The Digital Signature Algorithm Validation System (DSAVS)

March 10, 2004

Lawrence E. Bassham III

National Institute of Standards and Technology

Information Technology Laboratory

Computer Security Division

TABLE OF CONTENTS

1 Introduction

This document, *The Digital Signature Algorithm Validation System (DSAVS)* specifies the procedures involved in validating implementations of the Digital Signature Algorithm as approved in FIPS 186-2, *Digital Signature Standard (DSS)* [1]. The DSAVS is designed to perform automated testing on Implementations Under Test (IUTs). This document provides the basic design and configuration of the DSAVS. Included are the specifications for testing the individual DSA components of the IUT. These components are:

- Domain Parameter Generation,
- Domain Parameter Verification,
- Key Pair Generation,
- Signature Generation, and
- Signature Verification.

This document defines the purpose, the design philosophy, and the high-level description of the validation process for DSA. The requirements and administrative procedures to be followed by those seeking formal validation of an implementation of DSA are presented. The requirements described include the a specification of the data communicated between the IUT and the DSAVS, the details of the tests that the IUT must pass for formal validation, and general instruction for interfacing with the DSAVS. Additionally, an appendix is also provided containing samples of input and output files for the DSAVS.

2 Scope

This document specifies the tests required to validate IUTs for conformance to the DSA as specified in [1]. When applied to IUTs that implement DSA, the DSAVS provides testing to determine the correctness of the algorithm components contained in the implementation. The DSAVS is composed of five separate tests - one to validate each of the various algorithm components. In addition to determining conformance to the cryptographic specifications, the DSAVS is structured to detect implementation flaws including pointer problems, insufficient allocation of space, improper error handling, and incorrect behavior of the DSA implementation.

3 Conformance

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

4 Definitions and Abbreviations

4.1 Definitions

DEFINITION	MEANING
CMT laboratory	Cryptographic Module Testing laboratory that operates the DSAVS
Digital Signature Algorithm	The algorithm specified in FIPS 186-2, *Digital Signature Algorithm (DSA).*

4.2 Abbreviations

ABBREVIATION	MEANING
DSA	Digital Signature Algorithm specified in FIPS 186-2
DSAVS	Digital Signature Algorithm Validation System
IUT	Implementation Under Test

5 Design Philosophy Of The Digital Signature Algorithm Validation System

The DSAVS is designed to test conformance to DSA 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 DSAVS has the following design philosophy:

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

2. The testing performed within the DSAVS 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.

6 DSAVS Tests

The DSAVS for DSA consists of separate tests for each of five distinct components of DSA. The DSAVS provides conformance testing for each of the components of the algorithm, as well as testing for apparent implementation errors. The components tested are:

- Domain Parameter Generation
- Domain Parameter Validation
- Key Pair Generation
- Signature Generation
- Signature Validation

6.1 Configuration Information

To initiate the validation process of the DSAVS, a vendor submits an application to an accredited laboratory requesting the validation of its implementation of DSA. 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 DSAVS 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);
7. The modulus size(s) supported by the IUT; and,
8. If the IUT only handles specific values of PQG, these must be supplied to the CMT lab.

6.2 The Domain Parameter Generation Test

The domain parameters (*p*, *q*, and *g*) must be generated in the manner prescribed in Appendix 2 and Appendix 4 of FIPS 186-2. The algorithm used to generate the parameters requires a *SEED* value as input and produces as output, along with the domain parameters, a *counter* value and the value *h* used to derive *g*.

The DSAVS tests the generation of domain parameters by asking the IUT to generate approximately five domain parameter sets for each modulus size selected by the vendor. This test verifies that the *SEED* value supplied results in the correct values for *p*, *q*, and *counter*. Additionally, the derived value *g* is consistent with the value of *h* returned by the IUT.

The DSAVS:

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

   1. The Product Name;
   2. The modulus size(s) supported; and
   3. The number of Domain Parameter sets to be generated for each mod size.

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

The IUT:

A. Generates the requested domain parameters specified in the *REQUEST* file.
B. Creates a *RESPONSE* file (Filename: PQGGen.rsp) containing:

   1. The Product Name;
   2. The modulus size(s) supported; and
   3. The following domain parameters generated by the IUT:
      a. *p* – the prime modulus,
      b. *q* – the prime divisor of *p*-1,
      c. *Seed* – the seed used to generate q,
      d. *counter* – the value of the counter output from the generation of *p*,
      e. *g* – a group element of order *q*, and
      f. *h* – the value used to generate g.

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

The DSAVS:

A. Verifies that *SEED* produces the values of *p*, *q*, and *counter* using the algorithm in Appendix 2.2 of FIPS 186-2, and that the value of *h* produces the value *g* as specified in Appendix 4 of FIPS 186-2.

B. If all conditions are met, records PASS for this test; otherwise, records FAIL.

6.3 The Domain Parameter Validation Test

The prime parameters *p* and *q* must be generated by the method specified in Appendix 2 of FIPS 186-2. Therefore, if an IUT accepts values of *p*, *q*, and *g* from an external source, the IUT assumes that Appendix 2 and Appendix 4 were used to generate those values. For each modulus size, the DSAVS supplies sextets (*SEED*, *q*, *p*, *counter*, *g*, *h*) to the IUT. Some of the values in some of the sextets are modified before being passed to the IUT. The IUT verifies the correctness of each sextet, and returns the results to the DSAVS, which compares these received results with its own stored results. Note that FIPS 186-2 does not require the implementation of a test for correct generation of these parameters. However, if an IUT implements such a test, the DSAVS test will verify its accuracy.

The DSAVS:

A. Generates five correct sets of domain parameter for each modulus sizes supported by the IUT. Each set of parameters contains:

   1. *p* - the prime modulus,
   2. *q* – the prime divisor of *p*-1,
   3. *SEED* – the seed value used to generate *q*,
   4. *counter* – the value of the counter output from the generation of *p*,
   5. *g* – a group element of order *q*, and
   6. *h* – the value used to generate *g*.

B. Modify the valid domain parameter sets created above. One parameter from each of the sets is modified in the following manner:

   1. Modify *p* such that the result is not prime,
   2. Modify *q* such that it does not divide *p*-1;
   3. Modify the *SEED*;
   4. Modify *g* such that $g \neq h^{(p-1)/q} \bmod p$; or
   5. No modification is performed.

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

   1. The Product Name; and
   2. The domain parameter sets from step B, containing:
      a. *p* - the prime modulus,

b. q – the prime divisor of p-1,

c. *SEED* – the seed value used to generate q,

d. *counter* – the value of the counter output from the generation of p,

e. g – a group element of order q, and

f. h – the value used to generate g.

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

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

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

2. For each domain parameter set, an indication of whether the set should pass the domain parameter validation test.

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

The IUT:

A. For each domain parameter set found in the *REQUEST* file, verifies that the *SEED* provided generates the same set of domain parameters using the procedures found in Appendix 2 and Appendix 4 of FIPS 186-2.

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

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

2. For each domain parameter set, an indication of whether the set was properly regenerated.

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

The DSAVS:

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

B. If the results for all domain parameter sets match, records PASS for this test; otherwise, records FAIL.

6.4 Key Pair Generation Test

Key pairs for DSA consist of pairs x and y, the private and public key respectively. The private key is generated by the Random Number Generation (RNG) method specified in Appendix 3 of FIPS 186-2. Testing of the RNG method is performed with the RNGVS test that is an independent test outside of the DSAVS. In order to have the private key component validated the RNGVS must also be performed.

The DSAVS tests the generation of key pairs for correctness by having the IUT provide domain parameters, *p*, *q*, and *g*; and ten sets of private key, *x*, and public key, *y*, pairs. The DSAVS validates that the private key is in the proper range and the public key is derived from the private key.

The DSAVS:

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

   1. The Product Name; and

   2. The number of key pairs to be generated per mod size.

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

B. Creates a *FAX* file (Filename: KeyPair.fax) containing the information from the *REQUEST* file.

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

The IUT:

A. Generates the key pairs specified in the *REQUEST* file.

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

   1. The Product Name;

   2. For each modulus size supported, the following information:

      a. Domain Parameters for the supported modulus size, and

      b. The requested number of sets of *x* and *y* values.

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

The DSAVS:

A. Verifies that the *x* value is in the correct range ($0<x<q$), and that $y = g^x \bmod p$.

B. If all conditions are met, records PASS for this test; otherwise, records FAIL.

6.5 Signature Generation Test

An implementation of the DSA 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, the DSAVS supplies ten messages to the IUT. The IUT generates the corresponding signatures and returns them to the DSAVS. The DSAVS validates the signatures by using the associated public key to verify the signature.

The DSAVS:

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

1. The Product Name;
2. For each modulus size supported, ten 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* file.

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

1. The Product Name;
2. The Domain Parameters used to sign the messages;
3. The messages that are signed;
4. The public key, *y*, corresponding to the private key, *x*, used to generate the signature; and
5. 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 DSAVS.

The DSAVS:

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

B. If all conditions are met, records PASS for this test; otherwise, records FAIL.

6.6 Signature Verification Test

This option tests the ability of the IUT to recognize valid and invalid signatures. For each mod size selected, the DSAVS generates a key pair, (*x*, *y*), of which the private key *x* is used to sign 15 pseudorandom messages of 1024 bits. Some of the messages or signatures are altered so that signature verification should fail. The messages, signatures, domain parameters, and public key *y* values are then forwarded to the IUT. The IUT then attempts to verify the signatures and returns the results to the DSAVS, which compares the received results with its own stored results.

The DSAVS:

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

1. A pseudorandom message,
2. A public/private key pair, and
3. A signature for the message using the private key.

B. For approximately half of the message/signature sets, alter either the message, the public key, or the signature such that the message verification fails.

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

1. The Product Name;
2. Domain parameters for the supported modulus size,
3. The information from step B, including:
   a. The pseudorandom message,
   b. A public key corresponding to the private key used to sign the messages, and
   c. The signature components *r* and *s*.

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 set, an indication of whether the signature verification process should pass or fail. (Note: The SigVer.fax file also contains the private key used to create the original signature.)

The IUT:

A. Attempts to verify the signatures for the messages supplied in the *REQUEST* file using the corresponding domain parameters and 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 set, 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 DSAVS.

The DSAVS:

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

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

Appendix A References

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

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

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

The following examples contain values that are longer than one line. These values should be on one line. For example:

```
P =
f73accd5721dad7307a70cd5c00e3d028e323781e362e17c327b239077f53cfd0496b14a1fa57e
0bc18fd308fcc6c8bd2c5fcbb457bc5146cb1128f92fc9c7b3b8608e40c56c343fd0adb47c6a5d
9f55065ae42e4aabc900c70fcc19cfdfd9b7c19ca5118dbfc5ed4f26dd9a7dc010580c49ed2cf5
12b7239b15a1eddca82e45
```

Is the character sequence ‘P’, <space>, ‘=’, <space>, ‘f’, ‘7’, ‘3’, …, ‘4’, ‘5’ followed by a <newline>.

B.1 Examples of *REQUEST* Files

B.1.1 PQGGen.req

```
#  CAVS 2.2
#  "PQGGen" information for "Demo Product"
#  Mod sizes selected: 1024
#  Generated on Thu Jul 31 14:12:33 2003

[mod = 1024]

N = 5
```

B.1.2 PQGVer.req

```
#  CAVS 2.2
#  "PQGVer" information for "Demo Product"
#  Mod sizes selected: 1024
#  Generated on Thu Jul 24 10:32:24 2003

[mod = 1024]

P =
bc72aacb599a1301b4260b620f3391046cc8719291b7259f7d2f1d57942e0400bdf145a2cac51a
b15c27fa217f09aa3fd84d2f4742f786717a5d8089564e03e6224b05bb3f52f8a9775f1f2d8d48
6dc9d3bff78650e22df40d7c070d36d971816aa904d81ef90aed42332679b84b5f75baf069293b
ea3fda832c6eb342002701
Q = df0e3c75a268319201c6b309aa666db1f046888d
G =
a5d2ca30330f66e0fb5fda4bccf32922305852d1724f2dd10d7363e660395f67e8d10ddad970ca
bf42046f58bfce3aad4a9549ddac9c0e00a3458c4d9158502674a90570eab0e6a814241ddab410
```

```
def8a0ab937fcf8d359fd8f4db773bf0eecc121bace11bd64c19acca914ddef0447169f4e3f9b2
5af99e1680ff8cb8a391d6
Seed = 46b82836e092da94a4eb1c291450121718159500
c = 177
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002

P =
e31f0dd7c7ab52631a528a583359b4a21c01ed03b1cba14b806ad85ff4aef822e3ea4ac3af9574
ea0412487d0afa53f905b33d76c4987a0bf5bf1ef0575b852ae42c0574a3216628862cc719cad8
42de5869ee861efaa1aef916ee5ba12ad76ee97149cd8422911c095527d556dd13830e99bd76d0
5dd6c286bc8cd5822688d3
Q = ed928212f675f4a9881ee0f657d2c924a7e028c9
G =
0010c7cc0d56665b37e4a1160cc647d54243599e0febba57beb6e009d395f66bde5116bc821f6f
fe9ccd851b9c9056ef57c74680f3ea968209d7daf83544056d9e11d500ef8ddea29b412cb4f39b
253c6e67b5c16502db717f4d47b667848a1f5cb14d050adb7667b7c24fbcdea9192ae74bbf4ac1
ae2c227dfbe7db1db688bb
Seed = f6d57f5f1a055fada254fe759ea480d8fa42d1b2
c = 346
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002

P =
fc602845fae0d1f7048aaea3dd5f633b69447654f24ba184a8556b2647cd95bb9accdee8ba652c
4de4170f6e278323be98af9f204465b512cc151f8944e2f54908f90fcd7424b040d70b0b94183f
890bd0154236aaacd570c239da15d91ba998144d049dc8557b7afe42d6801184368be30a4904dd
26ebb47b4e05238ccb7049
Q = 8f07df47e6f6240b96499492178acd14397355bf
G =
3a73e588e210e58bf8447739bb2235ecdd8b67915605f8a82310b2dc3d761ef9f9504387446400
3e7da4954647f858397f8561b989fe2916a98fbd77ca37db89cf884d44466594de1055c53ccb6d
5808217d5f4c76a423d84b3fb19e0093c1b65ee4456895c8f3e4459d228d4754f8165fe76abf41
da171f4e938dee2ec2fb58
Seed = 03f5fc40998f59e9a1ae9e7a113c98dc381d2ecc
c = 629
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002

P =
cfaacdeadab66b588840516b0d86aafa1292ece8b96578277fa2367ae53e1d45359d2fc7e1a033
2a246deb01a2765654f9f5a463e4b42264e9cf3ec6aadab38c65fc0306456f3283aaa8b58d9845
8cf24e24c331da3b746f53446b84162c25a38272e4bb0544cf8feff856bba336684349a99c5508
7a3a326b6c303dda8535eb
Q = bc2888b3e820154c269fe2567bb5d8dd7f7ba36b
```

```
G =
16a5ef50ad89e194733dd08d98582030d0d0912ac6bff5d8e948797aa1b0c840d36a3ba9cd3181
d59b902e5babce642ce33897884967102ea6c0be7a2828d4e0d9127fcdf1c4ff10a3c50fd6557e
8104102e646651bce523b383f0a6a0c76269dac6cb969e51484ee44a869f21738f144de286b7a6
60e831724773ddc8044b71
Seed = d048769bd51a9d8d09a1e469a4826aa0e25b6368
c = 125
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002

P =
d942109feb8dd72e9fd5b7f1adf87411a090a4571e261035648499f4f0b509bf093038cc8ea0ba
c7354027281d4b35c93d2e1aeb0827e8fa44b1bc33378a3c99bcc246a0a2d0ec73da3e8a608d8e
4ec90642a9d8f7c97ecd6fdd4606da4e4e31e28e58a39ab45a1f1786e2bdb1c0b2863688a133e9
7ffbdb12f4741dc75e8f89
Q = d938dcf43182f580ad974fff95c6b9c9e1683907
G =
7ad2c400c4ea6f00b077a2193e16e6e5edbb2d791d2ddb38db0dd9fe21f7a643fbed5db37b7018
c3ab54a9599180a40a3f58dffea5170ca72cf36c619ca18ee6dfe53ef006d89d5cd3d22acd7c97
6b8fbdfb8f698606145a860e23e66f2a57c990e66e51680cf0a21664378944821996a808e881d9
26f873e278c05bc3354fac
Seed = d32755fc624f9f18638b6593c918c4aa2a41a5da
c = 6
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002
```

B.1.3 KeyPair.req

```
#  CAVS 2.2
#  "KeyPair" information for "Demo Product"
#  Mod sizes selected: 1024
#  Generated on Thu Jul 24 12:43:25 2003

[mod = 1024]

N = 10
```

B.1.4 SigGen.req

```
#  CAVS 2.2
#  "SigGen" information for "Demo Product"
#  Mod sizes selected: 1024
#  Generated on Thu Jul 24 12:43:25 2003

[mod = 1024]
```

Msg =
229a053b64fabae455a482742ec07be01f8a7feee79b549aa36a23b9e3122cdc0356b777b9e24e
43ead329e0c27aeabf035d8b3f9d7f941680e291f3ae49c362944216ef9a64538ef9d6973acc11
04dd6be6b670f4c2f8632a31b83f83a1398a7c6908eb3009318e29b3b2ca760b3001fd2ce9c813
ebea484a5f82e48aa1f61d

Msg =
de31e0d133db28637c41734d9c8cd1b03c905b90620a6936452605d260459f65c5fc02deb46086
836c8187934134172aef16f0642ecdacc5869139d965ec87176fbd830b158349b569d8952c303c
7b86391459fceef2094a29175b554937c210847c4da07fcdd9bf1b4f865e922c678ec4947ea0cb
02e78bd5c1538f33aeb818

Msg =
ef0974fa4832a69fe5f5d00f0d4f86da23eb5d9478a15b7c633eab5a948395aea570ae06f2c24c
b0abba3d912720b9557b8894c94cd4b884e1fad3cd7c074db9eb647d945a581c826bcffa66895a
ef037976156231113473ee4a7ef681797d9ce96f496a27fffe5f4ebd6d56da05122e423f4727d1
62b68fb1b7149f49e00da0

Msg =
9799ae10374d1a7b2b0d45f9f622e6b61ec8d86f8332148eeecfdd97edcc3ac2dfdaa9ea4b3112
a576d4fab53417f99ffe5f6e99452a71a9064f090c9f869fd5e12ab3d6663ecec324afb89543d8
ea2d2c4b463ae3cf065c96a5f38a7610d7b1c514349d307d361d6023e762cc6da2a9d114ca1a04
29bbefc75a01d81a71c99e

Msg =
bc0bc84b82cc93ff67587600a6160b0f4bee6c6fde5cf69a41c24d34db03a03df74d2f8a66360a
766c0b1bd5da64662977fc9019a4c09e1e40260080cac0ce81c51151d7619fc56057495d1215db
88311be073c4a5b8cf498aead4a864bb8666f1ff371bb92f4d26f1bc459fa0a3f88d00421d5927
691083e6b5d294f2195054

Msg =
03788f568945451dc141ac17823185d6a8d3a2b0c3c441c011a1982eaa6cb1b0fb32785175eb13
7286a2710ec9d626427a1f760c2c15af53be6dbd278b65f84be16340f0b5d84cc4946b3f2bdd54
7ccc2e05bc501c105e662745fe0bec1a48089d510ebcafd4991bd2e43df72672307faccd9d05fb
7ef30434708361375 54af1

Msg =
95eb19ec8dcd4dff898281b4b9409ca369f662d49091a225a678b1ebb75818dcb6278a2d136319
f78f9ba9df5031a4f6305eefde5b761d2f196ee318e89bcc4acebc2e11ed3b5dc458b01e6025a7
5f70c4a325308f63c5f1a16357bfeca6684286b3efe244de822e8ac8ca7f612935d8cacdea1153
dd0235e760f528ea01528d

Msg =
f98ec431f01142e19f069e58d6c95867325bf9c3a6a949625b11c128ba2243c3c7a309d4b0d7dc
4fa5008624eb22891f2c09110c128d2820141529948f5a7793186e6e5611fc9a8e7ad127020a9b
99797ef1beda3294e092eef53e3602f7be6995f5dc013a07e665c4816b395cbdf13ed01be6732e
45d98192b8ea553c807f0f

Msg =
619c4628111a605c32bf9d670b839eb764e286319897af1beca89c3a1fa22f3743261c48cba49e
0ce46769b609d2df6dd1e986f30c13ba850f1d9f034c835a5126eb81fd03f3cf22a22c1d8caf66
8d1c942f096e9396ecba1135fef8356ea648b2f45b90e18d5c671317a13225c9118c55bcf5ec53
aaad819cf5a16103eb7be3

```
Msg =
e44d45b0aa7b782270142fbbaf7ad38e3efb0bf32253332ca7720a48b080aa484b1fbe8188f0ef
418c589fb5e184da0a10aa89d37292e9ab43563c1bf866bfbed2cedba2b4bc9ff2323c6ed2ea47
f58b17fc60e8632dcee0fd1d0274ec885bdba3e406ddd5e7727d8a4904da73cb0d577a78f9fa9e
2bc912fe51c31d33f067e8
```

B.1.5 SigVer.req

```
#  CAVS 2.2
#  "SigVer" information for "Demo Product"
#  Mod sizes selected: 1024
#  Generated on Thu Jul 24 13:16:04 2003

[mod = 1024]

P =
b26bc3fbe326f4c2cfddf9ae3e397f9ca773c300a35067c3ab492cea5910a4bc0994a9053b0d35
3c555247f0e3725be872a0711c234f6de8ace5211bc0d842d387ae835e527e4609b5c73dd600f5
f29c8430817e7b305bd5abd02f21b3d8eddb9777e47e6cccb96bddaa9604e7d4551153abba959a
a28c27d9cfadf3cf3a0c4b
Q = a45f2a270949b6fe73eb957d00f342fc7847b0d5
G =
5c571649efc8fb4bee07453b6a1df3e5ebeead1113e352e30dc02125faf0931c534ddc0d76d2fe
c2d7726469533d33bde134f25a6783e0d31cd6414d16e86c5a0795219aa3c4b9059d11cbc8c49d
001af4852aa9203cba67e5ed31b211fb1f73ec6129adc768b23f38ead987839e7e1918ddc2c35b
166dcecf889107e02ba854

Msg =
c22163ea1e1c878481a2245d2b449c1cb7817ee44e305bd61b1ed6d8fef7fb95856ad2c5188833
af736ddbec5a23c06d87c3a2c0e8dde38e071a9869ca20e0c45cb675436b29803694eeb2601b88
90fce0ad0e028ea460a616f10d215c3445b52f4f74eb7fc71720ca6dcf3fd83db3d0a886eb32aa
4b7b242fe95c8b1dfbd16f
Y =
adcfe2d6d2dd6e9ddc6482fffcf067b6ed065d38dd1ae91b2402ab1d7e82da0372d38241b04cca
ec45ab0e0ecf19c673f2b82d3ed2bacf584550f7a962e3db2f77e2fff389fb5cee2b071af20cc2
45683841336a06976a0f44942019609744cb409e75bfd019cb8ccf2b1c578950e45bfbbd3e78bf
e69c9b9c0c9838bf02686b
R = 7c03ff0303f5659dc71fb1403d9db83784ec6858
S = 0a253a7c4a27a543a11edfe5b377114a38f38dc1

Msg =
7105e2f27aaedd5a765c27c0bc60de958b49609440501848ccf398cf66dfe8dd7d131e04f1432f
32827a057b8904d218e68ba3b0398038d755bd13d5f168cfa8a11ab34c0540873940c2a62eace3
552dcd6953c683fdb29983d4e417078f1988c560c9521e6f8c78997c32618fc510db282a985f86
8f2d973f82351d111d6f86
Y =
4f654e6a3a6ab452aaad0c965c68386b298945181d75dc77d4cc5ace6180ff05195e304d13c815
54d4a3c041700367fdc75ee8b0908b07a9f2133e6e9cf5b732907af741ceceaa33e9be41b3a8c6
3b051897f6b7499547fccbf72ac095c582ee9c8fc816e4c7c0e307d3a66c596ca26c21146fad7c
47d1243c3ef12072e86b35
R = 986d3af33e7bce7258b2f774d9d07e9c97f893ec
```

```
S = 6556d6f315ed958c96139c527dfb964da834df86

Msg =
ff20f0955c152cd30ff7d910c6c8c37f367be0c7bd061db546b85d2d6ecdbf67e540205816e0e2
6d0aa6eb7f8946f0048304f382afc90a4a72766362027885c3cb9dd8c4122568d7d81de67301e8
f051b51f91db079b0ce2d4cfd58fee5be19c7adf1fc3970d47774103d2d374d749d09473c3ba0c
a3aae5366cbd9c7ba05b5a
Y =
6628fbc3d5f6b65e1293c00ccc85cbd1f499437e78a03568090b5b628182ada2b5bcd8644ec494
c1eaa05f7a42d2fd7a6a94ffd28d5739891c6baca39d5485f5df6cca70c36f9073ee1b3c054009
23f3acc122250b2d24f293ff337547d1d6c52118683205f3e113c2b0255c542dfef325aee84197
77fbd3e2fc1c7860911a1e
R = 5c6ad0f0e43e2316e542ffd0f24e7e6972737f23
S = 230bab349fd181ca4c531b2053050875c1ebd470

Msg =
0623089764ffd5501a7ebea62573daa572ec8d6facb8fede5326cb6b0e10fc4f421836e8e33231
5d8a636c85c8c82005bbd972b9deefec5625042e4d4abae1f2619fedddb3b0ec90c91cde5bc74a
1e7dfc1c958cb6762d175bfa8889b516f3508e41953f7d81ec31ff317bf0c901bc555d3e5cb0dc
54a7691b9142e8f82b18b3
Y =
541b1c90eb4cc544ac1aafffc764385196ea85e78a29675fbf927fb452b860c261ffbc8d9ca3a4
c6fb67ed5a5033b98f96895be01f612d72f802fe939f74c71abe231ac1ca21a44b4cc133ed7d9e
223c3f8e4a3b6ee6ed5d2e3c582d9d177ef340712dc4f9319385b402b7785b61aa613ef8c13544
d0c4c32a170646baa3def0
R = 861a7297d773baa641baae5fb2982e099738e43a
S = 426962891625cdaeecae70403264938fddd70fd0

Msg =
f22cd6836e04ad28495d2863cf619dc79f443c500c1c95e2c3f35af2ae1a668319c1ff5514c558
5918c95a67ed88a433ca69d17ebf55f98950c57acf631ff8f35c42a2f8865fb7b0b50c49772993
4221b690a43022bb154acf029aeb99dba35802d848d48d7bd215674d7df94c2a7c76a9df3ecffe
f7f00e87d143ae1bf66f98
Y =
459d1a582c7e65024ded686c330b3b0a4c0c725415048d66de1d049b0af9ee91ce2bf721294e76
18638600682750e62986b98f73f4900084cb71851a35b1e4992795a01202eed157d9c66562a46a
5233db3e297f83a2a47a71368917a64777875c28b566673ba909a17dac1d7a182a1c4c6e9b10e8
b83c6fd54ef2fb781d6e5d
R = 7f6a33f5a096715f66f8a5216ede08d97123f1f5
S = 16dada2e06014c65e23c0ecbf32fd33f2b67d1ea

Msg =
7fef236d9016e7b72e0307e730871b02186cdeaa8a103de80353ae28c7b3c3851bb6ff47b589e8
aa71e65de2453a2a5b7708da450d88cd5086958ab4c7c6557558da05e5d059106a8e78e881aa3d
8a032be553a87b8316c918e96d6a8bcb4c779e22dc4ecacf867eef814dce48d862829dcbf2d9ba
4743da2118ff50fc0dd014
Y =
b1a4645004b16906846a0e85435ac77b29f20c145d0a1b821fed7cacedc2ef869e540868b79a34
2e35bdb70e6a50338e5c3c689e9fca8661b621e3ebfde64880130fa20add5535448f2e71a5a00c
c31ad837f514c01773db03050364fa83491a9fcaf8d3092c953513a54a7a3fee14a34852a8845e
b85ef0bbd86d85a0a3a271
R = 010aaefbd84d0c70ad0ba2c12a0037516c0da5d1
S = 18d76c91c66c9f0a5cb4bc37687c8ec426e4cd38
```

```
Msg =
824e7fdceb7cf8a62a27049f2e8eb61852b2d74a3db0e647064d5d319cd336aa661cae8b26ec49
d9238416f58773341206b095ecc0e602b8690f5f56a74431cebbd35dfa649332800074aa04f55a
ed9b4f2c1782ab273b105379a8e9aa0b6b75cb9e15906d19be830a21493340ebea99774ee672c4
1d9a380db3bf506ecfec85
Y =
6aad60071209228ad00f19f5bf67d36f6294822fa6f2828e8a90bea48f8a76484b6f342c77c126
839e57578d949a5fc7fe4d6022215cbdba980ec6fc49372a96ff22d1d4eccf3e2153ccb201b2b2
1dbb7e2ab8cf3722bef2e3d83e63da5ccc9fc4ea99e13fa9847c8b8eed0e1814afb23c4d14c78e
597cfa03ff721961633602
R = 3afaf03cacb83c87abe7e62bc82cb3274a434b4d
S = 34a8e5b9041e396e5fc5539ae1873da8502b9c51

Msg =
7e34ce3fe304a910851aad715edfb0ae16a6cc47bf8db5f4c2a449e719526951bff4082765c681
2667072e15fe58364ab766a66f24c8c486d12ba02b79aceb197a850cf087ec71369d38239b3846
9e81c61bdfbb5ccabe95a8987e15275fa38197300321b03c20460ff5b58c73708f5b2b0e9eb4cf
5b4c2a2f360d2e89333890
Y =
adf79fe12af9954ca699830984ad88ce4d7bd3321c0eec9e870898ef622c99f24cfb23ccf401e3
76a7667cf718ffd648add9a688c0e841025cd1e1d941a2cfda6f5e534c5bda2ea1979119952b3e
4b1ac4b6fdf1669e119a074ffbbb7badcdc9a4110501d49b69022c52318dc06e934a78e5fedf7a
58dec2556e8c052154a9cb
R = 841fb9aa6d648be24698688017d1bf530ceb1ee1
S = 9f54ed100dfe791e6fbcf60af43baf5c6e5452c3

Msg =
d8e745e683201b24ce6fdd1497877fae8ab23526957386b69f6aa29d7779f5680a25fc70da3f58
a4abc321887f007c7ec5f97045ce0cf5bf80d14ef74e4599626828a5652ea30318eb2e604ac0b1
12c5dee9f0d2f80e6700f9b3ca22f2edea9756b7e7ce69954508f678426040e267093c4a5ed8fd
c2030270d7bd2649b90f8e
Y =
122e8c7f13b04d71718bf0eea9fe17572034235b845d5ae8eba4fd422becc9fcc41ba364b0e40e
219922acefe2dcbd73f881b30be44fd1d5473f3ac7e2a9cb1b8fe08d43c03e60ad73d50de1caf2
dd5c578d5a0f60e291e02d4fae9aeeaa79e985f6d42ed323e2ec7cd3a646132f23081691e0f587
eec08bd307f3972a8ab71b
R = 74e86a4068a9ce65ce99fc4eaa1a24bcd70129f6
S = 02d27e752a0f944d1077a05d9408c1bc7be05035

Msg =
1a7bdbe63042aa48e3ddf83e9b2800aff361d7e45f393a3d122a8a221f0a153ddee197e691f801
df47327842019fa1b7144f1ceace644e3d5c6b64baebed944b0e40a62d60a3b4a26a8b2ee6c737
2065858ab82bcf1a039cc985f765bc04b6b2734211a2e56e4bf7148e20133417062010bbb38eaa
83dfc2211d4b0cd87702da
Y =
83f88edf6e9b00c5597f3563fdae5c9e3250acbe71031bc97d765979080018e54de8a263dfc5e4
972e8b5588d1b11dd8722b850ab2936d0d5bf2092c2be1ae73eae9a988df46baeeeb27407d7db9
0013bd7ed4fbbe06926bd33a0871a8a11730d6c36494498b2bbe0586b8ad900bac6c916c4259c6
d7db3b8dd22e0be4d7e497
R = 784f49131670f16335bfa108fdba56e6f41d1256
S = 9b3e19e9f907cb960a8136390ddfbc3ab5af81bb

Msg =
6c31d64162866fe46adb6d37cbeaedf03239afe1fb4b77cdac17b27bc2b95d08b168238126a8c5
```

b28fc0bf38dd6f29de88dbdb26d4cad4255414dd94ac5969259aefc013381e5cfd7b9093f40003
77d30841fbcec152574ec7f0adfdea3bec1c32aef51d2052fc6e37313193bb0ea077b953560447
4bc6f10d916bdb04c9ae98
Y =
82acae44b80f579e329e0048f025b86008f1add053fbcdaaf60283eb7c13346b15ed1dd76a6751
dc5f2d3f67ce1edd6f92134b32d1f09ca53a4be79838c2337f7140768d08b49016f6a3f7f2cbd3
85c47dc9609a63a0142019a5b275ee73779ea2bfabc60960c1b141c7638104f0579bf355202bd1
cd5942498876720e3604d8
R = 2f6fa9ef0d930edf62c653593171091cbd128408
S = 9cae316ef7e6fc510244dccde3b1b758444f2547

Msg =
2c40089472c5ba01ee4e62777828b13c5357232a032177525ed162e5e6b5845556699bb77b57f7
6c457f2e001e7410527aa7ddf5b0e8b6d7082a52201587f25d458497deb695725c4be49ce0004e
07df7aaeb5aae35f2706f4fc1916536a6c82201964d2ca86131b280515dec5bd7e2d7bf4110f43
8db3264bce1f8f4967da0a
Y =
895c491e2d1721a8f8d3b733c49bf21cc0f3bad53d027295a0a82f53d068cbcac947e3245de447
a4af29535e38c229a637c50dd96cb44a288270c10073d9160672a91cc89ea1bb5028dc1b1a5b0a
a7136e58a94ae039b5691eaf6d094e5763f852c41d4124e53825c6b2a09b4b55f3d88a8af3bfe4
52c3402a188d211fb15e84
R = 03be2b2085a8e8e00d858f9f5f82ba3bb3f7c86a
S = 512836b807cda24170a9ab274e246095715cc39c

Msg =
ad1814037d6fea331b4e61d46527f30b3f5c476d3755fbb868d1a0c19d7906aebabbba6558d5ce
45b030d813baf03d3796c9b0282a14f5250d22eb26a3d0c9128a5ba832357642e6d79af996839e
1bec9187644043a1c454a9cf6342c11fe3b2e3a1e5505c7ace7e5a34cb4508581292f93f6b9fca
25efaf037f10fe3f8edaf8
Y =
87a01d390c5ec7a16fcee02c7546d8930e36bc32396c9acad1b5aa119e756c1b07d1ffb0b9ec93
2d9c8be862efdff1ace9117aa33affd34592cd4d16ef270fab365c8ee84856d59b21f2316409a7
e77b83f92ce87af9ee0e45341faf25271c61193205e2f1fa6dee0abe7960b9721d16e2a794d234
816444ae5d48ea464dcd2b
R = 64d2bdbb07b17251e7530c5710d7036a408149f2
S = 364a1e248e52831a69354f7da2deedfaae2933d6

Msg =
f904909092b63b8ee6193d48b5f60af8a273fe1698e7e7cb66edc4aaacb8cc9bfba6b217381728
9b417fa256d3ba5c25aca09ec2ecda3f39c1f4689b43b29af59da8f2836e05ac226fb0e7045596
a7a7f9422008b6ae32141258305fa199e5182732d93dfd28d00bb6d394b90131f465d1800d4fbc
0bc845a144a45e8e13b6eb
Y =
7e0a22d0acd91fade061554386b872e50649b311b08f21e00818bbd4d28ef26593d288cf9be0b3
843ae8499f84ac715df901edf2dcab934264e5c3479622823a44ecfeb3ab29cf09bc8d20440664
e7becd77e91dd66f51c718fe94d59b713146ad1ae98a889e88268a222fba616e846f5d6a5bf85c
b82ca20a1fe9ffb326b787
R = 0f49a52484ea14590f8791346bf83decb3a6452d
S = 661c938cca562c507f1212aa5c53cca19d516133

Msg =
6a9f368060b44b7eefadb19ed951dd13d68be13136773525c7bdb8e4f91ef261404c9c03baff62
561245e701a4190af8e23868f2f630211ea9bae0118349150333e3853c323005c9a4d182737ff2

```
45f2ee23755df863dee55d7ef0c3c09a0b6f0b0cfa131070bd3f6cf88bdeb1041769c4f3135a83
39f2e4abb2f3e1f9375b0c
Y =
38afc7afc91e47a2034981feb5428ecd9623896d27e2ebab72e6567626f9b8035892735d3db6c5
edb23b6d9147f60578f1bfe3996d47f2a8a9d957849740e7bb6988a1ddd6de32687a1777db6849
aab03cb10b0be63b32f86aebc87e84981434c6a72410d845e95975c803b786278e41bbcb79bc70
f25401a6088c609eb2ddbc
R = 9bedecdd7df5af52f6ee3a730f502a5a82076ccb
S = 442982810fcbf663b62a11eb8e0d8345358d1725
```

B.2 Examples of *FAX* Files

B.2.1 PQGGen.fax

```
#  CAVS 2.2
#  "PQGGen" information for "Demo Product"
#  Mod sizes selected: 1024
#  Generated on Thu Jul 31 14:12:33 2003

[mod = 1024]

N = 5
```

B.2.2 PQGVer.fax

```
#  CAVS 2.2
#  "PQGVer" information for "Demo Product"
#  Mod sizes selected: 1024
#  Generated on Thu Jul 24 10:32:24 2003

[mod = 1024]

P =
bc72aacb599a1301b4260b620f3391046cc8719291b7259f7d2f1d57942e0400bdf145a2cac51a
b15c27fa217f09aa3fd84d2f4742f786717a5d8089564e03e6224b05bb3f52f8a9775f1f2d8d48
6dc9d3bff78650e22df40d7c070d36d971816aa904d81ef90aed42332679b84b5f75baf069293b
ea3fda832c6eb342002701
Q = df0e3c75a268319201c6b309aa666db1f046888d
G =
a5d2ca30330f66e0fb5fda4bccf32922305852d1724f2dd10d7363e660395f67e8d10ddad970ca
bf42046f58bfce3aad4a9549ddac9c0e00a3458c4d9158502674a90570eab0e6a814241ddab410
def8a0ab937fcf8d359fd8f4db773bf0eecc121bace11bd64c19acca914ddef0447169f4e3f9b2
5af99e1680ff8cb8a391d6
Seed = 46b82836e092da94a4eb1c291450121718159500
c = 177
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002
```

```
Result = P

P =
e31f0dd7c7ab52631a528a583359b4a21c01ed03b1cba14b806ad85ff4aef822e3ea4ac3af9574
ea0412487d0afa53f905b33d76c4987a0bf5bf1ef0575b852ae42c0574a3216628862cc719cad8
42de5869ee861efaa1aef916ee5ba12ad76ee97149cd8422911c095527d556dd13830e99bd76d0
5dd6c286bc8cd5822688d3
Q = ed928212f675f4a9881ee0f657d2c924a7e028c9
G =
0010c7cc0d56665b37e4a1160cc647d54243599e0febba57beb6e009d395f66bde5116bc821f6f
fe9ccd851b9c9056ef57c74680f3ea968209d7daf83544056d9e11d500ef8ddea29b412cb4f39b
253c6e67b5c16502db717f4d47b667848a1f5cb14d050adb7667b7c24fbcdea9192ae74bbf4ac1
ae2c227dfbe7db1db688bb
Seed = f6d57f5f1a055fada254fe759ea480d8fa42d1b2
c = 346
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002
Result = F

P =
fc602845fae0d1f7048aaea3dd5f633b69447654f24ba184a8556b2647cd95bb9accdee8ba652c
4de4170f6e278323be98af9f204465b512cc151f8944e2f54908f90fcd7424b040d70b0b94183f
890bd0154236aaacd570c239da15d91ba998144d049dc8557b7afe42d6801184368be30a4904dd
26ebb47b4e05238ccb7049
Q = 8f07df47e6f6240b96499492178acd14397355bf
G =
3a73e588e210e58bf8447739bb2235ecdd8b67915605f8a82310b2dc3d761ef9f9504387446400
3e7da4954647f858397f8561b989fe2916a98fbd77ca37db89cf884d44466594de1055c53ccb6d
5808217d5f4c76a423d84b3fb19e0093c1b65ee4456895c8f3e4459d228d4754f8165fe76abf41
da171f4e938dee2ec2fb58
Seed = 03f5fc40998f59e9a1ae9e7a113c98dc381d2ecc
c = 629
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002
Result = F

P =
cfaacdeadab66b588840516b0d86aafa1292ece8b96578277fa2367ae53e1d45359d2fc7e1a033
2a246deb01a2765654f9f5a463e4b42264e9cf3ec6aadab38c65fc0306456f3283aaa8b58d9845
8cf24e24c331da3b746f53446b84162c25a38272e4bb0544cf8feff856bba336684349a99c5508
7a3a326b6c303dda8535eb
Q = bc2888b3e820154c269fe2567bb5d8dd7f7ba36b
G =
16a5ef50ad89e194733dd08d98582030d0d0912ac6bff5d8e948797aa1b0c840d36a3ba9cd3181
d59b902e5babce642ce33897884967102ea6c0be7a2828d4e0d9127fcdf1c4ff10a3c50fd6557e
8104102e646651bce523b383f0a6a0c76269dac6cb969e51484ee44a869f21738f144de286b7a6
60e831724773ddc8044b71
Seed = d048769bd51a9d8d09a1e469a4826aa0e25b6368
```

```
c = 125
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002
Result = F

P =
d942109feb8dd72e9fd5b7f1adf87411a090a4571e261035648499f4f0b509bf093038cc8ea0ba
c7354027281d4b35c93d2e1aeb0827e8fa44b1bc33378a3c99bcc246a0a2d0ec73da3e8a608d8e
4ec90642a9d8f7c97ecd6fdd4606da4e4e31e28e58a39ab45a1f1786e2bdb1c0b2863688a133e9
7ffbdb12f4741dc75e8f89
Q = d938dcf43182f580ad974fff95c6b9c9e1683907
G =
7ad2c400c4ea6f00b077a2193e16e6e5edbb2d791d2ddb38db0dd9fe21f7a643fbed5db37b7018
c3ab54a9599180a40a3f58dffea5170ca72cf36c619ca18ee6dfe53ef006d89d5cd3d22acd7c97
6b8fbdfb8f698606145a860e23e66f2a57c990e66e51680cf0a21664378944821996a808e881d9
26f873e278c05bc3354fac
Seed = d32755fc624f9f18638b6593c918c4aa2a41a5da
c = 6
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002
Result = F
```

B.2.3 KeyPair.fax

```
#  CAVS 2.2
#  "KeyPair" information for "Demo Product"
#  Mod sizes selected: 1024
#  Generated on Thu Jul 24 12:43:25 2003

[mod = 1024]

N = 10
```

B.2.4 SigGen.fax

```
#  CAVS 2.2
#  "SigGen" information for " Demo Product "
#  Mod sizes selected: 1024
#  Generated on Thu Jul 24 12:43:25 2003

[mod = 1024]

Msg =
229a053b64fabae455a482742ec07be01f8a7feee79b549aa36a23b9e3122cdc0356b777b9e24e
43ead329e0c27aeabf035d8b3f9d7f941680e291f3ae49c362944216ef9a64538ef9d6973acc11
```

04dd6be6b670f4c2f8632a31b83f83a1398a7c6908eb3009318e29b3b2ca760b3001fd2ce9c813
ebea484a5f82e48aa1f61d

Msg =
de31e0d133db28637c41734d9c8cd1b03c905b90620a6936452605d260459f65c5fc02deb46086
836c8187934134172aef16f0642ecdacc5869139d965ec87176fbd830b158349b569d8952c303c
7b86391459fceef2094a29175b554937c210847c4da07fcdd9bf1b4f865e922c678ec4947ea0cb
02e78bd5c1538f33aeb818

Msg =
ef0974fa4832a69fe5f5d00f0d4f86da23eb5d9478a15b7c633eab5a948395aea570ae06f2c24c
b0abba3d912720b9557b8894c94cd4b884e1fad3cd7c074db9eb647d945a581c826bcffa66895a
ef037976156231113473ee4a7ef681797d9ce96f496a27fffe5f4ebd6d56da05122e423f4727d1
62b68fb1b7149f49e00da0

Msg =
9799ae10374d1a7b2b0d45f9f622e6b61ec8d86f8332148eeecfdd97edcc3ac2dfdaa9ea4b3112
a576d4fab53417f99ffe5f6e99452a71a9064f090c9f869fd5e12ab3d6663ecec324afb89543d8
ea2d2c4b463ae3cf065c96a5f38a7610d7b1c514349d307d361d6023e762cc6da2a9d114ca1a04
29bbefc75a01d81a71c99e

Msg =
bc0bc84b82cc93ff67587600a6160b0f4bee6c6fde5cf69a41c24d34db03a03df74d2f8a66360a
766c0b1bd5da64662977fc9019a4c09e1e40260080cac0ce81c51151d7619fc56057495d1215db
88311be073c4a5b8cf498aead4a864bb8666f1ff371bb92f4d26f1bc459fa0a3f88d00421d5927
691083e6b5d294f2195054

Msg =
03788f568945451dc141ac17823185d6a8d3a2b0c3c441c011a1982eaa6cb1b0fb32785175eb13
7286a2710ec9d626427a1f760c2c15af53be6dbd278b65f84be16340f0b5d84cc4946b3f2bdd54
7ccc2e05bc501c105e662745fe0bec1a48089d510ebcafd4991bd2e43df72672307faccd9d05fb
7ef30434708361375 54af1

Msg =
95eb19ec8dcd4dff898281b4b9409ca369f662d49091a225a678b1ebb75818dcb6278a2d136319
f78f9ba9df5031a4f6305eefde5b761d2f196ee318e89bcc4acebc2e11ed3b5dc458b01e6025a7
5f70c4a325308f63c5f1a16357bfeca6684286b3efe244de822e8ac8ca7f612935d8cacdea1153
dd0235e760f528ea01528d

Msg =
f98ec431f01142e19f069e58d6c95867325bf9c3a6a949625b11c128ba2243c3c7a309d4b0d7dc
4fa5008624eb22891f2c09110c128d2820141529948f5a7793186e6e5611fc9a8e7ad127020a9b
99797ef1beda3294e092eef53e3602f7be6995f5dc013a07e665c4816b395cbdf13ed01be6732e
45d98192b8ea553c807f0f

Msg =
619c4628111a605c32bf9d670b839eb764e286319897af1beca89c3a1fa22f3743261c48cba49e
0ce46769b609d2df6dd1e986f30c13ba850f1d9f034c835a5126eb81fd03f3cf22a22c1d8caf66
8d1c942f096e9396ecba1135fef8356ea648b2f45b90e18d5c671317a13225c9118c55bcf5ec53
aaad819cf5a16103eb7be3

Msg =
e44d45b0aa7b782270142fbbaf7ad38e3efb0bf32253332ca7720a48b080aa484b1fbe8188f0ef
418c589fb5e184da0a10aa89d37292e9ab43563c1bf866bfbed2cedba2b4bc9ff2323c6ed2ea47

```
f58b17fc60e8632dcee0fd1d0274ec885bdba3e406ddd5e7727d8a4904da73cb0d577a78f9fa9e
2bc912fe51c31d33f067e8
```

B.2.5 SigVer.fax

```
#  CAVS 2.2
#  "SigVer" information for "Demo Product"
#  Mod sizes selected: 1024
#  Generated on Thu Jul 24 13:16:04 2003

[mod = 1024]

P =
b26bc3fbe326f4c2cfddf9ae3e397f9ca773c300a35067c3ab492cea5910a4bc0994a9053b0d35
3c555247f0e3725be872a0711c234f6de8ace5211bc0d842d387ae835e527e4609b5c73dd600f5
f29c8430817e7b305bd5abd02f21b3d8eddb9777e47e6cccb96bddaa9604e7d4551153abba959a
a28c27d9cfadf3cf3a0c4b
Q = a45f2a270949b6fe73eb957d00f342fc7847b0d5
G =
5c571649efc8fb4bee07453b6a1df3e5ebeead1113e352e30dc02125faf0931c534ddc0d76d2fe
c2d7726469533d33bde134f25a6783e0d31cd6414d16e86c5a0795219aa3c4b9059d11cbc8c49d
001af4852aa9203cba67e5ed31b211fb1f73ec6129adc768b23f38ead987839e7e1918ddc2c35b
166dcecf889107e02ba854

Msg =
c22163ea1e1c878481a2245d2b449c1cb7817ee44e305bd61b1ed6d8fef7fb95856ad2c5188833
af736ddbec5a23c06d87c3a2c0e8dde38e071a9869ca20e0c45cb675436b29803694eeb2601b88
90fce0ad0e028ea460a616f10d215c3445b52f4f74eb7fc71720ca6dcf3fd83db3d0a886eb32aa
4b7b242fe95c8b1dfbd16f
X = 4f84f5d971c54027e956058bd32a37177d6ca62f
Y =
adcfe2d6d2dd6e9ddc6482fffcf067b6ed065d38dd1ae91b2402ab1d7e82da0372d38241b04cca
ec45ab0e0ecf19c673f2b82d3ed2bacf584550f7a962e3db2f77e2fff389fb5cee2b071af20cc2
45683841336a06976a0f44942019609744cb409e75bfd019cb8ccf2b1c578950e45bfbbd3e78bf
e69c9b9c0c9838bf02686b
R = 7c03ff0303f5659dc71fb1403d9db83784ec6858
S = 0a253a7c4a27a543a11edfe5b377114a38f38dc1
Result = P

Msg =
7105e2f27aaedd5a765c27c0bc60de958b49609440501848ccf398cf66dfe8dd7d131e04f1432f
32827a057b8904d218e68ba3b0398038d755bd13d5f168cfa8a11ab34c0540873940c2a62eace3
552dcd6953c683fdb29983d4e417078f1988c560c9521e6f8c78997c32618fc510db282a985f86
8f2d973f82351d111d6f86
X = 51db29d4e04a1e406a37242d2b1a7ff96c437332
Y =
4f654e6a3a6ab452aaad0c965c68386b298945181d75dc77d4cc5ace6180ff05195e304d13c815
54d4a3c041700367fdc75ee8b0908b07a9f2133e6e9cf5b732907af741ceceaa33e9be41b3a8c6
3b051897f6b7499547fccbf72ac095c582ee9c8fc816e4c7c0e307d3a66c596ca26c21146fad7c
47d1243c3ef12072e86b35
R = 986d3af33e7bce7258b2f774d9d07e9c97f893ec
S = 6556d6f315ed958c96139c527dfb964da834df86
```

```
Result = F

Msg =
ff20f0955c152cd30ff7d910c6c8c37f367be0c7bd061db546b85d2d6ecdbf67e540205816e0e2
6d0aa6eb7f8946f0048304f382afc90a4a72766362027885c3cb9dd8c4122568d7d81de67301e8
f051b51f91db079b0ce2d4cfd58fee5be19c7adf1fc3970d47774103d2d374d749d09473c3ba0c
a3aae5366cbd9c7ba05b5a
X = 09b42520b2ae9ded22487c5a8c917b90082e96fc
Y =
6628fbc3d5f6b65e1293c00ccc85cbd1f499437e78a03568090b5b628182ada2b5bcd8644ec494
c1eaa05f7a42d2fd7a6a94ffd28d5739891c6baca39d5485f5df6cca70c36f9073ee1b3c054009
23f3acc122250b2d24f293ff337547d1d6c52118683205f3e113c2b0255c542dfef325aee84197
77fbd3e2fc1c7860911a1e
R = 5c6ad0f0e43e2316e542ffd0f24e7e6972737f23
S = 230bab349fd181ca4c531b2053050875c1ebd470
Result = F

Msg =
0623089764ffd5501a7ebea62573daa572ec8d6facb8fede5326cb6b0e10fc4f421836e8e33231
5d8a636c85c8c82005bbd972b9deefec5625042e4d4abae1f2619fedddb3b0ec90c91cde5bc74a
1e7dfc1c958cb6762d175bfa8889b516f3508e41953f7d81ec31ff317bf0c901bc555d3e5cb0dc
54a7691b9142e8f82b18b3
X = 0a9c750dbd27c4548d36792db94f985108056d96
Y =
541b1c90eb4cc544ac1aafffc764385196ea85e78a29675fbf927fb452b860c261ffbc8d9ca3a4
c6fb67ed5a5033b98f96895be01f612d72f802fe939f74c71abe231ac1ca21a44b4cc133ed7d9e
223c3f8e4a3b6ee6ed5d2e3c582d9d177ef340712dc4f9319385b402b7785b61aa613ef8c13544
d0c4c32a170646baa3def0
R = 861a7297d773baa641baae5fb2982e099738e43a
S = 426962891625cdaeecae70403264938fddd70fd0
Result = F

Msg =
f22cd6836e04ad28495d2863cf619dc79f443c500c1c95e2c3f35af2ae1a668319c1ff5514c558
5918c95a67ed88a433ca69d17ebf55f98950c57acf631ff8f35c42a2f8865fb7b0b50c49772993
4221b690a43022bb154acf029aeb99dba35802d848d48d7bd215674d7df94c2a7c76a9df3ecffe
f7f00e87d143ae1bf66f98
X = 9c298633beeea89c8f8cfbb6cf12f17a19d8a8f6
Y =
459d1a582c7e65024ded686c330b3b0a4c0c725415048d66de1d049b0af9ee91ce2bf721294e76
18638600682750e62986b98f73f4900084cb71851a35b1e4992795a01202eed157d9c66562a46a
5233db3e297f83a2a47a71368917a64777875c28b566673ba909a17dac1d7a182a1c4c6e9b10e8
b83c6fd54ef2fb781d6e5d
R = 7f6a33f5a096715f66f8a5216ede08d97123f1f5
S = 16dada2e06014c65e23c0ecbf32fd33f2b67d1ea
Result = P

Msg =
7fef236d9016e7b72e0307e730871b02186cdeaa8a103de80353ae28c7b3c3851bb6ff47b589e8
aa71e65de2453a2a5b7708da450d88cd5086958ab4c7c6557558da05e5d059106a8e78e881aa3d
8a032be553a87b8316c918e96d6a8bcb4c779e22dc4ecacf867eef814dce48d862829dcbf2d9ba
4743da2118ff50fc0dd014
X = 9cb534327127e02ad61407a39e9101ced4b2f3f5
```

```
Y =
b1a4645004b16906846a0e85435ac77b29f20c145d0a1b821fed7cacedc2ef869e540868b79a34
2e35bdb70e6a50338e5c3c689e9fca8661b621e3ebfde64880130fa20add5535448f2e71a5a00c
c31ad837f514c01773db03050364fa83491a9fcaf8d3092c953513a54a7a3fee14a34852a8845e
b85ef0bbd86d85a0a3a271
R = 010aaefbd84d0c70ad0ba2c12a0037516c0da5d1
S = 18d76c91c66c9f0a5cb4bc37687c8ec426e4cd38
Result = P

Msg =
824e7fdceb7cf8a62a27049f2e8eb61852b2d74a3db0e647064d5d319cd336aa661cae8b26ec49
d9238416f58773341206b095ecc0e602b8690f5f56a74431cebbd35dfa649332800074aa04f55a
ed9b4f2c1782ab273b105379a8e9aa0b6b75cb9e15906d19be830a21493340ebea99774ee672c4
1d9a380db3bf506ecfec85
X = 5307513d5836600db926c707b51042f180ce3bba
Y =
6aad60071209228ad00f19f5bf67d36f6294822fa6f2828e8a90bea48f8a76484b6f342c77c126
839e57578d949a5fc7fe4d6022215cbdba980ec6fc49372a96ff22d1d4eccf3e2153ccb201b2b2
1dbb7e2ab8cf3722bef2e3d83e63da5ccc9fc4ea99e13fa9847c8b8eed0e1814afb23c4d14c78e
597cfa03ff721961633602
R = 3afaf03cacb83c87abe7e62bc82cb3274a434b4d
S = 34a8e5b9041e396e5fc5539ae1873da8502b9c51
Result = F

Msg =
7e34ce3fe304a910851aad715edfb0ae16a6cc47bf8db5f4c2a449e719526951bff4082765c681
2667072e15fe58364ab766a66f24c8c486d12ba02b79aceb197a850cf087ec71369d38239b3846
9e81c61bdfbb5ccabe95a8987e15275fa38197300321b03c20460ff5b58c73708f5b2b0e9eb4cf
5b4c2a2f360d2e89333890
X = 07301f3826ba2d5f6c78907cd331de2071b1b660
Y =
adf79fe12af9954ca699830984ad88ce4d7bd3321c0eec9e870898ef622c99f24cfb23ccf401e3
76a7667cf718ffd648add9a688c0e841025cd1e1d941a2cfda6f5e534c5bda2ea1979119952b3e
4b1ac4b6fdf1669e119a074ffbbb7badcdc9a4110501d49b69022c52318dc06e934a78e5fedf7a
58dec2556e8c052154a9cb
R = 841fb9aa6d648be24698688017d1bf530ceb1ee1
S = 9f54ed100dfe791e6fbcf60af43baf5c6e5452c3
Result = F

Msg =
d8e745e683201b24ce6fdd1497877fae8ab23526957386b69f6aa29d7779f5680a25fc70da3f58
a4abc321887f007c7ec5f97045ce0cf5bf80d14ef74e4599626828a5652ea30318eb2e604ac0b1
12c5dee9f0d2f80e6700f9b3ca22f2edea9756b7e7ce69954508f678426040e267093c4a5ed8fd
c2030270d7bd2649b90f8e
X = 4846f984b5d768c030ef0a4f3f0af4fd1d57b8ed
Y =
122e8c7f13b04d71718bf0eea9fe17572034235b845d5ae8eba4fd422becc9fcc41ba364b0e40e
219922acefe2dcbd73f881b30be44fd1d5473f3ac7e2a9cb1b8fe08d43c03e60ad73d50de1caf2
dd5c578d5a0f60e291e02d4fae9aeeaa79e985f6d42ed323e2ec7cd3a646132f23081691e0f587
eec08bd307f3972a8ab71b
R = 74e86a4068a9ce65ce99fc4eaa1a24bcd70129f6
S = 02d27e752a0f944d1077a05d9408c1bc7be05035
Result = F
```

```
Msg =
1a7bdbe63042aa48e3ddf83e9b2800aff361d7e45f393a3d122a8a221f0a153ddee197e691f801
df47327842019fa1b7144f1ceace644e3d5c6b64baebed944b0e40a62d60a3b4a26a8b2ee6c737
2065858ab82bcf1a039cc985f765bc04b6b2734211a2e56e4bf7148e20133417062010bbb38eaa
83dfc2211d4b0cd87702da
X = 28510f6b50470f8195890e00f982d4000480a0ad
Y =
83f88edf6e9b00c5597f3563fdae5c9e3250acbe71031bc97d765979080018e54de8a263dfc5e4
972e8b5588d1b11dd8722b850ab2936d0d5bf2092c2be1ae73eae9a988df46baeeeb27407d7db9
0013bd7ed4fbbe06926bd33a0871a8a11730d6c36494498b2bbe0586b8ad900bac6c916c4259c6
d7db3b8dd22e0be4d7e497
R = 784f49131670f16335bfa108fdba56e6f41d1256
S = 9b3e19e9f907cb960a8136390ddfbc3ab5af81bb
Result = P

Msg =
6c31d64162866fe46adb6d37cbeaedf03239afe1fb4b77cdac17b27bc2b95d08b168238126a8c5
b28fc0bf38dd6f29de88dbdb26d4cad4255414dd94ac5969259aefc013381e5cfd7b9093f40003
77d30841fbcec152574ec7f0adfdea3bec1c32aef51d2052fc6e37313193bb0ea077b953560447
4bc6f10d916bdb04c9ae98
X = 6214effbc9269a93a1781ba4b38d781434ef9c90
Y =
82acae44b80f579e329e0048f025b86008f1add053fbcdaaf60283eb7c13346b15ed1dd76a6751
dc5f2d3f67ce1edd6f92134b32d1f09ca53a4be79838c2337f7140768d08b49016f6a3f7f2cbd3
85c47dc9609a63a0142019a5b275ee73779ea2bfabc60960c1b141c7638104f0579bf355202bd1
cd5942498876720e3604d8
R = 2f6fa9ef0d930edf62c653593171091cbd128408
S = 9cae316ef7e6fc510244dccde3b1b758444f2547
Result = P

Msg =
2c40089472c5ba01ee4e62777828b13c5357232a032177525ed162e5e6b5845556699bb77b57f7
6c457f2e001e7410527aa7ddf5b0e8b6d7082a52201587f25d458497deb695725c4be49ce0004e
07df7aaeb5aae35f2706f4fc1916536a6c82201964d2ca86131b280515dec5bd7e2d7bf4110f43
8db3264bce1f8f4967da0a
X = 1274fe0c701d44abe966859fefbef2b46c453028
Y =
895c491e2d1721a8f8d3b733c49bf21cc0f3bad53d027295a0a82f53d068cbcac947e3245de447
a4af29535e38c229a637c50dd96cb44a288270c10073d9160672a91cc89ea1bb5028dc1b1a5b0a
a7136e58a94ae039b5691eaf6d094e5763f852c41d4124e53825c6b2a09b4b55f3d88a8af3bfe4
52c3402a188d211fb15e84
R = 03be2b2085a8e8e00d858f9f5f82ba3bb3f7c86a
S = 512836b807cda24170a9ab274e246095715cc39c
Result = F

Msg =
ad1814037d6fea331b4e61d46527f30b3f5c476d3755fbb868d1a0c19d7906aebabbba6558d5ce
45b030d813baf03d3796c9b0282a14f5250d22eb26a3d0c9128a5ba832357642e6d79af996839e
1bec9187644043a1c454a9cf6342c11fe3b2e3a1e5505c7ace7e5a34cb4508581292f93f6b9fca
25efaf037f10fe3f8edaf8
X = 273fdb7748a3d2945536ac8c905875e60b8d78b0
Y =
87a01d390c5ec7a16fcee02c7546d8930e36bc32396c9acad1b5aa119e756c1b07d1ffb0b9ec93
2d9c8be862efdff1ace9117aa33affd34592cd4d16ef270fab365c8ee84856d59b21f2316409a7
```

```
e77b83f92ce87af9ee0e45341faf25271c61193205e2f1fa6dee0abe7960b9721d16e2a794d234
816444ae5d48ea464dcd2b
R = 64d2bdbb07b17251e7530c5710d7036a408149f2
S = 364a1e248e52831a69354f7da2deedfaae2933d6
Result = F

Msg =
f904909092b63b8ee6193d48b5f60af8a273fe1698e7e7cb66edc4aaacb8cc9bfba6b217381728
9b417fa256d3ba5c25aca09ec2ecda3f39c1f4689b43b29af59da8f2836e05ac226fb0e7045596
a7a7f9422008b6ae32141258305fa199e5182732d93dfd28d00bb6d394b90131f465d1800d4fbc
0bc845a144a45e8e13b6eb
X = 4153440b55248dbe7736863e0c999a445795e015
Y =
7e0a22d0acd91fade061554386b872e50649b311b08f21e00818bbd4d28ef26593d288cf9be0b3
843ae8499f84ac715df901edf2dcab934264e5c3479622823a44ecfeb3ab29cf09bc8d20440664
e7becd77e91dd66f51c718fe94d59b713146ad1ae98a889e88268a222fba616e846f5d6a5bf85c
b82ca20a1fe9ffb326b787
R = 0f49a52484ea14590f8791346bf83decb3a6452d
S = 661c938cca562c507f1212aa5c53cca19d516133
Result = P

Msg =
6a9f368060b44b7eefadb19ed951dd13d68be13136773525c7bdb8e4f91ef261404c9c03baff62
561245e701a4190af8e23868f2f630211ea9bae0118349150333e3853c323005c9a4d182737ff2
45f2ee23755df863dee55d7ef0c3c09a0b6f0b0cfa131070bd3f6cf88bdeb1041769c4f3135a83
39f2e4abb2f3e1f9375b0c
X = 405d1ccae2bc08d990c4b9357e530e0cfc25a6f1
Y =
38afc7afc91e47a2034981feb5428ecd9623896d27e2ebab72e6567626f9b8035892735d3db6c5
edb23b6d9147f60578f1bfe3996d47f2a8a9d957849740e7bb6988a1ddd6de32687a1777db6849
aab03cb10b0be63b32f86aebc87e84981434c6a72410d845e95975c803b786278e41bbcb79bc70
f25401a6088c609eb2ddbc
R = 9bedecdd7df5af52f6ee3a730f502a5a82076ccb
S = 442982810fcbf663b62a11eb8e0d8345358d1725
Result = P
```

B.3 Examples of *RESPONSE* Files

B.3.1 PQGGen.rsp

```
#  CAVS 2.2
#  "PQGGen" information for "Demo Product"
#  Mod sizes selected: 1024

[mod = 1024]

P =
d3aed1876054db831d0c1348fbb1ada72507e5fbf9a62cbd47a63aeb7859d69214adeb9146a6ec
3f43520f0fd8e3125dd8bbc5d87405d1ac5f82073cd762a3f8d774322657c9da88a7d2f0e1a9ce
b84a39cb40876179e6a76e400498de4bb9379b05f5feb7b91eb8fea97ee17a955a0a8a37587a27
2c4719d6feb6b54ba4ab69
Q = 9c916d121de9a03f71fb21bc2e1c0d116f065a4f
```

G =
8157c5f68ca40b3ded11c353327ab9b8af3e186dd2e8dade98761a0996dda99ab0250d3409063a
d99efae48b10c6ab2bba3ea9a67b12b911a372a2bba260176fadb4b93247d9712aad13aa70216c
55da9858f7a298deb670a403eb1e7c91b847f1eccfbd14bd806fd42cf45dbb69cd6d6b43add2a7
8f7d16928eaa04458dea44
Seed = 0cb1990c1fd3626055d7a0096f8fa99807399871
c = 98
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002

P =
f5c73304080353357de1b5967597c27d65f70aa2fe9b6aed1d0afc2b499adf22f8e37937096d88
548ac36c4a067f8353c7fed73f96f0d688b19b0624aedbae5dbb0ee8835a4c269288c0e1d69479
e701ee266bb767af39d748fe7d6afc73fdf44be3eb6e661e599670061203e75fc8b3dbd59e40b5
4f358d0097013a0f3867f9
Q = f8751166cf4f6f3b07c081fd2a9071f23ca1988d
G =
1e288a442e02461c418ed67a66d24cacbeb8936fbde62ff995f5fd569dee6be624e4f0f9f8c809
3f5d192ab3b3f9ae3f2665d95d27fb10e382f45cd356e7f4eb7a665db432113ed06478f93b7cf1
88ec7a1ee97aec8f91ea7bfceaf8b6e7e5a349c4ad3225362ef440c57cbc6e69df15b6699caac8
5f733555075f04781b2b33
Seed = 34b3520d45d240a8861b82c8b61ffa16e67b5cce
c = 622
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002

P =
c6c6f4f4eed927fb1c3b0c81010967e530658e6f9698ebe058b4f47b2dc8fcbc7b69296b9e8b6c
f55681181fe72492668061b262b0046a0d409902e269b0cb69a455ed1a086caf41927f5912bf0e
0cbc45ee81a4f98bf6146f6168a228aec80e9cc1162d6f6aa412efe82d4f18b95e34ab790daac5
bd7aef0b22fa08ba5dbaad
Q = d32b29f065c1394a30490b6fcbf812a32a8634ab
G =
06f973c879e2e89345d0ac04f9c34ad69b9eff1680f18d1c8f3e1596c2e8fa8e1ecef6830409e9
012d4788bef6ec7414d09c981b47c941b77f39dfc49caff5e714c97abe25a7a8b5d1fe88700bb9
6eff91cca64d53700a28b1146d81bad1212d23180154c95a01f5aeebb553a8365c38a5ebe05539
b51734233776ce9aff98b2
Seed = b6ec750da2f824cb42c5f7e28c81350d97f75125
c = 185
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002

P =
b827a9dc9221a6ed1bec7b64d61232aacb2812f888b0a0b3a95033d7a22e77d0bff23bfeed0fb1
281b21b8ff7421f0c727d1fb8aa2b843d6885f067e763f83d41fd800ab15a7e2b12f71ec2058ee

```
7bd62cd72c26989b272e519785da57bfa1f974bc652e1a2d6cfb68477de5635fd019b37add656c
ff0b802558b31b6d2851e5
Q = de822c03445b77cec4ad3a6fb0ca39ff97059ddf
G =
65a9e2d43a378d7063813104586868cacf2fccd51aec1e0b6af8ba3e66dee6371681254c3fb5e3
929d65e3c4bcd20abd4ddc7cf815623e17b9fc92f02b8d44278b848480ffd193104cf561263951
1e45bd247708ff6028bd3824f8844c263b46c691f2076f8cd13c5d0be95f1f2a1a17ab1f7e5bc7
3500bac27d57b473ba9748
Seed = cd2221dd73815a75224e9fde7faf52829b81ac7a
c = 62
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000002

P =
898a8d93e295c8ef2ffd46976225a1543640640d155a576fafa0be32136165803ba2eff2782a2b
e75cc9ec65db6bd3238cca695b3a5a14726a2a314775c377d891354b3de6c89e714a05599ca041
32c987f889f72c4fe298ccb31f711c03b07e1d98d72af590754cf3847398b60cecd55a4611692b
308809560a83880404c227
Q = c6d786643d2acfc6b8d576863fda8cfbfbd5e03f
G =
2fd38b8d21c58e8fb5315a177b8d5dc4c450d574e69348b7b9da367c26e72438daf8372e7f0bee
84ef5dcbbc3727194a2228431192f1779be24837f22a0e14d10d5344da1b8b403df9f9b2655095
b3d0f67418ed6cd989f35aa4232e4b7001764fbe85d6b2c716980f13272fc4271ac1e234f7e24c
023cfc2d2dc0aa1e9af2fb
Seed = 73483e697599871af983a281e3afa22e0ed86b68
c = 272
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000002
```

B.3.2 PQGVer.rsp

```
#  CAVS 2.2
#  "PQGVer" information for "Demo Product"
#  Mod sizes selected: 1024

[mod = 1024]

P =
bc72aacb599a1301b4260b620f3391046cc8719291b7259f7d2f1d57942e0400bdf145a2cac51a
b15c27fa217f09aa3fd84d2f4742f786717a5d8089564e03e6224b05bb3f52f8a9775f1f2d8d48
6dc9d3bff78650e22df40d7c070d36d971816aa904d81ef90aed42332679b84b5f75baf069293b
ea3fda832c6eb342002701
Q = df0e3c75a268319201c6b309aa666db1f046888d
G =
a5d2ca30330f66e0fb5fda4bccf32922305852d1724f2dd10d7363e660395f67e8d10ddad970ca
bf42046f58bfce3aad4a9549ddac9c0e00a3458c4d9158502674a90570eab0e6a814241ddab410
```

```
def8a0ab937fcf8d359fd8f4db773bf0eecc121bace11bd64c19acca914ddef0447169f4e3f9b2
5af99e1680ff8cb8a391d6
Seed = 46b82836e092da94a4eb1c291450121718159500
c = 177
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002
Result = P

P =
e31f0dd7c7ab52631a528a583359b4a21c01ed03b1cba14b806ad85ff4aef822e3ea4ac3af9574
ea0412487d0afa53f905b33d76c4987a0bf5bf1ef0575b852ae42c0574a3216628862cc719cad8
42de5869ee861efaa1aef916ee5ba12ad76ee97149cd8422911c095527d556dd13830e99bd76d0
5dd6c286bc8cd5822688d3
Q = ed928212f675f4a9881ee0f657d2c924a7e028c9
G =
0010c7cc0d56665b37e4a1160cc647d54243599e0febba57beb6e009d395f66bde5116bc821f6f
fe9ccd851b9c9056ef57c74680f3ea968209d7daf83544056d9e11d500ef8ddea29b412cb4f39b
253c6e67b5c16502db717f4d47b667848a1f5cb14d050adb7667b7c24fbcdea9192ae74bbf4ac1
ae2c227dfbe7db1db688bb
Seed = f6d57f5f1a055fada254fe759ea480d8fa42d1b2
c = 346
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002
Result = F

P =
fc602845fae0d1f7048aaea3dd5f633b69447654f24ba184a8556b2647cd95bb9accdee8ba652c
4de4170f6e278323be98af9f204465b512cc151f8944e2f54908f90fcd7424b040d70b0b94183f
890bd0154236aaacd570c239da15d91ba998144d049dc8557b7afe42d6801184368be30a4904dd
26ebb47b4e05238ccb7049
Q = 8f07df47e6f6240b96499492178acd14397355bf
G =
3a73e588e210e58bf8447739bb2235ecdd8b67915605f8a82310b2dc3d761ef9f9504387446400
3e7da4954647f858397f8561b989fe2916a98fbd77ca37db89cf884d44466594de1055c53ccb6d
5808217d5f4c76a423d84b3fb19e0093c1b65ee4456895c8f3e4459d228d4754f8165fe76abf41
da171f4e938dee2ec2fb58
Seed = 03f5fc40998f59e9a1ae9e7a113c98dc381d2ecc
c = 629
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002
Result = F

P =
cfaacdeadab66b588840516b0d86aafa1292ece8b96578277fa2367ae53e1d45359d2fc7e1a033
2a246deb01a2765654f9f5a463e4b42264e9cf3ec6aadab38c65fc0306456f3283aaa8b58d9845
```

```
8cf24e24c331da3b746f53446b84162c25a38272e4bb0544cf8feff856bba336684349a99c5508
7a3a326b6c303dda8535eb
Q = bc2888b3e820154c269fe2567bb5d8dd7f7ba36b
G =
16a5ef50ad89e194733dd08d98582030d0d0912ac6bff5d8e948797aa1b0c840d36a3ba9cd3181
d59b902e5babce642ce33897884967102ea6c0be7a2828d4e0d9127fcdf1c4ff10a3c50fd6557e
8104102e646651bce523b383f0a6a0c76269dac6cb969e51484ee44a869f21738f144de286b7a6
60e831724773ddc8044b71
Seed = d048769bd51a9d8d09a1e469a4826aa0e25b6368
c = 125
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000002
Result = F

P =
d942109feb8dd72e9fd5b7f1adf87411a090a4571e261035648499f4f0b509bf093038cc8ea0ba
c7354027281d4b35c93d2e1aeb0827e8fa44b1bc33378a3c99bcc246a0a2d0ec73da3e8a608d8e
4ec90642a9d8f7c97ecd6fdd4606da4e4e31e28e58a39ab45a1f1786e2bdb1c0b2863688a133e9
7ffbdb12f4741dc75e8f89
Q = d938dcf43182f580ad974fff95c6b9c9e1683907
G =
7ad2c400c4ea6f00b077a2193e16e6e5edbb2d791d2ddb38db0dd9fe21f7a643fbed5db37b7018
c3ab54a9599180a40a3f58dffea5170ca72cf36c619ca18ee6dfe53ef006d89d5cd3d22acd7c97
6b8fbdfb8f698606145a860e23e66f2a57c990e66e51680cf0a21664378944821996a808e881d9
26f873e278c05bc3354fac
Seed = d32755fc624f9f18638b6593c918c4aa2a41a5da
c = 6
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000002
Result = F
```

B.3.3 KeyPair.rsp

```
#  CAVS 2.2
#  "KeyPair" information for "Demo Product"
#  Mod sizes selected: 1024

[mod = 1024]

P =
ccf7b0a36b0df61a2bf53035483388d36e9fc23db23ca1bf0a0d93b62b0a97b2e0343964a49b34
ef57f934ab39a5f2d299a4648d953cfa52fe33473b313e80103b8d2adaf0678185ac54c53cf9fe
11d0fec944a9deabc516d9861f0b1247bc3ad239e5406cb25fa59d671c707bd3674c6ec65ae211
a1e7a5f1539c885f2d22e5
Q = b544b62236cfd5dc0d9327bd4f24b4f422ea26ab
```

G =
874ab129ee314470b57938fb35633a09de78b49283ab1137e5b2288f79737f57e80cbbe4d3d147
4b088be975af979bf0ae9619da55da924937d8009a10010f5f28443a03499d2fc98d164dd6fc40
23f71f6f669398d8685bca4141c8e0058b5f756d6b9e359bea59aa9bbac2ab31cbfaff19897ff4
de5e4b9b9a345bcd03b226

X = 60c6b08a425639e5bffc0cfaee5612fa05021b53
Y =
31950d5f761d5bb8438812704c73c1679bd33fa62426fdc1bc422df96ef5f7689d77adcc2c00cc
9dd58df02fde37424d03e5e2c8cab0d871f7e524a7723b23a737c3c0ee4f3fcc49b8c04e9b6722
2e8fe584d684e2c22ce2c7e726d11a68fbe17f749ea3977c12100a0ef0e2bb6f5301de29893b4f
7044e328fc4996e254d5f8

X = 175a0b9bf057fd24c63849cfeeec21b7c97efea8
Y =
1a5193f9b4c2ff711b87190b2a20594746e15ac872503dc226b5acdd9b3c355231c2c9f91cdfa9
f69d8ec0b9bdcd0758eb8fae6a98f4b7988e531d9b8ccb093664f6ddccf222ea0ef9c9a4ab6d64
7dfc7c6226ea40d694bfd091104f1e01208acac305c9cf73ad4947815810602 9db0f6ab5218292
85971b6ea292f35d05f1ae

X = 705eef1e17f975731a2b6ef4f1e29eb514dacb00
Y =
c5249c90a4611ed04f12d6e696e7afbca6a6a8ea69125ec39bbd834d3210d17df08f50c1f2d841
ac8d1be587a3a19e102463de4035358960a702b3cb82c4d34ae89d644b943fd1081816f12648fe
e41c54d0dff51133438e8703ed6a490dd444d6ed6f7acb6e75f82b2614d0c9a407231c9d1441c5
1882570add2fbdaa15aeff

X = 25143a093ddb9799b916f64717972f9f0b9c1e32
Y =
190ba0fc9381fb5010bace3612d5f36b1d5dfaaa43ae675e4eaf0f86587bd4c2a5539330eb2f5a
ff8f0cfb852f2e6b75cba3326f7d47ab47df75b099f73423ba7db0d8874992cd7234f8993cf204
dc17ea8a7f58dab0a66b3615756b444d2eef910132fa7506720d52798a8fdbcb56771c60d4a87d
de3a90ea78a453c2838f55

X = 18ebbeff4efd1c167c5d9b7b5e062945e3e99fb1
Y =
5840ce185ded8bc049fa629ec92ff66c30e5fb908e3c0d4efc0d0249dcdc4bc024bddd1eea7d8c
835b53ec61f0bb81733c83a5fb79352e34af95e239d6aaa943946b8b4cd620609ee3203f26f5ff
f6c7756e138847b0661debc0469d500aef9f5a21969aa4fb6ac9fec944179d4f0e7cd9b0ca4c5a
9f6be57bf88551f985a26e

X = 8d87638ada9c12d9a84c86655488bcaa88ae8630
Y =
9f5a744ffd20330250717c94322a6fd39602288cbbc833bef0128d98e9511533e6a653fb293ca9
7f56eb2b4bb6f6ff7d269e6e0b7170a9c2ae9339fb29355dc0e6274acb794ebdc0365c61c2bcc6
3a2b5fc17ebf84c5ebde89c4601a73e3400c020f9a42e142e862c66da94049c09a4c4c6bf0123c
c996da3092a5f89c95691f

X = 404f46feb08247a3cca3a9d1ccdefa503636651f
Y =
a3bbf4674a9d08d74acd874d7d120371035464fd0e6801c6bd8d03ecd7a34551b72599e6479e67
c6badb227cf78fd988ab3187197bbd2e438da6d6cc434294fad1ed9ccc150241d739cf1fa57c1a
c97ff5e854834619fc1502e5bd0932eb84b89f875cd3a938950c48aa55623a45697791e2e17137
64d49d6fc4bcae653cf2c7

```
X = 623f9ef6550b4e80b89f0b26057fe92b1b56603c
Y =
74fffa8568d6c35d473e7e7e441303bf6d2244766800c328a15ed9522363b5274650f2e4df63ae
a7ec07ec6e4c76076e3974d077ecf7da30a56ea268e3e3af3c36387c69459301adbf184f2794f4
59aecc8a03f1778b2b908775b6bb2c21c7e6f4661e964b0e6c99803c184317c4c68cd45c7283d8
0ddf7d968a32455b7117d1

X = 2d85c0c090a9d0d5a8eb53ee82cbe59284a1fefa
Y =
9a54a6084140984105391f642995fcd74053050b7b2ba436e2c533d6ea99bfc5fe90063c751973
7a2dd40562b91ea255e6a1538b22860b964c78531347d377901a871aeb2747327048949276ff48
07f679235608c3006cd5d412ab0e1948abdbb67634d2bdf78f868032e126014bc07cc4f621ba4c
026a4f1e7ff425ec44d17c

X = 786e7175e724ebb367af639512723e215296d1e2
Y =
5b244e39bc965c1dec463be5f56e057fbb9e833ea3d816050f00e4ae839ba0fad99106ee33c719
e0c9c415a7d5a82306b2642316a701a4d65f82d4f7bd99305f6d02e193ffc7af1851b0c524ca41
908d640f07d4f221accf930e6d1167765b376b8c99100b71ad4f5b272f1f1a7366a79a4c72eda8
1e8ad63c48a3e6df4b98c9
```

B.3.4 SigGen.rsp

```
#  CAVS 2.2
#  "SigGen" information for "Demo Product"
#  Mod sizes selected: 1024

[mod = 1024]

P =
ccf7b0a36b0df61a2bf53035483388d36e9fc23db23ca1bf0a0d93b62b0a97b2e0343964a49b34
ef57f934ab39a5f2d299a4648d953cfa52fe33473b313e80103b8d2adaf0678185ac54c53cf9fe
11d0fec944a9deabc516d9861f0b1247bc3ad239e5406cb25fa59d671c707bd3674c6ec65ae211
a1e7a5f1539c885f2d22e5
Q = b544b62236cfd5dc0d9327bd4f24b4f422ea26ab
G =
874ab129ee314470b57938fb35633a09de78b49283ab1137e5b2288f79737f57e80cbbe4d3d147
4b088be975af979bf0ae9619da55da924937d8009a10010f5f28443a03499d2fc98d164dd6fc40
23f71f6f669398d8685bca4141c8e0058b5f756d6b9e359bea59aa9bbac2ab31cbfaff19897ff4
de5e4b9b9a345bcd03b226

Msg =
229a053b64fabae455a482742ec07be01f8a7feee79b549aa36a23b9e3122cdc0356b777b9e24e
43ead329e0c27aeabf035d8b3f9d7f941680e291f3ae49c362944216ef9a64538ef9d6973acc11
04dd6be6b670f4c2f8632a31b83f83a1398a7c6908eb3009318e29b3b2ca760b3001fd2ce9c813
ebea484a5f82e48aa1f61d
Y =
31950d5f761d5bb8438812704c73c1679bd33fa62426fdc1bc422df96ef5f7689d77adcc2c00cc
9dd58df02fde37424d03e5e2c8cab0d871f7e524a7723b23a737c3c0ee4f3fcc49b8c04e9b6722
2e8fe584d684e2c22ce2c7e726d11a68fbe17f749ea3977c12100a0ef0e2bb6f5301de29893b4f
7044e328fc4996e254d5f8
```

```
R = 968f4f98a550af1aef4b763a5bbf8b84dc579fc8
S = 7784c9efda43b1e5bf72344b63bcf610024ca285

Msg =
de31e0d133db28637c41734d9c8cd1b03c905b90620a6936452605d260459f65c5fc02deb46086
836c8187934134172aef16f0642ecdacc5869139d965ec87176fbd830b158349b569d8952c303c
7b86391459fceef2094a29175b554937c210847c4da07fcdd9bf1b4f865e922c678ec4947ea0cb
02e78bd5c1538f33aeb818
Y =
1a5193f9b4c2ff711b87190b2a20594746e15ac872503dc226b5acdd9b3c355231c2c9f91cdfa9
f69d8ec0b9bdcd0758eb8fae6a98f4b7988e531d9b8ccb093664f6ddccf222ea0ef9c9a4ab6d64
7dfc7c6226ea40d694bfd091104f1e01208acac305c9cf73ad49478158106029db0f6ab5218292
85971b6ea292f35d05f1ae
R = 56ee3ad274d1c5a2796153b251de256c2837cb8d
S = 964701374856c62ece7de4c6acbfef473182ed64

Msg =
ef0974fa4832a69fe5f5d00f0d4f86da23eb5d9478a15b7c633eab5a948395aea570ae06f2c24c
b0abba3d912720b9557b8894c94cd4b884e1fad3cd7c074db9eb647d945a581c826bcffa66895a
ef037976156231113473ee4a7ef681797d9ce96f496a27fffe5f4ebd6d56da05122e423f4727d1
62b68fb1b7149f49e00da0
Y =
c5249c90a4611ed04f12d6e696e7afbca6a6a8ea69125ec39bbd834d3210d17df08f50c1f2d841
ac8d1be587a3a19e102463de4035358960a702b3cb82c4d34ae89d644b943fd1081816f12648fe
e41c54d0dff51133438e8703ed6a490dd444d6ed6f7acb6e75f82b2614d0c9a407231c9d1441c5
1882570add2fbdaa15aeff
R = 8ca6fa81bb037bb9ba7439714e61720478fadef0
S = 860a6f022b4e8ff718df1207bbf8d633b2bf2c86

Msg =
9799ae10374d1a7b2b0d45f9f622e6b61ec8d86f8332148eeecfdd97edcc3ac2dfdaa9ea4b3112
a576d4fab53417f99ffe5f6e99452a71a9064f090c9f869fd5e12ab3d6663ecec324afb89543d8
ea2d2c4b463ae3cf065c96a5f38a7610d7b1c514349d307d361d6023e762cc6da2a9d114ca1a04
29bbefc75a01d81a71c99e
Y =
190ba0fc9381fb5010bace3612d5f36b1d5dfaaa43ae675e4eaf0f86587bd4c2a5539330eb2f5a
ff8f0cfb852f2e6b75cba3326f7d47ab47df75b099f73423ba7db0d8874992cd7234f8993cf204
dc17ea8a7f58dab0a66b3615756b444d2eef910132fa7506720d52798a8fdbcb56771c60d4a87d
de3a90ea78a453c2838f55
R = 74db5576c05bc801b2999522096524ef6a283a0a
S = 0673abe617c698a0cff4a514d2f59f5cb4ff52a9

Msg =
bc0bc84b82cc93ff67587600a6160b0f4bee6c6fde5cf69a41c24d34db03a03df74d2f8a66360a
766c0b1bd5da64662977fc9019a4c09e1e40260080cac0ce81c51151d7619fc56057495d1215db
88311be073c4a5b8cf498aead4a864bb8666f1ff371bb92f4d26f1bc459fa0a3f88d00421d5927
691083e6b5d294f2195054
Y =
5840ce185ded8bc049fa629ec92ff66c30e5fb908e3c0d4efc0d0249dcdc4bc024bddd1eea7d8c
835b53ec61f0bb81733c83a5fb79352e34af95e239d6aaa943946b8b4cd620609ee3203f26f5ff
f6c7756e138847b0661debc0469d500aef9f5a21969aa4fb6ac9fec944179d4f0e7cd9b0ca4c5a
9f6be57bf88551f985a26e
R = 5ad7e790eb62c8327c418de9c455fa8a97df80e9
S = 582baab03912f4d54c6b819e8fd30cbeeaf930dc
```

```
Msg =
03788f568945451dc141ac17823185d6a8d3a2b0c3c441c011a1982eaa6cb1b0fb32785175eb13
7286a2710ec9d626427a1f760c2c15af53be6dbd278b65f84be16340f0b5d84cc4946b3f2bdd54
7ccc2e05bc501c105e662745fe0bec1a48089d510ebcafd4991bd2e43df72672307faccd9d05fb
7ef3043470836137554af1
Y =
9f5a744ffd20330250717c94322a6fd39602288cbbc833bef0128d98e9511533e6a653fb293ca9
7f56eb2b4bb6f6ff7d269e6e0b7170a9c2ae9339fb29355dc0e6274acb794ebdc0365c61c2bcc6
3a2b5fc17ebf84c5ebde89c4601a73e3400c020f9a42e142e862c66da94049c09a4c4c6bf0123c
c996da3092a5f89c95691f
R = 603c901b5a2cf537966bb9c69016732f371f90ba
S = 988a8937c01b1b5005b46406c6596a165dfebdcc

Msg =
95eb19ec8dcd4dff898281b4b9409ca369f662d49091a225a678b1ebb75818dcb6278a2d136319
f78f9ba9df5031a4f6305eefde5b761d2f196ee318e89bcc4acebc2e11ed3b5dc458b01e6025a7
5f70c4a325308f63c5f1a16357bfeca6684286b3efe244de822e8ac8ca7f612935d8cacdea1153
dd0235e760f528ea01528d
Y =
a3bbf4674a9d08d74acd874d7d120371035464fd0e6801c6bd8d03ecd7a34551b72599e6479e67
c6badb227cf78fd988ab3187197bbd2e438da6d6cc434294fad1ed9ccc150241d739cf1fa57c1a
c97ff5e854834619fc1502e5bd0932eb84b89f875cd3a938950c48aa55623a45697791e2e17137
64d49d6fc4bcae653cf2c7
R = a61477d177de4c72dd17b4860e57277713e833b5
S = 5e4e1479791dd206bc5cb974085ac2bd585c4553

Msg =
f98ec431f01142e19f069e58d6c95867325bf9c3a6a949625b11c128ba2243c3c7a309d4b0d7dc
4fa5008624eb22891f2c09110c128d2820141529948f5a7793186e6e5611fc9a8e7ad127020a9b
99797ef1beda3294e092eef53e3602f7be6995f5dc013a07e665c4816b395cbdf13ed01be6732e
45d98192b8ea553c807f0f
Y =
74fffa8568d6c35d473e7e7e441303bf6d2244766800c328a15ed9522363b5274650f2e4df63ae
a7ec07ec6e4c76076e3974d077ecf7da30a56ea268e3e3af3c36387c69459301adbf184f2794f4
59aecc8a03f1778b2b908775b6bb2c21c7e6f4661e964b0e6c99803c184317c4c68cd45c7283d8
0ddf7d968a32455b7117d1
R = 882f1e36f4c54d981c45a2b28df96766814ab913
S = 542071ae6a82d97de62fd156e95b414f459b2d25

Msg =
619c4628111a605c32bf9d670b839eb764e286319897af1beca89c3a1fa22f3743261c48cba49e
0ce46769b609d2df6dd1e986f30c13ba850f1d9f034c835a5126eb81fd03f3cf22a22c1d8caf66
8d1c942f096e9396ecba1135fef8356ea648b2f45b90e18d5c671317a13225c9118c55bcf5ec53
aaad819cf5a16103eb7be3
Y =
9a54a6084140984105391f642995fcd74053050b7b2ba436e2c533d6ea99bfc5fe90063c751973
7a2dd40562b91ea255e6a1538b22860b964c78531347d377901a871aeb2747327048949276ff48
07f679235608c3006cd5d412ab0e1948abdbb67634d2bdf78f868032e126014bc07cc4f621ba4c
026a4f1e7ff425ec44d17c
R = 34eaca76bb704ef7f0a11769e266f22f65b1e4bf
S = 5bfee09dc8d4b0f8e5eba081c472edc38ecb212d
```

```
Msg =
e44d45b0aa7b782270142fbbaf7ad38e3efb0bf32253332ca7720a48b080aa484b1fbe8188f0ef
418c589fb5e184da0a10aa89d37292e9ab43563c1bf866bfbed2cedba2b4bc9ff2323c6ed2ea47
f58b17fc60e8632dcee0fd1d0274ec885bdba3e406ddd5e7727d8a4904da73cb0d577a78f9fa9e
2bc912fe51c31d33f067e8
Y =
5b244e39bc965c1dec463be5f56e057fbb9e833ea3d816050f00e4ae839ba0fad99106ee33c719
e0c9c415a7d5a82306b2642316a701a4d65f82d4f7bd99305f6d02e193ffc7af1851b0c524ca41
908d640f07d4f221accf930e6d1167765b376b8c99100b71ad4f5b272f1f1a7366a79a4c72eda8
1e8ad63c48a3e6df4b98c9
R = 968f4f98a550af1aef4b763a5bbf8b84dc579fc8
S = 959d0ac9492b57296c390c83781460254673fdb6
```

B.3.5 SigVer.rsp

```
#  CAVS 2.2
#  "SigVer" information for "Demo Product"
#  Mod sizes selected: 1024

[mod = 1024]

P =
b26bc3fbe326f4c2cfddf9ae3e397f9ca773c300a35067c3ab492cea5910a4bc0994a9053b0d35
3c555247f0e3725be872a0711c234f6de8ace5211bc0d842d387ae835e527e4609b5c73dd600f5
f29c8430817e7b305bd5abd02f21b3d8eddb9777e47e6cccb96bddaa9604e7d4551153abba959a
a28c27d9cfadf3cf3a0c4b
Q = a45f2a270949b6fe73eb957d00f342fc7847b0d5
G =
5c571649efc8fb4bee07453b6a1df3e5ebeead1113e352e30dc02125faf0931c534ddc0d76d2fe
c2d7726469533d33bde134f25a6783e0d31cd6414d16e86c5a0795219aa3c4b9059d11cbc8c49d
001af4852aa9203cba67e5ed31b211fb1f73ec6129adc768b23f38ead987839e7e1918ddc2c35b
166dcecf889107e02ba854

Msg =
c22163ea1e1c878481a2245d2b449c1cb7817ee44e305bd61b1ed6d8fef7fb95856ad2c5188833
af736ddbec5a23c06d87c3a2c0e8dde38e071a9869ca20e0c45cb675436b29803694eeb2601b88
90fce0ad0e028ea460a616f10d215c3445b52f4f74eb7fc71720ca6dcf3fd83db3d0a886eb32aa
4b7b242fe95c8b1dfbd16f
Y =
adcfe2d6d2dd6e9ddc6482fffcf067b6ed065d38dd1ae91b2402ab1d7e82da0372d38241b04cca
ec45ab0e0ecf19c673f2b82d3ed2bacf584550f7a962e3db2f77e2fff389fb5cee2b071af20cc2
45683841336a06976a0f44942019609744cb409e75bfd019cb8ccf2b1c578950e45bfbbd3e78bf
e69c9b9c0c9838bf02686b
R = 7c03ff0303f5659dc71fb1403d9db83784ec6858
S = 0a253a7c4a27a543a11edfe5b377114a38f38dc1
Result = P

Msg =
7105e2f27aaedd5a765c27c0bc60de958b49609440501848ccf398cf66dfe8dd7d131e04f1432f
32827a057b8904d218e68ba3b0398038d755bd13d5f168cfa8a11ab34c0540873940c2a62eace3
552dcd6953c683fdb29983d4e417078f1988c560c9521e6f8c78997c32618fc510db282a985f86
8f2d973f82351d111d6f86
```

```
Y =
4f654e6a3a6ab452aaad0c965c68386b298945181d75dc77d4cc5ace6180ff05195e304d13c815
54d4a3c041700367fdc75ee8b0908b07a9f2133e6e9cf5b732907af741ceceaa33e9be41b3a8c6
3b051897f6b7499547fccbf72ac095c582ee9c8fc816e4c7c0e307d3a66c596ca26c21146fad7c
47d1243c3ef12072e86b35
R = 986d3af33e7bce7258b2f774d9d07e9c97f893ec
S = 6556d6f315ed958c96139c527dfb964da834df86
Result = F

Msg =
ff20f0955c152cd30ff7d910c6c8c37f367be0c7bd061db546b85d2d6ecdbf67e540205816e0e2
6d0aa6eb7f8946f0048304f382afc90a4a72766362027885c3cb9dd8c4122568d7d81de67301e8
f051b51f91db079b0ce2d4cfd58fee5be19c7adf1fc3970d47774103d2d374d749d09473c3ba0c
a3aae5366cbd9c7ba05b5a
Y =
6628fbc3d5f6b65e1293c00ccc85cbd1f499437e78a03568090b5b628182ada2b5bcd8644ec494
c1eaa05f7a42d2fd7a6a94ffd28d5739891c6baca39d5485f5df6cca70c36f9073ee1b3c054009
23f3acc122250b2d24f293ff337547d1d6c52118683205f3e113c2b0255c542dfef325aee84197
77fbd3e2fc1c7860911a1e
R = 5c6ad0f0e43e2316e542ffd0f24e7e6972737f23
S = 230bab349fd181ca4c531b2053050875c1ebd470
Result = F

Msg =
0623089764ffd5501a7ebea62573daa572ec8d6facb8fede5326cb6b0e10fc4f421836e8e33231
5d8a636c85c8c82005bbd972b9deefec5625042e4d4abae1f2619fedddb3b0ec90c91cde5bc74a
1e7dfc1c958cb6762d175bfa8889b516f3508e41953f7d81ec31ff317bf0c901bc555d3e5cb0dc
54a7691b9142e8f82b18b3
Y =
541b1c90eb4cc544ac1aafffc764385196ea85e78a29675fbf927fb452b860c261ffbc8d9ca3a4
c6fb67ed5a5033b98f96895be01f612d72f802fe939f74c71abe231ac1ca21a44b4cc133ed7d9e
223c3f8e4a3b6ee6ed5d2e3c582d9d177ef340712dc4f9319385b402b7785b61aa613ef8c13544
d0c4c32a170646baa3def0
R = 861a7297d773baa641baae5fb2982e099738e43a
S = 426962891625cdaeecae70403264938fddd70fd0
Result = F

Msg =
f22cd6836e04ad28495d2863cf619dc79f443c500c1c95e2c3f35af2ae1a668319c1ff5514c558
5918c95a67ed88a433ca69d17ebf55f98950c57acf631ff8f35c42a2f8865fb7b0b50c49772993
4221b690a43022bb154acf029aeb99dba35802d848d48d7bd215674d7df94c2a7c76a9df3ecffe
f7f00e87d143ae1bf66f98
Y =
459d1a582c7e65024ded686c330b3b0a4c0c725415048d66de1d049b0af9ee91ce2bf721294e76
18638600682750e62986b98f73f4900084cb71851a35b1e4992795a01202eed157d9c66562a46a
5233db3e297f83a2a47a71368917a64777875c28b566673ba909a17dac1d7a182a1c4c6e9b10e8
b83c6fd54ef2fb781d6e5d
R = 7f6a33f5a096715f66f8a5216ede08d97123f1f5
S = 16dada2e06014c65e23c0ecbf32fd33f2b67d1ea
Result = P

Msg =
7fef236d9016e7b72e0307e730871b02186cdeaa8a103de80353ae28c7b3c3851bb6ff47b589e8
aa71e65de2453a2a5b7708da450d88cd5086958ab4c7c6557558da05e5d059106a8e78e881aa3d
```

```
8a032be553a87b8316c918e96d6a8bcb4c779e22dc4ecacf867eef814dce48d862829dcbf2d9ba
4743da2118ff50fc0dd014
Y =
b1a4645004b16906846a0e85435ac77b29f20c145d0a1b821fed7cacedc2ef869e540868b79a34
2e35bdb70e6a50338e5c3c689e9fca8661b621e3ebfde64880130fa20add5535448f2e71a5a00c
c31ad837f514c01773db03050364fa83491a9fcaf8d3092c953513a54a7a3fee14a34852a8845e
b85ef0bbd86d85a0a3a271
R = 010aaefbd84d0c70ad0ba2c12a0037516c0da5d1
S = 18d76c91c66c9f0a5cb4bc37687c8ec426e4cd38
Result = P

Msg =
824e7fdceb7cf8a62a27049f2e8eb61852b2d74a3db0e647064d5d319cd336aa661cae8b26ec49
d9238416f58773341206b095ecc0e602b8690f5f56a74431cebbd35dfa649332800074aa04f55a
ed9b4f2c1782ab273b105379a8e9aa0b6b75cb9e15906d19be830a21493340ebea99774ee672c4
1d9a380db3bf506ecfec85
Y =
6aad60071209228ad00f19f5bf67d36f6294822fa6f2828e8a90bea48f8a76484b6f342c77c126
839e57578d949a5fc7fe4d6022215cbdba980ec6fc49372a96ff22d1d4eccf3e2153ccb201b2b2
1dbb7e2ab8cf3722bef2e3d83e63da5ccc9fc4ea99e13fa9847c8b8eed0e1814afb23c4d14c78e
597cfa03ff721961633602
R = 3afaf03cacb83c87abe7e62bc82cb3274a434b4d
S = 34a8e5b9041e396e5fc5539ae1873da8502b9c51
Result = F

Msg =
7e34ce3fe304a910851aad715edfb0ae16a6cc47bf8db5f4c2a449e719526951bff4082765c681
2667072e15fe58364ab766a66f24c8c486d12ba02b79aceb197a850cf087ec71369d38239b3846
9e81c61bdfbb5ccabe95a8987e15275fa38197300321b03c20460ff5b58c73708f5b2b0e9eb4cf
5b4c2a2f360d2e89333890
Y =
adf79fe12af9954ca699830984ad88ce4d7bd3321c0eec9e870898ef622c99f24cfb23ccf401e3
76a7667cf718ffd648add9a688c0e841025cd1e1d941a2cfda6f5e534c5bda2ea1979119952b3e
4b1ac4b6fdf1669e119a074ffbbb7badcdc9a4110501d49b69022c52318dc06e934a78e5fedf7a
58dec2556e8c052154a9cb
R = 841fb9aa6d648be24698688017d1bf530ceb1ee1
S = 9f54ed100dfe791e6fbcf60af43baf5c6e5452c3
Result = F

Msg =
d8e745e683201b24ce6fdd1497877fae8ab23526957386b69f6aa29d7779f5680a25fc70da3f58
a4abc321887f007c7ec5f97045ce0cf5bf80d14ef74e4599626828a5652ea30318eb2e604ac0b1
12c5dee9f0d2f80e6700f9b3ca22f2edea9756b7e7ce69954508f678426040e267093c4a5ed8fd
c2030270d7bd2649b90f8e
Y =
122e8c7f13b04d71718bf0eea9fe17572034235b845d5ae8eba4fd422becc9fcc41ba364b0e40e
219922acefe2dcbd73f881b30be44fd1d5473f3ac7e2a9cb1b8fe08d43c03e60ad73d50de1caf2
dd5c578d5a0f60e291e02d4fae9aeeaa79e985f6d42ed323e2ec7cd3a646132f23081691e0f587
eec08bd307f3972a8ab71b
R = 74e86a4068a9ce65ce99fc4eaa1a24bcd70129f6
S = 02d27e752a0f944d1077a05d9408c1bc7be05035
Result = F
```

```
Msg =
1a7bdbe63042aa48e3ddf83e9b2800aff361d7e45f393a3d122a8a221f0a153ddee197e691f801
df47327842019fa1b7144f1ceace644e3d5c6b64baebed944b0e40a62d60a3b4a26a8b2ee6c737
2065858ab82bcf1a039cc985f765bc04b6b2734211a2e56e4bf7148e20133417062010bbb38eaa
83dfc2211d4b0cd87702da
Y =
83f88edf6e9b00c5597f3563fdae5c9e3250acbe71031bc97d765979080018e54de8a263dfc5e4
972e8b5588d1b11dd8722b850ab2936d0d5bf2092c2be1ae73eae9a988df46baeeeb27407d7db9
0013bd7ed4fbbe06926bd33a0871a8a11730d6c36494498b2bbe0586b8ad900bac6c916c4259c6
d7db3b8dd22e0be4d7e497
R = 784f49131670f16335bfa108fdba56e6f41d1256
S = 9b3e19e9f907cb960a8136390ddfbc3ab5af81bb
Result = P

Msg =
6c31d64162866fe46adb6d37cbeaedf03239afe1fb4b77cdac17b27bc2b95d08b168238126a8c5
b28fc0bf38dd6f29de88dbdb26d4cad4255414dd94ac5969259aefc013381e5cfd7b9093f40003
77d30841fbcec152574ec7f0adfdea3bec1c32aef51d2052fc6e37313193bb0ea077b953560447
4bc6f10d916bdb04c9ae98
Y =
82acae44b80f579e329e0048f025b86008f1add053fbcdaaf60283eb7c13346b15ed1dd76a6751
dc5f2d3f67ce1edd6f92134b32d1f09ca53a4be79838c2337f7140768d08b49016f6a3f7f2cbd3
85c47dc9609a63a0142019a5b275ee73779ea2bfabc60960c1b141c7638104f0579bf355202bd1
cd5942498876720e3604d8
R = 2f6fa9ef0d930edf62c653593171091cbd128408
S = 9cae316ef7e6fc510244dccde3b1b758444f2547
Result = P

Msg =
2c40089472c5ba01ee4e62777828b13c5357232a032177525ed162e5e6b5845556699bb77b57f7
6c457f2e001e7410527aa7ddf5b0e8b6d7082a52201587f25d458497deb695725c4be49ce0004e
07df7aaeb5aae35f2706f4fc1916536a6c82201964d2ca86131b280515dec5bd7e2d7bf4110f43
8db3264bce1f8f4967da0a
Y =
895c491e2d1721a8f8d3b733c49bf21cc0f3bad53d027295a0a82f53d068cbcac947e3245de447
a4af29535e38c229a637c50dd96cb44a288270c10073d9160672a91cc89ea1bb5028dc1b1a5b0a
a7136e58a94ae039b5691eaf6d094e5763f852c41d4124e53825c6b2a09b4b55f3d88a8af3bfe4
52c3402a188d211fb15e84
R = 03be2b2085a8e8e00d858f9f5f82ba3bb3f7c86a
S = 512836b807cda24170a9ab274e246095715cc39c
Result = F

Msg =
ad1814037d6fea331b4e61d46527f30b3f5c476d3755fbb868d1a0c19d7906aebabbba6558d5ce
45b030d813baf03d3796c9b0282a14f5250d22eb26a3d0c9128a5ba832357642e6d79af996839e
1bec9187644043a1c454a9cf6342c11fe3b2e3a1e5505c7ace7e5a34cb4508581292f93f6b9fca
25efaf037f10fe3f8edaf8
Y =
87a01d390c5ec7a16fcee02c7546d8930e36bc32396c9acad1b5aa119e756c1b07d1ffb0b9ec93
2d9c8be862efdff1ace9117aa33affd34592cd4d16ef270fab365c8ee84856d59b21f2316409a7
e77b83f92ce87af9ee0e45341faf25271c61193205e2f1fa6dee0abe7960b9721d16e2a794d234
816444ae5d48ea464dcd2b
R = 64d2bdbb07b17251e7530c5710d7036a408149f2
S = 364a1e248e52831a69354f7da2deedfaae2933d6
```

```
Result = F

Msg =
f904909092b63b8ee6193d48b5f60af8a273fe1698e7e7cb66edc4aaacb8cc9bfba6b217381728
9b417fa256d3ba5c25aca09ec2ecda3f39c1f4689b43b29af59da8f2836e05ac226fb0e7045596
a7a7f9422008b6ae32141258305fa199e5182732d93dfd28d00bb6d394b90131f465d1800d4fbc
0bc845a144a45e8e13b6eb
Y =
7e0a22d0acd91fade061554386b872e50649b311b08f21e00818bbd4d28ef26593d288cf9be0b3
843ae8499f84ac715df901edf2dcab934264e5c3479622823a44ecfeb3ab29cf09bc8d20440664
e7becd77e91dd66f51c718fe94d59b713146ad1ae98a889e88268a222fba616e846f5d6a5bf85c
b82ca20a1fe9ffb326b787
R = 0f49a52484ea14590f8791346bf83decb3a6452d
S = 661c938cca562c507f1212aa5c53cca19d516133
Result = P

Msg =
6a9f368060b44b7eefadb19ed951dd13d68be13136773525c7bdb8e4f91ef261404c9c03baff62
561245e701a4190af8e23868f2f630211ea9bae0118349150333e3853c323005c9a4d182737ff2
45f2ee23755df863dee55d7ef0c3c09a0b6f0b0cfa131070bd3f6cf88bdeb1041769c4f3135a83
39f2e4abb2f3e1f9375b0c
Y =
38afc7afc91e47a2034981feb5428ecd9623896d27e2ebab72e6567626f9b8035892735d3db6c5
edb23b6d9147f60578f1bfe3996d47f2a8a9d957849740e7bb6988a1ddd6de32687a1777db6849
aab03cb10b0be63b32f86aebc87e84981434c6a72410d845e95975c803b786278e41bbcb79bc70
f25401a6088c609eb2ddbc
R = 9bedecdd7df5af52f6ee3a730f502a5a82076ccb
S = 442982810fcbf663b62a11eb8e0d8345358d1725
Result = P
```

B.4 Examples of *SAMPLE* Files

B.4.1 PQGGen.sam

```
#  CAVS 2.2
#  "PQGGen" information for "Demo Product"
#  Mod sizes selected: 1024
#  Generated on Thu Jul 31 14:12:33 2003

[mod = 1024]

P = ?
Q = ?
G = ?
Seed = ?
c = ?
H = ?

P = ?
Q = ?
G = ?
Seed = ?
```

```
c = ?
H = ?

P = ?
Q = ?
G = ?
Seed = ?
c = ?
H = ?

P= ?
Q= ?
G= ?
Seed= ?
c= ?
H= ?

P= ?
Q= ?
G= ?
Seed= ?
c= ?
H= ?
```

B.4.2 PQGVer.sam

```
#  CAVS 2.2
#  "PQGVer" information for "Demo Product"
#  Mod sizes selected: 1024
#  Generated on Thu Jul 24 10:32:24 2003

[mod = 1024]

P =
bc72aacb599a1301b4260b620f3391046cc8719291b7259f7d2f1d57942e0400bdf145a2cac51a
b15c27fa217f09aa3fd84d2f4742f786717a5d8089564e03e6224b05bb3f52f8a9775f1f2d8d48
6dc9d3bff78650e22df40d7c070d36d971816aa904d81ef90aed42332679b84b5f75baf069293b
ea3fda832c6eb342002701
Q = df0e3c75a268319201c6b309aa666db1f046888d
G =
a5d2ca30330f66e0fb5fda4bccf32922305852d1724f2dd10d7363e660395f67e8d10ddad970ca
bf42046f58bfce3aad4a9549ddac9c0e00a3458c4d9158502674a90570eab0e6a814241ddab410
def8a0ab937fcf8d359fd8f4db773bf0eecc121bace11bd64c19acca914ddef0447169f4e3f9b2
5af99e1680ff8cb8a391d6
Seed = 46b82836e092da94a4eb1c291450121718159500
c = 177
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002
Result = ?
```

```
P =
e31f0dd7c7ab52631a528a583359b4a21c01ed03b1cba14b806ad85ff4aef822e3ea4ac3af9574
ea0412487d0afa53f905b33d76c4987a0bf5bf1ef0575b852ae42c0574a3216628862cc719cad8
42de5869ee861efaa1aef916ee5ba12ad76ee97149cd8422911c095527d556dd13830e99bd76d0
5dd6c286bc8cd5822688d3
Q = ed928212f675f4a9881ee0f657d2c924a7e028c9
G =
0010c7cc0d56665b37e4a1160cc647d54243599e0febba57beb6e009d395f66bde5116bc821f6f
fe9ccd851b9c9056ef57c74680f3ea968209d7daf83544056d9e11d500ef8ddea29b412cb4f39b
253c6e67b5c16502db717f4d47b667848a1f5cb14d050adb7667b7c24fbcdea9192ae74bbf4ac1
ae2c227dfbe7db1db688bb
Seed = f6d57f5f1a055fada254fe759ea480d8fa42d1b2
c = 346
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002
Result = ?

P =
fc602845fae0d1f7048aaea3dd5f633b69447654f24ba184a8556b2647cd95bb9accdee8ba652c
4de4170f6e278323be98af9f204465b512cc151f8944e2f54908f90fcd7424b040d70b0b94183f
890bd0154236aaacd570c239da15d91ba998144d049dc8557b7afe42d6801184368be30a4904dd
26ebb47b4e05238ccb7049
Q = 8f07df47e6f6240b96499492178acd14397355bf
G =
3a73e588e210e58bf8447739bb2235ecdd8b67915605f8a82310b2dc3d761ef9f9504387446400
3e7da4954647f858397f8561b989fe2916a98fbd77ca37db89cf884d44466594de1055c53ccb6d
5808217d5f4c76a423d84b3fb19e0093c1b65ee4456895c8f3e4459d228d4754f8165fe76abf41
da171f4e938dee2ec2fb58
Seed = 03f5fc40998f59e9a1ae9e7a113c98dc381d2ecc
c = 629
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002
Result = ?

P =
cfaacdeadab66b588840516b0d86aafa1292ece8b96578277fa2367ae53e1d45359d2fc7e1a033
2a246deb01a2765654f9f5a463e4b42264e9cf3ec6aadab38c65fc0306456f3283aaa8b58d9845
8cf24e24c331da3b746f53446b84162c25a38272e4bb0544cf8feff856bba336684349a99c5508
7a3a326b6c303dda8535eb
Q = bc2888b3e820154c269fe2567bb5d8dd7f7ba36b
G =
16a5ef50ad89e194733dd08d98582030d0d0912ac6bff5d8e948797aa1b0c840d36a3ba9cd3181
d59b902e5babce642ce33897884967102ea6c0be7a2828d4e0d9127fcdf1c4ff10a3c50fd6557e
8104102e646651bce523b383f0a6a0c76269dac6cb969e51484ee44a869f21738f144de286b7a6
60e831724773ddc8044b71
Seed = d048769bd51a9d8d09a1e469a4826aa0e25b6368
c = 125
```

```
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002
Result = ?

P =
d942109feb8dd72e9fd5b7f1adf87411a090a4571e261035648499f4f0b509bf093038cc8ea0ba
c7354027281d4b35c93d2e1aeb0827e8fa44b1bc33378a3c99bcc246a0a2d0ec73da3e8a608d8e
4ec90642a9d8f7c97ecd6fdd4606da4e4e31e28e58a39ab45a1f1786e2bdb1c0b2863688a133e9
7ffbdb12f4741dc75e8f89
Q = d938dcf43182f580ad974fff95c6b9c9e1683907
G =
7ad2c400c4ea6f00b077a2193e16e6e5edbb2d791d2ddb38db0dd9fe21f7a643fbed5db37b7018
c3ab54a9599180a40a3f58dffea5170ca72cf36c619ca18ee6dfe53ef006d89d5cd3d22acd7c97
6b8fbdfb8f698606145a860e23e66f2a57c990e66e51680cf0a21664378944821996a808e881d9
26f873e278c05bc3354fac
Seed = d32755fc624f9f18638b6593c918c4aa2a41a5da
c = 6
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002
Result = ?
```

B.4.3 KeyPair.sam

```
#  CAVS 2.2
#  "KeyPair" information for "Demo Product"
#  Mod sizes selected: 1024
#  Generated on Thu Jul 24 12:43:25 2003

[mod = 1024]

P = ?
Q = ?
G = ?

X = ?
Y = ?

X = ?
Y = ?

X = ?
Y = ?

X = ?
Y = ?
```

```
X = ?
Y = ?

X = ?
Y = ?

X = ?
Y = ?

X = ?
Y = ?

X = ?
Y = ?

X = ?
Y = ?
```

B.4.4 SigGen.sam

```
#  CAVS 2.2
#  "SigGen" information for "Demo Product"
#  Mod sizes selected: 1024
#  Generated on Thu Jul 24 12:43:25 2003

[mod = 1024]

P = ?
Q = ?
G = ?

Msg =
229a053b64fabae455a482742ec07be01f8a7feee79b549aa36a23b9e3122cdc0356b777b9e24e
43ead329e0c27aeabf035d8b3f9d7f941680e291f3ae49c362944216ef9a64538ef9d6973acc11
04dd6be6b670f4c2f8632a31b83f83a1398a7c6908eb3009318e29b3b2ca760b3001fd2ce9c813
ebea484a5f82e48aa1f61d
Y = ?
R = ?
S = ?

Msg =
de31e0d133db28637c41734d9c8cd1b03c905b90620a6936452605d260459f65c5fc02deb46086
836c8187934134172aef16f0642ecdacc5869139d965ec87176fbd830b158349b569d8952c303c
7b86391459fceef2094a29175b554937c210847c4da07fcdd9bf1b4f865e922c678ec4947ea0cb
02e78bd5c1538f33aeb818
Y = ?
R = ?
S = ?

Msg =
ef0974fa4832a69fe5f5d00f0d4f86da23eb5d9478a15b7c633eab5a948395aea570ae06f2c24c
b0abba3d912720b9557b8894c94cd4b884e1fad3cd7c074db9eb647d945a581c826bcffa66895a
```

```
ef037976156231113473ee4a7ef681797d9ce96f496a27fffe5f4ebd6d56da05122e423f4727d1
62b68fb1b7149f49e00da0
Y = ?
R = ?
S = ?

Msg =
9799ae10374d1a7b2b0d45f9f622e6b61ec8d86f8332148eeecfdd97edcc3ac2dfdaa9ea4b3112
a576d4fab53417f99ffe5f6e99452a71a9064f090c9f869fd5e12ab3d6663ecec324afb89543d8
ea2d2c4b463ae3cf065c96a5f38a7610d7b1c514349d307d361d6023e762cc6da2a9d114ca1a04
29bbefc75a01d81a71c99e
Y = ?
R = ?
S = ?

Msg =
bc0bc84b82cc93ff67587600a6160b0f4bee6c6fde5cf69a41c24d34db03a03df74d2f8a66360a
766c0b1bd5da64662977fc9019a4c09e1e40260080cac0ce81c51151d7619fc56057495d1215db
88311be073c4a5b8cf498aead4a864bb8666f1ff371bb92f4d26f1bc459fa0a3f88d00421d5927
691083e6b5d294f2195054
Y = ?
R = ?
S = ?

Msg =
03788f568945451dc141ac17823185d6a8d3a2b0c3c441c011a1982eaa6cb1b0fb32785175eb13
7286a2710ec9d626427a1f760c2c15af53be6dbd278b65f84be16340f0b5d84cc4946b3f2bdd54
7ccc2e05bc501c105e662745fe0bec1a48089d510ebcafd4991bd2e43df72672307faccd9d05fb
7ef30434708361375 54af1
Y = ?
R = ?
S = ?

Msg =
95eb19ec8dcd4dff898281b4b9409ca369f662d49091a225a678b1ebb75818dcb6278a2d136319
f78f9ba9df5031a4f6305eefde5b761d2f196ee318e89bcc4acebc2e11ed3b5dc458b01e6025a7
5f70c4a325308f63c5f1a16357bfeca6684286b3efe244de822e8ac8ca7f612935d8cacdea1153
dd0235e760f528ea01528d
Y = ?
R = ?
S = ?

Msg =
f98ec431f01142e19f069e58d6c95867325bf9c3a6a949625b11c128ba2243c3c7a309d4b0d7dc
4fa5008624eb22891f2c09110c128d2820141529948f5a7793186e6e5611fc9a8e7ad127020a9b
99797ef1beda3294e092eef53e3602f7be6995f5dc013a07e665c4816b395cbdf13ed01be6732e
45d98192b8ea553c807f0f
Y = ?
R = ?
S = ?

Msg =
619c4628111a605c32bf9d670b839eb764e286319897af1beca89c3a1fa22f3743261c48cba49e
0ce46769b609d2df6dd1e986f30c13ba850f1d9f034c835a5126eb81fd03f3cf22a22c1d8caf66
```

```
8d1c942f096e9396ecba1135fef8356ea648b2f45b90e18d5c671317a13225c9118c55bcf5ec53
aaad819cf5a16103eb7be3
Y = ?
R = ?
S = ?

Msg =
e44d45b0aa7b782270142fbbaf7ad38e3efb0bf32253332ca7720a48b080aa484b1fbe8188f0ef
418c589fb5e184da0a10aa89d37292e9ab43563c1bf866bfbed2cedba2b4bc9ff2323c6ed2ea47
f58b17fc60e8632dcee0fd1d0274ec885bdba3e406ddd5e7727d8a4904da73cb0d577a78f9fa9e
2bc912fe51c31d33f067e8
Y = ?
R = ?
S = ?
```

B.4.5 SigVer.sam

```
#  CAVS 2.2
#  "SigVer" information for "Demo Product"
#  Mod sizes selected: 1024
#  Generated on Thu Jul 24 13:16:04 2003

[mod = 1024]

P =
eed7b7a8d157758302067653e3fb1bbdb4d1119c4c2753ac36555ab1596e5739180f0762fc7aba
40f6758956d0789d123f9c1986725efef30d69c0034e342cb79d9de7ea22fca1ce09ee8d24101b
ddf6fc1c103c1623dc938f40b2cca6d1b8cd8cb9c17ec5525f771077edc97798b9cd8021827967
cc0c14dde3d22b9bf7cfd1
Q = 9f905b3525bf749d8c0a81d84934819df630682d
G =
914e61b23db5fc9e86afcd0a3dabb0fb9e15a259133083fcb718ed92a689d846ef56f0153004b8
0391e30e71f3a66f060c255a373b33eb104cee8b19375313e7cc455799884e9e0f928cec7bfe27
93227c174b9f246fb1fea6074d98b162fbab20a6d98c9e589fc4f3015cad1aaab06276ab7492b9
3108f7901fd5252bea1ab0

Msg =
6c796169b75b9afb3925bf1184c2810b7dab9249025a683dd0023fc4a47d5db6a18699bbf2281e
61b0766d6c067da16e9377f7970f428dcd32106affd15fbfb74b2c6cef2363c626ee9b98b37000
68580290fb1a368b1b50be2497fb8a7d8c5531d2e3ad92f51b71bbfa488d0a335cf3915fa67bbf
1e98ee3da8cd5d17bf4bb8
Y =
bd447994e187104d7aa4f0e43ea6f0278acc2827b8cde8efd370c551319920d5f46a28b282f659
46c01abb3c32dc6aea411b45d8504d3ba48ac107e623bc396d2d79e705c3cf5b8aebed0460ccb8
7d9a00bb7ef9ab2d9bedbd8fdec34425384feed793272fa79f445781e041ef839a5cba463dbc1d
559fb897241de41e9a8dd8
R = 8af12df07cfa9e092b80930993ebe5e95681f985
S = 7927a169b5188e70dc203eb5e13c4ef4a126cfea
Result = ?

Msg =
05f2c6475068649b7400e4b02383b53b66f33cf7eb72caa1a060cb4781c440c3aded6f83c059d8
```

8b5dd56cbc0ae6fa564168eabcc3752d773088747ed5e2a0b4c52d7ab32b60a5c8dee2d13e36f2
30e01f462eb96bf25d1e6d8caeefc38ee71973fb515f3a46b15b206f7abf506f41e127d671778b
b3409e7eb4e222f28efcf9
Y =
8a09a580b7218fb35114e223cfbcb69c31386f3dcd2b11ae1fd3828209beb416e80f9830157a2f
2dae2cb8af509618f8f1537c6d020d57692e3b740a16568cf1b7733dd1f8832e8cc83ef3130641
783e60e25c087ee1362f04c10ca98180d7fcf231622167a6a2fbc244fc2399d20d0ec2cc449598
936cc8a123f329ade97aea
R = 62843def24759cecda7c387c5a067cc7ec4df009
S = 04955f1757f0d975ac27e83963c9eecb94f2d131
Result = ?

Msg =
0767eedd7cefb1970614da4b28061e4353f9a3f7ffcab5d2fae6ba39ff6868ca8a8135e1eb1d0f
6199c34eb1cabde704407ae2de66300ed49bc5f393cef008234b9c266dd48d3dfbf44546009029
7898bfe0bf50dcfc6ae9d9dc2359d5d02513f17fa9886086a1eebe62a940a3903b8677f2225688
75319b59f134953e512721
Y =
24d8907783cc6b8c443c34d11cb6c1bf68067a0812c941c1792a21d7657c533f0ca1b37d668c79
8a80b4e5d966bc844df75f49b2d5cfffcc40bda2f80d29035ffee69021cb18f2003f52c16d3934
1fd22bca50875c5b310e70044a07131c0a5e0c82b01fcd5616688675ebbd7d6adcbfdfbc8f1409
3a75a391b47e07be8330dc
R = 1fe34959e62d3094e4c05355985e18a5179f3eae
S = 8962b16b4f4a353409dcf42cdb7ef85652bc9b3c
Result = ?

Msg =
4c26c846eee0d3316e9a32ecb909637e5a0660184bec199b0a422159f09aa820bfb8a9757af764
1d79e90fe2bc3ec99380e7cf4d107bf2f9ded94916d20f23b9e27a3fd1e32f40b09e9a5bc72765
53b16a9ba774070e0a0360f61307efda36dedeb4f3e4d1504df207f57e25a147e9e1416c5015d7
6e47c0b8e0e8b4f1c5c99a
Y =
b5ecf6eddc03be74fc7055030ef108405a89232c78e52992101dc50e67213d56f4cbff4b06510c
a308326a3585a58f7599bf91d4e7f8f6d6093b303c6c070589cb31dbc16e97e1c32aff7c231a2b
959c486e5ffe98c4d57b1ad5fb0493531c15d368dddf5c1685639586ccb5fd5c0f20859fbe7cba
a3ba27f164147281d064ec
R = 5b713e336c2b1f6b1a36eed134867e31bf46e4ed
S = 23db2d9e9e9c4f98cecd9a37708702d8bc8c4091
Result = ?

Msg =
6670dea983f4a7916d5573f0d57125c14f328959b4c0dd3fc4f5903d101249b718b02b3cb0f958
5ba817b3b8abedeb5f6805b557f0ca587b5ff86f85bf50ea6c299057f02da260727514940aa4c8
6ad484ed828a612d2f58b02833ebf522c9cce3f8e9ecc459c7801b329d0e886aaac8edd07a1acf
52697fff6f639879efed7f
Y =
2890eff631bfa4abdcc2500fd6920fdf1231b3893c17bb83f5d57ae5ff4fe20418378f137cc114
34c7ab128c3d242b57b0ce9dfcc4a73fbd27d60fd2b75864c2ad1573ad3d1e5ec744346803c0e0
e2f7b2ede622702708f5fe35b7e100f19cb497f16ee68c085978727c9b8e47e4a085d265b5f13b
117b8055767b0043a7b5bc
R = 6dc80b3ac2d3c5e5a86bc6ded1bdd86360587200
S = 21903d5f3894cb90bfa3081eb85ca825c7bdf02c
Result = ?

```
Msg =
f5104bb83a691b38f348574ea25cb6c2d94e7031aa4a50b35ebc0bba6957d03e9e5c2017a019e0
aa99b0adc72e196fd2b26a3121995630a630f431ce8cc218a8c0eab74a54c4e471f29bce6761b4
912ab88c07cacb62e113eaf5f76ccb8fddffc442b71a3d724ed5669463f625344311533d9bf427
758e42f247055d0dc54689
Y =
bc243185de50a1b917ca53cc4785bd0d5fb050671f397851a1dbb5f8acb6081689f1ed065ad73e
22b5e5554eda1737299b6ee77b4ecfd8882b3c001fe7800ab9ea31e2067196e0a3b718a26505f1
852072ee40186c557782fbaa371a5f1c4b588403180b23e74bf66508beb2b59616a3b418cf82ac
7dc1c91b8de16c9fea88b4
R = 6134bd543cc618438a28b754af036e6e7d073442
S = 8bece8ea668c55e31c796bce618ac546c060894b
Result = ?

Msg =
0208af0e6e70b92005d44e5bdd855d497a0aa331a07a1f99662ac60a8c8879130e473490f9bd88
2d7e894b2545788e5004aacf5c4ff0705ab279687dfdae391fdf5a2205b60e95e4a6c4eb24e8c2
57e365c1183d844ff3cb4072e1697d8e053d9c88e0f54d2cc84fa4cc96df702aa00dc899e75de6
5e91f3395c9956b5f1c574
Y =
8b718e6dc5538b83fe4f1615a6f33e5b4c7364a7655a633292e3031e4a75a430bcb5b41cfdb207
248fac01c1b815b274eced56ee96b51eb5c139edca1a66937a6e5ad2e456a700101bf40386162b
6c29e784e5366a5c7296d88a0feb3aa3a902e345469317f4990e1dca0949c19f69ae33c0342679
664ca588d0ac048dd80504
R = 8dc5686fe06b3df8acb55b0410455fe50ff6968e
S = 63d23bf25f5c81e343e0b502afd388c9cfc3c2f7
Result = ?

Msg =
aeb11b7cd6d513779e76da607adb2de89d646d891a79e81949c45aa06c9db46792c61b51bc5934
6e3ffe9fce6961c19367e4c74a6691e77cf952e97fbb64e7923509512a027d3386302cbb89ea22
f6c954c3dae4b7bc8913de39d401c059fedd5fdec3adef2a99e63b67363a450552b22c69aefc53
e35506c0e122ccc263826e
Y =
5f192a6f25ec8a7c65a903fe6c50016fdefdd4b2947dd6b14feeca7f1c10c4e71fb1d1a11be271
6e8d8cb91856b646e8f5e27014d27d8ad74d112679ab942f3280fcec2cfb99fffa50b26581e7e3
3f6e86f4c3b2b3aa6d059cf4e69e273ca3324972006b3f2ceed6069dae66deee1cea3bbbe37ebf
b013e4fc3ce17ec8d8e153
R = 70eeccdc1619be5d8315b45f94249effa929bf45
S = 88b979068ec1cfe4667e7fbe8ebe63160e5d8134
Result = ?

Msg =
d4ed2d86ba2ed51dde38782aad2c78ff39f419f37ed6e49fe9494a4d1b088aadea66d5caa8e1af
3da8f998a0ff43ec4688b908292b54ae245eddab63eb00b617f4a29c6e35749ac28ac80a11b1a4
43ad5015ba343ac66dc3eed1816761d529d4fd49cb5ae9105e148b4d17634b78449a9ab278fb33
55e8e3a1d0154102b2ab4c
Y =
306825ab2ef4933b475043c2e29c1b0551223c59a8d83a156348d74489b7c405f040651917597d
8bf7e4460c2ca0912c9d4f49f2a8aaa891a1096948eb9f35c5aa4d59461dd2aea5a84cce72a638
b91ced5bbdee3367cdaedc508a97a676a84a410d31a568367ba5460e7a2b11e7cc5e5f6cc70d74
ade20d2d77144b1b8692be
R = 68d86c285bc594286c45e8b30af6c11b9b5efd34
S = 6b032e9b2ece290c7d2fa734e90a78d6db64709a
```

```
Result = ?

Msg =
86972f9622b50d126767b66d2d7f4f366a1a2a969ad44729643b1b0c7a849138c17d4f0eb2c33a
3200353c9d7aa845ee34dd8f01e1b027c38491a94548384a0fab951cb6e2068eb179cd32683bc1
c48e514367b1ae74310faaa6eaacec1011a18ec520b77ce712341d1721f53631d4bd0b3639cdc7
8a6fb51d6068693072ed97
Y =
0d2785630308a804d6a3b8834547c86aed93141482dc411bd353c81c99e312ae284d55d28f033a
d51551ff80c190abd4a37bb87ff26369d0df9fb09f37f3e2c2fe16a74f7c3eb5b75ccb35a246d7
6ee256417d1dd6688e2214f3ee4ea35559dbb94f627d8abf04804e252d1d106664daf3eee5547c
c7a7acbd0aa56bc66f46ef
R = 75bb60eaf362c302c5aad0df23ed398d42525b4e
S = 34cf0d79ac3a51a8178fc6ba09bb92be65937257
Result = ?

Msg =
71eb6b3d7a1f306f8fff4e550473cfc742b3935361668d85fa0c3065369923422b623cae693dac
cacfe477c4a49b289de313c230d58df970e542a2f1b10369aa5d1dc2f92c7f22e7511f6eae0299
b478cf19196a327c12e167b2d7fb7d67155aaee2e324ec2df84ebc761b1b47b5dadfae8f7f099f
7a40602623b68dc50d91da
Y =
a5a1bea4315500b6e07a3309b9777a2ec2399e9092d7ec902695f85fd117df46d0b64e582cc8ae
fd867432990c810b8092761409b1b2621dfd0f25b5f0ef3dbd8e21599c33cd994d0e6bdbfc641d
399a89d81a61702a6b4b71b453cd6322a310cc32ef8faa7854ab7e0f28fae9f05bf0832eedd99d
ce7815fce434d18348e5e6
R = 4fcca88befe2476f082f7927c4ca544603a88cd9
S = 0249654001c3bd48c735bbb2084d6ab5f59bcc91
Result = ?

Msg =
b82fef8df994b4c14d69418b8c414db456c28ab201aa36cad510ec777cedc10fb4da8ca4471b85
283ddd12d550bcddcca0882afda8496846718005df05b087f5271dd99541d4e2cc9eeb5c0dd90a
e4d2962b4d866f9d3aa3324fec18494b58ed79817d29d0c6f4f4d81cc9f91134890e9e319c173f
afd5277f0448e92fc55c3f
Y =
21817e49843374f35ae59e5dabf7d35b2cb9a11c9c9ed6dc78b1197346b5596c1d3c9bcfbc133d
407612e9964f2a4eaf1e35586f356841bc95ffdbc5b455b995390b45f2fd31858bc192dd09430a
fdd191dba5497671a7760f989697c129f61e3dc512f20704b1d8bc13fae675871e7c825bf48a3a
4c9ddc0d6747f65c46371a
R = 5eac1566af33fb08a7a6a2539f1e78dca42bdf61
S = 3e9c4b1274996d872a3792e05840a0a12b5f0ca2
Result = ?

Msg =
d08099223b5f880f34b08ba5d09c89f04c3fc28cffac60c68d314ffe5edd4f504e404873a672dd
e04c574337362054df2415dfed8f924348dc503c0ad6e6fc295b907e56552e1725ed904e6ffbf0
edf5c0c05845d7a71ee269c6ce9fa13f0c4c5ff8e394319c5d267fe3511305147d7786c8d45cbf
f019db9b19ad84a5efa601
Y =
bc2cb2bb630c172ce3c73905c661c3cf40379518725eb97c187e6153f4a62fa9c23c5b0a7a0e41
dfd001b87ecee609b21439e6c6714fa507529915e5ced6d9064a6e9d11a9dbd404d868ae2fc3b3
8c9c75858851d1d8acec9bf2d4de5f877e87602979262d5bd33d632842ecf26b139fa349285b6e
2fe4331cf505841eaca9f2
```

```
R = 87d9244717417617dcf642b925e520160bd615d8
S = 3968cc0ec06e001427b557ec0f79aabf7f9df807
Result = ?

Msg =
aaefa5d715e6cce5afc87f96be99e9236169b4422ecbcd4019896850979645230444431b842b7cf
76a49a98780a1021284dee9c0fdd27a2eba88830023ea5efb73313b85bc5d75745bf1f8f259e30
5f95f1a084f106c53f69c26d5854d1cf63c700c24267e62deb7bcabf6c46c1e02c9317e77391f0
8d2ce12fa1eaee97fe2a7d
Y =
a6350641e221cd0965ba967b3c46c81ec15bc9c99eaaf1f22489bc883dd0c78c91f7a692b3c6ba
e2866cc7beb5e8205475e7b2b133b17802913edef92c208d9b65d358797b85c3ca8a436d38dad1
3a066320e03c560e82fa3c8ed714a64cab9436ddaf71d6b9aa3743211acaff5b8fb4f685d004e6
d923cdff3a5a6788eaa7ff
R = 042ab06550e5a8a8804d79840763cc879ad8f58d
S = 903af796d42627f18a3a3e12a43a140c1a8e2e1b
Result = ?

Msg =
efd4194ba03c87bb8afafcd3baa38ffdaefe42511516e450d78d35d655334c4af2d73618d25ee0
61e21236f1183c8d71fcf43edd673894398a3ce98033010bde4c29e51ea40a5b66f30175221808
c03ea48bf1989c78ccb57b9644b37717e47e05706d479f68c132c56fff4f4232f0ccb06ca2693e
ff522bb1438f55a99e9d94
Y =
8bbf338432fc5e953643e47937d8a87ef5693b2480d8561833f0ca2662d5baeb367c70b4df004d
c731cce3ef536bd2394ad0b345c199965303a65a53ca1a95188779883244c12d1389f58dc82e8b
66be9b9e9b4e07641d86b03fe6bb7f6a9814f8ff53a11ab5fcb41c05c86f555a6895beaae1c404
02ab0e1971b54e4432e737
R = 6aa54462f90298c48c6e785559b88a9da2ff3696
S = 255bc790c3fd46b245cc2fbb517221cc2de104e8
Result = ?
```

Appendix C Format of the *pqg_file.txt* File

```
[mod = 512]
P =
ced6c5bbce50e8cb0041a66a55bbd7e7435f24e8ae93da1a3fa1426bd0a5bd12e51b7b7661561b
1a178638bf2d5c4f7c4098892cae70a5a2506cfa3d6d97ad55
Q = f77c35f8097534347dcd3ec46ce98f545e275b6f
G =
afaea3210e612851077532d2c7a3a827495322468740b1f55fd7edef3d9e4ad4f1a2a477a747bc
3c177e20e183321a3e59931027a223c31a9f6d48ae22a0d432
Seed = b358f85b9e01ff82b16d118a21ca36aa54b42827
c = 137
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000002

[mod = 1024]
P =
b26bc3fbe326f4c2cfddf9ae3e397f9ca773c300a35067c3ab492cea5910a4bc0994a9053b0d35
3c555247f0e3725be872a0711c234f6de8ace5211bc0d842d387ae835e527e4609b5c73dd600f5
f29c8430817e7b305bd5abd02f21b3d8eddb9777e47e6cccb96bddaa9604e7d4551153abba959a
a28c27d9cfadf3cf3a0c4b
Q = a45f2a270949b6fe73eb957d00f342fc7847b0d5
G =
5c571649efc8fb4bee07453b6a1df3e5ebeead1113e352e30dc02125faf0931c534ddc0d76d2fe
c2d7726469533d33bde134f25a6783e0d31cd6414d16e86c5a0795219aa3c4b9059d11cbc8c49d
001af4852aa9203cba67e5ed31b211fb1f73ec6129adc768b23f38ead987839e7e1918ddc2c35b
166dcecf889107e02ba854
Seed = e8ea44c48c8cf6292f6d3213d39aa60a32f1840f
c = 1241
H =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000002
```