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

  Elliptic Curve Digital Signature Algorithm
     Curve: K-571
     Hash Algorithm: SHA3-512

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

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

  Signature Generation
    H:
4F6EC78F87630660E90B4682F70E2C1A739D20DC4F535E4EF3E4BB72D03
36391B7DA1A246EC12384551407C30F4F4E4256D950507FB4BF622C6C98
5AEEB36A38

    E:
4F6EC78F87630660E90B4682F70E2C1A739D20DC4F535E4EF3E4BB72D03
36391B7DA1A246EC12384551407C30F4F4E4256D950507FB4BF622C6C98
5AEEB36A38

    K:
104063C918DE62000A3FD87775D8D71398722BD153B8EA33060349C5FE6
CF6CB4677957E6BA50D3C8A8B5182B9CF962954A6BBB5F7868B88E5778A
A62A0CF8002BF19DA3049FF51

    Kinv:
75A02BEAEA51660A1D05053B173C9C6DCCAEBA80F72CA08DEC3C32E2A47
CBC5674998AD19FC77B6615BFBED482451AF7FD9B416B64B0E8F8429449
FA9685F2B9C8DC2108544D98

    R_x:
668758C313FBF1945F775D95B25866DBC8D001D9C7EF4FFA53774E8C689
27A52707F034CEBB3A712BE6D164F2FFE1897B069F8FBAEC4650B5372DD
FA31CDECCFA78569197CF50F1

    R_y:
3796EAB7DA927707DF47EBED5898B37B053998C717BB726EBF552027255
B1222D0B088EFC8C03F9D855C8BF9ED19AECEA681C33CBBE5F539B3EF92
E98F88B2E75C1C7FB6D39F302

    R:
```

```
68758C313FBF1945F775D95B25866DBC8D001D9C7EF4FFA53774E8C6892
7A52707F034957247CB5717A5B6D84AE6F6C688DBE59859BD6D03B48237
476742AFE37CEFE36D5B20EE

    D:
1042FDE4D66E76725E7957E208A85CF23BC0D5B8D001B36AEAFB34AD110
4004CCF99AFDFABCA11585A4EB5263C87052CB05EF7FB39D9E5F6CF495E
9DCE5840B83FBC5FF3AD8B2F3

    S:
1186A2C9FC3FF4B334099C16B3F1A96B6B1CE94018909874E2B8379B3C1
DEBB9C5FABFAFD0C977F423EABCB5B76B9ECF6BC76D22718CE03E95D7E4
9ED9A6C27929C693088178359

    Signature
        R:
68758C313FBF1945F775D95B25866DBC8D001D9C7EF4FFA53774E8C6892
7A52707F034957247CB5717A5B6D84AE6F6C688DBE59859BD6D03B48237
476742AFE37CEFE36D5B20EE

        S:
1186A2C9FC3FF4B334099C16B3F1A96B6B1CE94018909874E2B8379B3C1
DEBB9C5FABFAFD0C977F423EABCB5B76B9ECF6BC76D22718CE03E95D7E4
9ED9A6C27929C693088178359

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

  Signature Verification
    Q_x:
<4D9CFE0A7338FEA703E007F5D10BABD2DF3F319B47DF1E23C4F7E5ABF5
014C1390B78F117E6AF8258A48F56ACB9FAAC788530B5CCDB1AB7E9390E
C5DD7A39D5EEAF6C41BF50AC76>
    Q_y:
<64732C504F81DC5F9B0E882B6DA46E124E8241358F077896D25ECF028A
D0E6011993C85E68741A07D7817C400CF94B1A3F524F48668B5B9709726
18616DB4362A769D16CAC34BF0>

    H:
<4F6EC78F87630660E90B4682F70E2C1A739D20DC4F535E4EF3E4BB72D0
336391B7DA1A246EC12384551407C30F4F4E4256D950507FB4BF622C6C9
85AEEB36A38>

    E:
```

```
<4F6EC78F87630660E90B4682F70E2C1A739D20DC4F535E4EF3E4BB72D0
336391B7DA1A246EC12384551407C30F4F4E4256D950507FB4BF622C6C9
85AEEB36A38>

    Sinv:
<6828F0433F327C89A4D07601D0EB7202475156584DD20A2C0B3D1F3878
43F065C9B7F69F44DE1EF143C93B6D09D1D4C10473B376786C43179E7CD
129F198707FD189E4990AA9D4>

    U:
<7CBD000553A516C7E74F845AACA37D27D9EA5AD3574DE0C80D2395AD9E
3DC17886249719426619391476 2D38546A8AA9A8E6E3432CA5E33D67D88
F4B96873872EC9331E28E5F41>

    V:
<F075145F3588BC37E9CFBEE8EE3BBB4A83F90E90A490C005EFAA82BD02
8AA9ABFBE1AA4225867DE443820A69F379F8DA558B143AF65EFABB9372B
C3853651F4A06B2A457451C36>

    Rprime.X:
<668758C313FBF1945F775D95B25866DBC8D001D9C7EF4FFA53774E8C68
927A52707F034CEBB3A712BE6D164F2FFE1897B069F8FBAEC4650B5372D
DFA31CDECCFA78569197CF50F1>

    Rprime.Y:
<3796EAB7DA927707DF47EBED5898B37B053998C717BB726EBF55202725
5B1222D0B088EFC8C03F9D855C8BF9ED19AECEA681C33CBBE5F539B3EF9
2E98F88B2E75C1C7FB6D39F302>

    Rprime:
<68758C313FBF1945F775D95B25866DBC8D001D9C7EF4FFA53774E8C689
27A52707F034957247CB5717A5B6D84AE6F6C688DBE59859BD6D03B4823
7476742AFE37CEFE36D5B20EE>

Verification Passed!
```