The Elliptic Curve Digital Signature Algorithm Validation System (ECDSAVS)

September 7, 2004

Lawrence E. Bassham III

National Institute of Standards and Technology

Information Technology Laboratory

Computer Security Division

TABLE OF CONTENTS

1 Introduction

The Elliptic Curve Digital Signature Algorithm Validation System (ECDSAVS) specifies the procedures involved in validating implementations of the Elliptic Curve Digital Signature Algorithm (ECDSA) as approved in FIPS 186-2, *Digital Signature Standard (DSS)*[1] and specified in ANSI X9.62-1998, *Public Key Cryptography for Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*[2]. The ECDSAVS is designed to perform automated testing on Implementations Under Test (IUTs). This document provides the basic design and configuration of the ECDSAVS.

This document defines the purpose, the design philosophy, and the high-level description of the validation process for ECDSA. The requirements and administrative procedures to be followed by those seeking formal validation of an implementation of the ECDSA are presented. The requirements described include the specification of the data communicated between the IUT and the ECDSAVS, the details of the tests that the IUT must pass for formal validation, and general instruction for interfacing with the ECDSAVS.

2 Scope

This document specifies the tests required to validate IUTs for conformance to the ECDSA. When applied to IUTs that implement ECDSA, the ECDSAVS provides testing to determine the correctness of the algorithm components contained in the implementation. The ECDSAVS is composed of four separate tests – each one to validate a different algorithm component.

3 Conformance

The successful completion of the tests contained within the ECDSAVS is required to be validated as conforming to the ECDSA. Testing for the cryptographic module in which the ECDSA is implemented is defined in FIPS PUB 140-2, *Security Requirements for Cryptographic Modules* [4].

4 List of Abbreviations

ABBREVIATION	**MEANING**
CMT Laboratory	Cryptographic Module Testing laboratory that operates the ECDSAVS.
ECDSA	Elliptic Curve Digital Signature Algorithm approved in FIPS 186-2 [1] and specified in [2].

ECDSAVS	Elliptic Curve Digital Signature Algorithm Validation System.
FIPS	Federal Information Processing Standard.
IUT	Implementation Under Test.

5 Design Philosophy Of The Elliptic Curve Digital Signature Algorithm Validation System

The ECDSAVS is designed to test conformance to ECDSA rather than provide a measure of a product's security. The validation tests are designed to assist in the detection of accidental implementation errors, and are not designed to detect intentional attempts to misrepresent conformance. Thus, validation should not be interpreted as an evaluation or endorsement of overall product security.

The ECDSAVS has the following design philosophy:

1. The ECDSAVS is designed to allow the testing of an IUT at locations remote to the ECDSAVS. The ECDSAVS and the IUT communicate data via *REQUEST* and *RESPONSE* files.

2. The testing performed within the ECDSAVS utilizes statistical sampling (i.e., only a small number of the possible cases are tested); hence, the successful validation of a device does not imply 100% conformance with the standard.

3. The ECDSAVS is designed to test implementations using the Recommended Elliptic Curves For Federal Government Use found in [1, Appendix 6]. For the remainder of this document these curves will be referred to as the NIST Recommended Curves.

6 ECDSAVS Tests

The ECDSAVS for the ECDSA consists of separate tests for each of four distinct components of the ECDSA. The ECDSAVS provides conformance testing for each of the components of the algorithm, as well as testing for apparent implementation errors. The various components that are tested with the ECDSAVS are:

- Generation of Private and Public Key Pairs,
- Public Key Validation,
- Signature Generation, and

- Signature Verification.

6.1 Configuration Information

To initiate the validation process of the ECDSAVS, a vendor submits an application to an accredited laboratory requesting the validation of its ECDSA implementation. The vendor's implementation is referred to as the Implementation Under Test (IUT). The request for validation includes background information describing the IUT along with information needed by the ECDSAVS to perform the specific tests. More specifically, the request for validation includes:

1. Vendor Name;
2. Product Name;
3. Product Version;
4. Implementation in software, firmware, or hardware;
5. Processor and Operating System with which the IUT was tested if the IUT is implemented in software or firmware;
6. Brief description of the IUT or the product/product family in which the IUT is implemented by the vendor (2-3 sentences); and,
7. The list of NIST Recommended Curve(s) supported for each of the components to be tested.

6.2 Key Pair Generation Test

Key pairs for the ECDSA consist of pairs (d, Q), where the private key, d, is an integer, and the public key, Q, is an elliptic curve point. These pairs are generated using the technique described in Section 5.2.1 of ANSI X9.62.

The ECDSAVS tests the generation of key pairs for correctness by having the IUT produce 10 key pairs. The private key provided is used to compute the public key, Q'. The computed value Q' is then compared to the supplied public key, Q.

The ECDSAVS:

A. Creates a *REQUEST* file (Filename: KeyPair.req) containing:

   1. The Product Information (vendor, product name, version);
   2. An indication of the NIST Recommended Curve(s) supported.

   Note: The CMT laboratory sends the *REQUEST* file to the IUT.

The IUT:

A. Generates the 10 key pairs per curve specified in the *REQUEST* file.

B. Creates a *RESPONSE* file (Filename: KeyPair.rsp) containing:

1. The Product Information (vendor, product name, version); and

2. For each curve supported, the 10 key pairs consisting of the private key, *d*, and the public key, *Q*.

Note: The IUT sends the *RESPONSE* file to the CMT laboratory for processing by the ECDSAVS.

The ECDSAVS:

A. Recalculates the public key, *Q'*, from the private key supplied in the response file. The value *Q'* is then compared to the supplied value *Q*.

B. If all values of *Q'* match the supplied values of *Q*, records PASS for this test; otherwise, records FAIL.

6.3 Public Key Validation Test

An IUT may include a routine for EC public key validation, as specified in Section 5.2.2 of ANSI X9.62. If so, the ECDSAVS will generate 12 key pairs for each supported curve, modify some of the public keys to introduce errors, and determine whether or not the IUT can detect these errors.

The ECDSAVS:

A. Generates 12 sets of valid key pairs for each curve supported by the IUT.

B. Makes a copy of the valid public keys created above, modifies some of the public keys to introduce errors by changing the value of the key, and runs Public Key Validation on the modified keys to be sure that the modification does not inadvertently result in a valid key.

C. Creates a *REQUEST* file (Filename: PKV.req) containing:

1. The Product Information (vendor, product name, version); and

2. For each curve supported, the 12 public keys from step B above.

Note: The CMT laboratory sends the *REQUEST* file to the IUT.

D. Creates a *FAX* file (Filename: PKV.fax) containing:

1. The information from the *REQUEST* file; and

2. For each public key, an indication of whether the key should pass the Public Key Validation test.

Note: The CMT laboratory retains the *FAX* file.

The IUT:

A. For each public key found in the *REQUEST* file, determines whether or not the public key passes all the conditions in Section 5.2.2 of ANSI X9.62.

B. Creates a *RESPONSE* file (Filename: PKV.rsp) containing:

   1. The information from the *REQUEST* file; and

   2. For each public key, an indication of whether the key passes or fails the Public Key Validation test.

   Note: The IUT sends the *RESPONSE* file to the CMT laboratory for processing by the ECDSAVS.

The ECDSAVS:

A. Compares the contents of the *RESPONSE* file with the contents of the *FAX* file.

B. If the results for all public keys match, records PASS for this test; otherwise, records FAIL.

6.4 Signature Generation Test

An implementation of the ECDSA may generate the (*r*, *s*) pairs that represent a digital signature. This option tests the ability of an IUT to produce correct signatures. To test signature generation, 10 messages per curve supported are supplied to the IUT. The IUT then generates a signature for each of the messages. The message, public key, and signature components are returned. The ECDSAVS uses the signature validation routine to verify the signatures provided.

The ECDSAVS:

A. Creates a *REQUEST* file (Filename: SigGen.req) containing:

   1. The Product Information (vendor, product name, version); and,

   2. For each curve supported, 10 pseudorandom messages to be signed.

   Note: The CMT laboratory sends the *REQUEST* file to the IUT.

The IUT:

A. Generates the signatures for the messages supplied in the *REQUEST*.

B. Creates a *RESPONSE* file (Filename: SigGen.rsp) containing:

   1. The information from the *REQUEST* file;

2. The public key, *Q*, corresponding to the private key, *d*, used to generate the signature; and,

3. For each message, the computed signature values, *r* and *s*.

Note: The IUT sends the *RESPONSE* file to the CMT laboratory for processing by the ECDSAVS.

The ECDSAVS:

A. Uses the public keys to verify the signatures in the *RESPONSE* file.

B. If all signatures are correct, records PASS for this test; otherwise, records FAIL.

6.5 Signature Verification Test

This option tests the ability of the IUT to recognize valid and invalid signatures. For each curve supported, 15 pseudorandom messages, a public key, Q, and a signature components (r, s) are supplied to the IUT. Some of the supplied values are modified so that signature verification should fail. The IUT must correctly determine which of the sets of data passes signature verification and which ones fail. The ECDSAVS compares those responses with the expected values.

The ECDSAVS:

A. For each of the supported curves, generates 15 sets of the following information:

1. A public/private key pair, (*d*, *Q*);

2. A pseudorandom messages; and,

3. The corresponding signature using the private key, *d*, from above.

B. Makes a copy of the information generated in step A. For some of the message/signature sets, alters one of either the message, public key, or signature such that the message verification fails.

C. Creates a *REQUEST* file (Filename: SigVer.req) containing:

1. The Product Information (vendor, product name, version);

2. For each curve supported, the 15 sets of pseudorandom messages, public keys, and their corresponding signatures from step B.

Note: The CMT laboratory sends the *REQUEST* file to the IUT.

D. Creates a *FAX* file (Filename: SigVer.fax) containing:

1. The information from the *REQUEST* file; and

2. For each message/public key/signature pair, an indication of whether the signature verification process should pass or fail.

The IUT:

A. Attempts to verify the signatures for the messages supplied in the *REQUEST* file using the corresponding public key.

B. Creates a *RESPONSE* file (Filename: SigVer.rsp) containing:

1. The information from the *REQUEST* file;

2. For each message/public key/signature pair, an indication of whether the signature verification passed or failed.

Note: The IUT sends the *RESPONSE* file to the CMT laboratory for processing by the ECDSAVS.

The ECDSAVS:

A. Compares the contents of the *RESPONSE* file with the contents of the *FAX* file.

B. If the results for all message/signature sets match, records PASS for this test; otherwise, records FAIL.

References

[1] *Digital Signature Standard (DSS)*, FIPS Publication 186-2, National Institute of Standards and Technology, January 2000.

[2] *Public Key Cryptography for Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, ANSI X9.62-1988, January 1999.

[3] *Secure Hash Standard (SHS)*, FIPS Publication 180-1, National Institute of Standards and Technology, April 1995.

[4] *Security Requirements for Cryptographic Modules*, FIPS Publication 140-2, National Institute of Standards and Technology, May 2001.

Appendix B Examples of *REQUEST*, *FAX*, *RESPONSE*, and *SAMPLE* Files

The following are examples of *REQUEST*, *FAX*, *RESPONSE*, and *SAMPLE* files for each of the components tested by the ECDSAVS.

B.1 Examples of *REQUEST* Files

B.1.1 KeyPair.req

```
#  CAVS 3.0
#  "Key Pair" information for "ECDSA_Test"
#  Curves selected: P-192 K-233

[P-192]

N = 10

[K-233]

N = 10
```

B.1.2 PKV.req

```
#  CAVS 3.0
#  "PKV" information for "ECDSA_Test"
#  Curves selected: P-192 K-233

[P-192]

Qx = cd6d0f029a023e9aaca429615b8f577abee685d8257cc83a
Qy = 00019c410987680e9fb6c0b6ecc01d9a2647c8bae27721bacdfc

Qx = 00017f2fce203639e9eaf9fb50b81fc32776b30e3b02af16c73b
Qy = 95da95c5e72dd48e229d4748d4eee658a9a54111b23b2adb

Qx = 4f77f8bc7fccbadd5760f4938746d5f253ee2168c1cf2792
Qy = 000147156ff824d131629739817edb197717c41aab5c2a70f0f6

Qx = c58d61f88d905293bcd4cd0080bcb1b7f811f2ffa41979f6
Qy = 8804dc7a7c4c7f8b5d437f5156f3312ca7d6de8a0e11867f

Qx = cdf56c1aa3d8afc53c521adf3ffb96734a6a630a4a5b5a70
Qy = 97c1c44a5fb229007b5ec5d25f7413d170068ffd023caa4e

Qx = 89009c0dc361c81e99280c8e91df578df88cdf4b0cdedced
Qy = 27be44a529b7513e727251f128b34262a0fd4d8ec82377b9
```

```
Qx = 6a223d00bd22c52833409a163e057e5b5da1def2a197dd15
Qy = 7b482604199367f1f303f9ef627f922f97023e90eae08abf

Qx = 6dccbde75c0948c98dab32ea0bc59fe125cf0fb1a3798eda
Qy = 0001171a3e0fa60cf3096f4e116b556198de430e1fbd330c8835

Qx = d266b39e1f491fc4acbbbc7d098430931cfa66d55015af12
Qy = 193782eb909e391a3148b7764e6b234aa94e48d30a16dbb2

Qx = 9d6ddbcd439baa0c6b80a654091680e462a7d1d3f1ffeb43
Qy = 6ad8efc4d133ccf167c44eb4691c80abffb9f82b932b8caa

Qx = 146479d944e6bda87e5b35818aa666a4c998a71f4e95edbc
Qy = a86d6fe62bc8fbd88139693f842635f687f132255858e7f6

Qx = e594d4a598046f3598243f50fd2c7bd7d380edb055802253
Qy = 509014c0c4d6b536e3ca750ec09066af39b4c8616a53a923

[K-233]

Qx = 00534537f7762394d8ff46675d194aa212c4f9a2b5705f68df74e4e35d59
Qy = 01b4bb8fa0cd97777f60f4d7e4038cd65527eff4570b09204fdbedabc7d2

Qx = 0148dec1cffafce7ce21ae80652935bbb8b960bb1c4f27830d7ac0a786a5
Qy = 00c845acaaccc4549b8e2323a7f7ec17e0c8ae7a574c8e6a1ce337939c7b

Qx = 013ca0f0875f8fea41a1f44aa7603a85324507c7177b616627459feabd3b
Qy = 0061fc08300b6cf0c99c5f923ccc65f9be1fd9449b0625ed6a7f767e6a4d

Qx = 0079a6cbfe3a2e9e9eaef2b119787682ad51b7e1003e0bd952417f651d65
Qy = 00990e7736bed24326c49a683587e72b24d8e5b62c037495a99f21438bac

Qx = 00faa4e23af6d38eff68c8de405891a8e5eba2487bb854c8cc1d5a9d9fbc
Qy = 005c6cb3b3e608eda31bece7c755109d840b41550f09448db4122967bcae

Qx = 01883d8c99b33f5732a4fc226ec695d1664a30b6cd1e7e302da60d09ebdf
Qy = 011424b3e264102e4ac2c837925c03790c5f1053e2b9fbf77269d856e7dd

Qx = 00aa7822d4d5e939c4c9ab0b0a7a24c395a31f5ef138601d957fd48915d3
Qy = 00fcba0cb2522203754655e4a95be36b5c3227f9cf3aa6e9eee73acabc66

Qx = 01b84c30e07e761416b9a9a548c1f9c0e64ea3577277d3a3cfaac7b22303
Qy = 0117c9df876b0c309f02499075a98184ebd66e62abf8c60144db4bdc438b

Qx = 011cae8c5ee0ece8496471f45b6307edf97583ba70b793da4d76cc6db05f
Qy = 008690e754c7c74ea1f94c4616e653f7223387f14a0119407f255fc955ce

Qx = 01dc2d0dc408cd363f81e448fc46c9622b4f0ccc03ec277fe64af2be43c8
Qy = 00b5cdae6799fc82e9fdcb81798dc61ea0ecbc01a771908186f741103826

Qx = 00539b5e0779ac3631c28177558000a543882dda3c9fdf8a27df24bfeb05
Qy = 017a62d298132856e8a283787083131cf7ff93c3ff1d592d783760b438fe
```

```
Qx = 01e147f3a7653416b87a70c08dccf34e49dd1a630ba88d591c74e827ae72
Qy = 01a32a428f0f3b7786317753aba84f68ab0ea0b760a298f1a2286cc605b6
```

B.1.3 SigGen.req

```
#  CAVS 3.0
#  "SigGen" information for "ECDSA_Test"
#  Curves selected: P-192 K-233

[P-192]

Msg =
c70e287f3bb37422fcb2f277cb178a98eb6ab8e2d68ddef930e7df0cf9c3e95b06f292f6b2b827
c7d1e640d2e54398bc95301c8a5a8c42ac7cd69c3a3d91ad7d53edfbb19ca365090e21b7f4ede7
7c9f403114bb85d60680a47097f222bd9b6397458b39623dd8f19bac7f6449ccde49d5b3c5fcbf
32d17e90fef5bc100d5a14

Msg =
1a3cc54a8ad392749b2c1b59aa07b451bd1ebd8a5cac19a9a22ce2b493635a2fb0a02585c943b6
aa137c08ff7a558e7638f36cf6a718e70153ed1a9454ffeb4edb873ed50aee69760990e70b56c1
50225c0d885b48c4371218b77a3ef43cd999c2787802f5dd911fa5f12146e551e29e51f67a81e6
b8f2251710697c1c220a58

Msg =
5673828f6db66331f21f7e21a6bcb77db852d4c738fe90a0ce18ead2ac5cc394c14ca80a2fd0ed
0c0020fb2814e3eaea5e99535a51365fc7940f24c3fdfa326fbdb168f9d8780d62d9001c85c38a
de554a4fbe6643205aaf5a4ad68e03bc750cb36c6a634ff6ebbde586883f9af9bb46e33fc0f0f8
04a6df868fa739a4eab5f3

Msg =
ba8636a1e1cc77e34750061f11b5cd2b0da1a703961467beb9f81bc096f9923008961bad887890
3c4e039385ba2c1840f38a24eaceafd3bcf1b8a0dd3823e1d757e19148c1ac52dac99bb27407f4
aeb2fe417593fba66e7240717b3862f380cff08f1fda5510c6a3003fec54c2b6976b77ef2268e8
a03dc8f04b3537de107602

Msg =
6d3a19d8f63c7bb983468757a142cd14fcbef605229ca8498a0baa99d5b64921533bfa8ec9de40
69727fd0a343c9f47173ad2d5a3b0e1c8ddbbea279ddaa47989d51d88b097b546ca6270a60d4c5
fb6b52a5858904b043faf4562fdd98c709005366fdf73d7a806b27277bb5da9eababa09047ba06
e8e436dfb997ed8c755902

Msg =
35883c4a11985c37a1244af70260b885124411b0323d5b714a22627c0e691315809b2625b60500
8ddeb1d7ba7f9417790209040d707ea1807d6dd136c68fbdc8574c750f7075da7e8935bbb59345
3e548160820d07f782fea1253d3dd8e514b4c183732fc650b3b3a89a3f12c5dbf6bc9731d1d87e
0ec693bf31ecb8ccd5df82

Msg =
05d77ea4977ac96b8813fc1210483a037e7b6c502ceed8f7b22bf6655aa37e38d495c6492b314b
eaf8fe8d6cd67921e515ff012fb3ec263487055969c01346998ed1d2e41f08ae07cdf92cde96fb
```

5227cc652e880dae68d476d31e8a14f9eb9e9b54497c5b471a4b6fcd816e3817f6510a779a6224
7cc75de65feccd3e9d98d0

Msg =
c96009b6e816ef26695ef6bafcf76dcba3b0793fc12cc46574e2742025675a485ef06c4ddb1376
1de3cd0c48d9c9c3620edfa1aad9dcd1e8ea819b9cdbce94540880125ea1d8e39ffd9e3fc33166
fa97e212feb25798f95bd20553a721c263e27016e23061eda0745fd875712f547b30c74f7aa164
e8a484d777838a1fcd2fb8

Msg =
1ef4e272a78eb74d4a46ecdd514fb4172a6f93030e0d1e70e08c02e658d747dc603dd62bbe8039
c3f428a39c641d30f0b8756da8818b1b141e5130dee0e71f416c6c59766014146f397a4bc87438
06fbf3b6dbd3a33fb5235c5ad4b70857158b0828743bd372cfbbe0e4ed48c7c8be9ea3d7e46cba
527305604ef5581850b222

Msg =
942c6a4eba5e2760e8e7972f6208c91b5351dc5a6eb6c2a5d6e544313bd746e146a54dba389e3e
97ce96691e6780c5f268407d2ae0baac03682f65d14ec9f73cf2746fa86ff05ef57e24dc6998b6
ccea5bd862712f65e3bb292cac42308c766b5e41d801a87d0de2c23af8f83dcf656bf3c29215a4
deee37e185206a29474bd8

[K-233]

Msg =
baf9377601faf15c5a1288381efe55547d022599d1e330af2c354b6633dd5e5530ce17c16216e0
c0981e0f9dfe2d5d7f362f9a46aab59fb6213c83d791b2129b34367ac2de2048fb8e41934c436c
77b31134c60e73f8f938e31d6d75a89bcc10f0bbc8421e1f105665027c0b96c18b3a369a10b8d4
b4287e99606f07219f74fa

Msg =
34ab1130ce389d340fca232cc50b7536e62ad617742e022ea38a6fa63ef1d3ef476be66edea969
736395676cdf2ebb59a093d280245db26239323bed6198adf37b066bdba041ff974ce65dd6be42
6c7aa16ac24ceb88afee06747e122e84f7ea1aa429dfdea9668610e28ed029f091812fd82fe391
5702bb5376bf7c6a5db9bb

Msg =
693e50d3d13811c9897f260c809e0111e4566d52da89d74f7257ecd2da866a78d2272f6d5f7697
77c4030436ae0fbeaaaf39fef5ed5a45621cadf2a7a933146738557dfb51cc187256be7cd6b929
c0b16b8591d098a5834791dfa5b60a6c58ca851161060eff3cc329f9b37509b4b0310283506c41
343806bb342c8763fadea8

Msg =
a482cd28915c950f609b1324b71b42c681ed832540578f62a41bb0f25cfc31442c7f12a340ef01
5dc0a38625a4847eb6cac9cab9450548e9f96402756531a6a5bf9c37c146bb012fd4ced2dbb2c7
67dcb10a255476710a971693e290e346be618562a24a4cc87eccc4a35f0e8aeee77f5f37fbbd7b
a2bbb62330b70d7e415fbf

Msg =
292ea1755f9e587822372f4dcdf10bddfc0ff498a8af60ae94a0b482e873085c1cd52a5d181ce6
b99a1f8520d74b947d65f3e7e358e8ddc4ac4ae465e39d408eee1f09865159733f83f553cd93cf
de1c114fb3e32cf51cd418359016b3867df467b645d752808671a4609f3c49a67023c9ca617e6c
ffa544a10ac07ca05546f5

```
Msg =
60440c8df2b67e1fc1f7f354a1188ae14497175bb8d6c64b31cc018409fb93b405a20d3ada3368
37f007ede8655152335551267f59ca6fc94db591f45737716124d1dbc075d72126db23055fbe0a
d985a48fe5d1b0d709b269dda41cbe67b42346393ec8cc88f0130ab10562b52b6900baba1df9c8
e6de2d0eac01a44673a221

Msg =
d6344015544f6b63423cbb689274d70331832fb33966d51267378fa0cf0c2ac2ce1c110b41231e
b9f408af835ebdfd928b68a9cd59c09859e7b901604b63c412830ffeeaaeb5da337d92aacae415
362515fc5394aebbb8c7311d0e91b62d46ebdc572f3c05cb48d8c322d3c68d442ac6b7895692a1
1ede652eabddba77325756

Msg =
5c3fb5a4d2871bfa77e171056ff0a48eafe0fd4a653ea353940d62d9ff16aa15497fdb7f5a9fbf
41051158ebe707dd6892e1ff31ebff70c0d0d3a648fe3adda3320c5b8c8ff1f70e4077dc3c5e62
8b2314441ffd014dd5a8dd63cb56607508855f0dbd323925ca49713c84619ca9b6a67e2ee61670
d0d9f104e6596aec7135a3

Msg =
83c0f878b2428ab84cabecfc862d199e61933d6f7fca235635a1f13ae3cd13228030759b795bf5
5bbc5118230f8dfbeaa7478d37f6f4fccfc40c6d90810ff09ddacab3bb8ad776fb73633e9aed33
4e255ee953e00b84df692d271899481bb2abb8161aa08cbef4e19869c827c627f898ad02f63365
84b36d997a5b1cddf83f95

Msg =
39e3a58a0ce472f694294f9743a86db2d87894b98d35ffcd92a66d81bb9d75e1761f1ab3ffc59f
fcd7629dc672e652212f833c688e0ee6c59ea703f7b49cb953628b3f09a7c7aaa964fd04e60f18
9f99ab61a809f8ebff69e72e46a250f23953e76f3d166db23b062342ae7e8404fb23335c022433
95f2c056836109f8669ce8
```

B.1.4 SigVer.req

```
#  CAVS 3.0
#  "SigVer" information for "ECDSA_Test"
#  Curves selected: P-192 K-233

[P-192]

Msg =
84ce72aa8699df436059f052ac51b6398d2511e49631bcb7e71f89c499b9ee425dfbc13a5f6d40
8471b054f2655617cbbaf7937b7c80cd8865cf02c8487d30d2b0fbd8b2c4e102e16d828374bbc4
7b93852f212d5043c3ea720f086178ff798cc4f63f787b9c2e419efa033e7644ea7936f54462dc
21a6c4580725f7f0e7d158
Qx = d9dbfb332aa8e5ff091e8ce535857c37c73f6250ffb2e7ac
Qy = 282102e364feded3ad15ddf968f88d8321aa268dd483ebc4
R = 64dca58a20787c488d11d6dd96313f1b766f2d8efe122916
S = 1ecba28141e84ab4ecad92f56720e2cc83eb3d22dec72479

Msg =
94bb5bacd5f8ea765810024db87f4224ad71362a3c28284b2b9f39fab86db12e8beb94aae89976
```

8229be8fdb6c4f12f28912bb604703a79ccff769c1607f5a91450f30ba0460d359d9126cbd6296
be6d9c4bb96c0ee74cbb44197c207f6db326ab6f5a659113a9034e54be7b041ced9dcf6458d7fb
9cbfb2744d999f7dfd63f4
Qx = 3e53ef8d3112af3285c0e74842090712cd324832d4277ae7
Qy = cc75f8952d30aec2cbb719fc6aa9934590b5d0ff5a83adb7
R = 8285261607283ba18f335026130bab31840dcfd9c3e555af
S = 356d89e1b04541afc9704a45e9c535ce4a50929e33d7e06c

Msg =
f6227a8eeb34afed1621dcc89a91d72ea212cb2f476839d9b4243c66877911b37b4ad6f4448792
a7bbba76c63bdd63414b6facab7dc71c3396a73bd7ee14cdd41a659c61c99b779cecf07bc51ab3
91aa3252386242b9853ea7da67fd768d303f1b9b513d401565b6f1eb722dfdb96b519fe4f9bd5d
e67ae131e64b40e78c42dd
Qx = 16335dbe95f8e8254a4e04575d736befb258b8657f773cb7
Qy = 421b13379c59bc9dce38a1099ca79bbd06d647c7f6242336
R = 4141bd5d64ea36c5b0bd21ef28c02da216ed9d04522b1e91
S = 159a6aa852bcc579e821b7bb0994c0861fb08280c38daa09

Msg =
16b5f93afd0d02246f662761ed8e0dd9504681ed02a253006eb36736b563097ba39f81c8e1bce7
a16c1339e345efabbc6baa3efb0612948ae51103382a8ee8bc448e3ef71e9f6f7a9676694831d7
f5dd0db5446f179bcb737d4a526367a447bfe2c857521c7f40b6d7d7e01a180d92431fb0bbd29c
04a0c420a57b3ed26ccd8a
Qx = fd14cdf1607f5efb7b1793037b15bdf4baa6f7c16341ab0b
Qy = 83fa0795cc6c4795b9016dac928fd6bac32f3229a96312c4
R = 8dfdb832951e0167c5d762a473c0416c5c15bc1195667dc1
S = 1720288a2dc13fa1ec78f763f8fe2ff7354a7e6fdde44520

Msg =
08a2024b61b79d260e3bb43ef15659aec89e5b560199bc82cf7c65c77d39192e03b9a895d76665
5105edd9188242b91fbde4167f7862d4ddd61e5d4ab55196683d4f13ceb90d87aea6e07eb50a87
4e33086c4a7cb0273a8e1c4408f4b846bceae1ebaac1b2b2ea851a9b09de322efe34cebe601653
efd6ddc876ce8c2f2072fb
Qx = 674f941dc1a1f8b763c9334d726172d527b90ca324db8828
Qy = 65adfa32e8b236cb33a3e84cf59bfb9417ae7e8ede57a7ff
R = 9508b9fdd7daf0d8126f9e2bc5a35e4c6d800b5b804d7796
S = 36f2bf6b21b987c77b53bb801b3435a577e3d493744bfab0

Msg =
1843aba74b0789d4ac6b0b8923848023a644a7b70afa23b1191829bbe4397ce15b629bf21a8838
298653ed0c19222b95fa4f7390d1b4c844d96e645537e0aae98afb5c0ac3bd0e4c37f8daaff255
56c64e98c319c52687c904c4de7240a1cc55cd9756b7edaef184e6e23b385726e9ffcba8001b8f
574987c1a3fedaaa83ca6d
Qx = 10ecca1aad7220b56a62008b35170bfd5e35885c4014a19f
Qy = 04eb61984c6c12ade3bc47f3c629ece7aa0a033b9948d686
R = 82bfa4e82c0dfe9274169b86694e76ce993fd83b5c60f325
S = a97685676c59a65dbde002fe9d613431fb183e8006d05633

Msg =
5a478f4084ddd1a7fea038aa9732a822106385797d02311aeef4d0264f824f698df7a48cfb6b57
8cf3da416bc0799425bb491be5b5ecc37995b85b03420a98f2c4dc5c31a69a379e9e322fbe706b

```
bcaf0f77175e05cbb4fa162e0da82010a278461e3e974d137bc746d1880d6eb02aa95216014b37
480d84b87f717bb13f76e1
Qx = 6636653cb5b894ca65c448277b29da3ad101c4c2300f7c04
Qy = fdf1cbb3fc3fd6a4f890b59e554544175fa77dbdbeb656c1
R = eac2ddecddfb79931a9c3d49c08de0645c783a24cb365e1c
S = 3549fee3cfa7e5f93bc47d92d8ba100e881a2a93c22f8d50

Msg =
c598774259a058fa65212ac57eaa4f52240e629ef4c310722088292d1d4af6c39b49ce06ba77e4
247b20637174d0bd67c9723feb57b5ead232b47ea452d5d7a089f17c00b8b6767e434a5e16c231
ba0efa718a340bf41d67ea2d295812ff1b9277daacb8bc27b50ea5e6443bcf95ef4e9f5468fe78
485236313d53d1c68f6ba2
Qx = a82bd718d01d354001148cd5f69b9ebf38ff6f21898f8aaa
Qy = e67ceede07fc2ebfafd62462a51e4b6c6b3d5b537b7caf3e
R = 4d292486c620c3de20856e57d3bb72fcde4a73ad26376955
S = a85289591a6081d5728825520e62ff1c64f94235c04c7f95

Msg =
ca98ed9db081a07b7557f24ced6c7b9891269a95d2026747add9e9eb80638a961cf9c71a1b9f2c
29744180bd4c3d3db60f2243c5c0b7cc8a8d40a3f9a7fc910250f2187136ee6413ffc67f1a25e1
c4c204fa9635312252ac0e0481d89b6d53808f0c496ba87631803f6c572c1f61fa049737fdacce
4adff757afed4f05beb658
Qx = 7d3b016b57758b160c4fca73d48df07ae3b6b30225126c2f
Qy = 4af3790d9775742bde46f8da876711be1b65244b2b39e7ec
R = 95f778f5f656511a5ab49a5d69ddd0929563c29cbc3a9e62
S = 75c87fc358c251b4c83d2dd979faad496b539f9f2ee7a289

Msg =
31dd9a54c8338bea06b87eca813d555ad1850fac9742ef0bbe40dad400e10288acc9c11ea7dac7
9eb16378ebea9490e09536099f1b993e2653cd50240014c90a9c987f64545abc6a536b9bd2435e
b5e911fdfde2f13be96ea36ad38df4ae9ea387b29cced599af777338af2794820c9cce43b51d21
12380a35802ab7e396c97a
Qx = 9362f28c4ef96453d8a2f849f21e881cd7566887da8beb4a
Qy = e64d26d8d74c48a024ae85d982ee74cd16046f4ee5333905
R = f3923476a296c88287e8de914b0b324ad5a963319a4fe73b
S = f0baeed7624ed00d15244d8ba2aede085517dbdec8ac65f5

Msg =
b2b94e4432267c92f9fdb9dc6040c95ffa477652761290d3c7de312283f6450d89cc4aabe74855
4dfb6056b2d8e99c7aeaad9cdddebdee9dbc099839562d9064e68e7bb5f3a6bba0749ca9a53818
1fc785553a4000785d73cc207922f63e8ce1112768cb1de7b673aed83a1e4a74592f1268d8e2a4
e9e63d414b5d442bd0456d
Qx = cc6fc032a846aaac25533eb033522824f94e670fa997ecef
Qy = e25463ef77a029eccda8b294fd63dd694e38d223d30862f1
R = 066b1d07f3a40e679b620eda7f550842a35c18b80c5ebe06
S = a0b0fb201e8f2df65e2c4508ef303bdc90d934016f16b2dc

Msg =
4366fcadf10d30d086911de30143da6f579527036937007b337f7282460eae5678b15cccda8531
93ea5fc4bc0a6b9d7a31128f27e1214988592827520b214eed5052f7775b750b0c6b15f145453b
a3fee24a085d65287e10509eb5d5f602c440341376b95c24e5c4727d4b859bfe1483d20538acdd
92c7997fa9c614f0f839d7
```

```
Qx = 955c908fe900a996f7e2089bee2f6376830f76a19135e753
Qy = ba0c42a91d3847de4a592a46dc3fdaf45a7cc709b90de520
R = 1f58ad77fc04c782815a1405b0925e72095d906cbf52a668
S = f2e93758b3af75edf784f05a6761c9b9a6043c66b845b599

Msg =
543f8af57d750e33aa8565e0cae92bfa7a1ff78833093421c2942cadf9986670a5ff3244c02a82
25e790fbf30ea84c74720abf99cfd10d02d34377c3d3b41269bea763384f372bb786b5846f5893
2defa68023136cd571863b304886e95e52e7877f445b9364b3f06f3c28da12707673fecb4b8071
de06b6e0a3c87da160cef3
Qx = 31f7fa05576d78a949b24812d4383107a9a45bb5fccdd835
Qy = 8dc0eb65994a90f02b5e19bd18b32d61150746c09107e76b
R = be26d59e4e883dde7c286614a767b31e49ad88789d3a78ff
S = 8762ca831c1ce42df77893c9b03119428e7a9b819b619068

Msg =
d2e8454143ce281e609a9d748014dcebb9d0bc53adb02443a6aac2ffe6cb009f387c346ecb0517
91404f79e902ee333ad65e5c8cb38dc0d1d39a8dc90add5023572720e5b94b190d43dd0d787339
7504c0c7aef2727e628eb6a74411f2e400c65670716cb4a815dc91cbbfeb7cfe8c929e93184c93
8af2c078584da045e8f8d1
Qx = 66aa8edbbdb5cf8e28ceb51b5bda891cae2df84819fe25c0
Qy = 0c6bc2f69030a7ce58d4a00e3b3349844784a13b8936f8da
R = a4661e69b1734f4a71b788410a464b71e7ffe42334484f23
S = 738421cf5e049159d69c57a915143e226cac8355e149afe9

Msg =
6660717144040f3e2f95a4e25b08a7079c702a8b29babad5a19a87654bc5c5afa261512a11b998
a4fb36b5d8fe8bd942792ff0324b108120de86d63f65855e5461184fc96a0a8ffd2ce6d5dfb023
0cbbdd98f8543e361b3205f5da3d500fdc8bac6db377d75ebef3cb8f4d1ff738071ad093891788
9250b41dd1d98896ca06fb
Qx = bcfacf45139b6f5f690a4c35a5fffa498794136a2353fc77
Qy = 6f4a6c906316a6afc6d98fe1f0399d056f128fe0270b0f22
R = 9db679a3dafe48f7ccad122933acfe9da0970b71c94c21c1
S = 984c2db99827576c0a41a5da41e07d8cc768bc82f18c9da9

[K-233]

Msg =
f553c9a1a17d02161faac334dd5f15324c1c033def264d62b28961ae7c5e8694074a5b8ef04780
070aa79379f8565ed3fb5f4e1d08b1275e1e24f7bed6b749e83c1b9ab2dd76110021616ae5db32
340c1f813c5754e549c589ff09990dba4cb939d0705491911cc70ce032c2af7efea6608bb432fa
49195f9d24808848eff8ce
Qx = 0136ed170a3e06af2f542308c818ad113115662a0f24b86e8de8a8577340
Qy = 00cc263193d2844f48c02de4d5f8df5ddee4548703a5222eb2144ffe54e3
R = 0017c34e4c94c9ab1957b3ecd22f97c32eebc608ca337b0b314834726964
S = 006ac64d1221b4d5fb0ea95a5e154a1e64647f15a1a4f8ac6058968e05c6

Msg =
490d6c7d320a88286bee74e3ff2536a9c9af1d9c36d5a7554c14a178eb5e908b53825008e7e8fb
b031810d2325fec5aeaa40ce6456101e7079111fa95ef20c67cde89e95d45ce908c8e1800f8668
e04cfeb70cc2f317742efc4d1b9bcfccf931be299f4e82cf19d838f418d1a9cc512bcefc20de94
517139dcb2e075c6531f90
```

```
Qx = 010b9887c30189f70fdb353368a46e18ba0cfbce16274bfb456d183af21e
Qy = 01dc2e81158f6221382560a1bea6cdd8d099d0317ec09c9c5beda7942c6f
R = 00077eb49e722729af67db03650808c60e0122f7b7efb8792a7accf4fe54
S = 0026f591818d27aa189fabc1525646fa706f77cacda89f108c810598accb

Msg =
ace934c17c190a4cf59bf76a2b89bea316493a3688b5f35c6278efd108bbcb9112020adf4550ac
8cc19202767b3ac24fee2b57a00ed57a0d7ea106da028f08ae371d1697826ce34f469e10be5a82
44bfba737e277c7daa0406c273227f1c59d4830403f01bb3d61cec86c648aea76c7ce0ea59d4ba
f5abc964a4deb165ace489
Qx = 00e4c747929fccd4042bd3f7ac1d1659a59a888e8d81b670de19b2d9a305
Qy = 00bb27d7c664e68092333580ad94e67170e0e5e678278e9c43b9dbe94774
R = 00584c7b81ea80d78a2574654a3f6a36398c2133fae96f428ee638ad4d65
S = 000b0b36d180506386efb3cd6572cc3afefd751b75db4d1b9096ada948e2

Msg =
fd75c460df9a32bf0a837e08eaf81e6a3ecf628479bdfad8686bb97d16cc9915edaffeff1d903f
ce42b462f9417527d372da49be056a009c9e42ca8743666bc2785532efa8e07f82c73b82753655
453ee765edfec1c53dfb46045b507337d7e3e78fe9984831fac4e34166e592408190e399d8aa76
76b9dba7d8f5406de7e460
Qx = 01ccc8d325e42af6aff1a280ebde426050609883926dd18acbf24959d9c1
Qy = 009f314e10ad7c7f20e7061bb58a0a1128c1671ae2fa5f929eb05cfddada
R = 00053ada9d018679f8ff4352077e63baade5ca2c506450205cdbcbe37b93
S = 0024df72910c75b3b5d6fd6183267082776 60ae53489fdef984f01f2b720

Msg =
54f9ebe43a658c8cdceee7e2edcc5e8b04866ce99516385520486aa9a8633d02670bd5c4c066d4
de757e284f1ae626e9caa1dd54183fa4574849f653c0df8010b9a077bc3aca2f3147a2ea775617
ee8a02a2da5d0370391e5ec358bcd99655a7b28079d790dac70fba24d56387a5dbf817520a0b3e
f11f34c87e37ecdccee54e
Qx = 0169b6839488a2230eb8a55d4aee2cfdecde006beb1173428f6079fb5b2d
Qy = 00241ca64fc4d97b37c4721d28eddb25d8d187570f0c8e2bc9f2111d1255
R = 00369daf397bd022654b1b5b0b0de937e9aa9c830165415b6329b0bfb090
S = 001f591f44be300354755a0fb466e5b248597f7a5a9cb69f4d508415da8f

Msg =
dcd8bdb15a84862ca5ae26302d95320cd71c4ee7fec24d54b8d49a275ae2d6863e6fc243c3ec60
6996e8551430819286a01e33788b60a7ae715512ce31efef72d0b5fa7c76b94daab9cac96a1eea
b7efdd03af84e5d5b9202033b33bf86ff3e11a132d057ad1961797bd49d900baea6e17328ab315
0bcbd34ed64516b74928fa
Qx = 007345bf47179e1533eb451d0174e1c04f8bd34c202478f950ee54f736f8
Qy = 01706e0da88763ff81d6e1e853ce5f7484635a7f6d08b8d9730b389c8d0b
R = 002e1d25e5b4f7549fc39bfc9244c01843cd30ba3e7cec33c56bddc67a66
S = 00486550d28f3b79d135baadf8795c8d21951d76b88cd9110bca0d125133

Msg =
c5f62b24a16226b4a66a01893da87fa175bc523f9a91464909e2bdee42fc5b8b3fc502d005fd01
1f78c48834735c600b1831d8fe6516032f08d2202575db5aba3561b234818e39b20f0d82ca2cc9
57700bf7ab195d56d02121b5ea6abeb7a4474fd321983e9e3636144dd6918f75cd97f616b1d8a9
d816e8fc9402054516a1fa
Qx = 01b6dec64e5e1fd13ccd98ba680763c47583e95cec2d0dbf309bf69fe51b
Qy = 011221e50fc93677bbcb6e40b24f2de6eeed9bc26ba826e80e02f7eb5574
```

```
R = 00475802cf260aa2b4b14262eacfea1ce1e45f406d8ae411bbf187e062ba
S = 00293f771aa308ef1716ffa5fddfde490724016c6a570c7b1b807740421b

Msg =
1ab37b5c3e7accb783e80d93538e1ca59d6f7eb1270651aa268b811b0c733fc5a136af895554e1
89d49a038bdca1d59e4b995dff7d44db3dd445ff9c989b5ab70269136a93f8dbefaafe22475621
8bdc69b79e64cfd0be081c765ac66a33671466d40dc6a16da0312d9dd3916a1328a81d51aba8c2
b0e05324a5fa612a424d22
Qx = 00c57832cad1eef31b0545f0c48718106d27d6492addd718d6425c7fa056
Qy = 0026e7491ef66649a3f0d4bbc8d7fb4e1db86a3c2288658edf74a64fee43
R = 004009378a80c311db1a3ab914953d7dec0ba06568a6bd533b2537e55f5e
S = 0059cf2d301cd86e94d0d1bf0d3f21fe3b2aea683d2354c8781c440f23b1

Msg =
5a56096c7e86e5d4988347e117552975e687f720e3cf9fe893f1e84514e00470532668dd7f87db
06bde1cd6b1d57ebd7ccaef0e48cf7bec1626fad338ea323dac0d865b689a9acea10f27cbf06ed
31ebdc9bdb1433664b9094046e6f619edabb0b32a7fe86368005fa7ef9e4bc5f233a7c155fb6c0
626fda9178d3ff7319529a
Qx = 01e31fa7780137bb4a2ab01d354fd773901b9ef976a5b564a2a09dc9df8b
Qy = 0191cf897a2347a43e781e2c41d5bd50efcc705267fed96f52eabdf42027
R = 006729210e1d49542bde1e3ee0609368dac81bfeb51ce99fdd306ca9ac16
S = 002ea969db3ff2a494730cb2de1d177a6c5b3ca7a42b0f7bf6d1ab44ed8d

Msg =
2a5325bd0277f9c49be359fd2bbe5e63d1832de0e102e16d7da8c67a6501c8900f7b2b35fb6d7c
104157c74d6c6c0a438a4dea548418a515aca148af95ff2286274b7818f2a47a27c376761a75fc
4ca10a042298fbf3582ecb08be46e2e5051d994b742d9225dc524ac8ce2cf1790bc4792f3c72ed
9be4fe04669205f6ba5b9e
Qx = 00c6b220969d54cadf544316cffa60fd5a1595ac420f61fc5873ad78bb56
Qy = 0196b017ed347446c64d6ae8613e75f822938194a84952e364d67d2e0036
R = 000a4c1bd92de8907c3cd3930249b06d8556093ef7378bdb520d56791afd
S = 007f7b94affd65269dbcc29883064b69ccce7127ab23dd404eab59029787

Msg =
cd25a7f53bc44ac3eab1d4771883891358d2b77a86534ac000449aa4130b875bb41ac890711580
a8a737124af4f2371fefd54ed617b3f36c0a02d2aaf881bdef561efd2fd716e63c985eaf449a42
809b764ccbbb4c67e08afd44bcdb9afd22361cf8eedc550fa50626ed506ef3bb8b1054fdd9320d
b63aa241d3003fe2c6deba
Qx = 0078cd54849617d64c1bf3ee0c01639d4912411912513612512c0237bf43
Qy = 018a850cae6cb9b81fb4173847b4f29fb40b47a9bdfc119d2eb6fcc4146d
R = 0026170cca4ec53585b9ddc149f1811133815b8aa2f68f2d80e06746a6f4
S = 00100984fcbe5bc6a0d91473b40589433851aa725c3f4ffa744f340eefb2

Msg =
c292e847f4bf5a482ca63544d31ec7df4f05460726d415266776439c465b556c06c845351c71ca
659149daa9a8996da8c14f85f07d996b3023b33ba942fea2df9851e794339328f6d68ae7189eee
c59fe5c28cbe67e47364a3e29eb3850fe5b541d6d64a824ffd65c4106378fe46542d850465572d
dab628b1aa75a455b7a355
Qx = 0073108e1827566a63d94ef922f94b2835c91d53ac62371df25217989f2e
Qy = 00c0ce149e33218fc95a299c64dbccf80aa4062ca488e74340d9d0a40b83
R = 00561b14067d3fcf8d868ac17211d6a8747b6089638338810f7336aa988d
S = 0047e987aed01b51f888fbf4b2dc34a367b644cee4271f426314d63eed98
```

```
Msg =
0cb9c695b7585006751e32fa0761c185fefabf73c23f7cded931400066f6ed45f089e1a465b01a
305f2e9deaa53a18daf531c65e018893c1b704810fc52d4a285d00471435e49096d3df6504070a
cc55b9427c7ce421faf5e32c029dec4e28c6da86bf8b2fdcfa61599951ef34b72620d197a97676
f2f9a1e5128c50e142d047
Qx = 010c42d7b7557e2ba495373dff3cade13fbb56614f15b47fca217ca7d57e
Qy = 017abd698cc8dec5aae48ca111b533829d487a7ee333b24e74da4a50b889
R = 0f3e30cfcf4d3ba084dfaa43b625d5fb4f406336501b1fd43f9f82d2
S = 0060553f1b1d9d2ad62f74ba7a906204dee6c6f059b50fe7317141f3d443

Msg =
8159c84852c6229694bd484661ffc349342c8a504e91803c59413fd64c6714c18eda4aad5ef2ac
cc729b458adea76a793869fb8afa7fe58327efebad3276a7cd1b1ccb56db0caddd02a303cd9fc7
ea5c607a2ebefaaec598cb5b9cb7bed097027047d3ad91bb2eb08cfe09786a064cdcf387ab5217
c828638dafd95cba1dec47
Qx = 007ee60584691638fd6fe17a3b4ce3ebce1747ec6c44ba6ea8d235b130c1
Qy = 00881c53ec4e23e591764b5cb4047701c6e8035e37f77cbf83d0d7257d98
R = 000e690c9f1180e538bb790906e037cca39d07799032841370c74ea30b78
S = 006e1e028bd9d204b9d97bd9846429edaad8da32aeec6f3bb7e99f32ee8f

Msg =
39cd57963378c638c3b2a442f65d15d8b9c605c5f9356db208c2d19c436b0e85f26452696fae6c
738beb46712d71af863c9d5e1ebf6934274341c27f7d130ba831a68bc3532c78bc6b1a47c23e37
72faaaf37974d2fb275e7b0a1677b60275c7c03b098e261b727a2ce7b01c70d8e59dcb725cad78
11cbbd78c5d56e345fd34a
Qx = 004bc66f1524162fc952a41240b627e244be6d1823a0736be63adf559727
Qy = 011b167b34fc9be9589e7d8c1fe3dd033d6145a0f1794f911272dea141dc
R = 000d4dbfcb1069e09657f3d9614f3e6bdb0f812b281f0887c85b5e57c376
S = 0028055fdaaa8090d97568a23eee931d576fe6eae5aed9e11cf151f3a77f
```

B.2 Examples of *FAX* Files

B.2.1 KeyPair.fax

```
#  CAVS 3.0
#  "Key Pair" information for "ECDSA_Test"
#  Curves selected: P-192 K-233

[P-192]

N = 10

[K-233]

N = 10
```

B.2.2 PKV.fax

```
#  CAVS 3.0
#  "PKV" information for "ECDSA_Test"
#  Curves selected: P-192 K-233

[P-192]

Qx = cd6d0f029a023e9aaca429615b8f577abee685d8257cc83a
Qy = 00019c410987680e9fb6c0b6ecc01d9a2647c8bae27721bacdfc
Result = F (1)

Qx = 00017f2fce203639e9eaf9fb50b81fc32776b30e3b02af16c73b
Qy = 95da95c5e72dd48e229d4748d4eee658a9a54111b23b2adb
Result = F (1)

Qx = 4f77f8bc7fccbadd5760f4938746d5f253ee2168c1cf2792
Qy = 000147156ff824d131629739817edb197717c41aab5c2a70f0f6
Result = F (1)

Qx = c58d61f88d905293bcd4cd0080bcb1b7f811f2ffa41979f6
Qy = 8804dc7a7c4c7f8b5d437f5156f3312ca7d6de8a0e11867f
Result = P (0)

Qx = cdf56c1aa3d8afc53c521adf3ffb96734a6a630a4a5b5a70
Qy = 97c1c44a5fb229007b5ec5d25f7413d170068ffd023caa4e
Result = P (0)

Qx = 89009c0dc361c81e99280c8e91df578df88cdf4b0cdedced
Qy = 27be44a529b7513e727251f128b34262a0fd4d8ec82377b9
Result = P (0)

Qx = 6a223d00bd22c52833409a163e057e5b5da1def2a197dd15
Qy = 7b482604199367f1f303f9ef627f922f97023e90eae08abf
Result = P (0)

Qx = 6dccbde75c0948c98dab32ea0bc59fe125cf0fb1a3798eda
Qy = 0001171a3e0fa60cf3096f4e116b556198de430e1fbd330c8835
Result = F (1)

Qx = d266b39e1f491fc4acbbbc7d098430931cfa66d55015af12
Qy = 193782eb909e391a3148b7764e6b234aa94e48d30a16dbb2
Result = F (2)

Qx = 9d6ddbcd439baa0c6b80a654091680e462a7d1d3f1ffeb43
Qy = 6ad8efc4d133ccf167c44eb4691c80abffb9f82b932b8caa
Result = F (2)

Qx = 146479d944e6bda87e5b35818aa666a4c998a71f4e95edbc
Qy = a86d6fe62bc8fbd88139693f842635f687f132255858e7f6
Result = F (2)
```

```
Qx = e594d4a598046f3598243f50fd2c7bd7d380edb055802253
Qy = 509014c0c4d6b536e3ca750ec09066af39b4c8616a53a923
Result = F (2)

[K-233]

Qx = 00534537f7762394d8ff46675d194aa212c4f9a2b5705f68df74e4e35d59
Qy = 01b4bb8fa0cd97777f60f4d7e4038cd65527eff4570b09204fdbedabc7d2
Result = F (1)

Qx = 0148dec1cffafce7ce21ae80652935bbb8b960bb1c4f27830d7ac0a786a5
Qy = 00c845acaaccc4549b8e2323a7f7ec17e0c8ae7a574c8e6a1ce337939c7b
Result = P (0)

Qx = 013ca0f0875f8fea41a1f44aa7603a85324507c7177b616627459feabd3b
Qy = 0061fc08300b6cf0c99c5f923ccc65f9be1fd9449b0625ed6a7f767e6a4d
Result = F (2)

Qx = 0079a6cbfe3a2e9e9eaef2b119787682ad51b7e1003e0bd952417f651d65
Qy = 00990e7736bed24326c49a683587e72b24d8e5b62c037495a99f21438bac
Result = P (0)

Qx = 00faa4e23af6d38eff68c8de405891a8e5eba2487bb854c8cc1d5a9d9fbc
Qy = 005c6cb3b3e608eda31bece7c755109d840b41550f09448db4122967bcae
Result = F (1)

Qx = 01883d8c99b33f5732a4fc226ec695d1664a30b6cd1e7e302da60d09ebdf
Qy = 011424b3e264102e4ac2c837925c03790c5f1053e2b9fbf77269d856e7dd
Result = P (0)

Qx = 00aa7822d4d5e939c4c9ab0b0a7a24c395a31f5ef138601d957fd48915d3
Qy = 00fcba0cb2522203754655e4a95be36b5c3227f9cf3aa6e9eee73acabc66
Result = F (2)

Qx = 01b84c30e07e761416b9a9a548c1f9c0e64ea3577277d3a3cfaac7b22303
Qy = 0117c9df876b0c309f02499075a98184ebd66e62abf8c60144db4bdc438b
Result = F (2)

Qx = 011cae8c5ee0ece8496471f45b6307edf97583ba70b793da4d76cc6db05f
Qy = 008690e754c7c74ea1f94c4616e653f7223387f14a0119407f255fc955ce
Result = F (1)

Qx = 01dc2d0dc408cd363f81e448fc46c9622b4f0ccc03ec277fe64af2be43c8
Qy = 00b5cdae6799fc82e9fdcb81798dc61ea0ecbc01a771908186f741103826
Result = F (1)

Qx = 00539b5e0779ac3631c28177558000a543882dda3c9fdf8a27df24bfeb05
Qy = 017a62d298132856e8a283787083131cf7ff93c3ff1d592d783760b438fe
Result = P (0)

Qx = 01e147f3a7653416b87a70c08dccf34e49dd1a630ba88d591c74e827ae72
Qy = 01a32a428f0f3b7786317753aba84f68ab0ea0b760a298f1a2286cc605b6
```

```
Result = F (2)
```

B.2.3 SigGen.fax

```
#  CAVS 3.0
#  "SigGen" information for "ECDSA_Test"
#  Curves selected: P-192 K-233

[P-192]

Msg =
c70e287f3bb37422fcb2f277cb178a98eb6ab8e2d68ddef930e7df0cf9c3e95b06f292f6b2b827
c7d1e640d2e54398bc95301c8a5a8c42ac7cd69c3a3d91ad7d53edfbb19ca365090e21b7f4ede7
7c9f403114bb85d60680a47097f222bd9b6397458b39623dd8f19bac7f6449ccde49d5b3c5fcbf
32d17e90fef5bc100d5a14

Msg =
1a3cc54a8ad392749b2c1b59aa07b451bd1ebd8a5cac19a9a22ce2b493635a2fb0a02585c943b6
aa137c08ff7a558e7638f36cf6a718e70153ed1a9454ffeb4edb873ed50aee69760990e70b56c1
50225c0d885b48c4371218b77a3ef43cd999c2787802f5dd911fa5f12146e551e29e51f67a81e6
b8f2251710697c1c220a58

Msg =
5673828f6db66331f21f7e21a6bcb77db852d4c738fe90a0ce18ead2ac5cc394c14ca80a2fd0ed
0c0020fb2814e3eaea5e99535a51365fc7940f24c3fdfa326fbdb168f9d8780d62d9001c85c38a
de554a4fbe6643205aaf5a4ad68e03bc750cb36c6a634ff6ebbde586883f9af9bb46e33fc0f0f8
04a6df868fa739a4eab5f3

Msg =
ba8636a1e1cc77e34750061f11b5cd2b0da1a703961467beb9f81bc096f9923008961bad887890
3c4e039385ba2c1840f38a24eaceafd3bcf1b8a0dd3823e1d757e19148c1ac52dac99bb27407f4
aeb2fe417593fba66e7240717b3862f380cff08f1fda5510c6a3003fec54c2b6976b77ef2268e8
a03dc8f04b3537de107602

Msg =
6d3a19d8f63c7bb983468757a142cd14fcbef605229ca8498a0baa99d5b64921533bfa8ec9de40
69727fd0a343c9f47173ad2d5a3b0e1c8ddbbea279ddaa47989d51d88b097b546ca6270a60d4c5
fb6b52a5858904b043faf4562fdd98c709005366fdf73d7a806b27277bb5da9eababa09047ba06
e8e436dfb997ed8c755902

Msg =
35883c4a11985c37a1244af70260b885124411b0323d5b714a22627c0e691315809b2625b60500
8ddeb1d7ba7f9417790209040d707ea1807d6dd136c68fbdc8574c750f7075da7e8935bbb59345
3e548160820d07f782fea1253d3dd8e514b4c183732fc650b3b3a89a3f12c5dbf6bc9731d1d87e
0ec693bf31ecb8ccd5df82

Msg =
05d77ea4977ac96b8813fc1210483a037e7b6c502ceed8f7b22bf6655aa37e38d495c6492b314b
eaf8fe8d6cd67921e515ff012fb3ec263487055969c01346998ed1d2e41f08ae07cdf92cde96fb
5227cc652e880dae68d476d31e8a14f9eb9e9b54497c5b471a4b6fcd816e3817f6510a779a6224
7cc75de65feccd3e9d98d0
```

Msg =
c96009b6e816ef26695ef6bafcf76dcba3b0793fc12cc46574e2742025675a485ef06c4ddb1376
1de3cd0c48d9c9c3620edfa1aad9dcd1e8ea819b9cdbce94540880125ea1d8e39ffd9e3fc33166
fa97e212feb25798f95bd20553a721c263e27016e23061eda0745fd875712f547b30c74f7aa164
e8a484d777838a1fcd2fb8

Msg =
1ef4e272a78eb74d4a46ecdd514fb4172a6f93030e0d1e70e08c02e658d747dc603dd62bbe8039
c3f428a39c641d30f0b8756da8818b1b141e5130dee0e71f416c6c59766014146f397a4bc87438
06fbf3b6dbd3a33fb5235c5ad4b70857158b0828743bd372cfbbe0e4ed48c7c8be9ea3d7e46cba
527305604ef5581850b222

Msg =
942c6a4eba5e2760e8e7972f6208c91b5351dc5a6eb6c2a5d6e544313bd746e146a54dba389e3e
97ce96691e6780c5f268407d2ae0baac03682f65d14ec9f73cf2746fa86ff05ef57e24dc6998b6
ccea5bd862712f65e3bb292cac42308c766b5e41d801a87d0de2c23af8f83dcf656bf3c29215a4
deee37e185206a29474bd8

[K-233]

Msg =
baf9377601faf15c5a1288381efe55547d022599d1e330af2c354b6633dd5e5530ce17c16216e0
c0981e0f9dfe2d5d7f362f9a46aab59fb6213c83d791b2129b34367ac2de2048fb8e41934c436c
77b31134c60e73f8f938e31d6d75a89bcc10f0bbc8421e1f105665027c0b96c18b3a369a10b8d4
b4287e99606f07219f74fa

Msg =
34ab1130ce389d340fca232cc50b7536e62ad617742e022ea38a6fa63ef1d3ef476be66edea969
736395676cdf2ebb59a093d280245db26239323bed6198adf37b066bdba041ff974ce65dd6be42
6c7aa16ac24ceb88afee06747e122e84f7ea1aa429dfdea9668610e28ed029f091812fd82fe391
5702bb5376bf7c6a5db9bb

Msg =
693e50d3d13811c9897f260c809e0111e4566d52da89d74f7257ecd2da866a78d2272f6d5f7697
77c4030436ae0fbeaaaf39fef5ed5a45621cadf2a7a933146738557dfb51cc187256be7cd6b929
c0b16b8591d098a5834791dfa5b60a6c58ca851161060eff3cc329f9b37509b4b0310283506c41
343806bb342c8763fadea8

Msg =
a482cd28915c950f609b1324b71b42c681ed832540578f62a41bb0f25cfc31442c7f12a340ef01
5dc0a38625a4847eb6cac9cab9450548e9f96402756531a6a5bf9c37c146bb012fd4ced2dbb2c7
67dcb10a255476710a971693e290e346be618562a24a4cc87eccc4a35f0e8aeee77f5f37fbbd7b
a2bbb62330b70d7e415fbf

Msg =
292ea1755f9e587822372f4dcdf10bddfc0ff498a8af60ae94a0b482e873085c1cd52a5d181ce6
b99a1f8520d74b947d65f3e7e358e8ddc4ac4ae465e39d408eee1f09865159733f83f553cd93cf
de1c114fb3e32cf51cd418359016b3867df467b645d752808671a4609f3c49a67023c9ca617e6c
ffa544a10ac07ca05546f5

```
Msg =
60440c8df2b67e1fc1f7f354a1188ae14497175bb8d6c64b31cc018409fb93b405a20d3ada3368
37f007ede8655152335551267f59ca6fc94db591f45737716124d1dbc075d72126db23055fbe0a
d985a48fe5d1b0d709b269dda41cbe67b42346393ec8cc88f0130ab10562b52b6900baba1df9c8
e6de2d0eac01a44673a221

Msg =
d6344015544f6b63423cbb689274d70331832fb33966d51267378fa0cf0c2ac2ce1c110b41231e
b9f408af835ebdfd928b68a9cd59c09859e7b901604b63c412830ffeeaaeb5da337d92aacae415
362515fc5394aebbb8c7311d0e91b62d46ebdc572f3c05cb48d8c322d3c68d442ac6b7895692a1
1ede652eabddba77325756

Msg =
5c3fb5a4d2871bfa77e171056ff0a48eafe0fd4a653ea353940d62d9ff16aa15497fdb7f5a9fbf
41051158ebe707dd6892e1ff31ebff70c0d0d3a648fe3adda3320c5b8c8ff1f70e4077dc3c5e62
8b2314441ffd014dd5a8dd63cb56607508855f0dbd323925ca49713c84619ca9b6a67e2ee61670
d0d9f104e6596aec7135a3

Msg =
83c0f878b2428ab84cabecfc862d199e61933d6f7fca235635a1f13ae3cd13228030759b795bf5
5bbc5118230f8dfbeaa7478d37f6f4fccfc40c6d90810ff09ddacab3bb8ad776fb73633e9aed33
4e255ee953e00b84df692d271899481bb2abb8161aa08cbef4e19869c827c627f898ad02f63365
84b36d997a5b1cddf83f95

Msg =
39e3a58a0ce472f694294f9743a86db2d87894b98d35ffcd92a66d81bb9d75e1761f1ab3ffc59f
fcd7629dc672e652212f833c688e0ee6c59ea703f7b49cb953628b3f09a7c7aaa964fd04e60f18
9f99ab61a809f8ebff69e72e46a250f23953e76f3d166db23b062342ae7e8404fb23335c022433
95f2c056836109f8669ce8
```

B.2.4 SigVer.fax

```
#  CAVS 3.0
#  "SigVer" information for "ECDSA_Test"
#  Curves selected: P-192 K-233

[P-192]

Msg =
84ce72aa8699df436059f052ac51b6398d2511e49631bcb7e71f89c499b9ee425dfbc13a5f6d40
8471b054f2655617cbbaf7937b7c80cd8865cf02c8487d30d2b0fbd8b2c4e102e16d828374bbc4
7b93852f212d5043c3ea720f086178ff798cc4f63f787b9c2e419efa033e7644ea7936f54462dc
21a6c4580725f7f0e7d158
Qx = d9dbfb332aa8e5ff091e8ce535857c37c73f6250ffb2e7ac
Qy = 282102e364feded3ad15ddf968f88d8321aa268dd483ebc4
R = 64dca58a20787c488d11d6dd96313f1b766f2d8efe122916
S = 1ecba28141e84ab4ecad92f56720e2cc83eb3d22dec72479
Result = P (0)

Msg =
94bb5bacd5f8ea765810024db87f4224ad71362a3c28284b2b9f39fab86db12e8beb94aae89976
```

```
8229be8fdb6c4f12f28912bb604703a79ccff769c1607f5a91450f30ba0460d359d9126cbd6296
be6d9c4bb96c0ee74cbb44197c207f6db326ab6f5a659113a9034e54be7b041ced9dcf6458d7fb
9cbfb2744d999f7dfd63f4
Qx = 3e53ef8d3112af3285c0e74842090712cd324832d4277ae7
Qy = cc75f8952d30aec2cbb719fc6aa9934590b5d0ff5a83adb7
R = 8285261607283ba18f335026130bab31840dcfd9c3e555af
S = 356d89e1b04541afc9704a45e9c535ce4a50929e33d7e06c
Result = P (0)

Msg =
f6227a8eeb34afed1621dcc89a91d72ea212cb2f476839d9b4243c66877911b37b4ad6f4448792
a7bbba76c63bdd63414b6facab7dc71c3396a73bd7ee14cdd41a659c61c99b779cecf07bc51ab3
91aa3252386242b9853ea7da67fd768d303f1b9b513d401565b6f1eb722dfdb96b519fe4f9bd5d
e67ae131e64b40e78c42dd
Qx = 16335dbe95f8e8254a4e04575d736befb258b8657f773cb7
Qy = 421b13379c59bc9dce38a1099ca79bbd06d647c7f6242336
R = 4141bd5d64ea36c5b0bd21ef28c02da216ed9d04522b1e91
S = 159a6aa852bcc579e821b7bb0994c0861fb08280c38daa09
Result = F (3)

Msg =
16b5f93afd0d02246f662761ed8e0dd9504681ed02a253006eb36736b563097ba39f81c8e1bce7
a16c1339e345efabbc6baa3efb0612948ae51103382a8ee8bc448e3ef71e9f6f7a9676694831d7
f5dd0db5446f179bcb737d4a526367a447bfe2c857521c7f40b6d7d7e01a180d92431fb0bbd29c
04a0c420a57b3ed26ccd8a
Qx = fd14cdf1607f5efb7b1793037b15bdf4baa6f7c16341ab0b
Qy = 83fa0795cc6c4795b9016dac928fd6bac32f3229a96312c4
R = 8dfdb832951e0167c5d762a473c0416c5c15bc1195667dc1
S = 1720288a2dc13fa1ec78f763f8fe2ff7354a7e6fdde44520
Result = F (1)

Msg =
08a2024b61b79d260e3bb43ef15659aec89e5b560199bc82cf7c65c77d39192e03b9a895d76665
5105edd9188242b91fbde4167f7862d4ddd61e5d4ab55196683d4f13ceb90d87aea6e07eb50a87
4e33086c4a7cb0273a8e1c4408f4b846bceae1ebaac1b2b2ea851a9b09de322efe34cebe601653
efd6ddc876ce8c2f2072fb
Qx = 674f941dc1a1f8b763c9334d726172d527b90ca324db8828
Qy = 65adfa32e8b236cb33a3e84cf59bfb9417ae7e8ede57a7ff
R = 9508b9fdd7daf0d8126f9e2bc5a35e4c6d800b5b804d7796
S = 36f2bf6b21b987c77b53bb801b3435a577e3d493744bfab0
Result = F (2)

Msg =
1843aba74b0789d4ac6b0b8923848023a644a7b70afa23b1191829bbe4397ce15b629bf21a8838
298653ed0c19222b95fa4f7390d1b4c844d96e645537e0aae98afb5c0ac3bd0e4c37f8daaff255
56c64e98c319c52687c904c4de7240a1cc55cd9756b7edaef184e6e23b385726e9ffcba8001b8f
574987c1a3fedaaa83ca6d
Qx = 10ecca1aad7220b56a62008b35170bfd5e35885c4014a19f
Qy = 04eb61984c6c12ade3bc47f3c629ece7aa0a033b9948d686
R = 82bfa4e82c0dfe9274169b86694e76ce993fd83b5c60f325
S = a97685676c59a65dbde002fe9d613431fb183e8006d05633
Result = F (3)
```

```
Msg =
5a478f4084ddd1a7fea038aa9732a822106385797d02311aeef4d0264f824f698df7a48cfb6b57
8cf3da416bc0799425bb491be5b5ecc37995b85b03420a98f2c4dc5c31a69a379e9e322fbe706b
bcaf0f77175e05cbb4fa162e0da82010a278461e3e974d137bc746d1880d6eb02aa95216014b37
480d84b87f717bb13f76e1
Qx = 6636653cb5b894ca65c448277b29da3ad101c4c2300f7c04
Qy = fdf1cbb3fc3fd6a4f890b59e554544175fa77dbdbeb656c1
R = eac2ddecddfb79931a9c3d49c08de0645c783a24cb365e1c
S = 3549fee3cfa7e5f93bc47d92d8ba100e881a2a93c22f8d50
Result = F (4)

Msg =
c598774259a058fa65212ac57eaa4f52240e629ef4c310722088292d1d4af6c39b49ce06ba77e4
247b20637174d0bd67c9723feb57b5ead232b47ea452d5d7a089f17c00b8b6767e434a5e16c231
ba0efa718a340bf41d67ea2d295812ff1b9277daacb8bc27b50ea5e6443bcf95ef4e9f5468fe78
485236313d53d1c68f6ba2
Qx = a82bd718d01d354001148cd5f69b9ebf38ff6f21898f8aaa
Qy = e67ceede07fc2ebfafd62462a51e4b6c6b3d5b537b7caf3e
R = 4d292486c620c3de20856e57d3bb72fcde4a73ad26376955
S = a85289591a6081d5728825520e62ff1c64f94235c04c7f95
Result = F (2)

Msg =
ca98ed9db081a07b7557f24ced6c7b9891269a95d2026747add9e9eb80638a961cf9c71a1b9f2c
29744180bd4c3d3db60f2243c5c0b7cc8a8d40a3f9a7fc910250f2187136ee6413ffc67f1a25e1
c4c204fa9635312252ac0e0481d89b6d53808f0c496ba87631803f6c572c1f61fa049737fdacce
4adff757afed4f05beb658
Qx = 7d3b016b57758b160c4fca73d48df07ae3b6b30225126c2f
Qy = 4af3790d9775742bde46f8da876711be1b65244b2b39e7ec
R = 95f778f5f656511a5ab49a5d69ddd0929563c29cbc3a9e62
S = 75c87fc358c251b4c83d2dd979faad496b539f9f2ee7a289
Result = F (4)

Msg =
31dd9a54c8338bea06b87eca813d555ad1850fac9742ef0bbe40dad400e10288acc9c11ea7dac7
9eb16378ebea9490e09536099f1b993e2653cd50240014c90a9c987f64545abc6a536b9bd2435e
b5e911fdfde2f13be96ea36ad38df4ae9ea387b29cced599af777338af2794820c9cce43b51d21
12380a35802ab7e396c97a
Qx = 9362f28c4ef96453d8a2f849f21e881cd7566887da8beb4a
Qy = e64d26d8d74c48a024ae85d982ee74cd16046f4ee5333905
R = f3923476a296c88287e8de914b0b324ad5a963319a4fe73b
S = f0baeed7624ed00d15244d8ba2aede085517dbdec8ac65f5
Result = P (0)

Msg =
b2b94e4432267c92f9fdb9dc6040c95ffa477652761290d3c7de312283f6450d89cc4aabe74855
4dfb6056b2d8e99c7aeaad9cdddebdee9dbc099839562d9064e68e7bb5f3a6bba0749ca9a53818
1fc785553a4000785d73cc207922f63e8ce1112768cb1de7b673aed83a1e4a74592f1268d8e2a4
e9e63d414b5d442bd0456d
Qx = cc6fc032a846aaac25533eb033522824f94e670fa997ecef
Qy = e25463ef77a029eccda8b294fd63dd694e38d223d30862f1
```

```
R = 066b1d07f3a40e679b620eda7f550842a35c18b80c5ebe06
S = a0b0fb201e8f2df65e2c4508ef303bdc90d934016f16b2dc
Result = F (1)

Msg =
4366fcadf10d30d086911de30143da6f579527036937007b337f7282460eae5678b15cccda8531
93ea5fc4bc0a6b9d7a31128f27e1214988592827520b214eed5052f7775b750b0c6b15f145453b
a3fee24a085d65287e10509eb5d5f602c440341376b95c24e5c4727d4b859bfe1483d20538acdd
92c7997fa9c614f0f839d7
Qx = 955c908fe900a996f7e2089bee2f6376830f76a19135e753
Qy = ba0c42a91d3847de4a592a46dc3fdaf45a7cc709b90de520
R = 1f58ad77fc04c782815a1405b0925e72095d906cbf52a668
S = f2e93758b3af75edf784f05a6761c9b9a6043c66b845b599
Result = F (1)

Msg =
543f8af57d750e33aa8565e0cae92bfa7a1ff78833093421c2942cadf9986670a5ff3244c02a82
25e790fbf30ea84c74720abf99cfd10d02d34377c3d3b41269bea763384f372bb786b5846f5893
2defa68023136cd571863b304886e95e52e7877f445b9364b3f06f3c28da12707673fecb4b8071
de06b6e0a3c87da160cef3
Qx = 31f7fa05576d78a949b24812d4383107a9a45bb5fccdd835
Qy = 8dc0eb65994a90f02b5e19bd18b32d61150746c09107e76b
R = be26d59e4e883dde7c286614a767b31e49ad88789d3a78ff
S = 8762ca831c1ce42df77893c9b03119428e7a9b819b619068
Result = F (2)

Msg =
d2e8454143ce281e609a9d748014dcebb9d0bc53adb02443a6aac2ffe6cb009f387c346ecb0517
91404f79e902ee333ad65e5c8cb38dc0d1d39a8dc90add5023572720e5b94b190d43dd0d787339
7504c0c7aef2727e628eb6a74411f2e400c65670716cb4a815dc91cbbfeb7cfe8c929e93184c93
8af2c078584da045e8f8d1
Qx = 66aa8edbbdb5cf8e28ceb51b5bda891cae2df84819fe25c0
Qy = 0c6bc2f69030a7ce58d4a00e3b3349844784a13b8936f8da
R = a4661e69b1734f4a71b788410a464b71e7ffe42334484f23
S = 738421cf5e049159d69c57a915143e226cac8355e149afe9
Result = F (3)

Msg =
6660717144040f3e2f95a4e25b08a7079c702a8b29babad5a19a87654bc5c5afa261512a11b998
a4fb36b5d8fe8bd942792ff0324b108120de86d63f65855e5461184fc96a0a8ffd2ce6d5dfb023
0cbbdd98f8543e361b3205f5da3d500fdc8bac6db377d75ebef3cb8f4d1ff738071ad093891788
9250b41dd1d98896ca06fb
Qx = bcfacf45139b6f5f690a4c35a5fffa498794136a2353fc77
Qy = 6f4a6c906316a6afc6d98fe1f0399d056f128fe0270b0f22
R = 9db679a3dafe48f7ccad122933acfe9da0970b71c94c21c1
S = 984c2db99827576c0a41a5da41e07d8cc768bc82f18c9da9
Result = F (4)

[K-233]

Msg =
f553c9a1a17d02161faac334dd5f15324c1c033def264d62b28961ae7c5e8694074a5b8ef04780
```

070aa79379f8565ed3fb5f4e1d08b1275e1e24f7bed6b749e83c1b9ab2dd76110021616ae5db32
340c1f813c5754e549c589ff09990dba4cb939d0705491911cc70ce032c2af7efea6608bb432fa
49195f9d24808848eff8ce
Qx = 0136ed170a3e06af2f542308c818ad113115662a0f24b86e8de8a8577340
Qy = 00cc263193d2844f48c02de4d5f8df5ddee4548703a5222eb2144ffe54e3
R = 0017c34e4c94c9ab1957b3ecd22f97c32eebc608ca337b0b314834726964
S = 006ac64d1221b4d5fb0ea95a5e154a1e64647f15a1a4f8ac6058968e05c6
Result = F (2)

Msg =
490d6c7d320a88286bee74e3ff2536a9c9af1d9c36d5a7554c14a178eb5e908b53825008e7e8fb
b031810d2325fec5aeaa40ce6456101e7079111fa95ef20c67cde89e95d45ce908c8e1800f8668
e04cfeb70cc2f317742efc4d1b9bcfccf931be299f4e82cf19d838f418d1a9cc512bcefc20de94
517139dcb2e075c6531f90
Qx = 010b9887c30189f70fdb353368a46e18ba0cfbce16274bfb456d183af21e
Qy = 01dc2e81158f6221382560a1bea6cdd8d099d0317ec09c9c5beda7942c6f
R = 00077eb49e722729af67db03650808c60e0122f7b7efb8792a7accf4fe54
S = 0026f591818d27aa189fabc1525646fa706f77cacda89f108c810598accb
Result = P (0)

Msg =
ace934c17c190a4cf59bf76a2b89bea316493a3688b5f35c6278efd108bbcb9112020adf4550ac
8cc19202767b3ac24fee2b57a00ed57a0d7ea106da028f08ae371d1697826ce34f469e10be5a82
44bfba737e277c7daa0406c273227f1c59d4830403f01bb3d61cec86c648aea76c7ce0ea59d4ba
f5abc964a4deb165ace489
Qx = 00e4c747929fccd4042bd3f7ac1d1659a59a888e8d81b670de19b2d9a305
Qy = 00bb27d7c664e68092333580ad94e67170e0e5e678278e9c43b9dbe94774
R = 00584c7b81ea80d78a2574654a3f6a36398c2133fae96f428ee638ad4d65
S = 000b0b36d180506386efb3cd6572cc3afefd751b75db4d1b9096ada948e2
Result = F (3)

Msg =
fd75c460df9a32bf0a837e08eaf81e6a3ecf628479bdfad8686bb97d16cc9915edaffeff1d903f
ce42b462f9417527d372da49be056a009c9e42ca8743666bc2785532efa8e07f82c73b82753655
453ee765edfec1c53dfb46045b507337d7e3e78fe9984831fac4e34166e592408190e399d8aa76
76b9dba7d8f5406de7e460
Qx = 01ccc8d325e42af6aff1a280ebde426050609883926dd18acbf24959d9c1
Qy = 009f314e10ad7c7f20e7061bb58a0a1128c1671ae2fa5f929eb05cfddada
R = 00053ada9d018679f8ff4352077e63baade5ca2c506450205cdbcbe37b93
S = 0024df72910c75b3b5d6fd618326708277660ae53489fdef984f01f2b720
Result = F (4)

Msg =
54f9ebe43a658c8cdceee7e2edcc5e8b04866ce99516385520486aa9a8633d02670bd5c4c066d4
de757e284f1ae626e9caa1dd54183fa4574849f653c0df8010b9a077bc3aca2f3147a2ea775617
ee8a02a2da5d0370391e5ec358bcd99655a7b28079d790dac70fba24d56387a5dbf817520a0b3e
f11f34c87e37ecdccee54e
Qx = 0169b6839488a2230eb8a55d4aee2cfdecde006beb1173428f6079fb5b2d
Qy = 00241ca64fc4d97b37c4721d28eddb25d8d187570f0c8e2bc9f2111d1255
R = 00369daf397bd022654b1b5b0b0de937e9aa9c830165415b6329b0bfb090
S = 001f591f44be300354755a0fb466e5b248597f7a5a9cb69f4d508415da8f
Result = F (1)

```
Msg =
dcd8bdb15a84862ca5ae26302d95320cd71c4ee7fec24d54b8d49a275ae2d6863e6fc243c3ec60
6996e8551430819286a01e33788b60a7ae715512ce31efef72d0b5fa7c76b94daab9cac96a1eea
b7efdd03af84e5d5b9202033b33bf86ff3e11a132d057ad1961797bd49d900baea6e17328ab315
0bcbd34ed64516b74928fa
Qx = 007345bf47179e1533eb451d0174e1c04f8bd34c202478f950ee54f736f8
Qy = 01706e0da88763ff81d6e1e853ce5f7484635a7f6d08b8d9730b389c8d0b
R = 002e1d25e5b4f7549fc39bfc9244c01843cd30ba3e7cec33c56bddc67a66
S = 00486550d28f3b79d135baadf8795c8d21951d76b88cd9110bca0d125133
Result = F (3)

Msg =
c5f62b24a16226b4a66a01893da87fa175bc523f9a91464909e2bdee42fc5b8b3fc502d005fd01
1f78c48834735c600b1831d8fe6516032f08d2202575db5aba3561b234818e39b20f0d82ca2cc9
57700bf7ab195d56d02121b5ea6abeb7a4474fd321983e9e3636144dd6918f75cd97f616b1d8a9
d816e8fc9402054516a1fa
Qx = 01b6dec64e5e1fd13ccd98ba680763c47583e95cec2d0dbf309bf69fe51b
Qy = 011221e50fc93677bbcb6e40b24f2de6eeed9bc26ba826e80e02f7eb5574
R = 00475802cf260aa2b4b14262eacfea1ce1e45f406d8ae411bbf187e062ba
S = 00293f771aa308ef1716ffa5fddfde490724016c6a570c7b1b807740421b
Result = F (4)

Msg =
1ab37b5c3e7accb783e80d93538e1ca59d6f7eb1270651aa268b811b0c733fc5a136af895554e1
89d49a038bdca1d59e4b995dff7d44db3dd445ff9c989b5ab70269136a93f8dbefaafe22475621
8bdc69b79e64cfd0be081c765ac66a33671466d40dc6a16da0312d9dd3916a1328a81d51aba8c2
b0e05324a5fa612a424d22
Qx = 00c57832cad1eef31b0545f0c48718106d27d6492addd718d6425c7fa056
Qy = 0026e7491ef66649a3f0d4bbc8d7fb4e1db86a3c2288658edf74a64fee43
R = 004009378a80c311db1a3ab914953d7dec0ba06568a6bd533b2537e55f5e
S = 0059cf2d301cd86e94d0d1bf0d3f21fe3b2aea683d2354c8781c440f23b1
Result = F (1)

Msg =
5a56096c7e86e5d4988347e117552975e687f720e3cf9fe893f1e84514e00470532668dd7f87db
06bde1cd6b1d57ebd7ccaef0e48cf7bec1626fad338ea323dac0d865b689a9acea10f27cbf06ed
31ebdc9bdb1433664b9094046e6f619edabb0b32a7fe86368005fa7ef9e4bc5f233a7c155fb6c0
626fda9178d3ff7319529a
Qx = 01e31fa7780137bb4a2ab01d354fd773901b9ef976a5b564a2a09dc9df8b
Qy = 0191cf897a2347a43e781e2c41d5bd50efcc705267fed96f52eabdf42027
R = 006729210e1d49542bde1e3ee0609368dac81bfeb51ce99fdd306ca9ac16
S = 002ea969db3ff2a494730cb2de1d177a6c5b3ca7a42b0f7bf6d1ab44ed8d
Result = P (0)

Msg =
2a5325bd0277f9c49be359fd2bbe5e63d1832de0e102e16d7da8c67a6501c8900f7b2b35fb6d7c
104157c74d6c6c0a438a4dea548418a515aca148af95ff2286274b7818f2a47a27c376761a75fc
4ca10a042298fbf3582ecb08be46e2e5051d994b742d9225dc524ac8ce2cf1790bc4792f3c72ed
9be4fe04669205f6ba5b9e
Qx = 00c6b220969d54cadf544316cffa60fd5a1595ac420f61fc5873ad78bb56
Qy = 0196b017ed347446c64d6ae8613e75f822938194a84952e364d67d2e0036
```

```
R = 000a4c1bd92de8907c3cd3930249b06d8556093ef7378bdb520d56791afd
S = 007f7b94affd65269dbcc29883064b69ccce7127ab23dd404eab59029787
Result = F (2)

Msg =
cd25a7f53bc44ac3eab1d4771883891358d2b77a86534ac000449aa4130b875bb41ac890711580
a8a737124af4f2371fefd54ed617b3f36c0a02d2aaf881bdef561efd2fd716e63c985eaf449a42
809b764ccbbb4c67e08afd44bcdb9afd22361cf8eedc550fa50626ed506ef3bb8b1054fdd9320d
b63aa241d3003fe2c6deba
Qx = 0078cd54849617d64c1bf3ee0c01639d4912411912513612512c0237bf43
Qy = 018a850cae6cb9b81fb4173847b4f29fb40b47a9bdfc119d2eb6fcc4146d
R = 0026170cca4ec53585b9ddc149f1811133815b8aa2f68f2d80e06746a6f4
S = 00100984fcbe5bc6a0d91473b40589433851aa725c3f4ffa744f340eefb2
Result = F (4)

Msg =
c292e847f4bf5a482ca63544d31ec7df4f05460726d415266776439c465b556c06c845351c71ca
659149daa9a8996da8c14f85f07d996b3023b33ba942fea2df9851e794339328f6d68ae7189eee
c59fe5c28cbe67e47364a3e29eb3850fe5b541d6d64a824ffd65c4106378fe46542d850465572d
dab628b1aa75a455b7a355
Qx = 0073108e1827566a63d94ef922f94b2835c91d53ac62371df25217989f2e
Qy = 00c0ce149e33218fc95a299c64dbccf80aa4062ca488e74340d9d0a40b83
R = 00561b14067d3fcf8d868ac17211d6a8747b6089638338810f7336aa988d
S = 0047e987aed01b51f888fbf4b2dc34a367b644cee4271f426314d63eed98
Result = F (2)

Msg =
0cb9c695b7585006751e32fa0761c185fefabf73c23f7cded931400066f6ed45f089e1a465b01a
305f2e9deaa53a18daf531c65e018893c1b704810fc52d4a285d00471435e49096d3df6504070a
cc55b9427c7ce421faf5e32c029dec4e28c6da86bf8b2fdcfa61599951ef34b72620d197a97676
f2f9a1e5128c50e142d047
Qx = 010c42d7b7557e2ba495373dff3cade13fbb56614f15b47fca217ca7d57e
Qy = 017abd698cc8dec5aae48ca111b533829d487a7ee333b24e74da4a50b889
R = 0f3e30cfcf4d3ba084dfaa43b625d5fb4f406336501b1fd43f9f82d2
S = 0060553f1b1d9d2ad62f74ba7a906204dee6c6f059b50fe7317141f3d443
Result = P (0)

Msg =
8159c84852c6229694bd484661ffc349342c8a504e91803c59413fd64c6714c18eda4aad5ef2ac
cc729b458adea76a793869fb8afa7fe58327efebad3276a7cd1b1ccb56db0caddd02a303cd9fc7
ea5c607a2ebefaaec598cb5b9cb7bed097027047d3ad91bb2eb08cfe09786a064cdcf387ab5217
c828638dafd95cba1dec47
Qx = 007ee60584691638fd6fe17a3b4ce3ebce1747ec6c44ba6ea8d235b130c1
Qy = 00881c53ec4e23e591764b5cb4047701c6e8035e37f77cbf83d0d7257d98
R = 000e690c9f1180e538bb790906e037cca39d0779903284137 0c74ea30b78
S = 006e1e028bd9d204b9d97bd9846429edaad8da32aeec6f3bb7e99f32ee8f
Result = F (3)

Msg =
39cd57963378c638c3b2a442f65d15d8b9c605c5f9356db208c2d19c436b0e85f26452696fae6c
738beb46712d71af863c9d5e1ebf6934274341c27f7d130ba831a68bc3532c78bc6b1a47c23e37
```

```
72faaaf37974d2fb275e7b0a1677b60275c7c03b098e261b727a2ce7b01c70d8e59dcb725cad78
11cbbd78c5d56e345fd34a
Qx = 004bc66f1524162fc952a41240b627e244be6d1823a0736be63adf559727
Qy = 011b167b34fc9be9589e7d8c1fe3dd033d6145a0f1794f911272dea141dc
R = 000d4dbfcb1069e09657f3d9614f3e6bdb0f812b281f0887c85b5e57c376
S = 0028055fdaaa8090d97568a23eee931d576fe6eae5aed9e11cf151f3a77f
Result = F (1)
```

B.3 Examples of *RESPONSE* Files

B.3.1 KeyPair.rsp

```
#  CAVS 3.0
#  "Key Pair" information for "ECDSA_Test"
#  Curves selected: P-192 K-233

[P-192]

d = d1c0622c0620d6c30667d9485da2086cab0e3b2345825f48
Qx = a26168f3d32ea1063f117b16db4b725b9dbffaff7589e15b
Qy = d86db5da7520e76bd186169892eeb7f8fb362ee69686b0fd

d = 7d32e2273cb0f1bfe56d56f7f033ca9fdaee609365909406
Qx = 3b0c34791fd69ac4dd8d9b8e18bdf4427be063349197e0a9
Qy = f0163b8dd514f4656674c83c1374944bf58f09b4e2b2e6c1

d = b04c14fd8d72d37d5960d25b3f4e3241133cb9729ba5f2c5
Qx = 3271c7199a377c8cd0f5b151f1511a134ca8aa3e331f26a0
Qy = 3fe30eece433078b2fba3961520cb5f162b5dab2b935555f

d = e33a65728d2f44920aa5a09dd5ba33142358cda2335fede2
Qx = 4dea2eb87ee4ca6348acd963588411388b3ce14c8c447059
Qy = 10ff129b4a3b33a9c2f1b2f683d44dd3e51d6d6da7c4a4a4

d = 0418a7052744f7c342342e711f03a652e693b6431a3c5c86
Qx = 195a5a322dab33e8483bf68d51499aead126338851ad870f
Qy = de300971b88ced44e030c46f568ce0738ecb7aa37c4c4a44

d = bb2761752b3a88183e09ea96f36b00a3761f183abbc9e6c7
Qx = e6814d1b84187ae3badb84bc649cef9895ae60e1576befac
Qy = 8943e839ae6ee0f45580861ebd4b3963570edb8b28f31728

d = acb4c811c17d1d93ef73af9b4e28b9ab5346fad5841795c6
Qx = 03fb1039cfad16f3feea2dacde1a069f49c90692b75d0b19
Qy = 2103c5f0e78f073d8b18dfc82ad16b68ab3a14e20bb0fab5

d = db84f7af6c5850cdda565f4299b83bdb75004eb413fcf95f
Qx = 2902bceb5fbbeeac3863a792b3e552b471a3bfab1406f33d
Qy = e2fb5606461888eec893f60f557a0138cdb1ff762cc0d7cc

d = 40ffb9da1e51333e411f9110cd4dfdfb41deb5e097d3db89
```

```
Qx = c5166c06f37665918f201f2b42d6ff097855b95af55c07c2
Qy = e95937fe8030d8d44363cb2c833617be8c6887f4077441ad

d = 69de16a5cbc01f8d6b6523f59aa8fc356a3ec63022085e28
Qx = 2dfd8cc138d3b2f1ffd1f8c5c438305d56bcef2fae27f340
Qy = 24723a6e7e36581ca041af5a14525ab4320f25bcaf01976a

[K-233]

d = 7ef51fa225232a0af18046eeb01dac44cda065199843d7a4ff21616c54
Qx = 00ea982d89dccb61acd284d346b7ec237ed8bbe273810ab5f8696a103a91
Qy = 01c294d7c86bf404aa269dc1dc6bd6b6f935fa7a26e6e16f949fa7f5bd19

d = 613283db2d1c61df821703eefab9ed3f1ea2f1a44aed370d6977451807
Qx = 00e834e3bbb0ed735c7e374a4003f4bfa8fde0ae77d043f744fe15abbd88
Qy = 01c49eafff11a33f33b7e3e367c7f3755e016546aee49764c4e7eb7a5626

d = 6126da59fbe4a8c4bd98a93b944cdd8793ddaae9212de6d27a8c18a8b7
Qx = 018adcc10f6b0a98a1c241abb6ff5780dd2bf04f91028dcee30d2f8d3fb4
Qy = 01379f970145c5e2cd2ce90e6ca247b4de178a14baaef12ded6cf78f7fb5

d = 5180b283a1d01566e45110b9764effc6fe944e4db193f406e226213fba
Qx = 001f9526e2b0cb7e82593d7c3cae548973ecfabaaf0d6e1e63710d4db7e8
Qy = 00d02b8c45ef123246eec0a310274be30943f90432b9eca4dbe915561acd

d = 16772dd28553517560a1b686ad3199435b136e21d3d8008f3eb59d22d5
Qx = 010a574052cac6b245f2c50e44bf171819c139918429f68590d62db0cabd
Qy = 0016160655a6bcb3e530d89bfb91185ca2a12a47ee3a538528ce759e7d35

d = 066f9178cc33fe1e789783cb5edb300c0b4659b6313da2de974a1cd10a
Qx = 0002403feaaacb263aa253661ae893182cb2052b00671d5e51ba38aca276
Qy = 01d6c3373c0ac55c7c9ad0c5e26bcbe0516d2a18a5a9bb686ffaec73bdd1

d = 1878227e8d940f788896bc8ba70230db2ae22171b073472ed891184ded
Qx = 01d88db0ec51096cc5ed0d376986289cd25489f5c29350280c673f42726e
Qy = 01e122b628f8b8fe49af54af2f7a9d603e3bb00b249c8d34238da13de42e

d = 3e8b6e2c2bc42801c49b6179317432c87faea86ed7f74ebcaba892d603
Qx = 0149ee2bd4bb0f41b3762f98f68edc389d1edbb5dd604d3ef4c17258ce04
Qy = 00e9aed2e4d9a3d07c86478cd39e535389b0d3f30504f554affad5da49c0

d = 4b3c96267f592a286d1fb8a66731fd5b21387097e43aa88bd6c04bd614
Qx = 0014e6dbfd74189734e9d0dd86cfcce93634b57623acb1124a6ccad9c957
Qy = 00462a852da9cfb5b218acf339409a6ecc3b05962f9ec86f7a1b16e7a92e

d = 583c507556164da99ff1990b20a7b2163b2b4722642e492404938f8018
Qx = 01d9c7f8cc47eedd7c39a903311aace2e04d72ad6c9a282be1144980d091
Qy = 011f83ddea60a151471b2d6ef156d4604294af90e2d3425763d43b1a2e88
```

B.3.2 PKV.rsp

```
#  CAVS 3.0
#  "PKV" information for "ECDSA_Test"
#  Curves selected: P-192 K-233

[P-192]

Qx = cd6d0f029a023e9aaca429615b8f577abee685d8257cc83a
Qy = 00019c410987680e9fb6c0b6ecc01d9a2647c8bae27721bacdfc
Result = F

Qx = 00017f2fce203639e9eaf9fb50b81fc32776b30e3b02af16c73b
Qy = 95da95c5e72dd48e229d4748d4eee658a9a54111b23b2adb
Result = F

Qx = 4f77f8bc7fccbadd5760f4938746d5f253ee2168c1cf2792
Qy = 000147156ff824d131629739817edb197717c41aab5c2a70f0f6
Result = F

Qx = c58d61f88d905293bcd4cd0080bcb1b7f811f2ffa41979f6
Qy = 8804dc7a7c4c7f8b5d437f5156f3312ca7d6de8a0e11867f
Result = P

Qx = cdf56c1aa3d8afc53c521adf3ffb96734a6a630a4a5b5a70
Qy = 97c1c44a5fb229007b5ec5d25f7413d170068ffd023caa4e
Result = P

Qx = 89009c0dc361c81e99280c8e91df578df88cdf4b0cdedced
Qy = 27be44a529b7513e727251f128b34262a0fd4d8ec82377b9
Result = P

Qx = 6a223d00bd22c52833409a163e057e5b5da1def2a197dd15
Qy = 7b482604199367f1f303f9ef627f922f97023e90eae08abf
Result = P

Qx = 6dccbde75c0948c98dab32ea0bc59fe125cf0fb1a3798eda
Qy = 0001171a3e0fa60cf3096f4e116b556198de430e1fbd330c8835
Result = F

Qx = d266b39e1f491fc4acbbbc7d098430931cfa66d55015af12
Qy = 193782eb909e391a3148b7764e6b234aa94e48d30a16dbb2
Result = F

Qx = 9d6ddbcd439baa0c6b80a654091680e462a7d1d3f1ffeb43
Qy = 6ad8efc4d133ccf167c44eb4691c80abffb9f82b932b8caa
Result = F

Qx = 146479d944e6bda87e5b35818aa666a4c998a71f4e95edbc
Qy = a86d6fe62bc8fbd88139693f842635f687f132255858e7f6
Result = F
```

```
Qx = e594d4a598046f3598243f50fd2c7bd7d380edb055802253
Qy = 509014c0c4d6b536e3ca750ec09066af39b4c8616a53a923
Result = F

[K-233]

Qx = 00534537f7762394d8ff46675d194aa212c4f9a2b5705f68df74e4e35d59
Qy = 01b4bb8fa0cd97777f60f4d7e4038cd65527eff4570b09204fdbedabc7d2
Result = F

Qx = 0148dec1cffafce7ce21ae80652935bbb8b960bb1c4f27830d7ac0a786a5
Qy = 00c845acaaccc4549b8e2323a7f7ec17e0c8ae7a574c8e6a1ce337939c7b
Result = P

Qx = 013ca0f0875f8fea41a1f44aa7603a85324507c7177b616627459feabd3b
Qy = 0061fc08300b6cf0c99c5f923ccc65f9be1fd9449b0625ed6a7f767e6a4d
Result = F

Qx = 0079a6cbfe3a2e9e9eaef2b119787682ad51b7e1003e0bd952417f651d65
Qy = 00990e7736bed24326c49a683587e72b24d8e5b62c037495a99f21438bac
Result = P

Qx = 00faa4e23af6d38eff68c8de405891a8e5eba2487bb854c8cc1d5a9d9fbc
Qy = 005c6cb3b3e608eda31bece7c755109d840b41550f09448db4122967bcae
Result = F

Qx = 01883d8c99b33f5732a4fc226ec695d1664a30b6cd1e7e302da60d09ebdf
Qy = 011424b3e264102e4ac2c837925c03790c5f1053e2b9fbf77269d856e7dd
Result = P

Qx = 00aa7822d4d5e939c4c9ab0b0a7a24c395a31f5ef138601d957fd48915d3
Qy = 00fcba0cb2522203754655e4a95be36b5c3227f9cf3aa6e9eee73acabc66
Result = F

Qx = 01b84c30e07e761416b9a9a548c1f9c0e64ea3577277d3a3cfaac7b22303
Qy = 0117c9df876b0c309f02499075a98184ebd66e62abf8c60144db4bdc438b
Result = F

Qx = 011cae8c5ee0ece8496471f45b6307edf97583ba70b793da4d76cc6db05f
Qy = 008690e754c7c74ea1f94c4616e653f7223387f14a0119407f255fc955ce
Result = F

Qx = 01dc2d0dc408cd363f81e448fc46c9622b4f0ccc03ec277fe64af2be43c8
Qy = 00b5cdae6799fc82e9fdcb81798dc61ea0ecbc01a771908186f741103826
Result = F

Qx = 00539b5e0779ac3631c28177558000a543882dda3c9fdf8a27df24bfeb05
Qy = 017a62d298132856e8a283787083131cf7ff93c3ff1d592d783760b438fe
Result = P

Qx = 01e147f3a7653416b87a70c08dccf34e49dd1a630ba88d591c74e827ae72
Qy = 01a32a428f0f3b7786317753aba84f68ab0ea0b760a298f1a2286cc605b6
Result = F
```

B.3.3 SigGen.rsp

```
#  CAVS 3.0
#  "SigGen" information for "ECDSA_Test"
#  Curves selected: P-192 K-233

[P-192]

Msg =
c70e287f3bb37422fcb2f277cb178a98eb6ab8e2d68ddef930e7df0cf9c3e95b06f292f6b2b827
c7d1e640d2e54398bc95301c8a5a8c42ac7cd69c3a3d91ad7d53edfbb19ca365090e21b7f4ede7
7c9f403114bb85d60680a47097f222bd9b6397458b39623dd8f19bac7f6449ccde49d5b3c5fcbf
32d17e90fef5bc100d5a14
Qx = a26168f3d32ea1063f117b16db4b725b9dbffaff7589e15b
Qy = d86db5da7520e76bd186169892eeb7f8fb362ee69686b0fd
R = 3b0c34791fd69ac4dd8d9b8e18bdf4427be063349197e0a9
S = e90138270f3aa30370baa7a8b044d46e026be81ea6d75f47

Msg =
1a3cc54a8ad392749b2c1b59aa07b451bd1ebd8a5cac19a9a22ce2b493635a2fb0a02585c943b6
aa137c08ff7a558e7638f36cf6a718e70153ed1a9454ffeb4edb873ed50aee69760990e70b56c1
50225c0d885b48c4371218b77a3ef43cd999c2787802f5dd911fa5f12146e551e29e51f67a81e6
b8f2251710697c1c220a58
Qx = 3271c7199a377c8cd0f5b151f1511a134ca8aa3e331f26a0
Qy = 3fe30eece433078b2fba3961520cb5f162b5dab2b935555f
R = 4dea2eb87ee4ca6348acd963588411388b3ce14c8c447059
S = c29fe44581bb0bb8a3df74c247c8fd13763bcfaab37f704b

Msg =
5673828f6db66331f21f7e21a6bcb77db852d4c738fe90a0ce18ead2ac5cc394c14ca80a2fd0ed
0c0020fb2814e3eaea5e99535a51365fc7940f24c3fdfa326fbdb168f9d8780d62d9001c85c38a
de554a4fbe6643205aaf5a4ad68e03bc750cb36c6a634ff6ebbde586883f9af9bb46e33fc0f0f8
04a6df868fa739a4eab5f3
Qx = 195a5a322dab33e8483bf68d51499aead126338851ad870f
Qy = de300971b88ced44e030c46f568ce0738ecb7aa37c4c4a44
R = e6814d1b84187ae3badb84bc649cef9895ae60e1576befac
S = 8f7d791a9e262e7af517c6c7ac30738202fe4ecdb760a478

Msg =
ba8636a1e1cc77e34750061f11b5cd2b0da1a703961467beb9f81bc096f9923008961bad887890
3c4e039385ba2c1840f38a24eaceafd3bcf1b8a0dd3823e1d757e19148c1ac52dac99bb27407f4
aeb2fe417593fba66e7240717b3862f380cff08f1fda5510c6a3003fec54c2b6976b77ef2268e8
a03dc8f04b3537de107602
Qx = 03fb1039cfad16f3feea2dacde1a069f49c90692b75d0b19
Qy = 2103c5f0e78f073d8b18dfc82ad16b68ab3a14e20bb0fab5
R = 2902bceb5fbbeeac3863a792b3e552b471a3bfab1406f33d
S = c9f1e6b63b2bdb1ddf046dfd1ac71279fcb169814343c8ff

Msg =
6d3a19d8f63c7bb983468757a142cd14fcbef605229ca8498a0baa99d5b64921533bfa8ec9de40
69727fd0a343c9f47173ad2d5a3b0e1c8ddbbea279ddaa47989d51d88b097b546ca6270a60d4c5
```

```
fb6b52a5858904b043faf4562fdd98c709005366fdf73d7a806b27277bb5da9eababa09047ba06
e8e436dfb997ed8c755902
Qx = c5166c06f37665918f201f2b42d6ff097855b95af55c07c2
Qy = e95937fe8030d8d44363cb2c833617be8c6887f4077441ad
R = 2dfd8cc138d3b2f1ffd1f8c5c438305d56bcef2fae27f340
S = 12474645c225f07d87480f9db7d42e3165f7341baee23b6a

Msg =
35883c4a11985c37a1244af70260b885124411b0323d5b714a22627c0e691315809b2625b60500
8ddeb1d7ba7f9417790209040d707ea1807d6dd136c68fbdc8574c750f7075da7e8935bbb59345
3e548160820d07f782fea1253d3dd8e514b4c183732fc650b3b3a89a3f12c5dbf6bc9731d1d87e
0ec693bf31ecb8ccd5df82
Qx = 49dc1218aaa059b15cc9d43942cb6ddf96000a0013b3911f
Qy = d2ddc8caf788caf91b9e042b2ae9cd00a9ebb273d5a52667
R = 0f6add736344f4b0436f895afbedfd3d9d127b9d450ca677
S = 0cef17f2e244df4e53c253c23f2ecfa068299cb5266aa406

Msg =
05d77ea4977ac96b8813fc1210483a037e7b6c502ceed8f7b22bf6655aa37e38d495c6492b314b
eaf8fe8d6cd67921e515ff012fb3ec263487055969c01346998ed1d2e41f08ae07cdf92cde96fb
5227cc652e880dae68d476d31e8a14f9eb9e9b54497c5b471a4b6fcd816e3817f6510a779a6224
7cc75de65feccd3e9d98d0
Qx = e634ae4fb20d5a12d14abc6b92bd4c426a1316924edc04bd
Qy = 34fe751d4ff0502eb5602f3d111d11bc197f3764fec79e1c
R = b9af12913a8754ebecfec83dabd5513eb2d830a01898203b
S = cf7e259f52cbb8e7f9a1bd3fed332121462f6aa2a659a155


Msg =
c96009b6e816ef26695ef6bafcf76dcba3b0793fc12cc46574e2742025675a485ef06c4ddb1376
1de3cd0c48d9c9c3620edfa1aad9dcd1e8ea819b9cdbce94540880125ea1d8e39ffd9e3fc33166
fa97e212feb25798f95bd20553a721c263e27016e23061eda0745fd875712f547b30c74f7aa164
e8a484d777838a1fcd2fb8
Qx = 007580624c39b159d5245f128e9527b6d9b76658394081d8
Qy = 82ef3376d99150ee5adc9574bb39ca99390aa9ff42456beb
R = 973ad35df6efd859ed384c8a01e4f9dd894be1a98512150e
S = abb2dc5f89403b950d716944e18805246b26236de1ea8f1c

Msg =
1ef4e272a78eb74d4a46ecdd514fb4172a6f93030e0d1e70e08c02e658d747dc603dd62bbe8039
c3f428a39c641d30f0b8756da8818b1b141e5130dee0e71f416c6c59766014146f397a4bc87438
06fbf3b6dbd3a33fb5235c5ad4b70857158b0828743bd372cfbbe0e4ed48c7c8be9ea3d7e46cba
527305604ef5581850b222
Qx = f989329fc43931c6501601acc3a03668ee220aab2f664efd
Qy = a71899567ba02718e7ada7bb98105105eb578341a17f08f1
R = d61c3e430ddfe082b7283f258481a8e856dfd3c4008a1097
S = bd15bc01ddb25bd9d5d5806895c14e79d49c554e60828d5d

Msg =
942c6a4eba5e2760e8e7972f6208c91b5351dc5a6eb6c2a5d6e544313bd746e146a54dba389e3e
97ce96691e6780c5f268407d2ae0baac03682f65d14ec9f73cf2746fa86ff05ef57e24dc6998b6
```

```
ccea5bd862712f65e3bb292cac42308c766b5e41d801a87d0de2c23af8f83dcf656bf3c29215a4
deee37e185206a29474bd8
Qx = 742a99af55aabae1b21b2f307e7eea9719f874b104904624
Qy = 435335c3873e2955880c683737f4cabe58e1247dbada60f4
R = 1323aba0ff586a58d8cb9c782877a1e0ea43c64635a4a992
S = a1e1d3467334cbee1fd435a4b90fdc717ecfeac72bea42a1

[K-233]

Msg =
baf9377601faf15c5a1288381efe55547d022599d1e330af2c354b6633dd5e5530ce17c16216e0
c0981e0f9dfe2d5d7f362f9a46aab59fb6213c83d791b2129b34367ac2de2048fb8e41934c436c
77b31134c60e73f8f938e31d6d75a89bcc10f0bbc8421e1f105665027c0b96c18b3a369a10b8d4
b4287e99606f07219f74fa
Qx = 001ab211ef6d91e35d79ca370b15630d8f0642122528a2f5d89d3be9a89d
Qy = 009a28ab00ba31c234405072f0c20147fabd9187594a9cc9540ec074140e
R = 2714031ba3e801de7e8439fc3f8ca73bc446f20e9087b4e244adf31a5e
S = 28391b3622e76a27accdf046687ebefc4c384178a8cbd063cc662aa68f

Msg =
34ab1130ce389d340fca232cc50b7536e62ad617742e022ea38a6fa63ef1d3ef476be66edea969
736395676cdf2ebb59a093d280245db26239323bed6198adf37b066bdba041ff974ce65dd6be42
6c7aa16ac24ceb88afee06747e122e84f7ea1aa429dfdea9668610e28ed029f091812fd82fe391
5702bb5376bf7c6a5db9bb
Qx = 0032c0e426be8363a2b9d30c5b951afdcbd1851d1e27482bf2fe9bb08fb1
Qy = 004235f83d5b5aa6689d2c6dd91bdf2df1e51f346e1cfbbd1f03b798d6e0
R = 28dbd11d8ea6d6c97e80e5accfc7899d496102e23f9f5aabce80fd485a
S = 0965a3891d6c15b8a080c72e6071e375181137078933a6aff988979447

Msg =
693e50d3d13811c9897f260c809e0111e4566d52da89d74f7257ecd2da866a78d2272f6d5f7697
77c4030436ae0fbeaaaf39fef5ed5a45621cadf2a7a933146738557dfb51cc187256be7cd6b929
c0b16b8591d098a5834791dfa5b60a6c58ca851161060eff3cc329f9b37509b4b0310283506c41
343806bb342c8763fadea8
Qx = 00fdc95f89c28bdd27764139f53774e531247423cfb1412b9eb454f0eb50
Qy = 01272fc9bf2f4b04927792a9a712217220739d127634265b9fc44ec9ec7a
R = 3305addb4286d12a4df49242ce69faabc78a3200046bfb33dc6b1ccbeb
S = 184f81bd4e02386bc252d433efa8662dc98e5a63002e916f97f93ec38e

Msg =
a482cd28915c950f609b1324b71b42c681ed832540578f62a41bb0f25cfc31442c7f12a340ef01
5dc0a38625a4847eb6cac9cab9450548e9f96402756531a6a5bf9c37c146bb012fd4ced2dbb2c7
67dcb10a255476710a971693e290e346be618562a24a4cc87eccc4a35f0e8aeee77f5f37fbbd7b
a2bbb62330b70d7e415fbf
Qx = 0086592c31569443d7aea90b6380613e35a5ab7de41d510dcc9a73c6a3d7
Qy = 0186461c389ab0d870ecdac1a1167ec34339314e70d3e9e17cafc2c843bd
R = 62cf8e6d5596ce66a53c475ff99a142ac6c60e746cddb6ec6666039bec
S = 40ea1d17c641614cd7751632f0e60a3155f74c7f3e01b4bdae066f02f0

Msg =
292ea1755f9e587822372f4dcdf10bddfc0ff498a8af60ae94a0b482e873085c1cd52a5d181ce6
b99a1f8520d74b947d65f3e7e358e8ddc4ac4ae465e39d408eee1f09865159733f83f553cd93cf
```

```
de1c114fb3e32cf51cd418359016b3867df467b645d752808671a4609f3c49a67023c9ca617e6c
ffa544a10ac07ca05546f5
Qx = 004d8f57c8668993d5fe9fb982eadbc27719ca141f0a72fec2f73e7a3ec5
Qy = 01aeab00f8ab964db48ee55c27f7eaf356f3115c034e2b16b453a6693dbc
R = 0e270644aa79ef30d82472af87387e523a423413427d127503a98cf35e
S = 6fa98b11d7a201b8f8660239871742364cdfd89d5be4fb707a54a6c252

Msg =
60440c8df2b67e1fc1f7f354a1188ae14497175bb8d6c64b31cc018409fb93b405a20d3ada3368
37f007ede8655152335551267f59ca6fc94db591f45737716124d1dbc075d72126db23055fbe0a
d985a48fe5d1b0d709b269dda41cbe67b42346393ec8cc88f0130ab10562b52b6900baba1df9c8
e6de2d0eac01a44673a221
Qx = 00a1683885fc823adeaca0108aa252d8c697399c15a57f8fe5eba8bbce13
Qy = 01e4de4b6409322f2c7b41e779f693084fc120339c49a6854712de88a9a6
R = 71d4bc9111bf9cbffcffc592687cbcc5d7d26e6f357ab85e73679e388e
S = 0972e6ed1e580c53c3b281b851c7e7bd3e64d61108249e4e4c6e46b3e3

Msg =
d6344015544f6b63423cbb689274d70331832fb33966d51267378fa0cf0c2ac2ce1c110b41231e
b9f408af835ebdfd928b68a9cd59c09859e7b901604b63c412830ffeeaaeb5da337d92aacae415
362515fc5394aebbb8c7311d0e91b62d46ebdc572f3c05cb48d8c322d3c68d442ac6b7895692a1
1ede652eabddba77325756
Qx = 018c9198d9a653adf62943cba2dee26fdfd9dcc5ac050dfa6f6fc426acd8
Qy = 0136f0ee4506d95ae6c6cd5f91316df3b8e57e51eb143a3e587ae0aa3cbf
R = 04c24cf7dd5b712bd3b886e9f59a8fef244264dfce1cf468b1a0bf3972
S = 17b4e121d74e51c5beb4b985bdb99204531c8af54e924acf72ddebe70d

Msg =
5c3fb5a4d2871bfa77e171056ff0a48eafe0fd4a653ea353940d62d9ff16aa15497fdb7f5a9fbf
41051158ebe707dd6892e1ff31ebff70c0d0d3a648fe3adda3320c5b8c8ff1f70e4077dc3c5e62
8b2314441ffd014dd5a8dd63cb56607508855f0dbd323925ca49713c84619ca9b6a67e2ee61670
d0d9f104e6596aec7135a3
Qx = 00d5f0f357be258d782c7ab1a2d106625d4a14574cd3047721b601841e1e
Qy = 010f2eb7ea8503b735b8985f43c7972f72446064995b6d0db05f1e89b67e
R = 2fa3aeb78b03bce1c546d3e9f9b5b97eef95baef65beb4f8e698d2f911
S = 7e12ab98c850f33c08887890ef665110abddea620527307bcf2f8cfbb3

Msg =
83c0f878b2428ab84cabecfc862d199e61933d6f7fca235635a1f13ae3cd13228030759b795bf5
5bbc5118230f8dfbeaa7478d37f6f4fccfc40c6d90810ff09ddacab3bb8ad776fb73633e9aed33
4e255ee953e00b84df692d271899481bb2abb8161aa08cbef4e19869c827c627f898ad02f63365
84b36d997a5b1cddf83f95
Qx = 019408f4aebcf735aa858ab7e051d5b0935f8c136d57ef417d27dfaa9adf
Qy = 0126037bf1115d2b6cea74a6478ae0bd8b3e70a62088aa17dbdafe44a991
R = 5886c8cc517d210d3b49a5cf8822fd855ab8297d6ccab156258dd37c7b
S = 3eb4bcf6d316f0c1c9fd0d839fbc101e9938167552287d431912e29530

Msg =
39e3a58a0ce472f694294f9743a86db2d87894b98d35ffcd92a66d81bb9d75e1761f1ab3ffc59f
fcd7629dc672e652212f833c688e0ee6c59ea703f7b49cb953628b3f09a7c7aaa964fd04e60f18
9f99ab61a809f8ebff69e72e46a250f23953e76f3d166db23b062342ae7e8404fb23335c022433
95f2c056836109f8669ce8
```

```
Qx = 018c3c099fb6f2f6f4a24c4ea567788e02214287ff3145cc5e3c5891151e
Qy = 01956a7614fd043415a1e771c46800ef1498793b8fb477cd59a621fa861d
R = 2f26fb08d49cc7e1cbbcf2924952f5bed89698dabc550afe6c4d9d650f
S = 363c26cf8dc49d0640611169760fc14664d1764743d49ed687ae3a4add
```

B.3.4 SigVer.rsp

```
#  CAVS 3.0
#  "SigVer" information for "ECDSA_Test"
#  Curves selected: P-192 K-233

[P-192]

Msg =
84ce72aa8699df436059f052ac51b6398d2511e49631bcb7e71f89c499b9ee425dfbc13a5f6d40
8471b054f2655617cbbaf7937b7c80cd8865cf02c8487d30d2b0fbd8b2c4e102e16d828374bbc4
7b93852f212d5043c3ea720f086178ff798cc4f63f787b9c2e419efa033e7644ea7936f54462dc
21a6c4580725f7f0e7d158
Qx = d9dbfb332aa8e5ff091e8ce535857c37c73f6250ffb2e7ac
Qy = 282102e364feded3ad15ddf968f88d8321aa268dd483ebc4
R = 64dca58a20787c488d11d6dd96313f1b766f2d8efe122916
S = 1ecba28141e84ab4ecad92f56720e2cc83eb3d22dec72479
Result = P

Msg =
94bb5bacd5f8ea765810024db87f4224ad71362a3c28284b2b9f39fab86db12e8beb94aae89976
8229be8fdb6c4f12f28912bb604703a79ccff769c1607f5a91450f30ba0460d359d9126cbd6296
be6d9c4bb96c0ee74cbb44197c207f6db326ab6f5a659113a9034e54be7b041ced9dcf6458d7fb
9cbfb2744d999f7dfd63f4
Qx = 3e53ef8d3112af3285c0e74842090712cd324832d4277ae7
Qy = cc75f8952d30aec2cbb719fc6aa9934590b5d0ff5a83adb7
R = 8285261607283ba18f335026130bab31840dcfd9c3e555af
S = 356d89e1b04541afc9704a45e9c535ce4a50929e33d7e06c
Result = P

Msg =
f6227a8eeb34afed1621dcc89a91d72ea212cb2f476839d9b4243c66877911b37b4ad6f4448792
a7bbba76c63bdd63414b6facab7dc71c3396a73bd7ee14cdd41a659c61c99b779cecf07bc51ab3
91aa3252386242b9853ea7da67fd768d303f1b9b513d401565b6f1eb722dfdb96b519fe4f9bd5d
e67ae131e64b40e78c42dd
Qx = 16335dbe95f8e8254a4e04575d736befb258b8657f773cb7
Qy = 421b13379c59bc9dce38a1099ca79bbd06d647c7f6242336
R = 4141bd5d64ea36c5b0bd21ef28c02da216ed9d04522b1e91
S = 159a6aa852bcc579e821b7bb0994c0861fb08280c38daa09
Result = F

Msg =
16b5f93afd0d02246f662761ed8e0dd9504681ed02a253006eb36736b563097ba39f81c8e1bce7
a16c1339e345efabbc6baa3efb0612948ae51103382a8ee8bc448e3ef71e9f6f7a9676694831d7
f5dd0db5446f179bcb737d4a526367a447bfe2c857521c7f40b6d7d7e01a180d92431fb0bbd29c
04a0c420a57b3ed26ccd8a
```

```
Qx = fd14cdf1607f5efb7b1793037b15bdf4baa6f7c16341ab0b
Qy = 83fa0795cc6c4795b9016dac928fd6bac32f3229a96312c4
R = 8dfdb832951e0167c5d762a473c0416c5c15bc1195667dc1
S = 1720288a2dc13fa1ec78f763f8fe2ff7354a7e6fdde44520
Result = F

Msg =
08a2024b61b79d260e3bb43ef15659aec89e5b560199bc82cf7c65c77d39192e03b9a895d76665
5105edd9188242b91fbde4167f7862d4ddd61e5d4ab55196683d4f13ceb90d87aea6e07eb50a87
4e33086c4a7cb0273a8e1c4408f4b846bceae1ebaac1b2b2ea851a9b09de322efe34cebe601653
efd6ddc876ce8c2f2072fb
Qx = 674f941dc1a1f8b763c9334d726172d527b90ca324db8828
Qy = 65adfa32e8b236cb33a3e84cf59bfb9417ae7e8ede57a7ff
R = 9508b9fdd7daf0d8126f9e2bc5a35e4c6d800b5b804d7796
S = 36f2bf6b21b987c77b53bb801b3435a577e3d493744bfab0
Result = F

Msg =
1843aba74b0789d4ac6b0b8923848023a644a7b70afa23b1191829bbe4397ce15b629bf21a8838
298653ed0c19222b95fa4f7390d1b4c844d96e645537e0aae98afb5c0ac3bd0e4c37f8daaff255
56c64e98c319c52687c904c4de7240a1cc55cd9756b7edaef184e6e23b385726e9ffcba8001b8f
574987c1a3fedaaa83ca6d
Qx = 10ecca1aad7220b56a62008b35170bfd5e35885c4014a19f
Qy = 04eb61984c6c12ade3bc47f3c629ece7aa0a033b9948d686
R = 82bfa4e82c0dfe9274169b86694e76ce993fd83b5c60f325
S = a97685676c59a65dbde002fe9d613431fb183e8006d05633
Result = F

Msg =
5a478f4084ddd1a7fea038aa9732a822106385797d02311aeef4d0264f824f698df7a48cfb6b57
8cf3da416bc0799425bb491be5b5ecc37995b85b03420a98f2c4dc5c31a69a379e9e322fbe706b
bcaf0f77175e05cbb4fa162e0da82010a278461e3e974d137bc746d1880d6eb02aa95216014b37
480d84b87f717bb13f76e1
Qx = 6636653cb5b894ca65c448277b29da3ad101c4c2300f7c04
Qy = fdf1cbb3fc3fd6a4f890b59e554544175fa77dbdbeb656c1
R = eac2ddecddfb79931a9c3d49c08de0645c783a24cb365e1c
S = 3549fee3cfa7e5f93bc47d92d8ba100e881a2a93c22f8d50
Result = F

Msg =
c598774259a058fa65212ac57eaa4f52240e629ef4c310722088292d1d4af6c39b49ce06ba77e4
247b20637174d0bd67c9723feb57b5ead232b47ea452d5d7a089f17c00b8b6767e434a5e16c231
ba0efa718a340bf41d67ea2d295812ff1b9277daacb8bc27b50ea5e6443bcf95ef4e9f5468fe78
485236313d53d1c68f6ba2
Qx = a82bd718d01d354001148cd5f69b9ebf38ff6f21898f8aaa
Qy = e67ceede07fc2ebfafd62462a51e4b6c6b3d5b537b7caf3e
R = 4d292486c620c3de20856e57d3bb72fcde4a73ad26376955
S = a85289591a6081d5728825520e62ff1c64f94235c04c7f95
Result = F

Msg =
ca98ed9db081a07b7557f24ced6c7b9891269a95d2026747add9e9eb80638a961cf9c71a1b9f2c
```

```
29744180bd4c3d3db60f2243c5c0b7cc8a8d40a3f9a7fc910250f2187136ee6413ffc67f1a25e1
c4c204fa9635312252ac0e0481d89b6d53808f0c496ba87631803f6c572c1f61fa049737fdacce
4adff757afed4f05beb658
Qx = 7d3b016b57758b160c4fca73d48df07ae3b6b30225126c2f
Qy = 4af3790d9775742bde46f8da876711be1b65244b2b39e7ec
R = 95f778f5f656511a5ab49a5d69ddd0929563c29cbc3a9e62
S = 75c87fc358c251b4c83d2dd979faad496b539f9f2ee7a289
Result = F

Msg =
31dd9a54c8338bea06b87eca813d555ad1850fac9742ef0bbe40dad400e10288acc9c11ea7dac7
9eb16378ebea9490e09536099f1b993e2653cd50240014c90a9c987f64545abc6a536b9bd2435e
b5e911fdfde2f13be96ea36ad38df4ae9ea387b29cced599af777338af2794820c9cce43b51d21
12380a35802ab7e396c97a
Qx = 9362f28c4ef96453d8a2f849f21e881cd7566887da8beb4a
Qy = e64d26d8d74c48a024ae85d982ee74cd16046f4ee5333905
R = f3923476a296c88287e8de914b0b324ad5a963319a4fe73b
S = f0baeed7624ed00d15244d8ba2aede085517dbdec8ac65f5
Result = P

Msg =
b2b94e4432267c92f9fdb9dc6040c95ffa477652761290d3c7de312283f6450d89cc4aabe74855
4dfb6056b2d8e99c7aeaad9cdddebdee9dbc099839562d9064e68e7bb5f3a6bba0749ca9a53818
1fc785553a4000785d73cc207922f63e8ce1112768cb1de7b673aed83a1e4a74592f1268d8e2a4
e9e63d414b5d442bd0456d
Qx = cc6fc032a846aaac25533eb033522824f94e670fa997ecef
Qy = e25463ef77a029eccda8b294fd63dd694e38d223d30862f1
R = 066b1d07f3a40e679b620eda7f550842a35c18b80c5ebe06
S = a0b0fb201e8f2df65e2c4508ef303bdc90d934016f16b2dc
Result = F

Msg =
4366fcadf10d30d086911de30143da6f579527036937007b337f7282460eae5678b15cccda8531
93ea5fc4bc0a6b9d7a31128f27e1214988592827520b214eed5052f7775b750b0c6b15f145453b
a3fee24a085d65287e10509eb5d5f602c440341376b95c24e5c4727d4b859bfe1483d20538acdd
92c7997fa9c614f0f839d7
Qx = 955c908fe900a996f7e2089bee2f6376830f76a19135e753
Qy = ba0c42a91d3847de4a592a46dc3fdaf45a7cc709b90de520
R = 1f58ad77fc04c782815a1405b0925e72095d906cbf52a668
S = f2e93758b3af75edf784f05a6761c9b9a6043c66b845b599
Result = F

Msg =
543f8af57d750e33aa8565e0cae92bfa7a1ff78833093421c2942cadf9986670a5ff3244c02a82
25e790fbf30ea84c74720abf99cfd10d02d34377c3d3b41269bea763384f372bb786b5846f5893
2defa68023136cd571863b304886e95e52e7877f445b9364b3f06f3c28da12707673fecb4b8071
de06b6e0a3c87da160cef3
Qx = 31f7fa05576d78a949b24812d4383107a9a45bb5fccdd835
Qy = 8dc0eb65994a90f02b5e19bd18b32d61150746c09107e76b
R = be26d59e4e883dde7c286614a767b31e49ad88789d3a78ff
S = 8762ca831c1ce42df77893c9b03119428e7a9b819b619068
Result = F
```

```
Msg =
d2e8454143ce281e609a9d748014dcebb9d0bc53adb02443a6aac2ffe6cb009f387c346ecb0517
91404f79e902ee333ad65e5c8cb38dc0d1d39a8dc90add5023572720e5b94b190d43dd0d787339
7504c0c7aef2727e628eb6a74411f2e400c65670716cb4a815dc91cbbfeb7cfe8c929e93184c93
8af2c078584da045e8f8d1
Qx = 66aa8edbbdb5cf8e28ceb51b5bda891cae2df84819fe25c0
Qy = 0c6bc2f69030a7ce58d4a00e3b3349844784a13b8936f8da
R = a4661e69b1734f4a71b788410a464b71e7ffe42334484f23
S = 738421cf5e049159d69c57a915143e226cac8355e149afe9
Result = F

Msg =
6660717144040f3e2f95a4e25b08a7079c702a8b29babad5a19a87654bc5c5afa261512a11b998
a4fb36b5d8fe8bd942792ff0324b108120de86d63f65855e5461184fc96a0a8ffd2ce6d5dfb023
0cbbdd98f8543e361b3205f5da3d500fdc8bac6db377d75ebef3cb8f4d1ff738071ad093891788
9250b41dd1d98896ca06fb
Qx = bcfacf45139b6f5f690a4c35a5fffa498794136a2353fc77
Qy = 6f4a6c906316a6afc6d98fe1f0399d056f128fe0270b0f22
R = 9db679a3dafe48f7ccad122933acfe9da0970b71c94c21c1
S = 984c2db99827576c0a41a5da41e07d8cc768bc82f18c9da9
Result = F

[K-233]

Msg =
f553c9a1a17d02161faac334dd5f15324c1c033def264d62b28961ae7c5e8694074a5b8ef04780
070aa79379f8565ed3fb5f4e1d08b1275e1e24f7bed6b749e83c1b9ab2dd76110021616ae5db32
340c1f813c5754e549c589ff09990dba4cb939d0705491911cc70ce032c2af7efea6608bb432fa
49195f9d24808848eff8ce
Qx = 0136ed170a3e06af2f542308c818ad113115662a0f24b86e8de8a8577340
Qy = 00cc263193d2844f48c02de4d5f8df5ddee4548703a5222eb2144ffe54e3
R = 0017c34e4c94c9ab1957b3ecd22f97c32eebc608ca337b0b314834726964
S = 006ac64d1221b4d5fb0ea95a5e154a1e64647f15a1a4f8ac6058968e05c6
Result = F

Msg =
490d6c7d320a88286bee74e3ff2536a9c9af1d9c36d5a7554c14a178eb5e908b53825008e7e8fb
b031810d2325fec5aeaa40ce6456101e7079111fa95ef20c67cde89e95d45ce908c8e1800f8668
e04cfeb70cc2f317742efc4d1b9bcfccf931be299f4e82cf19d838f418d1a9cc512bcefc20de94
517139dcb2e075c6531f90
Qx = 010b9887c30189f70fdb353368a46e18ba0cfbce16274bfb456d183af21e
Qy = 01dc2e81158f6221382560a1bea6cdd8d099d0317ec09c9c5beda7942c6f
R = 00077eb49e722729af67db03650808c60e0122f7b7efb8792a7accf4fe54
S = 0026f591818d27aa189fabc1525646fa706f77cacda89f108c810598accb
Result = P

Msg =
ace934c17c190a4cf59bf76a2b89bea316493a3688b5f35c6278efd108bbcb9112020adf4550ac
8cc19202767b3ac24fee2b57a00ed57a0d7ea106da028f08ae371d1697826ce34f469e10be5a82
44bfba737e277c7daa0406c273227f1c59d4830403f01bb3d61cec86c648aea76c7ce0ea59d4ba
f5abc964a4deb165ace489
```

```
Qx = 00e4c747929fccd4042bd3f7ac1d1659a59a888e8d81b670de19b2d9a305
Qy = 00bb27d7c664e68092333580ad94e67170e0e5e678278e9c43b9dbe94774
R = 00584c7b81ea80d78a2574654a3f6a36398c2133fae96f428ee638ad4d65
S = 000b0b36d180506386efb3cd6572cc3afefd751b75db4d1b9096ada948e2
Result = F

Msg =
fd75c460df9a32bf0a837e08eaf81e6a3ecf628479bdfad8686bb97d16cc9915edaffeff1d903f
ce42b462f9417527d372da49be056a009c9e42ca8743666bc2785532efa8e07f82c73b82753655
453ee765edfec1c53dfb46045b507337d7e3e78fe9984831fac4e34166e592408190e399d8aa76
76b9dba7d8f5406de7e460
Qx = 01ccc8d325e42af6aff1a280ebde426050609883926dd18acbf24959d9c1
Qy = 009f314e10ad7c7f20e7061bb58a0a1128c1671ae2fa5f929eb05cfddada
R = 00053ada9d018679f8ff4352077e63baade5ca2c506450205cdbcbe37b93
S = 0024df72910c75b3b5d6fd618326708277660ae53489fdef984f01f2b720
Result = F

Msg =
54f9ebe43a658c8cdceee7e2edcc5e8b04866ce99516385520486aa9a8633d02670bd5c4c066d4
de757e284f1ae626e9caa1dd54183fa4574849f653c0df8010b9a077bc3aca2f3147a2ea775617
ee8a02a2da5d0370391e5ec358bcd99655a7b28079d790dac70fba24d56387a5dbf817520a0b3e
f11f34c87e37ecdccee54e
Qx = 0169b6839488a2230eb8a55d4aee2cfdecde006beb1173428f6079fb5b2d
Qy = 00241ca64fc4d97b37c4721d28eddb25d8d187570f0c8e2bc9f2111d1255
R = 00369daf397bd022654b1b5b0b0de937e9aa9c830165415b6329b0bfb090
S = 001f591f44be300354755a0fb466e5b248597f7a5a9cb69f4d508415da8f
Result = F

Msg =
dcd8bdb15a84862ca5ae26302d95320cd71c4ee7fec24d54b8d49a275ae2d6863e6fc243c3ec60
6996e8551430819286a01e33788b60a7ae715512ce31efef72d0b5fa7c76b94daab9cac96a1eea
b7efdd03af84e5d5b9202033b33bf86ff3e11a132d057ad1961797bd49d900baea6e17328ab315
0bcbd34ed64516b74928fa
Qx = 007345bf47179e1533eb451d0174e1c04f8bd34c202478f950ee54f736f8
Qy = 01706e0da88763ff81d6e1e853ce5f7484635a7f6d08b8d9730b389c8d0b
R = 002e1d25e5b4f7549fc39bfc9244c01843cd30ba3e7cec33c56bddc67a66
S = 00486550d28f3b79d135baadf8795c8d21951d76b88cd9110bca0d125133
Result = F

Msg =
c5f62b24a16226b4a66a01893da87fa175bc523f9a91464909e2bdee42fc5b8b3fc502d005fd01
1f78c48834735c600b1831d8fe6516032f08d2202575db5aba3561b234818e39b20f0d82ca2cc9
57700bf7ab195d56d02121b5ea6abeb7a4474fd321983e9e3636144dd6918f75cd97f616b1d8a9
d816e8fc9402054516a1fa
Qx = 01b6dec64e5e1fd13ccd98ba680763c47583e95cec2d0dbf309bf69fe51b
Qy = 011221e50fc93677bbcb6e40b24f2de6eeed9bc26ba826e80e02f7eb5574
R = 00475802cf260aa2b4b14262eacfea1ce1e45f406d8ae411bbf187e062ba
S = 00293f771aa308ef1716ffa5fddfde490724016c6a570c7b1b807740421b
Result = F

Msg =
1ab37b5c3e7accb783e80d93538e1ca59d6f7eb1270651aa268b811b0c733fc5a136af895554e1
```

```
89d49a038bdca1d59e4b995dff7d44db3dd445ff9c989b5ab70269136a93f8dbefaafe22475621
8bdc69b79e64cfd0be081c765ac66a33671466d40dc6a16da0312d9dd3916a1328a81d51aba8c2
b0e05324a5fa612a424d22
Qx = 00c57832cad1eef31b0545f0c48718106d27d6492addd718d6425c7fa056
Qy = 0026e7491ef66649a3f0d4bbc8d7fb4e1db86a3c2288658edf74a64fee43
R = 004009378a80c311db1a3ab914953d7dec0ba06568a6bd533b2537e55f5e
S = 0059cf2d301cd86e94d0d1bf0d3f21fe3b2aea683d2354c8781c440f23b1
Result = F

Msg =
5a56096c7e86e5d4988347e117552975e687f720e3cf9fe893f1e84514e00470532668dd7f87db
06bde1cd6b1d57ebd7ccaef0e48cf7bec1626fad338ea323dac0d865b689a9acea10f27cbf06ed
31ebdc9bdb1433664b9094046e6f619edabb0b32a7fe86368005fa7ef9e4bc5f233a7c155fb6c0
626fda9178d3ff7319529a
Qx = 01e31fa7780137bb4a2ab01d354fd773901b9ef976a5b564a2a09dc9df8b
Qy = 0191cf897a2347a43e781e2c41d5bd50efcc705267fed96f52eabdf42027
R = 006729210e1d49542bde1e3ee0609368dac81bfeb51ce99fdd306ca9ac16
S = 002ea969db3ff2a494730cb2de1d177a6c5b3ca7a42b0f7bf6d1ab44ed8d
Result = P

Msg =
2a5325bd0277f9c49be359fd2bbe5e63d1832de0e102e16d7da8c67a6501c8900f7b2b35fb6d7c
104157c74d6c6c0a438a4dea548418a515aca148af95ff2286274b7818f2a47a27c376761a75fc
4ca10a042298fbf3582ecb08be46e2e5051d994b742d9225dc524ac8ce2cf1790bc4792f3c72ed
9be4fe04669205f6ba5b9e
Qx = 00c6b220969d54cadf544316cffa60fd5a1595ac420f61fc5873ad78bb56
Qy = 0196b017ed347446c64d6ae8613e75f822938194a84952e364d67d2e0036
R = 000a4c1bd92de8907c3cd3930249b06d8556093ef7378bdb520d56791afd
S = 007f7b94affd65269dbcc29883064b69ccce7127ab23dd404eab59029787
Result = F

Msg =
cd25a7f53bc44ac3eab1d4771883891358d2b77a86534ac000449aa4130b875bb41ac890711580
a8a737124af4f2371fefd54ed617b3f36c0a02d2aaf881bdef561efd2fd716e63c985eaf449a42
809b764ccbbb4c67e08afd44bcdb9afd22361cf8eedc550fa50626ed506ef3bb8b1054fdd9320d
b63aa241d3003fe2c6deba
Qx = 0078cd54849617d64c1bf3ee0c01639d4912411912513612512c0237bf43
Qy = 018a850cae6cb9b81fb4173847b4f29fb40b47a9bdfc119d2eb6fcc4146d
R = 0026170cca4ec53585b9ddc149f1811133815b8aa2f68f2d80e06746a6f4
S = 00100984fcbe5bc6a0d91473b40589433851aa725c3f4ffa744f340eefb2
Result = F

Msg =
c292e847f4bf5a482ca63544d31ec7df4f05460726d415266776439c465b556c06c845351c71ca
659149daa9a8996da8c14f85f07d996b3023b33ba942fea2df9851e794339328f6d68ae7189eee
c59fe5c28cbe67e47364a3e29eb3850fe5b541d6d64a824ffd65c4106378fe46542d850465572d
dab628b1aa75a455b7a355
Qx = 0073108e1827566a63d94ef922f94b2835c91d53ac62371df25217989f2e
Qy = 00c0ce149e33218fc95a299c64dbccf80aa4062ca488e74340d9d0a40b83
R = 00561b14067d3fcf8d868ac17211d6a8747b6089638338810f7336aa988d
S = 0047e987aed01b51f888fbf4b2dc34a367b644cee4271f426314d63eed98
Result = F
```

```
Msg =
0cb9c695b7585006751e32fa0761c185fefabf73c23f7cded931400066f6ed45f089e1a465b01a
305f2e9deaa53a18daf531c65e018893c1b704810fc52d4a285d00471435e49096d3df6504070a
cc55b9427c7ce421faf5e32c029dec4e28c6da86bf8b2fdcfa61599951ef34b72620d197a97676
f2f9a1e5128c50e142d047
Qx = 010c42d7b7557e2ba495373dff3cade13fbb56614f15b47fca217ca7d57e
Qy = 017abd698cc8dec5aae48ca111b533829d487a7ee333b24e74da4a50b889
R = 0f3e30cfcf4d3ba084dfaa43b625d5fb4f406336501b1fd43f9f82d2
S = 0060553f1b1d9d2ad62f74ba7a906204dee6c6f059b50fe7317141f3d443
Result = P

Msg =
8159c84852c6229694bd484661ffc349342c8a504e91803c59413fd64c6714c18eda4aad5ef2ac
cc729b458adea76a793869fb8afa7fe58327efebad3276a7cd1b1ccb56db0caddd02a303cd9fc7
ea5c607a2ebefaaec598cb5b9cb7bed097027047d3ad91bb2eb08cfe09786a064cdcf387ab5217
c828638dafd95cba1dec47
Qx = 007ee60584691638fd6fe17a3b4ce3ebce1747ec6c44ba6ea8d235b130c1
Qy = 00881c53ec4e23e591764b5cb4047701c6e8035e37f77cbf83d0d7257d98
R = 000e690c9f1180e538bb790906e037cca39d07799032841370c74ea30b78
S = 006e1e028bd9d204b9d97bd9846429edaad8da32aeec6f3bb7e99f32ee8f
Result = F

Msg =
39cd57963378c638c3b2a442f65d15d8b9c605c5f9356db208c2d19c436b0e85f26452696fae6c
738beb46712d71af863c9d5e1ebf6934274341c27f7d130ba831a68bc3532c78bc6b1a47c23e37
72faaaf37974d2fb275e7b0a1677b60275c7c03b098e261b727a2ce7b01c70d8e59dcb725cad78
11cbbd78c5d56e345fd34a
Qx = 004bc66f1524162fc952a41240b627e244be6d1823a0736be63adf559727
Qy = 011b167b34fc9be9589e7d8c1fe3dd033d6145a0f1794f911272dea141dc
R = 000d4dbfcb1069e09657f3d9614f3e6bdb0f812b281f0887c85b5e57c376
S = 0028055fdaaa8090d97568a23eee931d576fe6eae5aed9e11cf151f3a77f
Result = F
```

B.4 Examples of *SAMPLE* Files

B.4.1 KeyPair.sam

```
#  CAVS 3.0
#  "Key Pair" information for "ECDSA_Test"
#  Curves selected: P-192 K-233

[P-192]

d = ?
Qx = ?
Qy = ?

d = ?
Qx = ?
Qy = ?
```

d = ?
Qx = ?
Qy = ?

d = ?
Qx = ?
Qy = ?

d = ?
Qx = ?
Qy = ?

d = ?
Qx = ?
Qy = ?

d = ?
Qx = ?
Qy = ?

d = ?
Qx = ?
Qy = ?

d = ?
Qx = ?
Qy = ?

d = ?
Qx = ?
Qy = ?

[K-233]

d = ?
Qx = ?
Qy = ?

d = ?
Qx = ?
Qy = ?

d = ?
Qx = ?
Qy = ?

d = ?
Qx = ?
Qy = ?

```
d = ?
Qx = ?
Qy = ?

d = ?
Qx = ?
Qy = ?

d = ?
Qx = ?
Qy = ?

d = ?
Qx = ?
Qy = ?

d = ?
Qx = ?
Qy = ?

d = ?
Qx = ?
Qy = ?
```

B.4.2 PKV.sam

```
#  CAVS 3.0
#  "PKV" information for "ECDSA_Test"
#  Curves selected: P-192 K-233

[P-192]

Qx = cd6d0f029a023e9aaca429615b8f577abee685d8257cc83a
Qy = 00019c410987680e9fb6c0b6ecc01d9a2647c8bae27721bacdfc
Result = ?

Qx = 00017f2fce203639e9eaf9fb50b81fc32776b30e3b02af16c73b
Qy = 95da95c5e72dd48e229d4748d4eee658a9a54111b23b2adb
Result = ?

Qx = 4f77f8bc7fccbadd5760f4938746d5f253ee2168c1cf2792
Qy = 000147156ff824d131629739817edb197717c41aab5c2a70f0f6
Result = ?

Qx = c58d61f88d905293bcd4cd0080bcb1b7f811f2ffa41979f6
Qy = 8804dc7a7c4c7f8b5d437f5156f3312ca7d6de8a0e11867f
Result = ?

Qx = cdf56c1aa3d8afc53c521adf3ffb96734a6a630a4a5b5a70
Qy = 97c1c44a5fb229007b5ec5d25f7413d170068ffd023caa4e
Result = ?
```

```
Qx = 89009c0dc361c81e99280c8e91df578df88cdf4b0cdedced
Qy = 27be44a529b7513e727251f128b34262a0fd4d8ec82377b9
Result = ?

Qx = 6a223d00bd22c52833409a163e057e5b5da1def2a197dd15
Qy = 7b482604199367f1f303f9ef627f922f97023e90eae08abf
Result = ?

Qx = 6dccbde75c0948c98dab32ea0bc59fe125cf0fb1a3798eda
Qy = 0001171a3e0fa60cf3096f4e116b556198de430e1fbd330c8835
Result = ?

Qx = d266b39e1f491fc4acbbbc7d098430931cfa66d55015af12
Qy = 193782eb909e391a3148b7764e6b234aa94e48d30a16dbb2
Result = ?

Qx = 9d6ddbcd439baa0c6b80a654091680e462a7d1d3f1ffeb43
Qy = 6ad8efc4d133ccf167c44eb4691c80abffb9f82b932b8caa
Result = ?

Qx = 146479d944e6bda87e5b35818aa666a4c998a71f4e95edbc
Qy = a86d6fe62bc8fbd88139693f842635f687f132255858e7f6
Result = ?

Qx = e594d4a598046f3598243f50fd2c7bd7d380edb055802253
Qy = 509014c0c4d6b536e3ca750ec09066af39b4c8616a53a923
Result = ?

[K-233]

Qx = 00534537f7762394d8ff46675d194aa212c4f9a2b5705f68df74e4e35d59
Qy = 01b4bb8fa0cd97777f60f4d7e4038cd65527eff4570b09204fdbedabc7d2
Result = ?

Qx = 0148dec1cffafce7ce21ae80652935bbb8b960bb1c4f27830d7ac0a786a5
Qy = 00c845acaaccc4549b8e2323a7f7ec17e0c8ae7a574c8e6a1ce337939c7b
Result = ?

Qx = 013ca0f0875f8fea41a1f44aa7603a85324507c7177b616627459feabd3b
Qy = 0061fc08300b6cf0c99c5f923ccc65f9be1fd9449b0625ed6a7f767e6a4d
Result = ?

Qx = 0079a6cbfe3a2e9e9eaef2b119787682ad51b7e1003e0bd952417f651d65
Qy = 00990e7736bed24326c49a683587e72b24d8e5b62c037495a99f21438bac
Result = ?

Qx = 00faa4e23af6d38eff68c8de405891a8e5eba2487bb854c8cc1d5a9d9fbc
Qy = 005c6cb3b3e608eda31bece7c755109d840b41550f09448db4122967bcae
Result = ?

Qx = 01883d8c99b33f5732a4fc226ec695d1664a30b6cd1e7e302da60d09ebdf
```

```
Qy = 011424b3e264102e4ac2c837925c03790c5f1053e2b9fbf77269d856e7dd
Result = ?

Qx = 00aa7822d4d5e939c4c9ab0b0a7a24c395a31f5ef138601d957fd48915d3
Qy = 00fcba0cb2522203754655e4a95be36b5c3227f9cf3aa6e9eee73acabc66
Result = ?

Qx = 01b84c30e07e761416b9a9a548c1f9c0e64ea3577277d3a3cfaac7b22303
Qy = 0117c9df876b0c309f02499075a98184ebd66e62abf8c60144db4bdc438b
Result = ?

Qx = 011cae8c5ee0ece8496471f45b6307edf97583ba70b793da4d76cc6db05f
Qy = 008690e754c7c74ea1f94c4616e653f7223387f14a0119407f255fc955ce
Result = ?

Qx = 01dc2d0dc408cd363f81e448fc46c9622b4f0ccc03ec277fe64af2be43c8
Qy = 00b5cdae6799fc82e9fdcb81798dc61ea0ecbc01a771908186f741103826
Result = ?

Qx = 00539b5e0779ac3631c28177558000a543882dda3c9fdf8a27df24bfeb05
Qy = 017a62d298132856e8a283787083131cf7ff93c3ff1d592d783760b438fe
Result = ?

Qx = 01e147f3a7653416b87a70c08dccf34e49dd1a630ba88d591c74e827ae72
Qy = 01a32a428f0f3b7786317753aba84f68ab0ea0b760a298f1a2286cc605b6
Result = ?
```

B.4.3 SigGen.sam

```
#  CAVS 3.0
#  "SigGen" information for "ECDSA_Test"
#  Curves selected: P-192 K-233

[P-192]

Msg =
c70e287f3bb37422fcb2f277cb178a98eb6ab8e2d68ddef930e7df0cf9c3e95b06f292f6b2b827
c7d1e640d2e54398bc95301c8a5a8c42ac7cd69c3a3d91ad7d53edfbb19ca365090e21b7f4ede7
7c9f403114bb85d60680a47097f222bd9b6397458b39623dd8f19bac7f6449ccde49d5b3c5fcbf
32d17e90fef5bc100d5a14
Qx = ?
Qy = ?
R = ?
S = ?

Msg =
1a3cc54a8ad392749b2c1b59aa07b451bd1ebd8a5cac19a9a22ce2b493635a2fb0a02585c943b6
aa137c08ff7a558e7638f36cf6a718e70153ed1a9454ffeb4edb873ed50aee69760990e70b56c1
50225c0d885b48c4371218b77a3ef43cd999c2787802f5dd911fa5f12146e551e29e51f67a81e6
b8f2251710697c1c220a58
Qx = ?
```

```
Qy = ?
R = ?
S = ?

Msg =
5673828f6db66331f21f7e21a6bcb77db852d4c738fe90a0ce18ead2ac5cc394c14ca80a2fd0ed
0c0020fb2814e3eaea5e99535a51365fc7940f24c3fdfa326fbdb168f9d8780d62d9001c85c38a
de554a4fbe6643205aaf5a4ad68e03bc750cb36c6a634ff6ebbde586883f9af9bb46e33fc0f0f8
04a6df868fa739a4eab5f3
Qx = ?
Qy = ?
R = ?
S = ?

Msg =
ba8636a1e1cc77e34750061f11b5cd2b0da1a703961467beb9f81bc096f9923008961bad887890
3c4e039385ba2c1840f38a24eaceafd3bcf1b8a0dd3823e1d757e19148c1ac52dac99bb27407f4
aeb2fe417593fba66e7240717b3862f380cff08f1fda5510c6a3003fec54c2b6976b77ef2268e8
a03dc8f04b3537de107602
Qx = ?
Qy = ?
R = ?
S = ?

Msg =
6d3a19d8f63c7bb983468757a142cd14fcbef605229ca8498a0baa99d5b64921533bfa8ec9de40
69727fd0a343c9f47173ad2d5a3b0e1c8ddbbea279ddaa47989d51d88b097b546ca6270a60d4c5
fb6b52a5858904b043faf4562fdd98c709005366fdf73d7a806b27277bb5da9eababa09047ba06
e8e436dfb997ed8c755902
Qx = ?
Qy = ?
R = ?
S = ?

Msg =
35883c4a11985c37a1244af70260b885124411b0323d5b714a22627c0e691315809b2625b60500
8ddeb1d7ba7f9417790209040d707ea1807d6dd136c68fbdc8574c750f7075da7e8935bbb59345
3e548160820d07f782fea1253d3dd8e514b4c183732fc650b3b3a89a3f12c5dbf6bc9731d1d87e
0ec693bf31ecb8ccd5df82
Qx = ?
Qy = ?
R = ?
S = ?

Msg =
05d77ea4977ac96b8813fc1210483a037e7b6c502ceed8f7b22bf6655aa37e38d495c6492b314b
eaf8fe8d6cd67921e515ff012fb3ec263487055969c01346998ed1d2e41f08ae07cdf92cde96fb
5227cc652e880dae68d476d31e8a14f9eb9e9b54497c5b471a4b6fcd816e3817f6510a779a6224
7cc75de65feccd3e9d98d0
Qx = ?
Qy = ?
R = ?
```

```
S = ?

Msg =
c96009b6e816ef26695ef6bafcf76dcba3b0793fc12cc46574e2742025675a485ef06c4ddb1376
1de3cd0c48d9c9c3620edfa1aad9dcd1e8ea819b9cdbce94540880125ea1d8e39ffd9e3fc33166
fa97e212feb25798f95bd20553a721c263e27016e23061eda0745fd875712f547b30c74f7aa164
e8a484d777838a1fcd2fb8
Qx = ?
Qy = ?
R = ?
S = ?

Msg =
1ef4e272a78eb74d4a46ecdd514fb4172a6f93030e0d1e70e08c02e658d747dc603dd62bbe8039
c3f428a39c641d30f0b8756da8818b1b141e5130dee0e71f416c6c59766014146f397a4bc87438
06fbf3b6dbd3a33fb5235c5ad4b70857158b0828743bd372cfbbe0e4ed48c7c8be9ea3d7e46cba
527305604ef5581850b222
Qx = ?
Qy = ?
R = ?
S = ?

Msg =
942c6a4eba5e2760e8e7972f6208c91b5351dc5a6eb6c2a5d6e544313bd746e146a54dba389e3e
97ce96691e6780c5f268407d2ae0baac03682f65d14ec9f73cf2746fa86ff05ef57e24dc6998b6
ccea5bd862712f65e3bb292cac42308c766b5e41d801a87d0de2c23af8f83dcf656bf3c29215a4
deee37e185206a29474bd8
Qx = ?
Qy = ?
R = ?
S = ?

[K-233]

Msg =
baf9377601faf15c5a1288381efe55547d022599d1e330af2c354b6633dd5e5530ce17c16216e0
c0981e0f9dfe2d5d7f362f9a46aab59fb6213c83d791b2129b34367ac2de2048fb8e41934c436c
77b31134c60e73f8f938e31d6d75a89bcc10f0bbc8421e1f105665027c0b96c18b3a369a10b8d4
b4287e99606f07219f74fa
Qx = ?
Qy = ?
R = ?
S = ?

Msg =
34ab1130ce389d340fca232cc50b7536e62ad617742e022ea38a6fa63ef1d3ef476be66edea969
736395676cdf2ebb59a093d280245db26239323bed6198adf37b066bdba041ff974ce65dd6be42
6c7aa16ac24ceb88afee06747e122e84f7ea1aa429dfdea9668610e28ed029f091812fd82fe391
5702bb5376bf7c6a5db9bb
Qx = ?
Qy = ?
R = ?
```

```
S = ?

Msg =
693e50d3d13811c9897f260c809e0111e4566d52da89d74f7257ecd2da866a78d2272f6d5f7697
77c4030436ae0fbeaaaf39fef5ed5a45621cadf2a7a933146738557dfb51cc187256be7cd6b929
c0b16b8591d098a5834791dfa5b60a6c58ca851161060eff3cc329f9b37509b4b0310283506c41
343806bb342c8763fadea8
Qx = ?
Qy = ?
R = ?
S = ?

Msg =
a482cd28915c950f609b1324b71b42c681ed832540578f62a41bb0f25cfc31442c7f12a340ef01
5dc0a38625a4847eb6cac9cab9450548e9f96402756531a6a5bf9c37c146bb012fd4ced2dbb2c7
67dcb10a255476710a971693e290e346be618562a24a4cc87eccc4a35f0e8aeee77f5f37fbbd7b
a2bbb62330b70d7e415fbf
Qx = ?
Qy = ?
R = ?
S = ?

Msg =
292ea1755f9e587822372f4dcdf10bddfc0ff498a8af60ae94a0b482e873085c1cd52a5d181ce6
b99a1f8520d74b947d65f3e7e358e8ddc4ac4ae465e39d408eee1f09865159733f83f553cd93cf
de1c114fb3e32cf51cd418359016b3867df467b645d752808671a4609f3c49a67023c9ca617e6c
ffa544a10ac07ca05546f5
Qx = ?
Qy = ?
R = ?
S = ?

Msg =
60440c8df2b67e1fc1f7f354a1188ae14497175bb8d6c64b31cc018409fb93b405a20d3ada3368
37f007ede8655152335551267f59ca6fc94db591f45737716124d1dbc075d72126db23055fbe0a
d985a48fe5d1b0d709b269dda41cbe67b42346393ec8cc88f0130ab10562b52b6900baba1df9c8
e6de2d0eac01a44673a221
Qx = ?
Qy = ?
R = ?
S = ?

Msg =
d6344015544f6b63423cbb689274d70331832fb33966d51267378fa0cf0c2ac2ce1c110b41231e
b9f408af835ebdfd928b68a9cd59c09859e7b901604b63c412830ffeeaaeb5da337d92aacae415
362515fc5394aebbb8c7311d0e91b62d46ebdc572f3c05cb48d8c322d3c68d442ac6b7895692a1
1ede652eabddba77325756
Qx = ?
Qy = ?
R = ?
S = ?
```

```
Msg =
5c3fb5a4d2871bfa77e171056ff0a48eafe0fd4a653ea353940d62d9ff16aa15497fdb7f5a9fbf
41051158ebe707dd6892e1ff31ebff70c0d0d3a648fe3adda3320c5b8c8ff1f70e4077dc3c5e62
8b2314441ffd014dd5a8dd63cb56607508855f0dbd323925ca49713c84619ca9b6a67e2ee61670
d0d9f104e6596aec7135a3
Qx = ?
Qy = ?
R = ?
S = ?

Msg =
83c0f878b2428ab84cabecfc862d199e61933d6f7fca235635a1f13ae3cd13228030759b795bf5
5bbc5118230f8dfbeaa7478d37f6f4fccfc40c6d90810ff09ddacab3bb8ad776fb73633e9aed33
4e255ee953e00b84df692d271899481bb2abb8161aa08cbef4e19869c827c627f898ad02f63365
84b36d997a5b1cddf83f95
Qx = ?
Qy = ?
R = ?
S = ?

Msg =
39e3a58a0ce472f694294f9743a86db2d87894b98d35ffcd92a66d81bb9d75e1761f1ab3ffc59f
fcd7629dc672e652212f833c688e0ee6c59ea703f7b49cb953628b3f09a7c7aaa964fd04e60f18
9f99ab61a809f8ebff69e72e46a250f23953e76f3d166db23b062342ae7e8404fb23335c022433
95f2c056836109f8669ce8
Qx = ?
Qy = ?
R = ?
S = ?
```

B.4.4 SigVer.sam

```
#  CAVS 3.0
#  "SigVer" information for "ECDSA_Test"
#  Curves selected: P-192 K-233

[P-192]

Msg =
84ce72aa8699df436059f052ac51b6398d2511e49631bcb7e71f89c499b9ee425dfbc13a5f6d40
8471b054f2655617cbbaf7937b7c80cd8865cf02c8487d30d2b0fbd8b2c4e102e16d828374bbc4
7b93852f212d5043c3ea720f086178ff798cc4f63f787b9c2e419efa033e7644ea7936f54462dc
21a6c4580725f7f0e7d158
Qx = d9dbfb332aa8e5ff091e8ce535857c37c73f6250ffb2e7ac
Qy = 282102e364feded3ad15ddf968f88d8321aa268dd483ebc4
R = 64dca58a20787c488d11d6dd96313f1b766f2d8efe122916
S = 1ecba28141e84ab4ecad92f56720e2cc83eb3d22dec72479
Result = ?

Msg =
94bb5bacd5f8ea765810024db87f4224ad71362a3c28284b2b9f39fab86db12e8beb94aae89976
```

```
8229be8fdb6c4f12f28912bb604703a79ccff769c1607f5a91450f30ba0460d359d9126cbd6296
be6d9c4bb96c0ee74cbb44197c207f6db326ab6f5a659113a9034e54be7b041ced9dcf6458d7fb
9cbfb2744d999f7dfd63f4
Qx = 3e53ef8d3112af3285c0e74842090712cd324832d4277ae7
Qy = cc75f8952d30aec2cbb719fc6aa9934590b5d0ff5a83adb7
R = 8285261607283ba18f335026130bab31840dcfd9c3e555af
S = 356d89e1b04541afc9704a45e9c535ce4a50929e33d7e06c
Result = ?

Msg =
f6227a8eeb34afed1621dcc89a91d72ea212cb2f476839d9b4243c66877911b37b4ad6f4448792
a7bbba76c63bdd63414b6facab7dc71c3396a73bd7ee14cdd41a659c61c99b779cecf07bc51ab3
91aa3252386242b9853ea7da67fd768d303f1b9b513d401565b6f1eb722dfdb96b519fe4f9bd5d
e67ae131e64b40e78c42dd
Qx = 16335dbe95f8e8254a4e04575d736befb258b8657f773cb7
Qy = 421b13379c59bc9dce38a1099ca79bbd06d647c7f6242336
R = 4141bd5d64ea36c5b0bd21ef28c02da216ed9d04522b1e91
S = 159a6aa852bcc579e821b7bb0994c0861fb08280c38daa09
Result = ?

Msg =
16b5f93afd0d02246f662761ed8e0dd9504681ed02a253006eb36736b563097ba39f81c8e1bce7
a16c1339e345efabbc6baa3efb0612948ae51103382a8ee8bc448e3ef71e9f6f7a9676694831d7
f5dd0db5446f179bcb737d4a526367a447bfe2c857521c7f40b6d7d7e01a180d92431fb0bbd29c
04a0c420a57b3ed26ccd8a
Qx = fd14cdf1607f5efb7b1793037b15bdf4baa6f7c16341ab0b
Qy = 83fa0795cc6c4795b9016dac928fd6bac32f3229a96312c4
R = 8dfdb832951e0167c5d762a473c0416c5c15bc1195667dc1
S = 1720288a2dc13fa1ec78f763f8fe2ff7354a7e6fdde44520
Result = ?

Msg =
08a2024b61b79d260e3bb43ef15659aec89e5b560199bc82cf7c65c77d39192e03b9a895d76665
5105edd9188242b91fbde4167f7862d4ddd61e5d4ab55196683d4f13ceb90d87aea6e07eb50a87
4e33086c4a7cb0273a8e1c4408f4b846bceae1ebaac1b2b2ea851a9b09de322efe34cebe601653
efd6ddc876ce8c2f2072fb
Qx = 674f941dc1a1f8b763c9334d726172d527b90ca324db8828
Qy = 65adfa32e8b236cb33a3e84cf59bfb9417ae7e8ede57a7ff
R = 9508b9fdd7daf0d8126f9e2bc5a35e4c6d800b5b804d7796
S = 36f2bf6b21b987c77b53bb801b3435a577e3d493744bfab0
Result = ?

Msg =
1843aba74b0789d4ac6b0b8923848023a644a7b70afa23b1191829bbe4397ce15b629bf21a8838
298653ed0c19222b95fa4f7390d1b4c844d96e645537e0aae98afb5c0ac3bd0e4c37f8daaff255
56c64e98c319c52687c904c4de7240a1cc55cd9756b7edaef184e6e23b385726e9ffcba8001b8f
574987c1a3fedaaa83ca6d
Qx = 10ecca1aad7220b56a62008b35170bfd5e35885c4014a19f
Qy = 04eb61984c6c12ade3bc47f3c629ece7aa0a033b9948d686
R = 82bfa4e82c0dfe9274169b86694e76ce993fd83b5c60f325
S = a97685676c59a65dbde002fe9d613431fb183e8006d05633
Result = ?
```

```
Msg =
5a478f4084ddd1a7fea038aa9732a822106385797d02311aeef4d0264f824f698df7a48cfb6b57
8cf3da416bc0799425bb491be5b5ecc37995b85b03420a98f2c4dc5c31a69a379e9e322fbe706b
bcaf0f77175e05cbb4fa162e0da82010a278461e3e974d137bc746d1880d6eb02aa95216014b37
480d84b87f717bb13f76e1
Qx = 6636653cb5b894ca65c448277b29da3ad101c4c2300f7c04
Qy = fdf1cbb3fc3fd6a4f890b59e554544175fa77dbdbeb656c1
R = eac2ddecddfb79931a9c3d49c08de0645c783a24cb365e1c
S = 3549fee3cfa7e5f93bc47d92d8ba100e881a2a93c22f8d50
Result = ?

Msg =
c598774259a058fa65212ac57eaa4f52240e629ef4c310722088292d1d4af6c39b49ce06ba77e4
247b20637174d0bd67c9723feb57b5ead232b47ea452d5d7a089f17c00b8b6767e434a5e16c231
ba0efa718a340bf41d67ea2d295812ff1b9277daacb8bc27b50ea5e6443bcf95ef4e9f5468fe78
485236313d53d1c68f6ba2
Qx = a82bd718d01d354001148cd5f69b9ebf38ff6f21898f8aaa
Qy = e67ceede07fc2ebfafd62462a51e4b6c6b3d5b537b7caf3e
R = 4d292486c620c3de20856e57d3bb72fcde4a73ad26376955
S = a85289591a6081d5728825520e62ff1c64f94235c04c7f95
Result = ?

Msg =
ca98ed9db081a07b7557f24ced6c7b9891269a95d2026747add9e9eb80638a961cf9c71a1b9f2c
29744180bd4c3d3db60f2243c5c0b7cc8a8d40a3f9a7fc910250f2187136ee6413ffc67f1a25e1
c4c204fa9635312252ac0e0481d89b6d53808f0c496ba87631803f6c572c1f61fa049737fdacce
4adff757afed4f05beb658
Qx = 7d3b016b57758b160c4fca73d48df07ae3b6b30225126c2f
Qy = 4af3790d9775742bde46f8da876711be1b65244b2b39e7ec
R = 95f778f5f656511a5ab49a5d69ddd0929563c29cbc3a9e62
S = 75c87fc358c251b4c83d2dd979faad496b539f9f2ee7a289
Result = ?

Msg =
31dd9a54c8338bea06b87eca813d555ad1850fac9742ef0bbe40dad400e10288acc9c11ea7dac7
9eb16378ebea9490e09536099f1b993e2653cd50240014c90a9c987f64545abc6a536b9bd2435e
b5e911fdfde2f13be96ea36ad38df4ae9ea387b29cced599af777338af2794820c9cce43b51d21
12380a35802ab7e396c97a
Qx = 9362f28c4ef96453d8a2f849f21e881cd7566887da8beb4a
Qy = e64d26d8d74c48a024ae85d982ee74cd16046f4ee5333905
R = f3923476a296c88287e8de914b0b324ad5a963319a4fe73b
S = f0baeed7624ed00d15244d8ba2aede085517dbdec8ac65f5
Result = ?

Msg =
b2b94e4432267c92f9fdb9dc6040c95ffa477652761290d3c7de312283f6450d89cc4aabe74855
4dfb6056b2d8e99c7aeaad9cdddebdee9dbc099839562d9064e68e7bb5f3a6bba0749ca9a53818
1fc785553a4000785d73cc207922f63e8ce1112768cb1de7b673aed83a1e4a74592f1268d8e2a4
e9e63d414b5d442bd0456d
Qx = cc6fc032a846aaac25533eb033522824f94e670fa997ecef
Qy = e25463ef77a029eccda8b294fd63dd694e38d223d30862f1
```

```
R = 066b1d07f3a40e679b620eda7f550842a35c18b80c5ebe06
S = a0b0fb201e8f2df65e2c4508ef303bdc90d934016f16b2dc
Result = ?

Msg =
4366fcadf10d30d086911de30143da6f579527036937007b337f7282460eae5678b15cccda8531
93ea5fc4bc0a6b9d7a31128f27e1214988592827520b214eed5052f7775b750b0c6b15f145453b
a3fee24a085d65287e10509eb5d5f602c440341376b95c24e5c4727d4b859bfe1483d20538acdd
92c7997fa9c614f0f839d7
Qx = 955c908fe900a996f7e2089bee2f6376830f76a19135e753
Qy = ba0c42a91d3847de4a592a46dc3fdaf45a7cc709b90de520
R = 1f58ad77fc04c782815a1405b0925e72095d906cbf52a668
S = f2e93758b3af75edf784f05a6761c9b9a6043c66b845b599
Result = ?

Msg =
543f8af57d750e33aa8565e0cae92bfa7a1ff78833093421c2942cadf9986670a5ff3244c02a82
25e790fbf30ea84c74720abf99cfd10d02d34377c3d3b41269bea763384f372bb786b5846f5893
2defa68023136cd571863b304886e95e52e7877f445b9364b3f06f3c28da12707673fecb4b8071
de06b6e0a3c87da160cef3
Qx = 31f7fa05576d78a949b24812d4383107a9a45bb5fccdd835
Qy = 8dc0eb65994a90f02b5e19bd18b32d61150746c09107e76b
R = be26d59e4e883dde7c286614a767b31e49ad88789d3a78ff
S = 8762ca831c1ce42df77893c9b03119428e7a9b819b619068
Result = ?

Msg =
d2e8454143ce281e609a9d748014dcebb9d0bc53adb02443a6aac2ffe6cb009f387c346ecb0517
91404f79e902ee333ad65e5c8cb38dc0d1d39a8dc90add5023572720e5b94b190d43dd0d787339
7504c0c7aef2727e628eb6a74411f2e400c65670716cb4a815dc91cbbfeb7cfe8c929e93184c93
8af2c078584da045e8f8d1
Qx = 66aa8edbbdb5cf8e28ceb51b5bda891cae2df84819fe25c0
Qy = 0c6bc2f69030a7ce58d4a00e3b3349844784a13b8936f8da
R = a4661e69b1734f4a71b788410a464b71e7ffe42334484f23
S = 738421cf5e049159d69c57a915143e226cac8355e149afe9
Result = ?

Msg =
6660717144040f3e2f95a4e25b08a7079c702a8b29babad5a19a87654bc5c5afa261512a11b998
a4fb36b5d8fe8bd942792ff0324b108120de86d63f65855e5461184fc96a0a8ffd2ce6d5dfb023
0cbbdd98f8543e361b3205f5da3d500fdc8bac6db377d75ebef3cb8f4d1ff738071ad093891788
9250b41dd1d98896ca06fb
Qx = bcfacf45139b6f5f690a4c35a5fffa498794136a2353fc77
Qy = 6f4a6c906316a6afc6d98fe1f0399d056f128fe0270b0f22
R = 9db679a3dafe48f7ccad122933acfe9da0970b71c94c21c1
S = 984c2db99827576c0a41a5da41e07d8cc768bc82f18c9da9
Result = ?

[K-233]

Msg =
f553c9a1a17d02161faac334dd5f15324c1c033def264d62b28961ae7c5e8694074a5b8ef04780
```

070aa79379f8565ed3fb5f4e1d08b1275e1e24f7bed6b749e83c1b9ab2dd76110021616ae5db32
340c1f813c5754e549c589ff09990dba4cb939d0705491911cc70ce032c2af7efea6608bb432fa
49195f9d24808848eff8ce
Qx = 0136ed170a3e06af2f542308c818ad113115662a0f24b86e8de8a8577340
Qy = 00cc263193d2844f48c02de4d5f8df5ddee4548703a5222eb2144ffe54e3
R = 0017c34e4c94c9ab1957b3ecd22f97c32eebc608ca337b0b314834726964
S = 006ac64d1221b4d5fb0ea95a5e154a1e64647f15a1a4f8ac6058968e05c6
Result = ?

Msg =
490d6c7d320a88286bee74e3ff2536a9c9af1d9c36d5a7554c14a178eb5e908b53825008e7e8fb
b031810d2325fec5aeaa40ce6456101e7079111fa95ef20c67cde89e95d45ce908c8e1800f8668
e04cfeb70cc2f317742efc4d1b9bcfccf931be299f4e82cf19d838f418d1a9cc512bcefc20de94
517139dcb2e075c6531f90
Qx = 010b9887c30189f70fdb353368a46e18ba0cfbce16274bfb456d183af21e
Qy = 01dc2e81158f6221382560a1bea6cdd8d099d0317ec09c9c5beda7942c6f
R = 00077eb49e722729af67db03650808c60e0122f7b7efb8792a7accf4fe54
S = 0026f591818d27aa189fabc1525646fa706f77cacda89f108c810598accb
Result = ?

Msg =
ace934c17c190a4cf59bf76a2b89bea316493a3688b5f35c6278efd108bbcb9112020adf4550ac
8cc19202767b3ac24fee2b57a00ed57a0d7ea106da028f08ae371d1697826ce34f469e10be5a82
44bfba737e277c7daa0406c273227f1c59d4830403f01bb3d61cec86c648aea76c7ce0ea59d4ba
f5abc964a4deb165ace489
Qx = 00e4c747929fccd4042bd3f7ac1d1659a59a888e8d81b670de19b2d9a305
Qy = 00bb27d7c664e68092333580ad94e67170e0e5e678278e9c43b9dbe94774
R = 00584c7b81ea80d78a2574654a3f6a36398c2133fae96f428ee638ad4d65
S = 000b0b36d180506386efb3cd6572cc3afefd751b75db4d1b9096ada948e2
Result = ?

Msg =
fd75c460df9a32bf0a837e08eaf81e6a3ecf628479bdfad8686bb97d16cc9915edaffeff1d903f
ce42b462f9417527d372da49be056a009c9e42ca8743666bc2785532efa8e07f82c73b82753655
453ee765edfec1c53dfb46045b507337d7e3e78fe9984831fac4e34166e592408190e399d8aa76
76b9dba7d8f5406de7e460
Qx = 01ccc8d325e42af6aff1a280ebde426050609883926dd18acbf24959d9c1
Qy = 009f314e10ad7c7f20e7061bb58a0a1128c1671ae2fa5f929eb05cfddada
R = 00053ada9d018679f8ff4352077e63baade5ca2c506450205cdbcbe37b93
S = 0024df72910c75b3b5d6fd618326708277660ae53489fdef984f01f2b720
Result = ?

Msg =
54f9ebe43a658c8cdceee7e2edcc5e8b04866ce99516385520486aa9a8633d02670bd5c4c066d4
de757e284f1ae626e9caa1dd54183fa4574849f653c0df8010b9a077bc3aca2f3147a2ea775617
ee8a02a2da5d0370391e5ec358bcd99655a7b28079d790dac70fba24d56387a5dbf817520a0b3e
f11f34c87e37ecdccee54e
Qx = 0169b6839488a2230eb8a55d4aee2cfdecde006beb1173428f6079fb5b2d
Qy = 00241ca64fc4d97b37c4721d28eddb25d8d187570f0c8e2bc9f2111d1255
R = 00369daf397bd022654b1b5b0b0de937e9aa9c830165415b6329b0bfb090
S = 001f591f44be300354755a0fb466e5b248597f7a5a9cb69f4d508415da8f
Result = ?

```
Msg =
dcd8bdb15a84862ca5ae26302d95320cd71c4ee7fec24d54b8d49a275ae2d6863e6fc243c3ec60
6996e8551430819286a01e33788b60a7ae715512ce31efef72d0b5fa7c76b94daab9cac96a1eea
b7efdd03af84e5d5b9202033b33bf86ff3e11a132d057ad1961797bd49d900baea6e17328ab315
0bcbd34ed64516b74928fa
Qx = 007345bf47179e1533eb451d0174e1c04f8bd34c202478f950ee54f736f8
Qy = 01706e0da88763ff81d6e1e853ce5f7484635a7f6d08b8d9730b389c8d0b
R = 002e1d25e5b4f7549fc39bfc9244c01843cd30ba3e7cec33c56bddc67a66
S = 00486550d28f3b79d135baadf8795c8d21951d76b88cd9110bca0d125133
Result = ?

Msg =
c5f62b24a16226b4a66a01893da87fa175bc523f9a91464909e2bdee42fc5b8b3fc502d005fd01
1f78c48834735c600b1831d8fe6516032f08d2202575db5aba3561b234818e39b20f0d82ca2cc9
57700bf7ab195d56d02121b5ea6abeb7a4474fd321983e9e3636144dd6918f75cd97f616b1d8a9
d816e8fc9402054516a1fa
Qx = 01b6dec64e5e1fd13ccd98ba680763c47583e95cec2d0dbf309bf69fe51b
Qy = 011221e50fc93677bbcb6e40b24f2de6eeed9bc26ba826e80e02f7eb5574
R = 00475802cf260aa2b4b14262eacfea1ce1e45f406d8ae411bbf187e062ba
S = 00293f771aa308ef1716ffa5fddfde490724016c6a570c7b1b807740421b
Result = ?

Msg =
1ab37b5c3e7accb783e80d93538e1ca59d6f7eb1270651aa268b811b0c733fc5a136af895554e1
89d49a038bdca1d59e4b995dff7d44db3dd445ff9c989b5ab70269136a93f8dbefaafe22475621
8bdc69b79e64cfd0be081c765ac66a33671466d40dc6a16da0312d9dd3916a1328a81d51aba8c2
b0e05324a5fa612a424d22
Qx = 00c57832cad1eef31b0545f0c48718106d27d6492addd718d6425c7fa056
Qy = 0026e7491ef66649a3f0d4bbc8d7fb4e1db86a3c2288658edf74a64fee43
R = 004009378a80c311db1a3ab914953d7dec0ba06568a6bd533b2537e55f5e
S = 0059cf2d301cd86e94d0d1bf0d3f21fe3b2aea683d2354c8781c440f23b1
Result = ?

Msg =
5a56096c7e86e5d4988347e117552975e687f720e3cf9fe893f1e84514e00470532668dd7f87db
06bde1cd6b1d57ebd7ccaef0e48cf7bec1626fad338ea323dac0d865b689a9acea10f27cbf06ed
31ebdc9bdb1433664b9094046e6f619edabb0b32a7fe86368005fa7ef9e4bc5f233a7c155fb6c0
626fda9178d3ff7319529a
Qx = 01e31fa7780137bb4a2ab01d354fd773901b9ef976a5b564a2a09dc9df8b
Qy = 0191cf897a2347a43e781e2c41d5bd50efcc705267fed96f52eabdf42027
R = 006729210e1d49542bde1e3ee0609368dac81bfeb51ce99fdd306ca9ac16
S = 002ea969db3ff2a494730cb2de1d177a6c5b3ca7a42b0f7bf6d1ab44ed8d
Result = ?

Msg =
2a5325bd0277f9c49be359fd2bbe5e63d1832de0e102e16d7da8c67a6501c8900f7b2b35fb6d7c
104157c74d6c6c0a438a4dea548418a515aca148af95ff2286274b7818f2a47a27c376761a75fc
4ca10a042298fbf3582ecb08be46e2e5051d994b742d9225dc524ac8ce2cf1790bc4792f3c72ed
9be4fe04669205f6ba5b9e
Qx = 00c6b220969d54cadf544316cffa60fd5a1595ac420f61fc5873ad78bb56
Qy = 0196b017ed347446c64d6ae8613e75f822938194a84952e364d67d2e0036
```

```
R = 000a4c1bd92de8907c3cd3930249b06d8556093ef7378bdb520d56791afd
S = 007f7b94affd65269dbcc29883064b69ccce7127ab23dd404eab59029787
Result = ?

Msg =
cd25a7f53bc44ac3eab1d4771883891358d2b77a86534ac000449aa4130b875bb41ac890711580
a8a737124af4f2371fefd54ed617b3f36c0a02d2aaf881bdef561efd2fd716e63c985eaf449a42
809b764ccbbb4c67e08afd44bcdb9afd22361cf8eedc550fa50626ed506ef3bb8b1054fdd9320d
b63aa241d3003fe2c6deba
Qx = 0078cd54849617d64c1bf3ee0c01639d4912411912513612512c0237bf43
Qy = 018a850cae6cb9b81fb4173847b4f29fb40b47a9bdfc119d2eb6fcc4146d
R = 0026170cca4ec53585b9ddc149f1811133815b8aa2f68f2d80e06746a6f4
S = 00100984fcbe5bc6a0d91473b40589433851aa725c3f4ffa744f340eefb2
Result = ?

Msg =
c292e847f4bf5a482ca63544d31ec7df4f05460726d415266776439c465b556c06c845351c71ca
659149daa9a8996da8c14f85f07d996b3023b33ba942fea2df9851e794339328f6d68ae7189eee
c59fe5c28cbe67e47364a3e29eb3850fe5b541d6d64a824ffd65c4106378fe46542d850465572d
dab628b1aa75a455b7a355
Qx = 0073108e1827566a63d94ef922f94b2835c91d53ac62371df25217989f2e
Qy = 00c0ce149e33218fc95a299c64dbccf80aa4062ca488e74340d9d0a40b83
R = 00561b14067d3fcf8d868ac17211d6a8747b6089638338810f7336aa988d
S = 0047e987aed01b51f888fbf4b2dc34a367b644cee4271f426314d63eed98
Result = ?

Msg =
0cb9c695b7585006751e32fa0761c185fefabf73c23f7cded931400066f6ed45f089e1a465b01a
305f2e9deaa53a18daf531c65e018893c1b704810fc52d4a285d00471435e49096d3df6504070a
cc55b9427c7ce421faf5e32c029dec4e28c6da86bf8b2fdcfa61599951ef34b72620d197a97676
f2f9a1e5128c50e142d047
Qx = 010c42d7b7557e2ba495373dff3cade13fbb56614f15b47fca217ca7d57e
Qy = 017abd698cc8dec5aae48ca111b533829d487a7ee333b24e74da4a50b889
R = 0f3e30cfcf4d3ba084dfaa43b625d5fb4f406336501b1fd43f9f82d2
S = 0060553f1b1d9d2ad62f74ba7a906204dee6c6f059b50fe7317141f3d443
Result = ?

Msg =
8159c84852c6229694bd484661ffc349342c8a504e91803c59413fd64c6714c18eda4aad5ef2ac
cc729b458adea76a793869fb8afa7fe58327efebad3276a7cd1b1ccb56db0caddd02a303cd9fc7
ea5c607a2ebefaaec598cb5b9cb7bed097027047d3ad91bb2eb08cfe09786a064cdcf387ab5217
c828638dafd95cba1dec47
Qx = 007ee60584691638fd6fe17a3b4ce3ebce1747ec6c44ba6ea8d235b130c1
Qy = 00881c53ec4e23e591764b5cb4047701c6e8035e37f77cbf83d0d7257d98
R = 000e690c9f1180e538bb790906e037cca39d07799032841370c74ea30b78
S = 006e1e028bd9d204b9d97bd9846429edaad8da32aeec6f3bb7e99f32ee8f
Result = ?

Msg =
39cd57963378c638c3b2a442f65d15d8b9c605c5f9356db208c2d19c436b0e85f26452696fae6c
738beb46712d71af863c9d5e1ebf6934274341c27f7d130ba831a68bc3532c78bc6b1a47c23e37
```

```
72faaaf37974d2fb275e7b0a1677b60275c7c03b098e261b727a2ce7b01c70d8e59dcb725cad78
11cbbd78c5d56e345fd34a
Qx = 004bc66f1524162fc952a41240b627e244be6d1823a0736be63adf559727
Qy = 011b167b34fc9be9589e7d8c1fe3dd033d6145a0f1794f911272dea141dc
R = 000d4dbfcb1069e09657f3d9614f3e6bdb0f812b281f0887c85b5e57c376
S = 0028055fdaaa8090d97568a23eee931d576fe6eae5aed9e11cf151f3a77f
Result = ?
```