**##
###**

Elliptic Curve Digital Signature Algorithm
Curve: B-283
Hash Algorithm: SHA-512/256

Message to be signed: "Example of ECDSA with B-283"

**##
###**

Signature Generation
H:
D2BCEF34E8D0DC909A504C4071BE5D27ED47561CE173C555C57CCA1B194AF208

E:
D2BCEF34E8D0DC909A504C4071BE5D27ED47561CE173C555C57CCA1B194AF208

K:
100EC321393E6DD6C4D47BE5AE189E5E35408579D0862178F94CCBBA3C4049A4D88E297

Kinv:
AB6D18AF222D8FDE7D93894D4FAEEB36ACCD4FB68EC95D9E9BFF4C08AFF3C631A67BE4

R_x:
77CB284AC41E72EDA2A93EB8D6DFF58620F6C69D528DFE90D909AA5CABC03A34E5D5A76

R_y:
289997A39B5287D0905D9C4AF94EFEA4B9A1A7E7B983FDDC909E8ACF56EED7F97D7E1C0

R:
37CB284AC41E72EDA2A93EB8D6DFF58620F7CD99B927EEC7A060A8F6FB7D9265EAFA76F

D:
10652D37B0A9DB64D4033AC6549CD1DF37E1EEDE2612C2363257C6AFF6C8CB5DCB63648

S:
166759B4F981DD46AB64E3311D5102AA12AA8429ABC4DC0D7FCCF2D9496
7344E4B22D00

Signature
R:
37CB284AC41E72EDA2A93EB8D6DFF58620F7CD99B927EEC7A060A8F6FB7
D9265EAFA76F

S:
166759B4F981DD46AB64E3311D5102AA12AA8429ABC4DC0D7FCCF2D9496
7344E4B22D00

==========

Signature Verification
Q_x:
<390858E9327A714C74AF0C3ADEDF4E6C75CAFDCC46507A49E415B138A0
94B6F43E882AC>
Q_y:
<D4A65D973CD150A5221BEDF872A4BA207FF4427DFFFD4827C5BF169E71
9162504D0631>

H:
<D2BCEF34E8D0DC909A504C4071BE5D27ED47561CE173C555C57CCA1B19
4AF208>

E:
<D2BCEF34E8D0DC909A504C4071BE5D27ED47561CE173C555C57CCA1B19
4AF208>

Sinv:
<1EF53A0FC996E6516ABD02C5D9A4534AFAB22909152B820E5E2F0C75A3
2E93C6600CB36>

U:
<1E53D9020B9FBDAD4AD29F3DACB3495584B8658F71EEAF87D7042A1354
E2465CBAEBEFC>

V:
<292BB8429AA8F21D382B5E5B66E2A1E50C84AC28B7DA39BA1606092AA9
D1CAF8DC93E72>

Rprime.X:
<77CB284AC41E72EDA2A93EB8D6DFF58620F6C69D528DFE90D909AA5CAB
C03A34E5D5A76>

Rprime.Y:
<289997A39B5287D0905D9C4AF94EFEA4B9A1A7E7B983FDDC909E8ACF56
EED7F97D7E1C0>

Rprime:
<37CB284AC41E72EDA2A93EB8D6DFF58620F7CD99B927EEC7A060A8F6FB
7D9265EAFA76F>

Verification Passed!