

#####  
###

**Elliptic Curve Digital Signature Algorithm**

Curve: K-233

Hash Algorithm: SHA3-224

Message to be signed: "Example of ECDSA with K-233"

#####  
###

**Signature Generation**

H:

82002E97C4A760B35EEE9059D533B5F25EF3D736D78839C0398FAFAB

E:

82002E97C4A760B35EEE9059D533B5F25EF3D736D78839C0398FAFAB

K:

190DA60FE3B179B96611DB7C7E5217C9AFF0AEE435782EBFB2DFFF27F

$K_{inv}$ :

759A37371C026E261ADD7278B81EE15D18E2B0D9BD1A077AEBF96AA067

$R_x$ :

1BEA7231662E6516F11E37D59D500EAE71D116E9B7BBCE5964B88D4CC4D

$R_y$ :

C98F8C9A7D65880920C2FEBE552D8245979E6D67CE82A41EF1BAD22FD3

R:

3EA7231662E6516F11E37D59D500D70F09E62D64FE6FF445C9B479C8B0

D:

8434613F4B799B4C26E4D7AB8E9481B04B09E648C94AFFD14B611A20

S:

4CC71DA49B12F09C1DFABB3D7B5BC03CE4898B5E07B2AA3D4BF6569395

**Signature**

R:

3EA7231662E6516F11E37D59D500D70F09E62D64FE6FF445C9B479C8B0

S:

4CC71DA49B12F09C1DFABB3D7B5BC03CE4898B5E07B2AA3D4BF6569395

=====  
==

**Signature Verification**

**Q\_x:**

<17C9DD766AEFBE4DE4B15F46DB0671DC4CA0767ED51ECEA94757D9C662E>

**Q\_y:**

<1CDD726084837AE73C11C27D605C6EB2D5E31482358780305C2522B151B>

**H:**

<82002E97C4A760B35EEE9059D533B5F25EF3D736D78839C0398FAFAB>

**E:**

<82002E97C4A760B35EEE9059D533B5F25EF3D736D78839C0398FAFAB>

**Sinv:**

<61BE9CB202B9D2763C64BE6BB11BDCEBD607BD24820EBC8CCAA900FF78>

**U:**

<13F54BE5101ECDD071F51ADC8C5D01B0A0058E54541EF22636B5B537BF>

**V:**

<16E5FF82AEA8DE6FF673CA9DE1D53A33A752CDA334737DC0EEB8F7437B>

**Rprime.X:**

<1BEA7231662E6516F11E37D59D500EAE71D116E9B7BBCE5964B88D4CC4D>

**Rprime.Y:**

<C98F8C9A7D65880920C2FEBE552D8245979E6D67CE82A41EF1BAD22FD3>

**Rprime:**

<3EA7231662E6516F11E37D59D500D70F09E62D64FE6FF445C9B479C8B0>

**Verification Passed!**

