

#####  
###

**Elliptic Curve Digital Signature Algorithm**

Curve: K-283

Hash Algorithm: SHA3-256

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

#####  
###

**Signature Generation**

H:

1A58E77FF1E63D3294119CA946C481E77BDCB05EDFB265CCF904324A785  
C5422

E:

1A58E77FF1E63D3294119CA946C481E77BDCB05EDFB265CCF904324A785  
C5422

K:

E3084442D66FA9A02C42890163E57EE33CA1F4583C65BCBDE92781C7A3C  
83E89B773

$K_{inv}$ :

45D85F04239846DEB60444DA59F95CA0CA13FB9C30B6972E852E332E223  
067143D174D

$R_x$ :

7C973D58FD17A06AA8F39D5EC42E0A6B992F6CC61F157565DD7036C147D  
9005400C1328

$R_y$ :

12EB10ABED281AEDDA278423ECB45145E59AEFB5838C287AFD981F0D902  
38E0A8B13720

R:

1C973D58FD17A06AA8F39D5EC42E0A6B99339C1D57FF6F0EABD04ED57AE  
35F2E5C95E05

D:

69E6D19F7E454A83664FF49208F6038EAF842E164DF42D0F64948FF9C94  
B014988329

S:  
1E1A2E8C2CF4E4796B1B3F1C4D7B8F627D53888DF8CB1A7A2A499DC823E  
6E979AD7B285

Signature

R:  
1C973D58FD17A06AA8F39D5EC42E0A6B99339C1D57FF6F0EABD04ED57AE  
35F2E5C95E05

S:  
1E1A2E8C2CF4E4796B1B3F1C4D7B8F627D53888DF8CB1A7A2A499DC823E  
6E979AD7B285

=====  
==

Signature Verification

Q\_x:  
<1B64A60D4A365409635AAA27E1708D90B839AFA2D9820E12B79C3AF109  
4B6010AAEF5BE>

Q\_y:  
<334B5F30CA21756BDE6D47738F2458F56FBF6BDC76FCFB8F3E591455F0  
41A952EE87A8E>

H:  
<1A58E77FF1E63D3294119CA946C481E77BDCB05EDFB265CCF904324A78  
5C5422>

E:  
<1A58E77FF1E63D3294119CA946C481E77BDCB05EDFB265CCF904324A78  
5C5422>

Sinv:  
<1EE26BAF7FA9E5EDE97F10D27605301798B3CC0CC742F6800A5BD8DAC1  
DE7F13F9F0F>

U:  
<99E4231728A7CD32EEEF0955F02A20780130973CBC0C9EAA933E2F723A  
6AE97CCC722E>

V:  
<1559969D13DB35D9C290AEE28908508066F9FEE25EC86EAB53E918B015  
DE45119AA6FD2>

**Rprime.X:**  
**<7C973D58FD17A06AA8F39D5EC42E0A6B992F6CC61F157565DD7036C147  
D9005400C1328>**

**Rprime.Y:**  
**<12EB10ABED281AEDDA278423ECB45145E59AEFB5838C287AFD981F0D90  
238E0A8B13720>**

**Rprime:**  
**<1C973D58FD17A06AA8F39D5EC42E0A6B99339C1D57FF6F0EABD04ED57A  
E35F2E5C95E05>**

**Verification Passed!**