January = 893fea84a10e153829121584233c43ee mod(10000)
s4010423January = 43ee

s4010423February = de5781054aa8a418f8db3f297d191c3b mod(10000)
s4010423February = 1c3b

s4010423March = 98bc3cac2fa00c260cc9256a14a4873e mod(10000)
s4010423March = 873e

C1=g^plaintext * R1^n (mod n2)

g^plaintext (mod n2) =
399efaa960b5e09f307e6bab6f5694f3ca7c4300a00ae500e3066f96a689af1842d23bf426381
b0e47dbe948eba8b4192dfb06e0f2fad0e8a9a31e128511abfda8ae9247561dcbe94fc76c0d4f
be8c5b54d63f1772085f70944bff26ba9fb1943436d453d104738f372a31fbc7fdf83c003c0297
8b4c05e3e6efe503a12ffdc51fa3

R1^n (mod n2) =
81a4c5d903b7360650ce99b5221d627a4bf01313e05a667708a69a7ba6d194c2632ab1f5ebc
effb099347d92bf39ed3f9efdd21d7b2a651728a99d7a5a26ebd9e29bbaa851e9e3ce6e5e197
aa005f4097df47bfd09d34532f39be9d0af17b814790d7919c007408a4341ca3592e04a7bcd4
d96ba9a40adac01c7adbc0296873440302a0d812f9f0403290984711e59e32e73933dd66312
dbbec54beefa461e27650b927ffdf5c1f946d2d531f4405251289ee743c80138614ff78bee051e
60e9158ed9835f93d2848e6eeea482af903da5e6a9ba7a9e65747bd29f5c601e54a21e968a7
15807b8f63b96e5619d38ecc4a4e1cc35c423814e47c4c6e5d15327ba

C1 =
1d2e32b01dba85712d70b95f3d5cfaaee7b0fdd6f4ac7e7866aa2733ad8c244cda155b22a309
c7aaa01d1577f975dd95d55c8c1f4e2ff889aeefe1312e7175078be20bf99d4dd66bd4ebf69a7
da17b1a7e8466967bf49823bf2f61b57ac2275ed4a8993d30c2d49508e052c47cc2daf4eeade

cf14e1ab9fdbee56bf336585c585d1ac3ea8aa670aa858e77d9acb29330b992102e0bda31bc
8e07bfc2115d7444006050c0d0a4d7401a6ceaeed2255bd59c02741957ff19d7e7d1e07e931
b23be85de51e727bbb7158ca4a0a57d5ee16d755483d7cfce7c05d680bfb06a378ac49167f8
37c68f8b5a0715666c2f92d602081e4ae7da9d2668557d5a826ee7a81c7cc8986ab28d038b1
8498ce9f242e6a3a34883e33c313238febc9e696eb84eaec547373ff6b4c29578368a5e04b9c
535aae4c75937d06073900798f0e079c1e9521194ec6b19f564a2b763a6df59f5e1c778675c7
14c869c3d8104f482815db42de53f2cdb999acc8e0dfef6950453fac1d350ea952ee2d798864
8880113bde3d16e **mod**
(b8326d1d2f6cbc74b443b09d92f7d32372786b98079fbf57f0ec285f9258bd83651932b97cc7
cad481c2b25c80d165d5786b8ef91773575af1903dd919dbdf78b0e9114f7eb4b3f50ddb96a3
a1cabb12f850667324a52ed4ae3fcb615bd45e4074fd5b2bc04687c01bcff28083f4d902fa2b1
2111c25371f1615693c86e858fd426c221f0575da7881deaebff038d9e4e7f95a3d18bdf54b46
75c3fa8f82b7439314a87da193df8b82ff0bfd2527f65eb562c683391fe68ab22079f3f5f86ef0b9
16d427402a06e41898fb0ce2c4b2db942ee48b0f4ca9efb9f8b4eeaaf317af0401d2e5d06ad22
7b5bf7d94222828bf6d4d58003ec9ce9b13cc7422d74bc351)

C1 =
8c27d3e78c295171988e434dc3fe2e05054ce0d5a5c454c657f7116b18fde01fe54febd23c895
adb6022bf73042d7791562901d7a11284fd1a0e15bd86c8051cb25eb43316dfc5847047d841
cf8210782a42e3e1d9904e9427bd04bfea882d075db94ed860587f26344d2bd9a1736c01380
79a855274e8532f8713d4915cb80e1fbadd03ac1c03cf5f2eb697b1d96d304b0c08bd16a95b2
0479c1ad351132daea68a8c5c0b9aaa3941ef958be31fa45792306e34e47a086d5bbeb13ecd
4b25ce88623536cbd7f963be528a81dc4710fcd044933032e25d1968419a3ab02956f0ee295
52ea6d8f9fa9311782055f9892e013dfcb1a07e84da17e250b53904ceb9

C2=g^plaintext * R2^n (mod n2)

g^plaintext (mod n2) =
17f2441aab40d6c10d6cfaa2970a5a41473d3d431432cf8d0ee227de1c6ed55e279b07310ae
853abf96271649183bf685afdeee95d787cb612bd31a39046923ebd720878e33c8ce73b5072
9462b913e0e2690dcb9389ad5c3aebcb4c8e01bd8d0a7b5c5c992ecb204c775c8d6c987dc2
51012deaebf882675a8aa5f7e541f2a60d6e

R2^n (mod n2) =
47a75b07698f5bcd8d219de8bd9a0ffb7d950c7910646a8731f06b64227fd80604f08dc2c64ce
7a5f54109ec8740f9342791413d9171fd95ffb5366c8c3fc7f96967feb413471f7c327f3e57f1d8
39b4c7419e1794d6cd061936eeead01c82c80171d133fd7c820946452fa172c990214906b9b
addb5ee9b570073c693005396b81c245760bee0ede3867f3ed6abfa68c25dcd914efd4b0e0e
0528bfbd4d43e44392b880c89df398427271818634809fea3be02dfc310dd026e6e43a9ea563
491976fc5e415960df4b83073bb17e3783cc6a0bc44deddd7b938677b7deca8cce4c3e707f22
70b9ff90c990ca40b47309bf7cd0bea8a5cd9e175a0948d5f4c92

C2 =
6b3d871a299d14fb15254b2d772fa4f53557a2ebb10ea6e5381215dfdc183d304394d21d18a
d633210f3abbd35457f14e99b5d2c90d3c39150a40b298b0b196de4583446f317c826afcb0c0
3c03e16c7cb1d1da63c69cac5578196d875a15f7c655ac5ca90c0cde63ecdd3cccc3ddd7937
96118f8e7a30d7b8ce9b2ed6286ae75e9f481cbea308ba8e8164ec9f6ae2d63f90d7be46599c
872f60ebbbbf4c0a7f7677a2fa27e2ce418e6e97e3c0d31d50a37575b5d9b3a02d6e167adb84

bef8e41b8c51171ebef577b87e3148aaa9b95aa5028d562b6cf2a363a7bd81127b11ef175c24
e7c825cc8145e26f9b8711f804d6a9e7f766a6766081b667a3882882058039fddf1f8da5219db
a7aff35bbab404e9ff4af503917eb80d48d8557fad9c4f54d847549db1fe945c3204794ea1b124
701ffff2a2254efc7e42c9e5952ef819642d1488dd6343d749662b61f528e100a6393b7834e6c
1151ce6980a90205f5831964d4850b723ae7da399e91570b21e8308aadf5c99270538739584
2408250bc **mod**
(b8326d1d2f6cbc74b443b09d92f7d32372786b98079fbf57f0ec285f9258bd83651932b97cc7
cad481c2b25c80d165d5786b8ef91773575af1903dd919dbdf78b0e9114f7eb4b3f50ddb96a3
a1cabb12f850667324a52ed4ae3fcb615bd45e4074fd5b2bc04687c01bcff28083f4d902fa2b1
2111c25371f1615693c86e858fd426c221f0575da7881deaebff038d9e4e7f95a3d18bdf54b46
75c3fa8f82b7439314a87da193df8b82ff0bfd2527f65eb562c683391fe68ab22079f3f5f86ef0b9
16d427402a06e41898fb0ce2c4b2db942ee48b0f4ca9efb9f8b4eeaaf317af0401d2e5d06ad22
7b5bf7d94222828bf6d4d58003ec9ce9b13cc7422d74bc351)

C2 =
1e33f27b339002d5537f966b718816b872a04d811f95319e53f2977a2299df2bb26dc476bcbe
78ffba088b3407b9085b0b9614c7994c8e72f31015aa44a23cb555858d004994599edf7e0504
cb2ea821606812c9c8a8f6f0546e4408bcc88699dde710a3d44feb93e2aa054a32f639915035
98061093e944516b062885459e7d536355f343ecbf0000d6ef8d7240dc80d28542e201d2890
779a23badd152885f9f4ba294ba4381fb00384a709fcafb421be644c6c5f98bb3a09e0d26f09a
5c55270a8d6ca5d26433dc57117ffc06e78a1ded3ea29124b7b23c535dd0e71857469cda5e4
bdeec7887055a6891f394df57b40216f0171e6cd15b00e4c693b360e5

C3=g^plaintext * R3^n (mod n2)

g^plaintext (mod n2) =
72b7ef8344b553c4a93d6855e6ac9548071a9b7a4f9e820f56a3a54f69013796fefc26a1d5523
adef4d143beee86d03a7df61953184e637988d9517b66e897d6f2d2c4a8ef508cd7ce1e08ff53
afbe32eed407c83f987c886d68398c4a0250e1501389df4fe7db8edd71a0408efdd008fd50fe7
a1d28f26fa5002530ea9d85bb89d3

R3^n (mod n2) =
55c347f2f406da3e6540974cdc60838a58ec594693acb00ed83839e7ae7ea5b07b82e8762e4
f9354fff5b5a1789143a628e5d442a820766aba0e69368ad0962bfe0af9c1e825b3a9f7ed8157
dc4f92e6a724597f65816c27f0943be1f046eff0c52277b5312a7e3e34e7d772cd18c876d7fecc
05b305a65858cea91f73824209e53b461c0acc85b481acdf1acc6539b07f763cf9f1e906baa18
9bbeaa2f2d859711bfd576ab6d9bf37197b2b1e5f2904e1440ee427b5eedca4149547b70ba2c
096485c0447638e2522f3569fe5d6c1badf3bfb7a73526bcab831cf4f0ca5b7e2e2264a5e4db9
fcb475e5177e968d9872a75d3bc1a400416ec3c9142b85e6cc04

C3 =
266e94dfe975bf79ab14c5ef12bc4977c761150d4cae6c97aa70cdcbddaa1fc64357ffc33ec2c0
6955ac1eec8e78ff1bc8b1087bb1c7670022e8ee8753d5b21fbe4b54ef814a3e37a49c6627ae
4672123a5a1eff74ae13ef316d325d7ce2e03982b49c739a25a0c67ef9f3356af5e589d2bb3d0
990e5485ead3c959e85d8bb9a95f80be2305460807bec850afef1617b4621fd722fe016c9afb9
43896b8e0d04adcd10d10c466c0f1254a34f6656a81e7a0263043590ac5e3c15e31f84e09b1
0f6ecbd9904bccbcfe62e7338ba36a2d3fea6e06db4a472d084ee5ab6c24d0b186062a70a63
b5cce9db7ee9b912d7ab442dd95de15577fa016b11d01bccbeb843b171597aaabdec1ae5b6

daab032584aca904f03613e1aabdfd6f22313244f16d0aad51d572c769763061e737a7875629
02f39f6bf247bcb69c626d1ef2d0295fa02b719a84e82c14fa5067844d32e0eb3dfc91eb00b57
25e68b5997ca798a12a6dd39ba6ba102a91ceea282367ced0411874ef0992ea9759e2473ca
96890fb544b4c **mod**
(b8326d1d2f6cbc74b443b09d92f7d32372786b98079fbf57f0ec285f9258bd83651932b97cc7
cad481c2b25c80d165d5786b8ef91773575af1903dd919dbdf78b0e9114f7eb4b3f50ddb96a3
a1cabb12f850667324a52ed4ae3fcb615bd45e4074fd5b2bc04687c01bcff28083f4d902fa2b1
2111c25371f1615693c86e858fd426c221f0575da7881deaebff038d9e4e7f95a3d18bdf54b46
75c3fa8f82b7439314a87da193df8b82ff0bfd2527f65eb562c683391fe68ab22079f3f5f86ef0b9
16d427402a06e41898fb0ce2c4b2db942ee48b0f4ca9efb9f8b4eeaaf317af0401d2e5d06ad22
7b5bf7d94222828bf6d4d58003ec9ce9b13cc7422d74bc351)

C3 =
879c0b2b12bed2bffb258082f9f403b297bb31d19c9ac7e31d0f2e9ff90bdf044a25bbfbde8109
d4d7ab2d9c18f887b3bc326bced40c8e5d50c2581aefc679da74ad80e053b8d2b952fccd2bc7
d31de66c3d203959fb68203bbc1cba48abdd2184727e21ea883ca44ef7020692d54380d4613
8d184356f6940d20550810dbcd03cc3be177bc7da19e384c10e1aec3fcb8c87d214a82da3d3
d48a153df6321a6bd676aa5093cf3f69e3473aa5caff81f609c675ec5b4d66d406ee8ce64db62
2fe2bf03ac0b37f986a9673f7b63d8bd42b10aeeeea2d288ae6ac92a0d9a858eb94aee9d0286
092701a4d87ba3da24b2f965be4b512cae3234177fe941d5f563095

<u>Ciphertext</u>
C1 =
8c27d3e78c295171988e434dc3fe2e05054ce0d5a5c454c657f7116b18fde01fe54febd23c895
adb6022bf73042d7791562901d7a11284fd1a0e15bd86c8051cb25eb43316dfc5847047d841
cf8210782a42e3e1d9904e9427bd04bfea882d075db94ed860587f26344d2bd9a1736c01380
79a855274e8532f8713d4915cb80e1fbadd03ac1c03cf5f2eb697b1d96d304b0c08bd16a95b2
0479c1ad351132daea68a8c5c0b9aaa3941ef958be31fa45792306e34e47a086d5bbeb13ecd
4b25ce88623536cbd7f963be528a81dc4710fcd044933032e25d1968419a3ab02956f0ee295
52ea6d8f9fa9311782055f9892e013dfcb1a07e84da17e250b53904ceb9

C2 =
1e33f27b339002d5537f966b718816b872a04d811f95319e53f2977a2299df2bb26dc476bcbe
78ffba088b3407b9085b0b9614c7994c8e72f31015aa44a23cb555858d004994599edf7e0504
cb2ea821606812c9c8a8f6f0546e4408bcc88699dde710a3d44feb93e2aa054a32f639915035
98061093e944516b062885459e7d536355f343ecbf0000d6ef8d7240dc80d28542e201d2890
779a23badd152885f9f4ba294ba4381fb00384a709fcafb421be644c6c5f98bb3a09e0d26f09a
5c55270a8d6ca5d26433dc57117ffc06e78a1ded3ea29124b7b23c535dd0e71857469cda5e4
bdeec7887055a6891f394df57b40216f0171e6cd15b00e4c693b360e5

C3 =
879c0b2b12bed2bffb258082f9f403b297bb31d19c9ac7e31d0f2e9ff90bdf044a25bbfbde8109
d4d7ab2d9c18f887b3bc326bced40c8e5d50c2581aefc679da74ad80e053b8d2b952fccd2bc7
d31de66c3d203959fb68203bbc1cba48abdd2184727e21ea883ca44ef7020692d54380d4613
8d184356f6940d20550810dbcd03cc3be177bc7da19e384c10e1aec3fcb8c87d214a82da3d3
d48a153df6321a6bd676aa5093cf3f69e3473aa5caff81f609c675ec5b4d66d406ee8ce64db62
2fe2bf03ac0b37f986a9673f7b63d8bd42b10aeeeea2d288ae6ac92a0d9a858eb94aee9d0286
092701a4d87ba3da24b2f965be4b512cae3234177fe941d5f563095

3)

C = C1 * C2 * C3 (mod n^2) =

18a0ae7779edd91b00368de2958a6e14f26ec1989b1db956e468ae7b792340c97fa9cb15b35
637b8f576c5c7c8aeed8b3296e8d6c786a5479a6e3fc557a05d52763bee85e615001921b01d
b21d0457c94b860e717ffd95e720286c384fed8bb22dbf4850eb39badd72c81b5b000104a718
366e1a179ef9c72ad9b016f9310789d3f4231c2ad9d259be8827e0b1dedfe95637fd1a8e06a3
bdd53e142825fa2895f558d7fd7a43dbaba102262cea0fc56a9a7f5240cf38fdb53f3f21a3f1eed
1bdecd1b6992392a2586de3a28b0f88a788f48ea8b1cc05103d2284fbe8d39c6fc332c02f2bbf
671828c1c626f43a4e815161f7212e3fd960c388a3bc607f7189c5

4)

[(C(p-1)(q-1)(mod n2)-1)/n]*[(p-1)(q-1)]^-1(mod n)

(p-1)(q-1)=

fb9ddfe3e18439490359761969b6015ceacfae408eee0ed029bc375550550f25effb28812fe97
82ef6a8c4e8e43fba95d69782d628498ce5d042440a9b02869a *
dceeff6d1c6bff190218fe003b88c52581af11cd07778132f297a9198e6a635bc0f51188ebc8d0
3329779c734c4dcc60300e1cd4b5a7895a796d580c4a18bb54

(p-1)(q-1)=

d926943b7bd5060612867cb578d6e21cf2e6ee1432aee6c7f50643dfb5b670a654c47f22370e
f8e10dddb075f0c260fffed421c9a51917bd41e3cfb82d61a83e4018b321dace9590595d20ce
b87baac5034209532ef4090a27cbd01505aed3e11afd3713d7d9cfd48cef4850380232f7ca2d
016a5758c086b349512d796a888

[(p-1)(q-1)]^-1(mod n) =

caa84ade3ea9756638007f5a882eca0112a50859be592496053f709922b3526241e49d64bf4
bfff2bcbb7fd78647f109ab37a07713140552fbcc72e1a2dfaa184e38f3c0cbc43431efc8175220
ef44f281ebaf15d1aac3ffc86e13d9ce8bb0c92fdc9d48b45e22e83e445c57b4d0556becb8b4d
5e8c2bdf1d345f478aaf002b9

[C^(p-1)(q-1)(mod n2)-1)/n] =

d926943b7bd5060612867cb578d6e21cf2e6ee1432aee6c7f50643dfb5b670a654c47f22370e
f8e10dddb075f0c260fffed421c9a51917bd41e3cfb82d46f607e5e7bc92d15ff6093386bb96f6
4f2ceb6675875a18510c3a98d45d5cfc046e8cd99946c55243ae7440df9f9f6545d29639203b
dac52abed9963bb37f63bba4e

[C^(p-1)(q-1)(mod n2)-1)/n]*[(p-1)(q-1)]^-1(mod n) =

=

d926943b7bd5060612867cb578d6e21cf2e6ee1432aee6c7f50643dfb5b670a654c47f22370e
f8e10dddb075f0c260fffed421c9a51917bd41e3cfb82d46f607e5e7bc92d15ff6093386bb96f6
4f2ceb6675875a18510c3a98d45d5cfc046e8cd99946c55243ae7440df9f9f6545d29639203b

dac52abed9963bb37f63bba4e *
caa84ade3ea9756638007f5a882eca0112a50859be592496053f709922b3526241e49d64bf4

5)
Public Key (n):

d926943b7bd5060612867cb578d6e21cf2e6ee1432aee6c7f50643dfb5b670a654c47f22370ef8
e10dddb075f0c260ffffed421c9a51917bd41e3cfb82d61a85bc8e6a831b9d21bb0b08462690c6
812ebcb2e0a2c954d093bed09d702f1a5fbfc2a00d7b592fe55f68ef55e1340daa2583486fc1836
6a248b4e43129bcb1ea77

Inputs:

43ee, 1c3b, 873e

Encrypted values:

c1:
8c27d3e78c295171988e434dc3fe2e05054ce0d5a5c454c657f7116b18fde01fe54febd23c895a
db6022bf73042d7791562901d7a11284fd1a0e15bd86c8051cb25eb43316dfc5847047d841cf8
210782a42e3e1d9904e9427bd04bfea882d075db94ed860587f26344d2bd9a1736c0138079a85
5274e8532f8713d4915cb80e1fbadd03ac1c03cf5f2eb697b1d96d304b0c08bd16a95b20479c1a
d351132daea68a8c5c0b9aaa3941ef958be31fa45792306e34e47a086d5bbeb13ecd4b25ce8862
3536cbd7f963be528a81dc4710fcd044933032e25d1968419a3ab02956f0ee29552ea6d8f9fa93
11782055f9892e013dfcb1a07e84da17e250b53904ceb9

c2:
1e33f27b339002d5537f966b718816b872a04d811f95319e53f2977a2299df2bb26dc476bcbe7
8ffba088b3407b9085b0b9614c7994c8e72f31015aa44a23cb555858d004994599edf7e0504cb
2ea821606812c9c8a8f6f0546e4408bcc88699dde710a3d44feb93e2aa054a32f6399150359806
1093e944516b062885459e7d536355f343ecbf0000d6ef8d7240dc80d28542e201d2890779a23
badd152885f9f4ba294ba4381fb00384a709fcafb421be644c6c5f98bb3a09e0d26f09a5c55270a
8d6ca5d26433dc57117ffc06e78a1ded3ea29124b7b23c535dd0e71857469cda5e4bdeec78870
55a6891f394df57b40216f0171e6cd15b00e4c693b360e5

c3:
879c0b2b12bed2bffb258082f9f403b297bb31d19c9ac7e31d0f2e9ff90bdf044a25bbfbde8109d
4d7ab2d9c18f887b3bc326bced40c8e5d50c2581aefc679da74ad80e053b8d2b952fccd2bc7d31
de66c3d203959fb68203bbc1cba48abdd2184727e21ea883ca44ef7020692d54380d46138d184
356f6940d20550810dbcd03cc3be177bc7da19e384c10e1aec3fcb8c87d214a82da3d3d48a153
df6321a6bd676aa5093cf3f69e3473aa5caff81f609c675ec5b4d66d406ee8ce64db622fe2bf03ac

0b37f986a9673f7b63d8bd42b10aeeeea2d288ae6ac92a0d9a858eb94aee9d0286092701a4d87ba3da24b2f965be4b512cae3234177fe941d5f563095

Homomorphic sum ciphertext (csum):

18a0ae7779edd91b00368de2958a6e14f26ec1989b1db956e468ae7b792340c97fa9cb15b35637b8f576c5c7c8aeed8b3296e8d6c786a5479a6e3fc557a05d52763bee85e615001921b01db21d0457c94b860e717ffd95e720286c384fed8bb22dbf4850eb39badd72c81b5b000104a718366e1a179ef9c72ad9b016f9310789d3f4231c2ad9d259be8827e0b1dedfe95637fd1a8e06a3bdd53e142825fa2895f558d7fd7a43dbaba102262cea0fc56a9a7f5240cf38fdb53f3f21a3f1eed1bdecd1b6992392a2586de3a28b0f88a788f48ea8b1cc05103d2284fbe8d39c6fc332c02f2bbf671828c1c626f43a4e815161f7212e3fd960c388a3bc607f7189c5

bfff2bcbb7fd78647f109ab37a07713140552fbcc72e1a2dfaa184e38f3c0cbc43431efc8175220ef44f281ebaf15d1aac3ffc86e13d9ce8bb0c92fdc9d48b45e22e83e445c57b4d0556becb8b4d5e8c2bdf1d345f478aaf002b9

=
abe731c9e2342de14ef4b41e0ff1d74c6359b34611e011b4ece91ed9fdac84665586b2c1f33906a3eaf1eec0ee677dbc3f0b05616992105175d218aeab474c26187c175f57c25773fbc990a078a3685835967802ac9e2bb84a7b267bbcf07e1aad450d88f9e1e3b5fa84d08955b6424940c81b4488eed6c71dae2a92a8c7cc65469b549da6433c8c09f0765b55b33c15c66fdbe90a8b00a59f17b0fcf4a854c55a8e3d605bc8e8570e0851a16d0a3d9b9b54ef7262fcc6f558e522131c2ce4e281cd6d4ab5338100d1a1c1d695c9d8935740c886624c711ba67c9a48920c2c832d1bcf0663b1b3bd52ee767f6ba3e6589c4e615374cdccbb291ae9a3ddbe3e5e mod (d926943b7bd5060612867cb578d6e21cf2e6ee1432aee6c7f50643dfb5b670a654c47f22370ef8e10dddb075f0c260ffffed421c9a51917bd41e3cfb82d61a85bc8e6a831b9d21bb0b08462690c6812ebcb2e0a2c954d093bed09d702f1a5fbfc2a00d7b592fe55f68ef55e1340daa2583486fc18366a248b4e43129bcb1ea77)

= e767

e767 - 1c3b - 43ee = 873e
5)

Public Key (n):

d926943b7bd5060612867cb578d6e21cf2e6ee1432aee6c7f50643dfb5b670a654c47f22370ef8e10dddb075f0c260ffffed421c9a51917bd41e3cfb82d61a85bc8e6a831b9d21bb0b08462690c6812ebcb2e0a2c954d093bed09d702f1a5fbfc2a00d7b592fe55f68ef55e1340daa2583486fc18366a248b4e43129bcb1ea77

Inputs:

43ee, 1c3b, 873e

Encrypted values:

c1:
8c27d3e78c295171988e434dc3fe2e05054ce0d5a5c454c657f7116b18fde01fe54febd23c895
adb6022bf73042d7791562901d7a11284fd1a0e15bd86c8051cb25eb43316dfc5847047d841
cf8210782a42e3e1d9904e9427bd04bfea882d075db94ed860587f26344d2bd9a1736c01380
79a855274e8532f8713d4915cb80e1fbadd03ac1c03cf5f2eb697b1d96d304b0c08bd16a95b2
0479c1ad351132daea68a8c5c0b9aaa3941ef958be31fa45792306e34e47a086d5bbeb13ecd
4b25ce88623536cbd7f963be528a81dc4710fcd044933032e25d1968419a3ab02956f0ee295
52ea6d8f9fa9311782055f9892e013dfcb1a07e84da17e250b53904ceb9

c2:
1e33f27b339002d5537f966b718816b872a04d811f95319e53f2977a2299df2bb26dc476bcbe
78ffba088b3407b9085b0b9614c7994c8e72f31015aa44a23cb555858d004994599edf7e0504
cb2ea821606812c9c8a8f6f0546e4408bcc88699dde710a3d44feb93e2aa054a32f639915035
98061093e944516b062885459e7d536355f343ecbf0000d6ef8d7240dc80d28542e201d2890
779a23badd152885f9f4ba294ba4381fb00384a709fcafb421be644c6c5f98bb3a09e0d26f09a
5c55270a8d6ca5d26433dc57117ffc06e78a1ded3ea29124b7b23c535dd0e71857469cda5e4
bdeec7887055a6891f394df57b40216f0171e6cd15b00e4c693b360e5

c3:
879c0b2b12bed2bffb258082f9f403b297bb31d19c9ac7e31d0f2e9ff90bdf044a25bbfbde8109
d4d7ab2d9c18f887b3bc326bced40c8e5d50c2581aefc679da74ad80e053b8d2b952fccd2bc7
d31de66c3d203959fb68203bbc1cba48abdd2184727e21ea883ca44ef7020692d54380d4613
8d184356f6940d20550810dbcd03cc3be177bc7da19e384c10e1aec3fcb8c87d214a82da3d3
d48a153df6321a6bd676aa5093cf3f69e3473aa5caff81f609c675ec5b4d66d406ee8ce64db62
2fe2bf03ac0b37f986a9673f7b63d8bd42b10aeeeea2d288ae6ac92a0d9a858eb94aee9d0286
092701a4d87ba3da24b2f965be4b512cae3234177fe941d5f563095

Homomorphic sum ciphertext (csum):

18a0ae7779edd91b00368de2958a6e14f26ec1989b1db956e468ae7b792340c97fa9cb15b35
637b8f576c5c7c8aeed8b3296e8d6c786a5479a6e3fc557a05d52763bee85e615001921b01d
b21d0457c94b860e717ffd95e720286c384fed8bb22dbf4850eb39badd72c81b5b000104a718
366e1a179ef9c72ad9b016f9310789d3f4231c2ad9d259be8827e0b1dedfe95637fd1a8e06a3
bdd53e142825fa2895f558d7fd7a43dbaba102262cea0fc56a9a7f5240cf38fdb53f3f21a3f1eed
1bdecd1b6992392a2586de3a28b0f88a788f48ea8b1cc05103d2284fbe8d39c6fc332c02f2bbf
671828c1c626f43a4e815161f7212e3fd960c388a3bc607f7189c5

Q2

Secret (s):

12345678910

a1:

4010423

a2:

9845612374

Prime (p):

1340780792994259709957

Polynomial equation as below:

get polynomial equation

f(x) = s + a1x + a2x^2 mod p =
12345678910 + 4010423x + 9845612374x^2 mod 1340780792994259709957402499820584612747936582059239337772356144372176403007 37

compute 4 points

when x = 1, 2, 3, 4
(1, 22195301707)
(2, 51736149252)
(3, 100968221545)
(4, 169891518586)

Select any three points above to recover the secret (s):

select x1: 2
select y1: 51736149252

select x2: 3
select y2: 100968221545

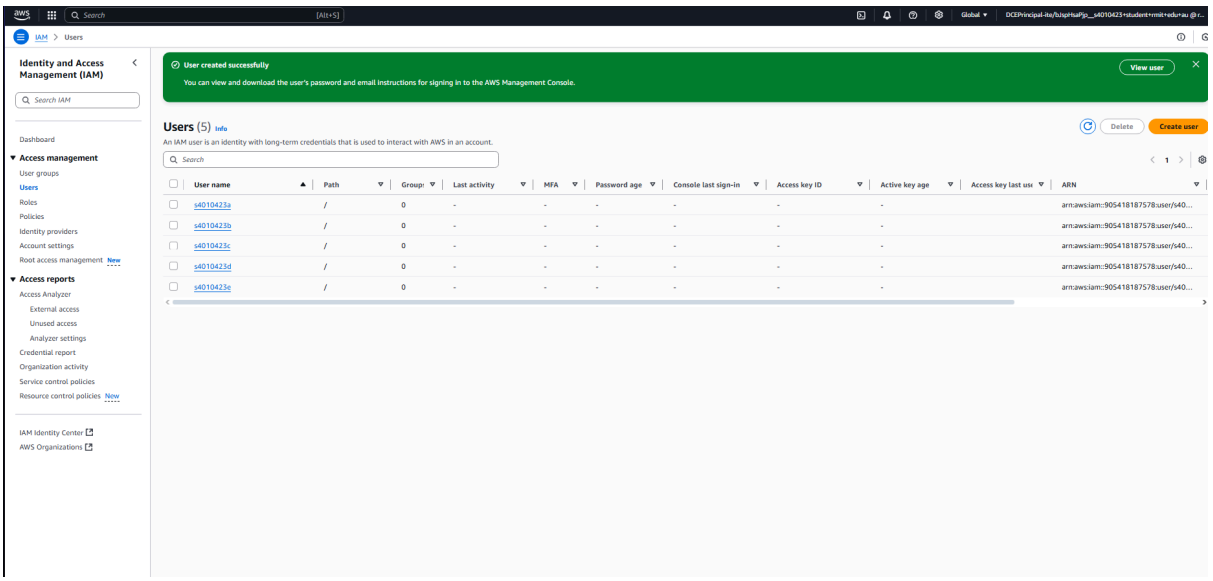
select x3: 4
select y3: 169891518586

recover secret s

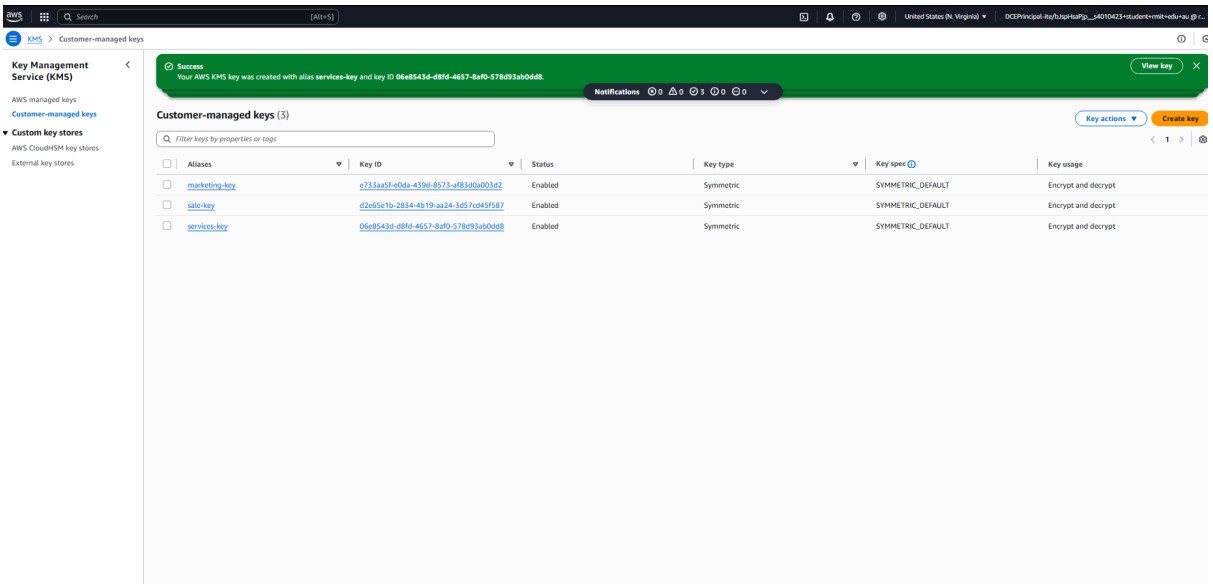
12345678910

4) Shamir Secret Sharing acts as a way to split the key into 4 shares. And these shares are distributed to different cloud services. This ensures that no cloud provider will have the completed key. Adding another security layers

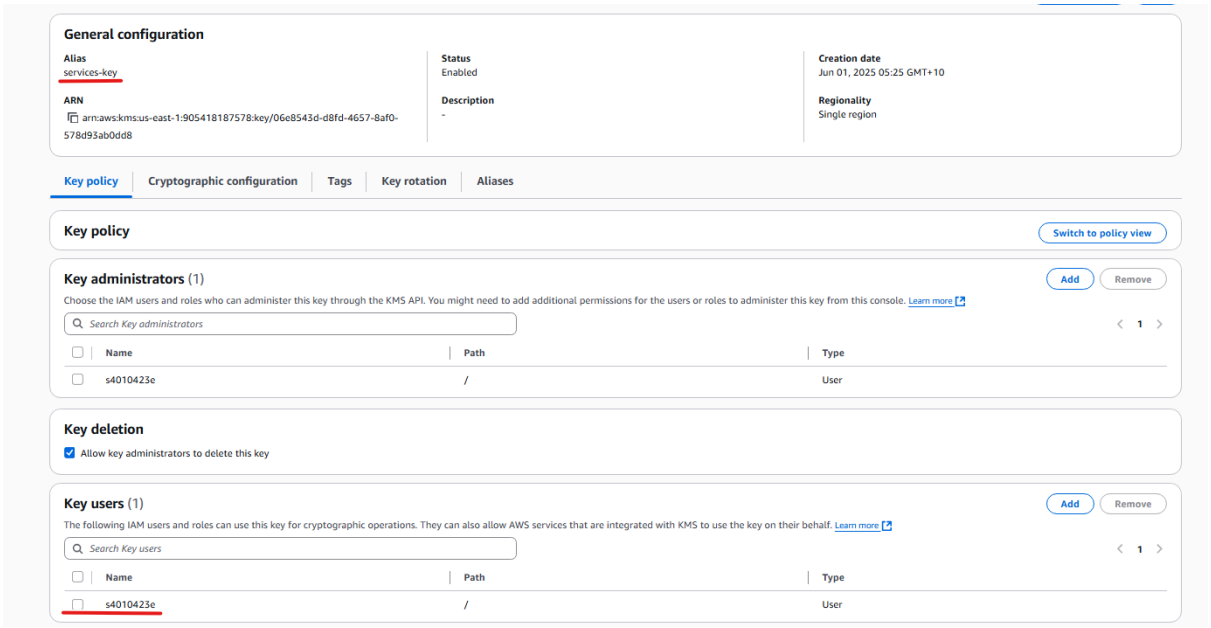
Q3 1)

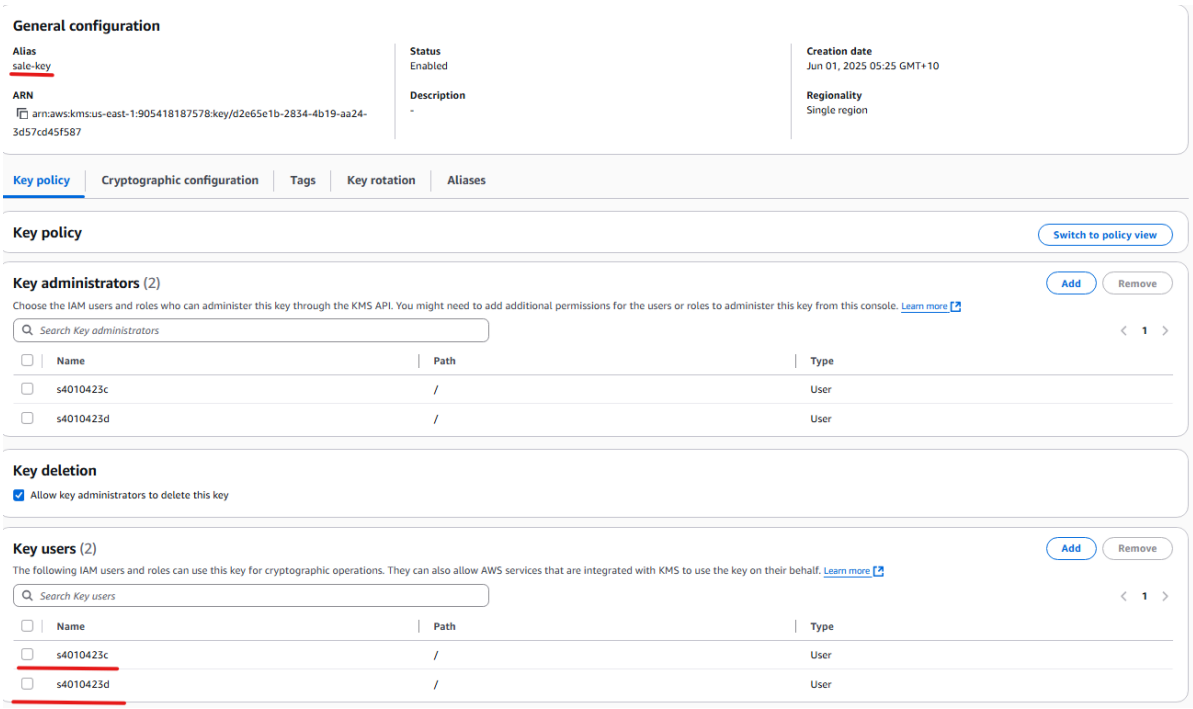

Search
[Alt+S]
Global
IAM > Users
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
Users (5) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Search
Delete
Create user
User name
Path
Group
Last activity
MFA
Password age
Console last sign-in
Access key ID
Active key age
Access key last use
ARN
s4010423a
s4010423b
s4010423c
s4010423d
s4010423e

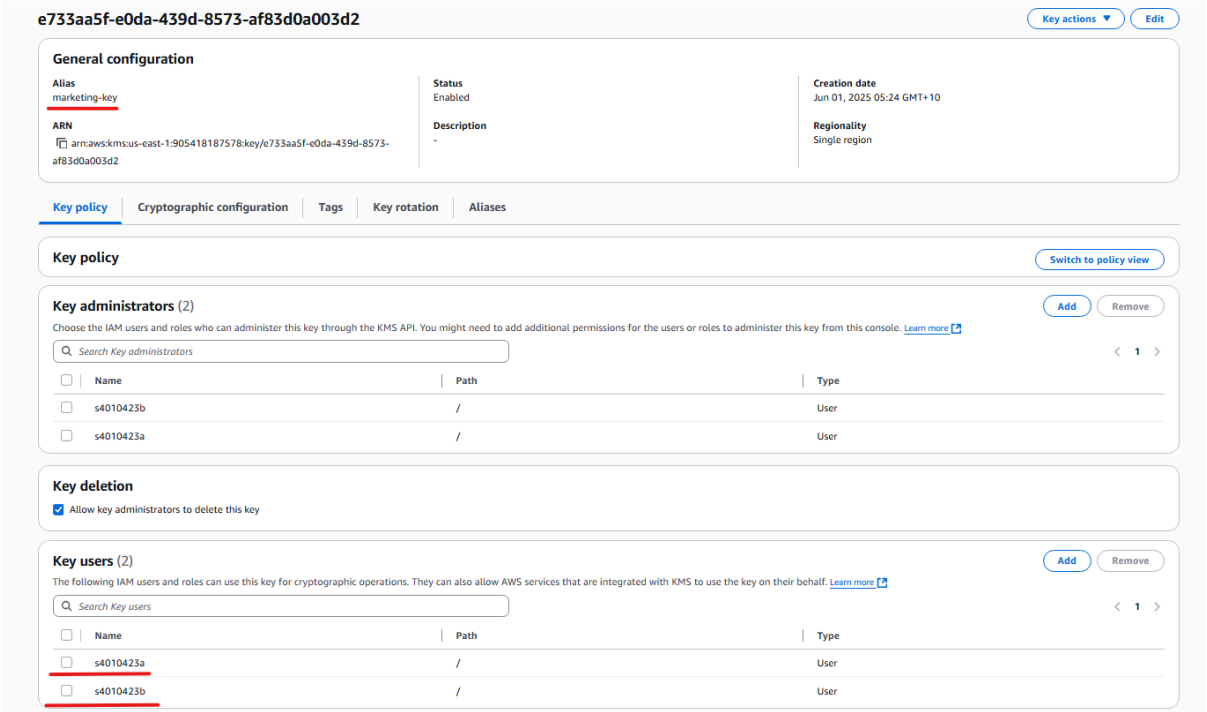
2)


Search
[Alt+S]
United States (N. Virginia)
KMS > Customer-managed keys
Key Management Service (KMS)
AWS managed keys
Customer-managed keys
Custom key stores
AWS CloudHSM key stores
External key stores
Success
Your AWS KMS key was created with alias services-key and key ID 06e8543d-d8fd-4657-8af0-578d93ab0dd8.
View key
Notifications
Customer-managed keys (3)
Filter keys by properties or tags
Key actions
Create key
Aliases
Key ID
Status
Key type
Key spec
Key usage
marketing-key
e733aa5f-e0da-439d-8573-af83d0a003d2
sale-key
d2e65e1b-2834-4b19-aa24-3d57cd45f587
services-key
06e8543d-d8fd-4657-8af0-578d93ab0dd8
Enabled
Symmetric
SYMMETRIC_DEFAULT
Encrypt and decrypt

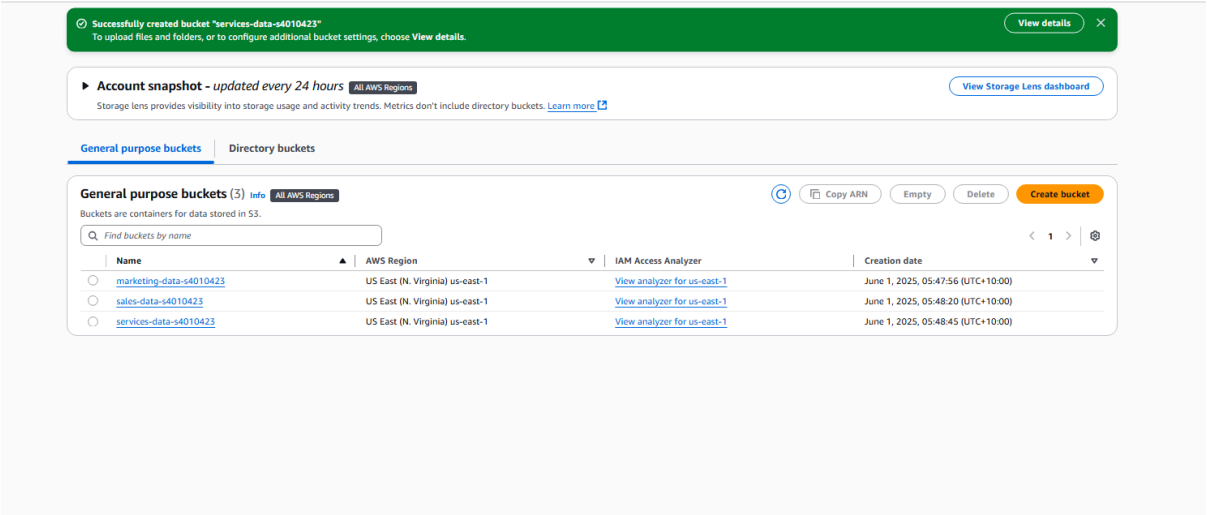
3)


General configuration
Alias
services-key
ARN
arn:aws:kms:us-east-1:905418187578:key/06e8543d-d8fd-4657-8af0-578d93ab0dd8
Status
Enabled
Description
-
Creation date
Jun 01, 2025 05:25 GMT+10
Regionality
Single region
Key policy
Cryptographic configuration
Tags
Key rotation
Aliases
Key policy
Switch to policy view
Key administrators (1)
Add
Remove
Choose the IAM users and roles who can administer this key through the KMS API. You might need to add additional permissions for the users or roles to administer this key from this console. Learn more
Search Key administrators
Name
Path
Type
s4010423e
/
User
Key deletion
Allow key administrators to delete this key
Key users (1)
Add
Remove
The following IAM users and roles can use this key for cryptographic operations. They can also allow AWS services that are integrated with KMS to use the key on their behalf. Learn more
Search Key users
Name
Path
Type
s4010423e
/
User


General configuration
Alias
sale-key
ARN
arn:aws:kms:us-east-1:905418187578:key/d2e65e1b-2834-4b19-aa24-3d57cd45f587
Status
Enabled
Description
-
Creation date
Jun 01, 2025 05:25 GMT+10
Regionality
Single region
Key policy
Cryptographic configuration
Tags
Key rotation
Aliases
Key policy
Switch to policy view
Key administrators (2)
Add
Remove
Choose the IAM users and roles who can administer this key through the KMS API. You might need to add additional permissions for the users or roles to administer this key from this console. Learn more
Search Key administrators
Name
Path
Type
s4010423c
/
User
s4010423d
/
User
Key deletion
Allow key administrators to delete this key
Key users (2)
Add
Remove
The following IAM users and roles can use this key for cryptographic operations. They can also allow AWS services that are integrated with KMS to use the key on their behalf. Learn more
Search Key users
Name
Path
Type
s4010423c
/
User
s4010423d
/
User


e733aa5f-e0da-439d-8573-af83d0a003d2
Key actions
Edit
General configuration
Alias
marketing-key
Status
Enabled
Creation date
Jun 01, 2025 05:24 GMT+10
ARN
arn:aws:kms:us-east-1:905418187578:key/e733aa5f-e0da-439d-8573-af83d0a003d2
Description
-
Regionality
Single region
Key policy
Cryptographic configuration
Tags
Key rotation
Aliases
Key policy
Switch to policy view
Key administrators (2)
Add
Remove
Choose the IAM users and roles who can administer this key through the KMS API. You might need to add additional permissions for the users or roles to administer this key from this console. Learn more
Search Key administrators
Name
Path
Type
s4010423b
/
User
s4010423a
/
User
Key deletion
Allow key administrators to delete this key
Key users (2)
Add
Remove
The following IAM users and roles can use this key for cryptographic operations. They can also allow AWS services that are integrated with KMS to use the key on their behalf. Learn more
Search Key users
Name
Path
Type
s4010423a
/
User
s4010423b
/
User

4)


Successfully created bucket "services-data-s4010423"
To upload files and folders, or to configure additional bucket settings, choose View details.
View details
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (3) Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
marketing-data-s4010423
US East (N. Virginia) us-east-1
View analyzer for us-east-1
June 1, 2025, 05:47:56 (UTC+10:00)
sales-data-s4010423
US East (N. Virginia) us-east-1
View analyzer for us-east-1
June 1, 2025, 05:48:20 (UTC+10:00)
services-data-s4010423
US East (N. Virginia) us-east-1
View analyzer for us-east-1
June 1, 2025, 05:48:45 (UTC+10:00)

5)

marketing-data-s4010423 Info

Objects | Metadata | Properties | Permissions | Metrics | Management | Access Points

Bucket overview

AWS Region
US East (N. Virginia) us-east-1

Amazon Resource Name (ARN)
arn:aws:s3:::marketing-data-s4010423

Creation date
June 1, 2025, 05:47:56 (UTC+10:00)

Bucket Versioning

Edit

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning
Disabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled

Tags (0)

Edit

You can use bucket tags to track storage costs and organize buckets. Learn more

Key	Value

No tags associated with this resource.

Default encryption Info

Edit

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info
Server-side encryption with AWS Key Management Service keys (SSE-KMS)

Encryption key ARN
arn:aws:kms:us-east-1:905418187578:key/e733aa5f-e0da-439d-8573-af83d0a003d2

Bucket Key
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. Learn more
Enabled

sales-data-s4010423 Info

Objects | Metadata | Properties | Permissions | Metrics | Management | Access Points

Bucket overview

AWS Region
US East (N. Virginia) us-east-1

Amazon Resource Name (ARN)
arn:aws:s3:::sales-data-s4010423

Creation date
June 1, 2025, 05:48:20 (UTC+10:00)

Bucket Versioning

Edit

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning
Disabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled

Tags (0)

Edit

You can use bucket tags to track storage costs and organize buckets. Learn more

Key	Value

No tags associated with this resource.

Default encryption Info

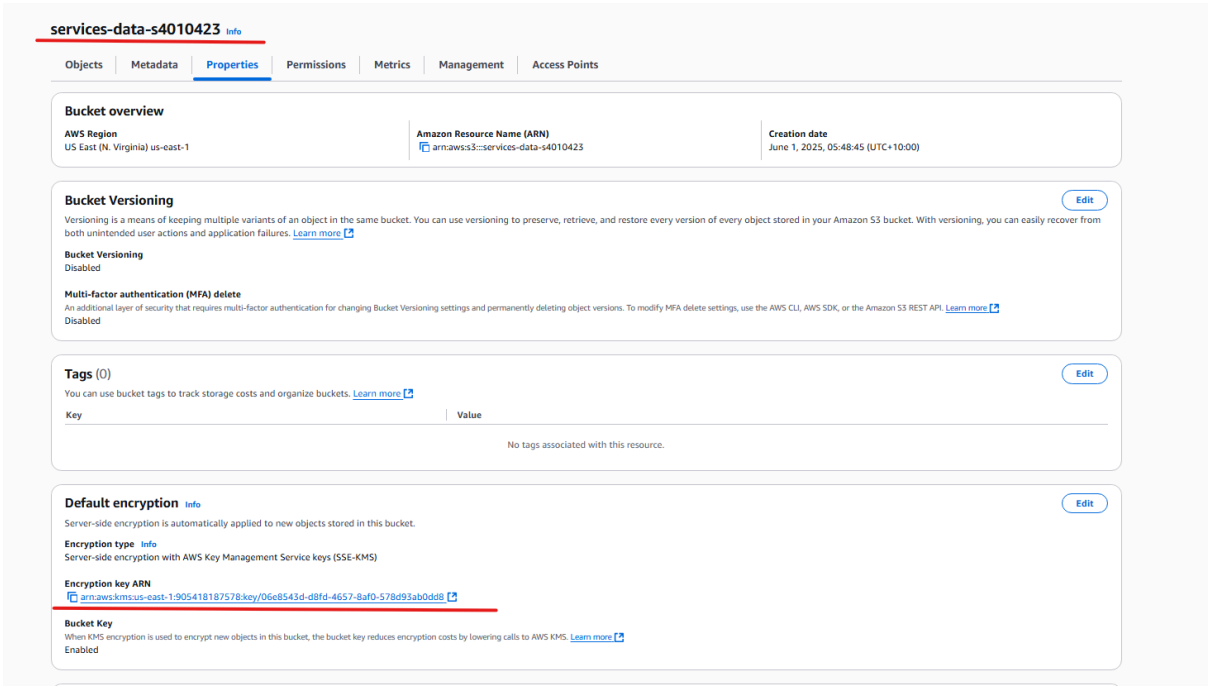
Edit

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info
Server-side encryption with AWS Key Management Service keys (SSE-KMS)

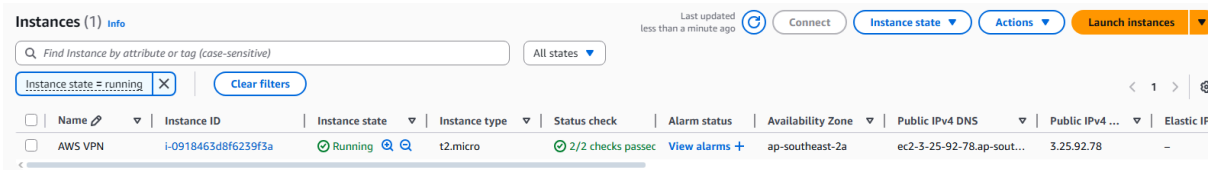
Encryption key ARN
arn:aws:kms:us-east-1:905418187578:key/d2e65e1b-2834-4b19-aa24-3d57cd45f587

Bucket Key
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. Learn more
Enabled

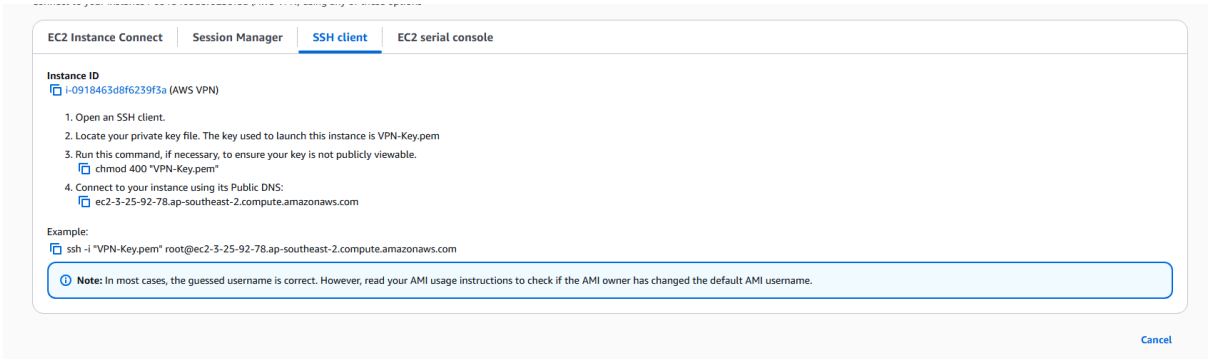

services-data-s4010423 Info
Objects
Metadata
Properties
Permissions
Metrics
Management
Access Points
Bucket overview
AWS Region
US East (N. Virginia) us-east-1
Amazon Resource Name (ARN)
arn:aws:s3:::services-data-s4010423
Creation date
June 1, 2025, 05:48:45 (UTC+10:00)
Bucket Versioning
Edit
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more
Bucket Versioning
Disabled
Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled
Tags (0)
Edit
You can use bucket tags to track storage costs and organize buckets. Learn more
Key
Value
No tags associated with this resource.
Default encryption Info
Edit
Server-side encryption is automatically applied to new objects stored in this bucket.
Encryption type Info
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
Encryption key ARN
arn:aws:kms:us-east-1:905418187578:key/06e8543d-d8fd-4657-8af0-578d93ab0dd8
Bucket Key
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. Learn more
Enabled

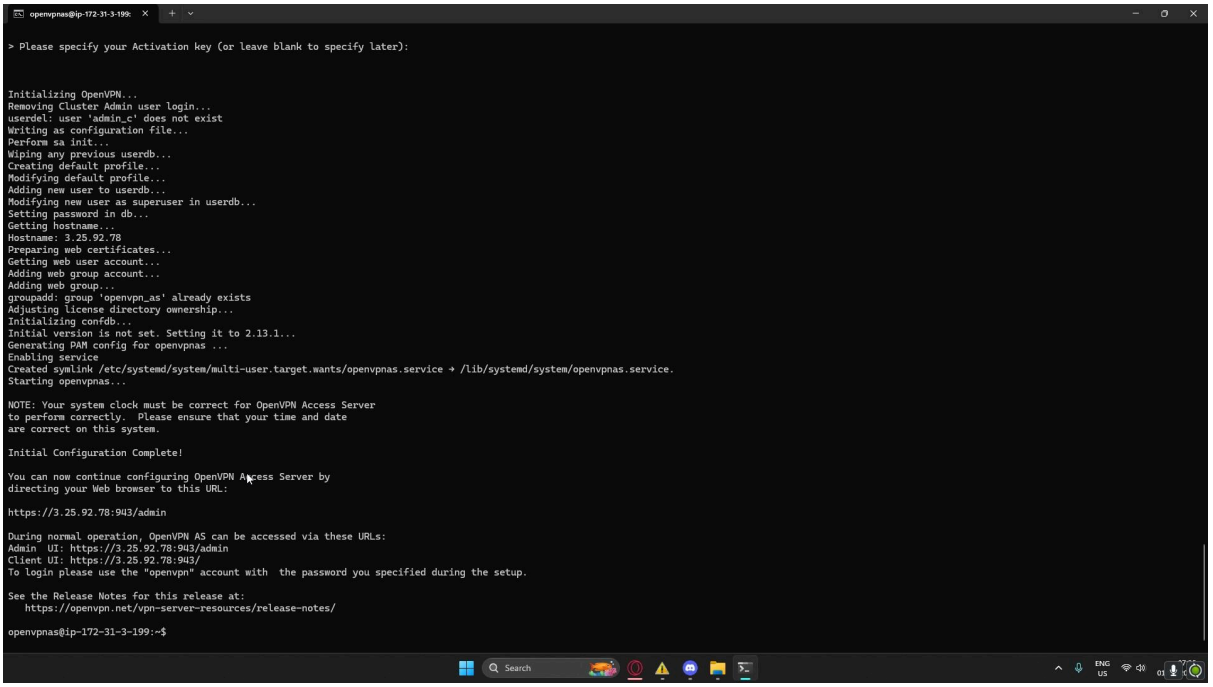
Q4

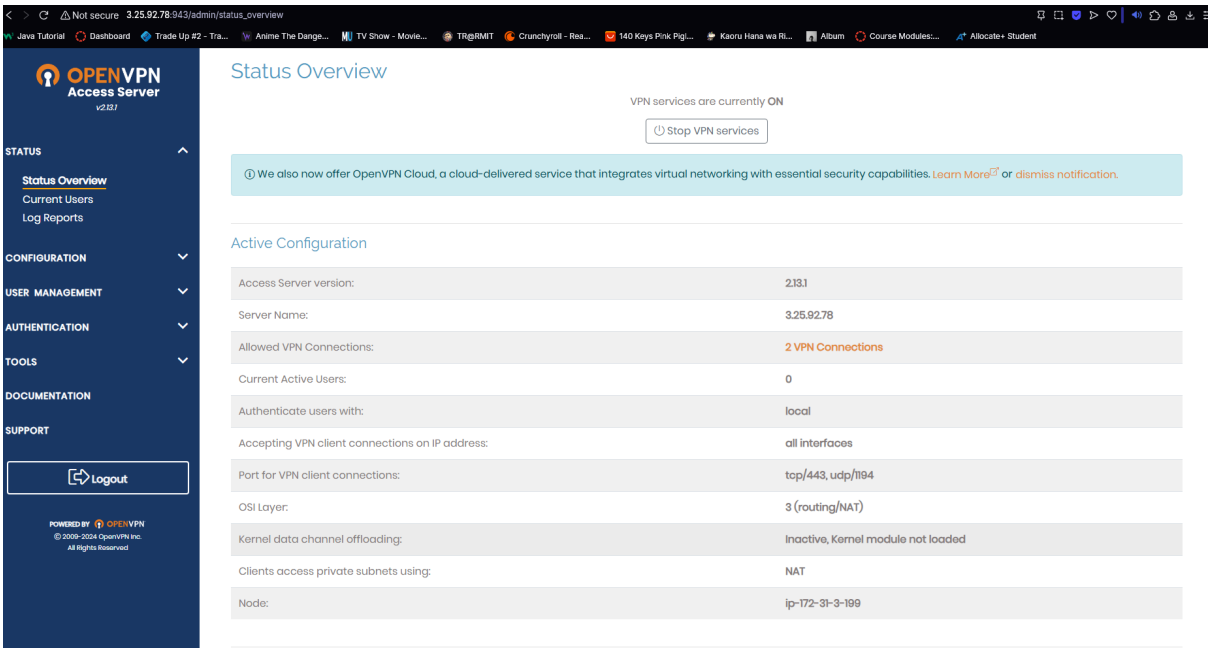
1)

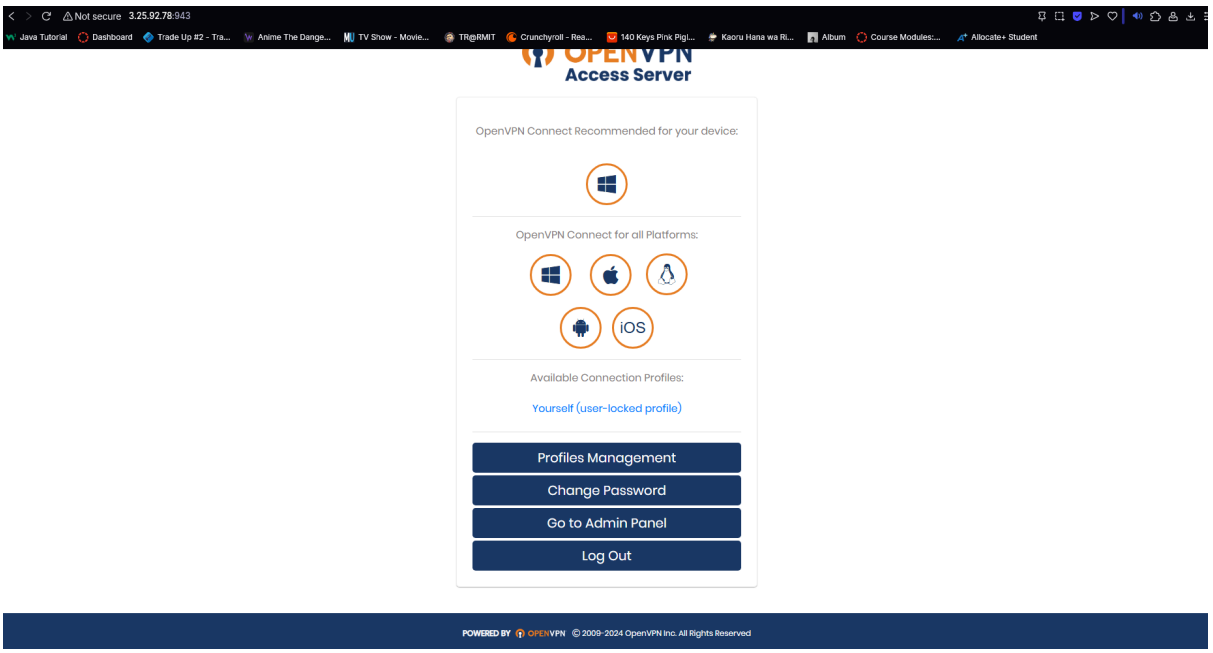

Instances (1) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Instance state = running
Clear filters
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic IP
AWS VPN
i-0918463d8f6239f3a
Running
t2.micro
2/2 checks passed
View alarms
ap-southeast-2a
ec2-3-25-92-78.ap-sout...
3.25.92.78
–

2)


EC2 Instance Connect
Session Manager
SSH client
EC2 serial console
Instance ID
i-0918463d8f6239f3a (AWS VPN)
1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is VPN-Key.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
chmod 400 "VPN-Key.pem"
4. Connect to your instance using its Public DNS:
ec2-3-25-92-78.ap-southeast-2.compute.amazonaws.com
Example:
ssh -i "VPN-Key.pem" root@ec2-3-25-92-78.ap-southeast-2.compute.amazonaws.com
Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.
Cancel


openvpnas@ip-172-31-3-199:
> Please specify your Activation key (or leave blank to specify later):
Initializing OpenVPN...
Removing Cluster Admin user login...
userdel: user 'admin_c' does not exist
Writing as configuration file...
Perform sa init...
Wiping any previous userdb...
Creating default profile...
Modifying default profile...
Adding new user to userdb...
Modifying new user as superuser in userdb...
Setting password in db...
Getting hostname...
Hostname: 3.25.92.78
Preparing web certificates...
Getting web user account...
Adding web group account...
Adding web group...
groupadd: group 'openvpn_as' already exists
Adjusting license directory ownership...
Initializing confdb...
Initial version is not set. Setting it to 2.13.1...
Generating PAM config for openvpnas ...
Enabling service
Created symlink /etc/systemd/system/multi-user.target.wants/openvpnas.service → /lib/systemd/system/openvpnas.service.
Starting openvpnas...
NOTE: Your system clock must be correct for OpenVPN Access Server
to perform correctly. Please ensure that your time and date
are correct on this system.
Initial Configuration Complete!
You can now continue configuring OpenVPN Access Server by
directing your Web browser to this URL:
https://3.25.92.78:943/admin
During normal operation, OpenVPN AS can be accessed via these URLs:
Admin UI: https://3.25.92.78:943/admin
Client UI: https://3.25.92.78:943/
To login please use the "openvpn" account with the password you specified during the setup.
See the Release Notes for this release at:
https://openvpn.net/vpn-server-resources/release-notes/
openvpnas@ip-172-31-3-199:~$
Search
ENG
US


Not secure 3.25.92.78:943/admin/status_overview
Java Tutorial
Dashboard
Trade Up #2 - Tra...
Anime The Dange...
TV Show - Movie...
TR@RMIT
Crunchyroll - Rea...
140 Keys Pink Pig...
Kaoru Hana wa Ri...
Album
Course Modules:...
Allocate+ Student
OPENVPN
Access Server
v2.13.1
STATUS
Status Overview
Current Users
Log Reports
CONFIGURATION
USER MANAGEMENT
AUTHENTICATION
TOOLS
DOCUMENTATION
SUPPORT
Logout
POWERED BY OPENVPN
© 2009-2024 OpenVPN Inc.
All Rights Reserved
Status Overview
VPN services are currently ON
Stop VPN services
We also now offer OpenVPN Cloud, a cloud-delivered service that integrates virtual networking with essential security capabilities. Learn More or dismiss notification.
Active Configuration
Access Server version: 2.13.1
Server Name: 3.25.92.78
Allowed VPN Connections: 2 VPN Connections
Current Active Users: 0
Authenticate users with: local
Accepting VPN client connections on IP address: all interfaces
Port for VPN client connections: tcp/443, udp/1194
OSI Layer: 3 (routing/NAT)
Kernel data channel offloading: Inactive, Kernel module not loaded
Clients access private subnets using: NAT
Node: ip-172-31-3-199



5) The implementation of VPN created an environment where sensitive information can be exchanged without the fear of a third party being able to see that data. This is because VPN acts as an extended private network. Not only that, openvpn requires users to provide credentials, adding another layer of security.