**##
###**

Elliptic Curve Digital Signature Algorithm
Curve: K-409
Hash Algorithm: SHA-384

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

**##
###**

Signature Generation
H:
B18623FE7D6B79C3947651CF64A066400F89DC989D07BFD8C1AAF75E3C9B3D48FC457204168DE4ED4ECA8E240E009B95

E:
B18623FE7D6B79C3947651CF64A066400F89DC989D07BFD8C1AAF75E3C9B3D48FC457204168DE4ED4ECA8E240E009B95

K:
1592048516CCD793C7B863B00985FDBA71C3D1EDF449F667AC0D05EF37D15A94AD3282F29F7E9FD9491872F931354A1CCFA39

Kinv:
64D066B74C9771A843F341A1853F0520696AA57338C21C4A839507B5EE65CB98A7F87C8E53037C02980CF5185300B709901D59

R_x:
EF421A230AA8B471939A77BF4F2C64FC0B4CAA39EDCD06337A9115AF89DF725E3C748AE018320E89D77ABCD3AA13A6CCF10C34

R_y:
164387FE0AEA8291398012577B93D53EDA51DD1A7F1BF5E7D921164A5796CDB822E90C8ABDA6D45616BF6387855FCBFA05AA4B7

R:
6F421A230AA8B471939A77BF4F2C64FC0B4CAA39EDCD06337A92B62BD70A883DFC65C68A9AD33AA5EFB061884D8FEDECD2AC65

D:
19F5789FE26E0E700C69E253E9F74D76EAFB4C979D0B1584D4FE98715D45B7BAAA851E02A1ECAED8B96602CF611D8A504BBD5

S:
425F2FF9CBBF1B9E3FC17C4B66303622D7749047373CC9F919758CD8842
0C4CD0FDF14B819A4ADA9961C3E6095000467C2F823

Signature
R:
6F421A230AA8B471939A77BF4F2C64FC0B4CAA39EDCD06337A92B62BD70
A883DFC65C68A9AD33AA5EFB061884D8FEDECD2AC65

S:
425F2FF9CBBF1B9E3FC17C4B66303622D7749047373CC9F919758CD8842
0C4CD0FDF14B819A4ADA9961C3E6095000467C2F823

==========

Signature Verification
Q_x:
<127065590DF9265FDFBA4ED6EDF76A9BC8CE880B58B6F571A1AB62BA34
01269441F3B95ECD0909465022240AE45C7B36A91DE58>
Q_y:
<3C85268D9267302090425BBC14C3D9AE1C1CFC78E0BFCCCFC1FB5DCA5B
195C6F8CFBE2D85E4071B71317AA2B0B65C391F82502>

H:
<B18623FE7D6B79C3947651CF64A066400F89DC989D07BFD8C1AAF75E3C
9B3D48FC457204168DE4ED4ECA8E240E009B95>

E:
<B18623FE7D6B79C3947651CF64A066400F89DC989D07BFD8C1AAF75E3C
9B3D48FC457204168DE4ED4ECA8E240E009B95>

Sinv:
<7ADBF46AC13A5F3A7E0F494B54622933D5F57963EF2F4BF3CB56ABE5FC
9454860FEB07FC80A9B6CDF505977510D92A64B5B41B>

U:
<7FC6BDB66A9D2A23BF69D4F96BB3E7E24E365B45D111C666747A42B392
75ED0BA4F2866D3723DD13851A45208C864525D5F530>

V:
<5E16D63457088B1F3012E844C852E23C9F1225AA569A883DE8A5828DDE
30917D23C4D807A371AA1FC5DB25149ABBCD53F7558>

Rprime.X:
<EF421A230AA8B471939A77BF4F2C64FC0B4CAA39EDCD06337A9115AF89DF725E3C748AE018320E89D77ABCD3AA13A6CCF10C34>

Rprime.Y:
<164387FE0AEA8291398012577B93D53EDA51DD1A7F1BF5E7D921164A5796CDB822E90C8ABDA6D45616BF6387855FCBFA05AA4B7>

Rprime:
<6F421A230AA8B471939A77BF4F2C64FC0B4CAA39EDCD06337A92B62BD70A883DFC65C68A9AD33AA5EFB061884D8FEDECD2AC65>

Verification Passed!