

###

Elliptic Curve Digital Signature Algorithm

Curve: K-409

Hash Algorithm: SHA3-384

Message to be signed: "Example of ECDSA with K-409"

###

Signature Generation

H:

7FE0DD371839A9C84EAE70FACBFF763AB81F7D1B02FBFBCF9601B09DE08
6CE0E742ACEAA98A84D6C8B9A5287E7763598

E:

7FE0DD371839A9C84EAE70FACBFF763AB81F7D1B02FBFBCF9601B09DE08
6CE0E742ACEAA98A84D6C8B9A5287E7763598

K:

1592048516CCD793C7B863B00985FDBA71C3D1EDF449F667AC0D05EF37D
15A94AD3282F29F7E9FD9491872F931354A1CCFA39

K_{inv}:

64D066B74C9771A843F341A1853F0520696AA57338C21C4A839507B5EE6
5CB98A7F87C8E53037C02980CF5185300B709901D59

R_x:

EF421A230AA8B471939A77BF4F2C64FC0B4CAA39EDCD06337A9115AF89D
F725E3C748AE018320E89D77ABCD3AA13A6CCF10C34

R_y:

164387FE0AEA8291398012577B93D53EDA51DD1A7F1BF5E7D921164A579
6CDB822E90C8ABDA6D45616BF6387855FCBFA05AA4B7

R:

6F421A230AA8B471939A77BF4F2C64FC0B4CAA39EDCD06337A92B62BD70
A883DFC65C68A9AD33AA5EFB061884D8FEDECD2AC65

D:

19F5789FE26E0E700C69E253E9F74D76EAFB4C979D0B1584D4FE98715D4
5B7BAAA851E02A1ECAED8B96602CF611D8A504BBD5

S:
7116C6CF1FCDA7D13ACD5D3EB8C66D4769A642A6AAE1FA74A4C8F6B9C3C
D73C76EA3B6ED489D540C88EA92795EBF32849F3260

Signature

R:
6F421A230AA8B471939A77BF4F2C64FC0B4CAA39EDCD06337A92B62BD70
A883DFC65C68A9AD33AA5EFB061884D8FEDECD2AC65

S:
7116C6CF1FCDA7D13ACD5D3EB8C66D4769A642A6AAE1FA74A4C8F6B9C3C
D73C76EA3B6ED489D540C88EA92795EBF32849F3260

=====
==

Signature Verification

Q_x:
<127065590DF9265FDFBA4ED6EDF76A9BC8CE880B58B6F571A1AB62BA34
01269441F3B95ECD0909465022240AE45C7B36A91DE58>

Q_y:
<3C85268D9267302090425BBC14C3D9AE1C1CFC78E0BFCCCFC1FB5DCA5B
195C6F8CFBE2D85E4071B71317AA2B0B65C391F82502>

H:
<7FE0DD371839A9C84EAE70FACBFF763AB81F7D1B02FBFBCF9601B09DE0
86CE0E742ACEAA98A84D6C8B9A5287E7763598>

E:
<7FE0DD371839A9C84EAE70FACBFF763AB81F7D1B02FBFBCF9601B09DE0
86CE0E742ACEAA98A84D6C8B9A5287E7763598>

Sinv:
<791C5E2150CE0E8824067C2275BCF049021CCF356E616620CF516ACDB3
4520F329B1F2EFE6D78FE5A82209D4323D7B762C21E8>

U:
<51DD202D5731954F7523E804333CF56C9059D39D1D97A4966A6F1B291A
C868EF301A9ED055D39F3D3347007CBC1F523EF50207>

V:
<6DC6CDA8FC657CA5BB9AF149245317ACCEE90581B4147BE222BF46F241
AEAB6AEC627C298C7B63A4B52F41AE0AB28A2111C92D>

Rprime.X:

**<EF421A230AA8B471939A77BF4F2C64FC0B4CAA39EDCD06337A9115AF89
DF725E3C748AE018320E89D77ABCD3AA13A6CCF10C34>**

Rprime.Y:

**<164387FE0AEA8291398012577B93D53EDA51DD1A7F1BF5E7D921164A57
96CDB822E90C8ABDA6D45616BF6387855FCBFA05AA4B7>**

Rprime:

**<6F421A230AA8B471939A77BF4F2C64FC0B4CAA39EDCD06337A92B62BD7
0A883DFC65C68A9AD33AA5EFB061884D8FEDECD2AC65>**

Verification Passed!