**##
###**

Elliptic Curve Digital Signature Algorithm
Curve: B-283
Hash Algorithm: SHA3-256

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

**##
###**

Signature Generation
H:
B4809C0A000C5290B65D26DF9F12ADD919588FD4468958BC67CC7D9950A27EB8

E:
B4809C0A000C5290B65D26DF9F12ADD919588FD4468958BC67CC7D9950A27EB8

K:
100EC321393E6DD6C4D47BE5AE189E5E35408579D0862178F94CCBBA3C4049A4D88E297

Kinv:
AB6D18AF222D8FDE7D93894D4FAEEB36ACCD4FB68EC95D9E9BFF4C08AFF3C631A67BE4

R_x:
77CB284AC41E72EDA2A93EB8D6DFF58620F6C69D528DFE90D909AA5CABC03A34E5D5A76

R_y:
289997A39B5287D0905D9C4AF94EFEA4B9A1A7E7B983FDDC909E8ACF56EED7F97D7E1C0

R:
37CB284AC41E72EDA2A93EB8D6DFF58620F7CD99B927EEC7A060A8F6FB7D9265EAFA76F

D:
10652D37B0A9DB64D4033AC6549CD1DF37E1EEDE2612C2363257C6AFF6C8CB5DCB63648

S:
27A943BE3894A44E3EAA2A90CD83883767DBA364A10643BDECBE65C104A
E104589BED7A

Signature
R:
37CB284AC41E72EDA2A93EB8D6DFF58620F7CD99B927EEC7A060A8F6FB7
D9265EAFA76F

S:
27A943BE3894A44E3EAA2A90CD83883767DBA364A10643BDECBE65C104A
E104589BED7A

==========

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

H:
<B4809C0A000C5290B65D26DF9F12ADD919588FD4468958BC67CC7D9950
A27EB8>

E:
<B4809C0A000C5290B65D26DF9F12ADD919588FD4468958BC67CC7D9950
A27EB8>

Sinv:
<93B6AC351661E86BBC76029EBA8EBD9B65909AFE1C21BB2A50FFF3AC0C
806273514169>

U:
<11523C67EAF162AF0BE9468294492820B3E5DDFF752F800CD46975FD3A
4F533415707>

V:
<C1A5D2EE0DE80CB461F6A84F19D8CE615B5078A413F5B4614464D5A3BB
E3F73BE8098F>

Rprime.X:
<77CB284AC41E72EDA2A93EB8D6DFF58620F6C69D528DFE90D909AA5CAB
C03A34E5D5A76>

Rprime.Y:
<289997A39B5287D0905D9C4AF94EFEA4B9A1A7E7B983FDDC909E8ACF56
EED7F97D7E1C0>

Rprime:
<37CB284AC41E72EDA2A93EB8D6DFF58620F7CD99B927EEC7A060A8F6FB
7D9265EAFA76F>

Verification Passed!