```
###########################################################
###

  Elliptic Curve Digital Signature Algorithm
     Curve: B-571
     Hash Algorithm: SHA-512

     Message to be signed: "Example of ECDSA with B-571"

###########################################################
###

  Signature Generation
    H:
60EDEF7DA1D9D35A77D1DA441EBB63454501F2BB1AF8A4C49D281298E5F
4D4E6B7E9BCE4B66B2512BF590288B57915BFD3AED2C2604A5C574107DF
674FAF9779

    E:
60EDEF7DA1D9D35A77D1DA441EBB63454501F2BB1AF8A4C49D281298E5F
4D4E6B7E9BCE4B66B2512BF590288B57915BFD3AED2C2604A5C574107DF
674FAF9779

    K:
1062FF6D95C49AC610CB9AF9900D59C288669C3626306DB7EB7F119499B
A1D54CB6BE888758CAADA69952675CC0CD4999176879BC302A7E2A5118D
FC7D538DA114CCAC2BAF9AD08

    Kinv:
28C3AE12BD7922B837FE05066136BB45EDA0337D39E31C3D4B9164C93F1
7FD7549471EB0385FCCEA8768DD6E5925ADF1D1888826FF6AECC48F3DB3
9905D46A644EB2F0C3A3DCBBD

    R_x:
E17447E422A2C0085190354AC149210C1137A92C10F9B14D225E6510DA7
6B19EF44D39390DD9D808C9DFBAE67D9CF0E7BE79A9E72FA8FA1DFE89F4
3FB6D093A6CEB30E136EABA3

    R_y:
50F8519E19285DEE649F58F05D4E20B60755744C49D1D9189ED1E203664
FC73E87C83D4308731934628CF61EED6B9A30A897A5BE8FAC187AE67360
B1D662D67F0DB04253DD5E98C

    R:
```

```
E17447E422A2C0085190354AC149210C1137A92C10F9B14D225E6510DA7
6B19EF44D39390DD9D808C9DFBAE67D9CF0E7BE79A9E72FA8FA1DFE89F4
3FB6D093A6CEB30E136EABA3

    D:
3CCE32BA00DC3A7EEFC9EB6F6CBFB9C5F0E57F532B7EE6826D4A75D0E75
6FD533900F2CEA8CCCC50EE22CE079398D371EC4A2EC45CC24B88760667
8E9C67453D0F5E768E9D752

    S:
624E852C7B6A061B4B39A907B518200FED380FD692C9AE147C5250F4852
434AFA24A1CA5062C48E5FC217FB689AB3A7266B5522F176F32A5CEA22D
6BF2820D349E4193BCEE75C8

    Signature
        R:
E17447E422A2C0085190354AC149210C1137A92C10F9B14D225E6510DA7
6B19EF44D39390DD9D808C9DFBAE67D9CF0E7BE79A9E72FA8FA1DFE89F4
3FB6D093A6CEB30E136EABA3

        S:
624E852C7B6A061B4B39A907B518200FED380FD692C9AE147C5250F4852
434AFA24A1CA5062C48E5FC217FB689AB3A7266B5522F176F32A5CEA22D
6BF2820D349E4193BCEE75C8

===========================================================
==

  Signature Verification
    Q_x:
<310EAD2BEF3DDB84F9FC1777A7EE179FFCB77AAB497BDC00E290597A5F
CE306FE419D2F1F208E54850516526DB8E03B0519BEF60E3A3CC8198FBC
A8C469ACFE46AB70D5C31874F>
    Q_y:
<373CE6EA68F55D1501D5203ACA03C5AB709A337A8E03B03838F47C0676
2065FBDD08A102A08C42FF1760145BE54D8606D326EA22A54DF034FAC30
988049820BEBA2B0AF9F6404B3>

    H:
<60EDEF7DA1D9D35A77D1DA441EBB63454501F2BB1AF8A4C49D281298E5
F4D4E6B7E9BCE4B66B2512BF590288B57915BFD3AED2C2604A5C574107D
F674FAF9779>

    E:
```

```
<60EDEF7DA1D9D35A77D1DA441EBB63454501F2BB1AF8A4C49D281298E5
F4D4E6B7E9BCE4B66B2512BF590288B57915BFD3AED2C2604A5C574107D
F674FAF9779>

    Sinv:
<2099000A60926EEA55746EE9B672F7714156560E72B7F47028C87AB4DF
09A03E966556BAA3B7BB72FD87580828D281734CFE253B3E960D1A11815
35D6C86147530CC70B0D3F412E>

    U:
<1A73BE1676983C3B1583A8504C46E290AC2FFC3FD7866E6242AE2A3DC4
0F362E2B799173698175F7F094E9FA06EE09B3AA7D284549B8FCF467105
1B829AA38EF59D066B3554DE19>

    V:
<10DF449E4FB576079A7D63A59F000DA5E24DA7800FA29BF321084ED549
834B1ED95E5BAF48FD65830F2BD0957B6F709DAC14AF90BE29993FE428B
D7DF93206CC9ED9296230B8657>

    Rprime.X:
<E17447E422A2C0085190354AC149210C1137A92C10F9B14D225E6510DA
76B19EF44D39390DD9D808C9DFBAE67D9CF0E7BE79A9E72FA8FA1DFE89F
43FB6D093A6CEB30E136EABA3>

    Rprime.Y:
<50F8519E19285DEE649F58F05D4E20B60755744C49D1D9189ED1E20366
4FC73E87C83D4308731934628CF61EED6B9A30A897A5BE8FAC187AE6736
0B1D662D67F0DB04253DD5E98C>

    Rprime:
<E17447E422A2C0085190354AC149210C1137A92C10F9B14D225E6510DA
76B19EF44D39390DD9D808C9DFBAE67D9CF0E7BE79A9E72FA8FA1DFE89F
43FB6D093A6CEB30E136EABA3>

Verification Passed!
```