**##
###**

Elliptic Curve Digital Signature Algorithm
Curve: B-409
Hash Algorithm: SHA-384

Message to be signed: "Example of ECDSA with B-409"

**##
###**

Signature Generation
H:
4BBF1BC0DDF9D3B7BFE21FC68642B3E5508CA6BA4D365C1D00ABBFABDB0F3EC2B0BE995AE803DE47D0880BF192649EDC

E:
4BBF1BC0DDF9D3B7BFE21FC68642B3E5508CA6BA4D365C1D00ABBFABDB0F3EC2B0BE995AE803DE47D0880BF192649EDC

K:
6A0B81D9320B5C305D730B1C1E74B03FAFB88A7EC355990B75F9B70E8532433296A32492CBA06F8583D5B19C5B8C5D6D07EC

Kinv:
A202EA455D0E1A5EF09054B39259C768DB76FFD1A77B6281FC7056A4A23A1012CDD604E4D7993E0D9EDD422DEFD782C1225A1A

R_x:
1F3E4DA3101C64239D76831995C0EC1E56CE4690C42DDD53DBF3EF725D819DF090B8632F327499B5B99C280D7F410CD7105C8DB

R_y:
122C8D8E5BEEC67621FF662D16D96845ADD77930A1096913CFFC984E97DA8E7351F73AC33BEAD2C2FA5B3049FC53FCF38160AF5

R:
F3E4DA3101C64239D76831995C0EC1E56CE4690C42DDD53DBF3D147B0173CC15D87E749382CD5EBD9492FD568F43959763B768

D:
4AF896DB379ABDF70C8FADE9EBD28CD530F2ECB336B4DE84BD6E065EF56C8C548C532D00FA55CA8ACF3E98ADBCA9F78D241B

S:
292FA994DC6EA367236AD73956DBC1EB62B8779DF438165407141587E3F
EED883741CDF5542F255BEBC57B9D0C87AD403B8EAB

Signature
R:
F3E4DA3101C64239D76831995C0EC1E56CE4690C42DDD53DBF3D147B017
3CC15D87E749382CD5EBD9492FD568F43959763B768

S:
292FA994DC6EA367236AD73956DBC1EB62B8779DF438165407141587E3F
EED883741CDF5542F255BEBC57B9D0C87AD403B8EAB

==========

Signature Verification
Q_x:
<1951C5E41607E9317F247D49A389D0E120F479D47737543098AE5E1BB6
2BD59DE70E1C584AE655C702D39DD4F7883E1876C4A9B>
Q_y:
<16B16B98A3353D75BEB4D3576C64568BA381463CF77D4AEB85218D2D54
6E7A1EE3AB9316D8C7DF00D155B7891B2C0BF4B5E942E>

H:
<4BBF1BC0DDF9D3B7BFE21FC68642B3E5508CA6BA4D365C1D00ABBFABDB
0F3EC2B0BE995AE803DE47D0880BF192649EDC>

E:
<4BBF1BC0DDF9D3B7BFE21FC68642B3E5508CA6BA4D365C1D00ABBFABDB
0F3EC2B0BE995AE803DE47D0880BF192649EDC>

Sinv:
<19BAA800F6AD546E7E5D45F702C68BB4D4845C839B3D75AED776E7C8A9
D17D8EB41BD50FC7B707B49D10758977BD9472E7E998>

U:
<33D4F3CE2B7D4F2548F54C92420A8C30E6B02D768CBD6CA4AB020E88BE
82EEFE4D58A9B4DB2854561EAD8975E1A58FB45C2117>

V:
<EB0671192B38CBC911CADE604D9E048C7E660AF3C7085D54839C1B7549
691E5F7FFFDAB4003ADE05208775D4A0287E448740AF>

Rprime.X:
<1F3E4DA3101C64239D76831995C0EC1E56CE4690C42DDD53DBF3EF725D819DF090B8632F327499B5B99C280D7F410CD7105C8DB>

Rprime.Y:
<122C8D8E5BEEC67621FF662D16D96845ADD77930A1096913CFFC984E97DA8E7351F73AC33BEAD2C2FA5B3049FC53FCF38160AF5>

Rprime:
<F3E4DA3101C64239D76831995C0EC1E56CE4690C42DDD53DBF3D147B0173CC15D87E749382CD5EBD9492FD568F43959763B768>

Verification Passed!