

###

Elliptic Curve Digital Signature Algorithm

Curve: P-384

Hash Algorithm: SHA3-384

Message to be signed: "Example of ECDSA with P-384"

###

Signature Generation

H:

F492B9EB18A06F7AA479953B31C34FBFFCF42A7427B5D2EFF045DD6162B
24BCC37DA1AA7725ED71A650EAB7DE758FEFF

E:

F492B9EB18A06F7AA479953B31C34FBFFCF42A7427B5D2EFF045DD6162B
24BCC37DA1AA7725ED71A650EAB7DE758FEFF

K:

2E44EF1F8C0BEA8394E3DDA81EC6A7842A459B534701749E2ED95F054F0
137680878E0749FC43F85EDCAE06CC2F43FEF

K_{inv} :

AC227DA51929533DFC2E9EEFB4E0F7BD22392CA73289ED1C6C00B214E88
74D8007C8AC46B25D677DFE9B1C6C10A47E4A

R_x :

30EA514FC0D38D8208756F068113C7CADA9F66A3B40EA3B313D040D9B57
DD41A332795D02CC7D507FCEF9FAF01A27088

R_y :

C04E32465D14C50CBC3BCB88EA20F95B10616663FC62A8DCDB48D300632
7EA7CA104F6F9294C66EA2487BD50357010C6

R:

30EA514FC0D38D8208756F068113C7CADA9F66A3B40EA3B313D040D9B57
DD41A332795D02CC7D507FCEF9FAF01A27088

D:

F92C02ED629E4B48C0584B1C6CE3A3E3B4FAAE4AFC6ACB0455E73DFC392
E6A0AE393A8565E6B9714D1224B57D83F8A08

S:
691B9D4969451A98036D53AA725458602125DE74881BBC333012CA4FA55
BDE39D1BF16A6AAE3FE4992C567C6E7892337

Signature

R:
30EA514FC0D38D8208756F068113C7CADA9F66A3B40EA3B313D040D9B57
DD41A332795D02CC7D507FCEF9FAF01A27088

S:
691B9D4969451A98036D53AA725458602125DE74881BBC333012CA4FA55
BDE39D1BF16A6AAE3FE4992C567C6E7892337

=====
==

Signature Verification

Q_x:
<3BF701BC9E9D36B4D5F1455343F09126F2564390F2B487365071243C61
E6471FB9D2AB74657B82F9086489D9EF0F5CB5>

Q_y:
<D1A358EAFBF952E68D533855CCBDAA6FF75B137A510144319932558355
2A6295FFE5382D00CFDA30344A9B5B68DB855>

H:
<F492B9EB18A06F7AA479953B31C34FBFFCF42A7427B5D2EFF045DD6162
B24BCC37DA1AA7725ED71A650EAB7DE758FEFF>

E:
<F492B9EB18A06F7AA479953B31C34FBFFCF42A7427B5D2EFF045DD6162
B24BCC37DA1AA7725ED71A650EAB7DE758FEFF>

Sinv:
<2C9D828896FFB8BF5FA3DA96F13625D253AA74CDAC954FB0D8418EB72D
AAF9684DD39928A21A808CE54DCF8305B7E647>

U:
<B605245C6AAA6F78E36D028256B4FC59276A81FE66FDE423C5AD3FFA8A
9C4FB9746D54292D98FCA1EA82BD0B4F429262>

V:
<1DADF5712FD482442213313241DCCDEB50298448A2EAE87C965801EDF9
1259C4487B96B4BD39569346F7ABDDDB44E2246>

Rprime.X:

**<30EA514FC0D38D8208756F068113C7CADA9F66A3B40EA3B313D040D9B5
7DD41A332795D02CC7D507FCEF9FAF01A27088>**

Rprime.Y:

**<C04E32465D14C50CBC3BCB88EA20F95B10616663FC62A8DCDB48D30063
27EA7CA104F6F9294C66EA2487BD50357010C6>**

Rprime:

**<30EA514FC0D38D8208756F068113C7CADA9F66A3B40EA3B313D040D9B5
7DD41A332795D02CC7D507FCEF9FAF01A27088>**

Verification Passed!