**##
###**

** Elliptic Curve Digital Signature Algorithm**
**   Curve: P-384**
**   Hash Algorithm: SHA-384**

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

**##
###**

** Signature Generation**
**   H:**
5AEA187D1C4F6E1B35057D20126D836C6ADBBC7049EE0299C9529F5E0B3
F8B5A7411149D6C30D6CB2B8AF70E0A781E89

**   E:**
5AEA187D1C4F6E1B35057D20126D836C6ADBBC7049EE0299C9529F5E0B3
F8B5A7411149D6C30D6CB2B8AF70E0A781E89

**   K:**
2E44EF1F8C0BEA8394E3DDA81EC6A7842A459B534701749E2ED95F054F0
137680878E0749FC43F85EDCAE06CC2F43FEF

**   Kinv:**
AC227DA51929533DFC2E9EEFB4E0F7BD22392CA73289ED1C6C00B214E88
74D8007C8AC46B25D677DFE9B1C6C10A47E4A

**   R_x:**
30EA514FC0D38D8208756F068113C7CADA9F66A3B40EA3B313D040D9B57
DD41A332795D02CC7D507FCEF9FAF01A27088

**   R_y:**
C04E32465D14C50CBC3BCB88EA20F95B10616663FC62A8DCDB48D300632
7EA7CA104F6F9294C66EA2487BD50357010C6

**   R:**
30EA514FC0D38D8208756F068113C7CADA9F66A3B40EA3B313D040D9B57
DD41A332795D02CC7D507FCEF9FAF01A27088

**   D:**
F92C02ED629E4B48C0584B1C6CE3A3E3B4FAAE4AFC6ACB0455E73DFC392
E6A0AE393A8565E6B9714D1224B57D83F8A08

S:
CC808E504BE414F46C9027BCBF78ADF067A43922D6FCAA66C4476875FBB
7B94EFD1F7D5DBE620BFB821C46D549683AD8

Signature
R:
30EA514FC0D38D8208756F068113C7CADA9F66A3B40EA3B313D040D9B57
DD41A332795D02CC7D507FCEF9FAF01A27088

S:
CC808E504BE414F46C9027BCBF78ADF067A43922D6FCAA66C4476875FBB
7B94EFD1F7D5DBE620BFB821C46D549683AD8

==========

Signature Verification
Q_x:
<3BF701BC9E9D36B4D5F1455343F09126F2564390F2B487365071243C61
E6471FB9D2AB74657B82F9086489D9EF0F5CB5>
Q_y:
<D1A358EAFBF952E68D533855CCBDAA6FF75B137A510144319932558355
2A6295FFE5382D00CFCDA30344A9B5B68DB855>

H:
<5AEA187D1C4F6E1B35057D20126D836C6ADBBC7049EE0299C9529F5E0B
3F8B5A7411149D6C30D6CB2B8AF70E0A781E89>

E:
<5AEA187D1C4F6E1B35057D20126D836C6ADBBC7049EE0299C9529F5E0B
3F8B5A7411149D6C30D6CB2B8AF70E0A781E89>

Sinv:
<5D794F2787A1B53703944757B3D0EB0C66A3442A04C35259107D362C94
DC58882BA2948D0869700FF57910EFAA54550B>

U:
<9C0590EE8000B79832DC4C6776F7E5FD2A74BE161741C7C2D2F038D439
831696A1B8ECE4199D225B12B76DD9E637B250>

V:
<8F77BE5B0EB32A1A3B9274CFDA53518A01AAD4AFC4BD46A392B7C7DE4E
ED3FE6DEE54F3064234FE7FDE57AE45532C24D>

Rprime.X:
<30EA514FC0D38D8208756F068113C7CADA9F66A3B40EA3B313D040D9B5
7DD41A332795D02CC7D507FCEF9FAF01A27088>

Rprime.Y:
<C04E32465D14C50CBC3BCB88EA20F95B10616663FC62A8DCDB48D30063
27EA7CA104F6F9294C66EA2487BD50357010C6>

Rprime:
<30EA514FC0D38D8208756F068113C7CADA9F66A3B40EA3B313D040D9B5
7DD41A332795D02CC7D507FCEF9FAF01A27088>

Verification Passed!