**##
###**

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

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

**##
###**

Signature Generation
H:
**F0BF4AEF3F694EBDDE0A79445C897ADB2430B91877C772DA9B7362CB03A
EA87F**

E:
**F0BF4AEF3F694EBDDE0A79445C897ADB2430B91877C772DA9B7362CB03A
EA87F**

K:
**100EC321393E6DD6C4D47BE5AE189E5E35408579D0862178F94CCBBA3C4
049A4D88E297**

Kinv:
**AB6D18AF222D8FDE7D93894D4FAEEB36ACCD4FB68EC95D9E9BFF4C08AFF
3C631A67BE4**

R_x:
**77CB284AC41E72EDA2A93EB8D6DFF58620F6C69D528DFE90D909AA5CABC
03A34E5D5A76**

R_y:
**289997A39B5287D0905D9C4AF94EFEA4B9A1A7E7B983FDDC909E8ACF56E
ED7F97D7E1C0**

R:
**37CB284AC41E72EDA2A93EB8D6DFF58620F7CD99B927EEC7A060A8F6FB7
D9265EAFA76F**

D:
**10652D37B0A9DB64D4033AC6549CD1DF37E1EEDE2612C2363257C6AFF6C
8CB5DCB63648**

S:
A37AC10AEBFC22FC6E6EE22E8F235E3EEB0555A0F0F9DA92D9FFA734AD7
67956D27F23

Signature
R:
37CB284AC41E72EDA2A93EB8D6DFF58620F7CD99B927EEC7A060A8F6FB7
D9265EAFA76F

S:
A37AC10AEBFC22FC6E6EE22E8F235E3EEB0555A0F0F9DA92D9FFA734AD7
67956D27F23

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

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

H:
<F0BF4AEF3F694EBDDE0A79445C897ADB2430B91877C772DA9B7362CB03
AEA87F>

E:
<F0BF4AEF3F694EBDDE0A79445C897ADB2430B91877C772DA9B7362CB03
AEA87F>

Sinv:
<691C903459FF3E6F762F7FC5EEAE570BD514AC54AF645C1A4006C01991
B0629D550DC0>

U:
<1A9AF084B9E04574C178A2D00C97CFE36F25D5F834FCD7044235A92E89
AC3346C8C9AF3>

V:
<9949042A40D7613F3880CFCC3B3E9D22EE9C130651CEE1F263EFC881CF
9A53A564FBCE>

Rprime.X:
<77CB284AC41E72EDA2A93EB8D6DFF58620F6C69D528DFE90D909AA5CAB
C03A34E5D5A76>

Rprime.Y:
<289997A39B5287D0905D9C4AF94EFEA4B9A1A7E7B983FDDC909E8ACF56
EED7F97D7E1C0>

Rprime:
<37CB284AC41E72EDA2A93EB8D6DFF58620F7CD99B927EEC7A060A8F6FB
7D9265EAFA76F>

Verification Passed!