**##
###**

** Elliptic Curve Digital Signature Algorithm**
**   Curve: P-256**
**   Hash Algorithm: SHA3-256**

**   Message to be signed: "Example of ECDSA with P-256"**

**##
###**

** Signature Generation**
**   H:**
**3E39E85B251DF091BE8AA2E8C8831ECF688E0227E1D4C7042E674B9B646
5F3B**

**   E:**
**3E39E85B251DF091BE8AA2E8C8831ECF688E0227E1D4C7042E674B9B646
5F3B**

**   K:**
**7A1A7E52797FC8CAAA435D2A4DACE39158504BF204FBE19F14DBB427FAE
E50AE**

**   Kinv:**
**62159E5BA9E712FB098CCE8FE20F1BED8346554E98EF3C7C1FC3332BA67
D87EF**

**   R_x:**
**2B42F576D07F4165FF65D1F3B1500F81E44C316F1F0B3EF57325B69ACA4
6104F**

**   R_y:**
**3CE76603264661EA2F602DF7B4510BBC9ED939233C553EA5F42FB3F1338
174B5**

**   R:**
**2B42F576D07F4165FF65D1F3B1500F81E44C316F1F0B3EF57325B69ACA4
6104F**

**   D:**
**C477F9F65C22CCE20657FAA5B2D1D8122336F851A508A1ED04E479C3498
5BF96**

S:
A861C2526900245C73BACB9ADAEC1A5ACB3BA1F7114A3C334FDCD5B7690
DADD

Signature
R:
2B42F576D07F4165FF65D1F3B1500F81E44C316F1F0B3EF57325B69ACA4
6104F

S:
A861C2526900245C73BACB9ADAEC1A5ACB3BA1F7114A3C334FDCD5B7690
DADD

==========

Signature Verification
Q_x:
<B7E08AFDFE94BAD3F1DC8C734798BA1C62B3A0AD1E9EA2A38201CD0889
BC7A19>
Q_y:
<3603F747959DBF7A4BB226E41928729063ADC7AE43529E61B563BBC606
CC5E09>

H:
<3E39E85B251DF091BE8AA2E8C8831ECF688E0227E1D4C7042E674B9B64
65F3B>

E:
<3E39E85B251DF091BE8AA2E8C8831ECF688E0227E1D4C7042E674B9B64
65F3B>

Sinv:
<13AB6C3459517FA3C15F0B28E505961F670F62234FEFF83419E0E4366A
C12C6E>

U:
<BDF6F34A02AEEFE7B2E2047E6BFCCBB0FF9BF0FA86A6EDF5C47CBF37F5
580069>

V:
<DD9B1C0639B7FBEA8C79FA2DE793A2DB40383D0D18B295F957EE6CA93D
A191DD>

Rprime.X:
<2B42F576D07F4165FF65D1F3B1500F81E44C316F1F0B3EF57325B69ACA46104F>

Rprime.Y:
<3CE76603264661EA2F602DF7B4510BBC9ED939233C553EA5F42FB3F1338174B5>

Rprime:
<2B42F576D07F4165FF65D1F3B1500F81E44C316F1F0B3EF57325B69ACA46104F>

Verification Passed!