```
##############################################################

  Elliptic Curve Digital Signature Algorithm
    Curve = P-192
    Hash Length = 160

##############################################################

==============================================================

Private Key Generation

N is
        FFFFFFFF FFFFFFFF FFFFFFFF 99DEF836 146BC9B1 B4D22831


--------------------------------------------------------------

C is
        78916860 32FD8057 F636B44B 1F47CCE5 64D25099 23A7465A


--------------------------------------------------------------

D is
        78916860 32FD8057 F636B44B 1F47CCE5 64D25099 23A7465B


Q_x is
        FBA2AAC6 47884B50 4EB8CD5A 0A1287BA BCC62163 F606A9A2


Q_y is
        DAE6D4CC 05EF4F27 D79EE38B 71C9C8EF 4865D988 50D84AA5


==============================================================

Private Key Generation

N is
        FFFFFFFF FFFFFFFF FFFFFFFF 99DEF836 146BC9B1 B4D22831


--------------------------------------------------------------

C is
        D06CB0A0 EF2F708B 0744F08A A06B6DEE DEA9C0F8 0A69D846


--------------------------------------------------------------

K is
        D06CB0A0 EF2F708B 0744F08A A06B6DEE DEA9C0F8 0A69D847


==============================================================

Signature Generation

msg is "Example of ECDSA with P-192"
Hash length = 160
```

```
D is
        78916860 32FD8057 F636B44B 1F47CCE5 64D25099 23A7465B


--------------------------------------------------------------

K is
        D06CB0A0 EF2F708B 0744F08A A06B6DEE DEA9C0F8 0A69D847


R_x is
        F0ECBA72 B88CDE39 9CC5A18E 2A8B7DA5 4D81D04F B9802821


E is
                 1B376F0B 735C615C EEEB31BA EE654B0A 374825DB


Kinv is
        5A277943 C5A4D34B 3C7DD97B DFE9B82C 04258670 1088C00B


--------------------------------------------------------------

Signature:
  R is
        F0ECBA72 B88CDE39 9CC5A18E 2A8B7DA5 4D81D04F B9802821


  S is
        1E6D3D4A E2B1FAB2 BD2040F5 DABF00F8 54FA140B 6D21E8ED


==============================================================

Signature Verification

msg is "Example of ECDSA with P-192"
Hash length = 160
Signature:
  R is
        F0ECBA72 B88CDE39 9CC5A18E 2A8B7DA5 4D81D04F B9802821


  S is
        1E6D3D4A E2B1FAB2 BD2040F5 DABF00F8 54FA140B 6D21E8ED


Public Key:
  Q_x is
        FBA2AAC6 47884B50 4EB8CD5A 0A1287BA BCC62163 F606A9A2


  Q_y is
        DAE6D4CC 05EF4F27 D79EE38B 71C9C8EF 4865D988 50D84AA5


--------------------------------------------------------------

E is
                 1B376F0B 735C615C EEEB31BA EE654B0A 374825DB
```

```
U1 is
        785760FD 37767D54 6003FA66 933B7D20 26423523 31B15B84


U2 is
        DE074707 2E426E30 7BA1E19B D5C1B57F 9E29220A E97CC9BC


R_x is
        F0ECBA72 B88CDE39 9CC5A18E 2A8B7DA5 4D81D04F B9802821


V is
        F0ECBA72 B88CDE39 9CC5A18E 2A8B7DA5 4D81D04F B9802821


R' is
        F0ECBA72 B88CDE39 9CC5A18E 2A8B7DA5 4D81D04F B9802821


--------------------------------------------------------------

Signature is verified


##############################################################

  Elliptic Curve Digital Signature Algorithm
    Curve = P-224
    Hash Length = 224

##############################################################

==============================================================

Private Key Generation

N is
                                                     FFFFFFFF
        FFFFFFFF FFFFFFFF FFFF16A2 E0B8F03E 13DD2945 5C5C2A3D


--------------------------------------------------------------

C is
                                                     3F0C488E
        987C80BE 0FEE521F 8D90BE60 34EC69AE 11CA72AA 777481E7


--------------------------------------------------------------

D is
                                                     3F0C488E
        987C80BE 0FEE521F 8D90BE60 34EC69AE 11CA72AA 777481E8


Q_x is
                                                     E84FB0B8
        E7000CB6 57D7973C F6B42ED7 8B301674 276DF744 AF130B3E
```

```
Q_y is
                                                     4376675C
        6FC5612C 21A0FF2D 2A89D298 7DF7A2BC 52183B59 82298555


==============================================================

Private Key Generation

N is
                                                     FFFFFFFF
        FFFFFFFF FFFFFFFF FFFF16A2 E0B8F03E 13DD2945 5C5C2A3D


--------------------------------------------------------------

C is
                                                     A548803B
        79DF17C4 0CDE3FF0 E36D0251 43BCBBA1 46EC3290 8EB84936


--------------------------------------------------------------

K is
                                                     A548803B
        79DF17C4 0CDE3FF0 E36D0251 43BCBBA1 46EC3290 8EB84937


==============================================================

Signature Generation

msg is "Example of ECDSA with P-224"
Hash length = 224
D is
                                                     3F0C488E
        987C80BE 0FEE521F 8D90BE60 34EC69AE 11CA72AA 777481E8


--------------------------------------------------------------

K is
                                                     A548803B
        79DF17C4 0CDE3FF0 E36D0251 43BCBBA1 46EC3290 8EB84937


R_x is
                                                     C3A3F5B8
        27125320 04C6F6D1 DB672F55 D931C340 9EA1216D 0BE77380


E is
                                                     1F1E1CF8
        92926CFC CFC5A28F EEF3D807 D23F7780 08DBA4B3 5F04B2FD


Kinv is
                                                     B4D9D81F
        EFF7B325 E09E770C 40BACE8B 008D6074 37196732 6F39130C


--------------------------------------------------------------
```

```
Signature:
  R is
                                                     C3A3F5B8
        27125320 04C6F6D1 DB672F55 D931C340 9EA1216D 0BE77380


  S is
                                                     C5AA1EAE
        6095DEA3 4C9BD84D A3852CCA 41A8BD9D 5548F36D ABDF6617


==============================================================

Signature Verification

msg is "Example of ECDSA with P-224"
Hash length = 224
Signature:
  R is
                                                     C3A3F5B8
        27125320 04C6F6D1 DB672F55 D931C340 9EA1216D 0BE77380


  S is
                                                     C5AA1EAE
        6095DEA3 4C9BD84D A3852CCA 41A8BD9D 5548F36D ABDF6617


Public Key:
  Q_x is
                                                     E84FB0B8
        E7000CB6 57D7973C F6B42ED7 8B301674 276DF744 AF130B3E


  Q_y is
                                                     4376675C
        6FC5612C 21A0FF2D 2A89D298 7DF7A2BC 52183B59 82298555


--------------------------------------------------------------

E is
                                                     1F1E1CF8
        92926CFC CFC5A28F EEF3D807 D23F7780 08DBA4B3 5F04B2FD


U1 is
                                                     69DF611D
        F949498E BE20C1E4 53CF231C DD2F30AD EECBA933 5481295D


U2 is
                                                     86DAAF97
        DC9BB13A 66EC7B73 5E69BCCD 60F395EF B2CDFDED 8A3CCBCF


R_x is
                                                     C3A3F5B8
        27125320 04C6F6D1 DB672F55 D931C340 9EA1216D 0BE77380
```

```
V is
                                                     C3A3F5B8
        27125320 04C6F6D1 DB672F55 D931C340 9EA1216D 0BE77380


R' is
                                                     C3A3F5B8
        27125320 04C6F6D1 DB672F55 D931C340 9EA1216D 0BE77380


--------------------------------------------------------------

Signature is verified


##############################################################

  Elliptic Curve Digital Signature Algorithm
    Curve = P-256
    Hash Length = 256

##############################################################

==============================================================

Private Key Generation

N is
                                            FFFFFFFF 00000000
        FFFFFFFF FFFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551


--------------------------------------------------------------

C is
                                            C477F9F6 5C22CCE2
        0657FAA5 B2D1D812 2336F851 A508A1ED 04E479C3 4985BF95


--------------------------------------------------------------

D is
                                            C477F9F6 5C22CCE2
        0657FAA5 B2D1D812 2336F851 A508A1ED 04E479C3 4985BF96


Q_x is
                                            B7E08AFD FE94BAD3
        F1DC8C73 4798BA1C 62B3A0AD 1E9EA2A3 8201CD08 89BC7A19


Q_y is
                                            3603F747 959DBF7A
        4BB226E4 19287290 63ADC7AE 43529E61 B563BBC6 06CC5E09


==============================================================

Private Key Generation

N is
                                            FFFFFFFF 00000000
        FFFFFFFF FFFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551


--------------------------------------------------------------

C is
                                            7A1A7E52 797FC8CA
        AA435D2A 4DACE391 58504BF2 04FBE19F 14DBB427 FAEE50AD


--------------------------------------------------------------

K is
                                            7A1A7E52 797FC8CA
        AA435D2A 4DACE391 58504BF2 04FBE19F 14DBB427 FAEE50AE


==============================================================

Signature Generation

msg is "Example of ECDSA with P-256"
Hash length = 256
D is
                                            C477F9F6 5C22CCE2
        0657FAA5 B2D1D812 2336F851 A508A1ED 04E479C3 4985BF96


--------------------------------------------------------------

K is
                                            7A1A7E52 797FC8CA
        AA435D2A 4DACE391 58504BF2 04FBE19F 14DBB427 FAEE50AE


R_x is
                                            2B42F576 D07F4165
        FF65D1F3 B1500F81 E44C316F 1F0B3EF5 7325B69A CA46104F


E is
                                            A41A41A1 2A799548
        211C410C 65D8133A FDE34D28 BDD542E4 B680CF28 99C8A8C4


Kinv is
                                            62159E5B A9E712FB
        098CCE8F E20F1BED 8346554E 98EF3C7C 1FC3332B A67D87EF


--------------------------------------------------------------

Signature:
  R is
                                            2B42F576 D07F4165
        FF65D1F3 B1500F81 E44C316F 1F0B3EF5 7325B69A CA46104F


  S is
                                            DC42C212 2D6392CD
        3E3A993A 89502A81 98C1886F E69D262C 4B329BDB 6B63FAF1
```

```
==============================================================

Signature Verification

msg is "Example of ECDSA with P-256"
Hash length = 256
Signature:
  R is
                                            2B42F576 D07F4165
        FF65D1F3 B1500F81 E44C316F 1F0B3EF5 7325B69A CA46104F


  S is
                                            DC42C212 2D6392CD
        3E3A993A 89502A81 98C1886F E69D262C 4B329BDB 6B63FAF1


Public Key:
  Q_x is
                                            B7E08AFD FE94BAD3
        F1DC8C73 4798BA1C 62B3A0AD 1E9EA2A3 8201CD08 89BC7A19


  Q_y is
                                            3603F747 959DBF7A
        4BB226E4 19287290 63ADC7AE 43529E61 B563BBC6 06CC5E09


--------------------------------------------------------------

E is
                                            A41A41A1 2A799548
        211C410C 65D8133A FDE34D28 BDD542E4 B680CF28 99C8A8C4


U1 is
                                            B807BF32 81DD1384
        9958F444 FD9AEA80 8D074C2C 48EE8382 F6C47A43 5389A17E


U2 is
                                            1777F734 43A4D68C
        23D1FC4C B5F8B7F2 554578EE 87F04C25 3DF44EFD 181C184C


R_x is
                                            2B42F576 D07F4165
        FF65D1F3 B1500F81 E44C316F 1F0B3EF5 7325B69A CA46104F


V is
                                            2B42F576 D07F4165
        FF65D1F3 B1500F81 E44C316F 1F0B3EF5 7325B69A CA46104F


R' is
                                            2B42F576 D07F4165
        FF65D1F3 B1500F81 E44C316F 1F0B3EF5 7325B69A CA46104F


--------------------------------------------------------------
```

```
Signature is verified


##############################################################

  Elliptic Curve Digital Signature Algorithm
    Curve = P-384
    Hash Length = 384

##############################################################

==============================================================

Private Key Generation

N is
        FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
        C7634D81 F4372DDF 581A0DB2 48B0A77A ECEC196A CCC52973


--------------------------------------------------------------

C is
        F92C02ED 629E4B48 C0584B1C 6CE3A3E3 B4FAAE4A FC6ACB04
        55E73DFC 392E6A0A E393A856 5E6B9714 D1224B57 D83F8A07


--------------------------------------------------------------

D is
        F92C02ED 629E4B48 C0584B1C 6CE3A3E3 B4FAAE4A FC6ACB04
        55E73DFC 392E6A0A E393A856 5E6B9714 D1224B57 D83F8A08


Q_x is
        3BF701BC 9E9D36B4 D5F14553 43F09126 F2564390 F2B48736
        5071243C 61E6471F B9D2AB74 657B82F9 086489D9 EF0F5CB5


Q_y is
        D1A358EA FBF952E6 8D533855 CCBDAA6F F75B137A 51014431
        99325583 552A6295 FFE5382D 00CFCDA3 0344A9B5 B68DB855


==============================================================

Private Key Generation

N is
        FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
        C7634D81 F4372DDF 581A0DB2 48B0A77A ECEC196A CCC52973


--------------------------------------------------------------

C is
        2E44EF1F 8C0BEA83 94E3DDA8 1EC6A784 2A459B53 4701749E
        2ED95F05 4F013768 0878E074 9FC43F85 EDCAE06C C2F43FEE


--------------------------------------------------------------
```

```
K is
        2E44EF1F 8C0BEA83 94E3DDA8 1EC6A784 2A459B53 4701749E
        2ED95F05 4F013768 0878E074 9FC43F85 EDCAE06C C2F43FEF


==============================================================

Signature Generation

msg is "Example of ECDSA with P-384"
Hash length = 384
D is
        F92C02ED 629E4B48 C0584B1C 6CE3A3E3 B4FAAE4A FC6ACB04
        55E73DFC 392E6A0A E393A856 5E6B9714 D1224B57 D83F8A08


--------------------------------------------------------------


K is
        2E44EF1F 8C0BEA83 94E3DDA8 1EC6A784 2A459B53 4701749E
        2ED95F05 4F013768 0878E074 9FC43F85 EDCAE06C C2F43FEF


R_x is
        30EA514F C0D38D82 08756F06 8113C7CA DA9F66A3 B40EA3B3
        13D040D9 B57DD41A 332795D0 2CC7D507 FCEF9FAF 01A27088


E is
        5AEA187D 1C4F6E1B 35057D20 126D836C 6ADBBC70 49EE0299
        C9529F5E 0B3F8B5A 7411149D 6C30D6CB 2B8AF70E 0A781E89


Kinv is
        AC227DA5 1929533D FC2E9EEF B4E0F7BD 22392CA7 3289ED1C
        6C00B214 E8874D80 07C8AC46 B25D677D FE9B1C6C 10A47E4A


--------------------------------------------------------------

Signature:
  R is
        30EA514F C0D38D82 08756F06 8113C7CA DA9F66A3 B40EA3B3
        13D040D9 B57DD41A 332795D0 2CC7D507 FCEF9FAF 01A27088


  S is
        CC808E50 4BE414F4 6C9027BC BF78ADF0 67A43922 D6FCAA66
        C4476875 FBB7B94E FD1F7D5D BE620BFB 821C46D5 49683AD8


==============================================================

Signature Verification

msg is "Example of ECDSA with P-384"
Hash length = 384
Signature:
  R is
        30EA514F C0D38D82 08756F06 8113C7CA DA9F66A3 B40EA3B3
        13D040D9 B57DD41A 332795D0 2CC7D507 FCEF9FAF 01A27088
  S is
        CC808E50 4BE414F4 6C9027BC BF78ADF0 67A43922 D6FCAA66
        C4476875 FBB7B94E FD1F7D5D BE620BFB 821C46D5 49683AD8


Public Key:
  Q_x is
        3BF701BC 9E9D36B4 D5F14553 43F09126 F2564390 F2B48736
        5071243C 61E6471F B9D2AB74 657B82F9 086489D9 EF0F5CB5


  Q_y is
        D1A358EA FBF952E6 8D533855 CCBDAA6F F75B137A 51014431
        99325583 552A6295 FFE5382D 00CFCDA3 0344A9B5 B68DB855


--------------------------------------------------------------

E is
        5AEA187D 1C4F6E1B 35057D20 126D836C 6ADBBC70 49EE0299
        C9529F5E 0B3F8B5A 7411149D 6C30D6CB 2B8AF70E 0A781E89


U1 is
        9C0590EE 8000B798 32DC4C67 76F7E5FD 2A74BE16 1741C7C2
        D2F038D4 39831696 A1B8ECE4 199D225B 12B76DD9 E637B250


U2 is
        8F77BE5B 0EB32A1A 3B9274CF DA53518A 01AAD4AF C4BD46A3
        92B7C7DE 4EED3FE6 DEE54F30 64234FE7 FDE57AE4 5532C24D


R_x is
        30EA514F C0D38D82 08756F06 8113C7CA DA9F66A3 B40EA3B3
        13D040D9 B57DD41A 332795D0 2CC7D507 FCEF9FAF 01A27088


V is
        30EA514F C0D38D82 08756F06 8113C7CA DA9F66A3 B40EA3B3
        13D040D9 B57DD41A 332795D0 2CC7D507 FCEF9FAF 01A27088


R' is
        30EA514F C0D38D82 08756F06 8113C7CA DA9F66A3 B40EA3B3
        13D040D9 B57DD41A 332795D0 2CC7D507 FCEF9FAF 01A27088


--------------------------------------------------------------

Signature is verified


##############################################################

  Elliptic Curve Digital Signature Algorithm
    Curve = P-521
    Hash Length = 512

##############################################################
```

```
==============================================================

Private Key Generation

N is
                     01FF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
        FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFA 51868783 BF2F966B
        7FCC0148 F709A5D0 3BB5C9B8 899C47AE BB6FB71E 91386409


--------------------------------------------------------------


C is
                          C91E2349 EF6CA22D 2DE39DD5 1819B6AA
        D922D3AE CDEAB452 BA172F7D 63E370CE CD70575F 597C09A1
        74BA76BE D05A48E5 62BE0625 336D16B8 703147A6 A231D6BE


--------------------------------------------------------------

K is
                          C91E2349 EF6CA22D 2DE39DD5 1819B6AA
        D922D3AE CDEAB452 BA172F7D 63E370CE CD70575F 597C09A1
        74BA76BE D05A48E5 62BE0625 336D16B8 703147A6 A231D6BF


==============================================================

Signature Generation

msg is "Example of ECDSA with P-521"
Hash length = 512
D is
                     0100 085F47B8 E1B8B11B 7EB33028 C0B2888E
        304BFC98 501955B4 5BBA1478 DC184EEE DF09B86A 5F7C2199
        44060727 87205E69 A63709FE 35AA93BA 333514B2 4F961722


--------------------------------------------------------------

K is
                          C91E2349 EF6CA22D 2DE39DD5 1819B6AA
        D922D3AE CDEAB452 BA172F7D 63E370CE CD70575F 597C09A1
        74BA76BE D05A48E5 62BE0625 336D16B8 703147A6 A231D6BF


R_x is
                     0140 C8EDCA57 108CE3F7 E7A240DD D3AD74D8
        1E2DE624 51FC1D55 8FDC7926 9ADACD1C 2526EEEE F32F8C04
        32A9D56E 2B4A8A73 2891C37C 9B96641A 9254CCFE 5DC3E2BA


E is
                          9BF0E1DE EDA31E00 F925B77F 7CB6B1CE
        D7368DE1 DC75BB9F 94582C1C A709205D 32AF9002 5B02FA13
        2FBEBD6C DDCD9172 C0D66D8E 581767A8 B6F71DE6 0BE1F932


Kinv is
                     01EA B94335A7 ED337BCE 83C95DE9 5447925E
        DB0EE27F 8E837871 3E767D6D A570FCCF B4F13DCF 57F898E7
        7DDB540A 9453E0C3 D5C97AE8 D2EC8435 90BCB1D3 49044C09


--------------------------------------------------------------

Signature:
  R is
                     0140 C8EDCA57 108CE3F7 E7A240DD D3AD74D8
        1E2DE624 51FC1D55 8FDC7926 9ADACD1C 2526EEEE F32F8C04
        32A9D56E 2B4A8A73 2891C37C 9B96641A 9254CCFE 5DC3E2BA


  S is
                     00D7 2F15229D 0096376D A6651D99 85BFD7C0
        7F8D4958 3B545DB3 EAB20E0A 2C1E8615 BD9E2984 55BDEB6B
        61378E77 AF1C54EE E2CE37B2 C61F5C9A 8232951C B988B5B1


==============================================================

Signature Verification

msg is "Example of ECDSA with P-521"
Hash length = 512
Signature:
  R is
                     0140 C8EDCA57 108CE3F7 E7A240DD D3AD74D8
        1E2DE624 51FC1D55 8FDC7926 9ADACD1C 2526EEEE F32F8C04
        32A9D56E 2B4A8A73 2891C37C 9B96641A 9254CCFE 5DC3E2BA


  S is
                     00D7 2F15229D 0096376D A6651D99 85BFD7C0
        7F8D4958 3B545DB3 EAB20E0A 2C1E8615 BD9E2984 55BDEB6B
        61378E77 AF1C54EE E2CE37B2 C61F5C9A 8232951C B988B5B1


Public Key:
  Q_x is
                     0098 E91EEF9A 68452822 309C52FA B453F5F1
        17C1DA8E D796B255 E9AB8F64 10CCA16E 59DF403A 6BDC6CA4
        67A37056 B1E54B30 05D8AC03 0DECFEB6 8DF18B17 1885D5C4


  Q_y is
                     0164 350C321A ECFC1CCA 1BA4364C 9B156561
        50B4B78D 6A48D7D2 8E7F3198 5EF17BE8 554376B7 2900712C
        4B83AD66 83272315 26E313F5 F092999A 4632FD50 D946BC2E


--------------------------------------------------------------

E is
                          9BF0E1DE EDA31E00 F925B77F 7CB6B1CE
        D7368DE1 DC75BB9F 94582C1C A709205D 32AF9002 5B02FA13
        2FBEBD6C DDCD9172 C0D66D8E 581767A8 B6F71DE6 0BE1F932


U1 is
                     0169 7EEFB6BD 3A6DB024 254FE69F D19C80EB
        04B71CDD 16AF72F3 22106093 F971CB08 C29F6F89 50F0F61E
        45BF65BA C39A590D CB043758 C6606907 F216A759 B4EA4BE4


U2 is
                     014E 7FC3EE94 B91E092F 660253DC AF92A703
        06BDFA31 7A0AB7EF B2C82869 44BEE5F1 46114F2C 61950F8C
        8699CCE1 A22FE632 EA89967D 33FEFCB0 E7607B4B 66D157B6


R_x is
                     0140 C8EDCA57 108CE3F7 E7A240DD D3AD74D8
        1E2DE624 51FC1D55 8FDC7926 9ADACD1C 2526EEEE F32F8C04
        32A9D56E 2B4A8A73 2891C37C 9B96641A 9254CCFE 5DC3E2BA


V is
                     0140 C8EDCA57 108CE3F7 E7A240DD D3AD74D8
        1E2DE624 51FC1D55 8FDC7926 9ADACD1C 2526EEEE F32F8C04
        32A9D56E 2B4A8A73 2891C37C 9B96641A 9254CCFE 5DC3E2BA


R' is
                     0140 C8EDCA57 108CE3F7 E7A240DD D3AD74D8
        1E2DE624 51FC1D55 8FDC7926 9ADACD1C 2526EEEE F32F8C04
        32A9D56E 2B4A8A73 2891C37C 9B96641A 9254CCFE 5DC3E2BA


--------------------------------------------------------------

Signature is verified
```