The Random Number Generator Validation System (RNGVS)

January 31, 2005

Lawrence E. Bassham III

Sharon Keller

National Institute of Standards and Technology

Information Technology Laboratory

Computer Security Division

TABLE OF CONTENTS

1 Introduction

This document, *The Random Number Generation Validation System (RNGVS)* specifies the procedures involved in validating implementations of the various Random Number Generators (RNG) as specified and approved in FIPS 186-2, *Digital Signature Standard (DSS)* [1]; *ANSI X9.62-1998, Public Key Cryptography for the Financial Services Industry: Elliptic Curve Digital Signature Algorithm (ECDSA)* [2]; ANSI X9.31-1998, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)* [3]; and the "NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms" [5]. The RNGVS is designed to perform automated testing on Implementations Under Test (IUTs). This document provides the basic design and configuration of the RNGVS. Included are the specifications for testing the individual RNG algorithms from the approved standards implemented by the IUT. These algorithms are:

- DSA – FIPS 186-2 Appendix 3.1 – Algorithm for Computing *m* values of *x* (using SHA-1 and/or DEA),
- DSA – FIPS 186-2 Appendix 3.2 – Algorithm for Precomputing One or More *k* and *r* Values (using SHA-1 and/or DEA),
- ECDSA – ANSI X9.62-1998 Appendix A.4 - Pseudorandom Number Generation (using SHA-1 and/or DEA), and
- RSA – ANSI X9.31-1998 Appendix A.2.4 - Generating Pseudo Random Numbers Using the DEA.
- A NIST-recommended RNG based on ANSI X9.31 Appendix A.2.4 allowing the use of 3-Key Triple DES and AES.

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

2 Scope

This document specifies the tests required to validate IUTs for conformance to RNGs specified in various standards [1][2][3]. When applied to IUTs that implement an RNG, the RNGVS provides testing to determine the correctness of the RNGs contained in the implementation. The RNGVS is composed of two tests for each RNG algorithm implemented: the Variable Seed Test (VST) and the Monte Carlo Test (MCT). In addition to determining conformance to the cryptographic specifications, the RNGVS is structured to detect implementation flaws including

pointer problems, insufficient allocation of space, improper error handling, and incorrect behavior of the RNG implementation.

3 Conformance

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

4 Definitions and Abbreviations

4.1 Definitions

DEFINITION	**MEANING**
CMT laboratory	Cryptographic Module Testing laboratory that operates the RNGVS
Digital Signature Algorithm	The algorithm specified in FIPS 186-2, *Digital Signature Algorithm (DSA)*
Elliptic Curve Digital Signature Algorithm	The algorithm specified in ANSI X9.62-1998, *Public Key Cryptography for the Financial Services Industry: Elliptic Curve Digital Signature Algorithm (ECDSA)*
Reversible Digital Signature Algorithm	The algorithm specified in ANSI X9.31-1998, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*
Secure Hash Algorithm	The algorithm specified in FIPS 180-2, *Secure Hash Standard (SHS)*

4.2 Abbreviations

ABBREVIATION	**MEANING**
DEA	Data Encryption Algorithm
DSA	Digital Signature Algorithm specified in FIPS 186-2
ECDSA	Elliptic Curve Digital Signature Algorithm specified in ANSI X9.62-1998
FIPS	Federal Information Processing Standard
IUT	Implementation Under Test

MCT	Monte Carlo Test
rDSA	Reversible Digital Signature Algorithm specified in ANSI X9.31-1998
RNG	Random Number Generator
RNGVS	Random Number Generator Validation System
SHA-1	Secure Hash Algorithm-1 specified in FIPS 180-2
Triple DES	Triple Data Encryption Standard Algorithm
VST	Variable Seed Test

5 Design Philosophy of the Random Number Generator Validation System

The RNGVS is designed to test conformance to the various approved RNG specifications 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 RNGVS has the following design philosophy:

1. The RNGVS is designed to allow the testing of an IUT at locations remote to the RNGVS. The RNGVS and the IUT communicate data via *REQUEST* and *RESPONSE* files. The RNGVS also generates *SAMPLE* files to provide the IUT with a sample of what the *RESPONSE* file should look like.

2. The testing performed within the RNGVS 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 RNGVS Tests

The RNGVS tests various RNG algorithm implementations for their conformance to their respective standards. The testing for each algorithm consists of two tests: the Variable Seed Test (VST) and a Monte Carlo Test (MCT). The algorithms tested are:

- DSA – FIPS 186-2 Appendix 3.1 – Algorithm for Computing *m* values of *x* (using SHA-1 and/or DEA),

- DSA – FIPS 186-2 Appendix 3.2 – Algorithm for Precomputing One or More *k* and *r* Values (using SHA-1 and/or DEA),

- ECDSA – ANSI X9.62-1998 Appendix A.4 - Pseudorandom Number Generation (using SHA-1 and/or DEA), and

- rDSA – ANSI X9.31-1998 - Generating Pseudo Random Numbers Using the DEA, and

- A NIST-recommended RNG based on ANSI X9.31 Appendix A.2.4 allowing the use of 3-Key Triple DES and AES

6.1 Configuration Information

To initiate the validation process of the RNGVS, a vendor submits an application to an accredited laboratory requesting the validation of its implementation of an RNG. 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 RNGVS to perform the specific tests. More specifically, the request for validation includes:

1. Vendor Name;

2. Product Name;

3. Product Version;

4. Implementation in software, firmware, or hardware;

5. Processor and Operating System with which the IUT was tested if the IUT is implemented in software or firmware;

6. Brief description of the IUT or the product/product family in which the IUT is implemented by the vendor (2-3 sentences); and

7. Specific configuration information, as needed, for the RNG algorithms implemented by the IUT:

    a) DSA - Generation of X

        - Whether the implementation contains the original specification, the Change Notice (10/5/2001) specification, or both;

        - Whether the G function is constructed from SHA-1, DEA, or both;

- Whether the algorithm is used as specified or as a generic purpose random number generator[1], or both;

- The minimum and maximum seed lengths ($160 \leq minlen \leq maxlen \leq 512$) the implementation supports; and

- The value of the domain parameter Q if a specific value is required by the implementation.

b) DSA - Generation of K

- Whether the implementation contains the original specification, the Change Notice (10/5/2001) specification, or both;

- Whether the G function is constructed from SHA-1, DEA, or both;

- The minimum and maximum seed lengths ($160 \leq minlen \leq maxlen \leq 512$) the implementation supports; and

- The value of the domain parameter Q if a specific value is required by the implementation.

c) ECDSA - Pseudorandom Number Generation

- The specific NIST Recommended Curves the implementation supports;

- Whether the G function is constructed from SHA-1, DEA, or both; and

- The minimum and maximum seed lengths ($160 \leq minlen \leq maxlen \leq 512$) the implementation supports.

d) RSA – Pseudorandom Number Generation

- Which algorithm is used – DEA 2-Key, Triple DES 3-Key, or AES

- If AES, the key size(s) supported – 124, 192, and/or 256.

---

[1] As per the last section of the Change Notice 1 of FIPS 186-2, dated 2001 October 5, the algorithm specified in Appendix 3.1 of FIPS 186-2 or algorithm 1 of the Change Notice can be used as a general purpose RNG. In this case the “mod q” at the end of the algorithms is omitted. The file names associated with these test have “GEN” preceding the extension.

6.2 The Variable Seed Test

The Variable Seed Test provides a series of seeds, each with a one-bit difference from the previous seed. The algorithm uses the *SEED* value to generate the random value with the algorithm being tested.

The RNGVS:

A. Creates a *REQUEST* file (Filename: <Alg>_VST[GEN].req) containing:

   1. The Product Name;
   2. The algorithm being tested; and
   3. The *SEED* values used as input to the RNG algorithm.

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

B. Creates a *FAX* file (Filename: <Alg>_VST[GEN].fax) containing:

   1. The Product Name;
   2. The algorithm being tested;
   3. The *SEED* values used as input to the RNG algorithm; and
   4. The random values produced from the *SEED* provided.

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

The IUT:

A. Generates the requested random values from the *SEED*'s specified in the *REQUEST* file.

B. Creates a *RESPONSE* file (Filename: <Alg>_VST[GEN].rsp) containing:

   1. The Product Name;
   2. The algorithm being tested;
   3. The *SEED* values used as input to the RNG algorithm; and
   4. The random values produced from the *SEED* provided.

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

The RNGVS:

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

B. If all values match, records PASS for this test; otherwise, records FAIL.

6.3 The Monte Carlo Test

The Monte Carlo Test provides a *SEED* value to be used by the algorithm being tested. The algorithm uses the *SEED* value to generate a sequence of random value with the algorithm being tested. The algorithm being tested prescribes a method for creating a new *SEED* value from the existing value.

For each *SEED* value supplied, the IUT produces a sequence of 10,000 random values. The final random value is supplied in the *RESPONSE* file for verification.

The RNGVS:

A. Creates a *REQUEST* file (Filename: <Alg>_MCT[GEN].req) containing:

   1. The Product Name;
   2. The algorithm being tested; and
   3. One or more *SEED* values (depending on the algorithm being tested).

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

B. Creates a *FAX* file (Filename: <Alg>_MCT[GEN].fax) containing:

   1. The information from the *REQUEST* file; and
   2. For each *SEED* value present, the $10{,}000^{th}$ random value derived from the RNG algorithm being tested.

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

The IUT:

A. For each *SEED* value found in the *REQUEST* file, generates 10,000 random values.

B. Creates a *RESPONSE* file (Filename: <Alg>_MCT[GEN].rsp) containing:

   1. The information from the *REQUEST* file; and
   2. For each *SEED* value, the $10{,}000^{th}$ random value it produces.

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

The RNGVS:

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

B. If the results for all *SEED* values match, records PASS for this test; otherwise, records FAIL.

6.4 Specific Requirements for Testing the RNG found in ANSI X9.31 Appendix A.2.4

The SEED value specified in the VST and the MCT are used as the input vector V of ANSI X9.31-1998 Appendix A.2.4. The initial date/time vector and the two key values are supplied by the RNGVS. In the Monte Carlo Test, subsequent date/time vectors are calculated by incrementing the previous value by one.

6.5 Specific Requirements for Testing the NIST-Recommended RNG Based on ANSI X9.31 Appendix A.2.4 allowing 3-Key Triple DES and AES

The SEED value specified in the VST and the MCT are used as the input vector V of the document "NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES". The initial date/time vector and the appropriate number of key values are supplied by the RNGVS. For 3-Key Triple DES, three 64 bit keys will be supplied. For AES, the key supplied by the RNGVS will be of the key length specified - 128 bits, 192 bits, or 256 bits. In the Monte Carlo Test, subsequent date/time vectors are calculated by incrementing the previous value by one.

For all Triple DES implementations, the length of the SEED value, the date/time vector(DT), the intermediate value (I), and the answer (R) are 64 bits each.

For all AES implementations, the length of the SEED value, the date/time vector (DT), the intermediate value (I), and the answer (R) are 128 bits each.

Appendix A References

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

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

[3] *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*, ANSI X9.31-1988, September 1998.

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

[5] *NIST-Recommended Random Number Generator Based on ANSI X9.31Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms*, January 31, 2005.

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

The following are partial examples of *REQUEST*, *FAX*, *RESPONSE*, and *SAMPLE* files for each of the algorithms tested by the RNGVS.

B.1 Examples of *REQUEST* Files

B.1.1 FIPS186_VST.req

```
#  CAVS 2.2
#  "FIPS 186" information for "Demo Product"
#  Generators selected: Xorg
#  G-Functions selected: SHA-1 DES
#  Generated on Tue Jun 03 09:18:10 2003

[Xorg - SHA1]

Q = 9eedc3fde07ed95848e3e0f0c7e690ad1327e511

COUNT = 0
b = 160
XKey = 8000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

COUNT = 1
b = 160
XKey = c0000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

COUNT = 2
b = 160
XKey = e0000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

COUNT = 3
b = 160
XKey = f0000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

COUNT = 4
b = 160
XKey = f8000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

...

COUNT = 158
b = 160
XKey = fffffffffffffffffffffffffffffffffffffffe
XSeed = 0000000000000000000000000000000000000000

COUNT = 159
b = 160
XKey = ffffffffffffffffffffffffffffffffffffffff
XSeed = 0000000000000000000000000000000000000000
```

```
[Xorg - DES]

Q = 9eedc3fde07ed95848e3e0f0c7e690ad1327e511

COUNT = 0
b = 160
XKey = 8000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

COUNT = 1
b = 160
XKey = c0000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

COUNT = 2
b = 160
XKey = e0000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

COUNT = 3
b = 160
XKey = f0000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

COUNT = 4
b = 160
XKey = f8000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

...

COUNT = 158
b = 160
XKey = fffffffffffffffffffffffffffffffffffffffe
XSeed = 0000000000000000000000000000000000000000

COUNT = 159
b = 160
XKey = ffffffffffffffffffffffffffffffffffffffff
XSeed = 0000000000000000000000000000000000000000
```

B.1.2 FIPS186_MCT.req

```
#  CAVS 2.2
#  "FIPS 186" information for "Demo Product"
#  Generators selected: Xorg
#  G-Functions selected: SHA-1 DES
#  Generated on Tue Jun 03 09:18:10 2003

[Xorg - SHA1]

Q = 9eedc3fde07ed95848e3e0f0c7e690ad1327e511

COUNT = 0
b = 160
XKey = f6a2525581101c00a95c2c361b1036eacbde6f8c
XSeed = 0000000000000000000000000000000000000000
```

```
COUNT = 1
b = 168
XKey = 4a6c639722bc332d8c38ce71c6bbf42e3f8536c69e
XSeed = 000000000000000000000000000000000000000000

COUNT = 2
b = 176
XKey = 6972eaf9dcb2a0b73cffafe8cd1f16a022ea9b99dfff
XSeed = 00000000000000000000000000000000000000000000

...

COUNT = 43
b = 504
XKey =
9d889fc34c4742779964247113026 3a0f837545f4bcb2d55283d01995507f21a1923a23f51ceea
cac08ccf02a76cb111958dc6ab81e1c7f01631e9944e620f
XSeed =
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000

COUNT = 44
b = 512
XKey =
178f92b47a9142c23ccc567b714cb5fb56ad9f55423c3ed8d9597e9183201f101d48096fee4adf
91dcc6d6a8df23c8fab77784e4daa6691fb1cd334203e11488
XSeed =
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000

[Xorg - DES]

Q = 9eedc3fde07ed95848e3e0f0c7e690ad1327e511

COUNT = 0
b = 160
XKey = 996074f46f789f55e0a8c9ec1c2fc19b8f9a74e7
XSeed = 0000000000000000000000000000000000000000
```

B.1.3 ANSI962_VST.req

```
#  CAVS 2.2
#  "ANSI X9.62" information for "Demo Product"
#  Generators selected: P-192
#  G-Functions selected: SHA-1 DES
#  Generated on Tue Jun 03 09:18:15 2003

[P-192 - SHA1]

N = ffffffffffffffffffffff99def836146bc9b1b4d22831

COUNT = 0
b = 160
XKey = 8000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

COUNT = 1
```

```
b = 160
XKey = c000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

COUNT = 2
b = 160
XKey = e000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

COUNT = 3
b = 160
XKey = f000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

COUNT = 4
b = 160
XKey = f800000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

...

COUNT = 158
b = 160
XKey = fffffffffffffffffffffffffffffffffffffffe
XSeed = 0000000000000000000000000000000000000000

COUNT = 159
b = 160
XKey = ffffffffffffffffffffffffffffffffffffffff
XSeed = 0000000000000000000000000000000000000000

[P-192 - DES]

N = ffffffffffffffffffffff99def836146bc9b1b4d22831

COUNT = 0
b = 160
XKey = 800000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

COUNT = 1
b = 160
XKey = c000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

COUNT = 2
b = 160
XKey = e000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

COUNT = 3
b = 160
XKey = f000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000

COUNT = 4
b = 160
XKey = f800000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
```

```
...

COUNT = 158
b = 160
XKey = ffffffffffffffffffffffffffffffffffffffffe
XSeed = 0000000000000000000000000000000000000000

COUNT = 159
b = 160
XKey = fffffffffffffffffffffffffffffffffffffffff
XSeed = 0000000000000000000000000000000000000000
```

B.1.4 ANSI962_MCT.req

```
#  CAVS 2.2
#  "ANSI X9.62" information for "Demo Product"
#  Generators selected: P-192
#  G-Functions selected: SHA-1 DES
#  Generated on Tue Jun 03 09:18:15 2003

[P-192 - SHA1]

N = ffffffffffffffffffffff99def836146bc9b1b4d22831

COUNT = 0
b = 160
XKey = c5d2c492698ae4947f3a44647562f133cf47ab0b
XSeed = 0000000000000000000000000000000000000000

COUNT = 1
b = 168
XKey = 3d243bfd5274dea3f50dcedc764a12603858316a1d
XSeed = 0000000000000000000000000000000000000000

COUNT = 2
b = 176
XKey = 5ca84c37a0d41e02c3253ea9f45e72ad439c74b15839
XSeed = 0000000000000000000000000000000000000000

...

COUNT = 43
b = 504
XKey =
798c427f180ce56f0360ee885ab42683c5a115d3b85c6b7ef52d9e2c5223d57dbc0705a07c8e59
22b9d2d8033e03420f7e5a3a6bd54faa6f110c64b3312105
XSeed =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000

COUNT = 44
b = 512
XKey =
8716e89fe11be3d607873f205655de6369c8cb123afc7b5c89c053a482a86b329a5d9228ba3892
b79f0fb592814f87a3f24bdefe0ad41813c10aa4279c71c405
XSeed =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000
```

```
[P-192 - DES]

N = ffffffffffffffffffffffff99def836146bc9b1b4d22831

COUNT = 0
b = 160
XKey = 98419df16f74197c100b261b197a7b7e0c8cc178
XSeed = 000000000000000000000000000000000000000000
```

B.1.5 ANSI931_TDES2VST.req

```
#  CAVS 2.2
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jun 03 09:18:59 2003

COUNT = 0
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3c
V = 8000000000000000

COUNT = 1
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3d
V = c000000000000000

COUNT = 2
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3e
V = e000000000000000

COUNT = 3
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3f
V = f000000000000000

COUNT = 4
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f40
V = f800000000000000

...

COUNT = 62
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f7a
V = fffffffffffffffe

COUNT = 63
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f7b
```

```
V = ffffffffffffffff
```

B.1.6 ANSI931_TDES2MCT.req

```
#  CAVS 2.2
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jun 03 09:18:59 2003

Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3c
V = d5538f9cf450f53c
```

B.1.7 ANSI931_TDES3VST.req

```
#  CAVS 4.3
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jan 11 12:11:44 2005

[X9.31]
[3-Key TDES]

COUNT = 0
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b0e
V = 8000000000000000

COUNT = 1
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b0f
V = c000000000000000

COUNT = 2
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b10
V = e000000000000000

COUNT = 3
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b11
V = f000000000000000

COUNT = 4
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b12
V = f800000000000000
```

```
...
COUNT = 62
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b4c
V = fffffffffffffffe

COUNT = 63
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b4d
V = ffffffffffffffff
```

B.1.8 ANSI931_TDES3MCT.req

```
#  CAVS 4.3
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jan 11 12:11:44 2005

[X9.31]
[3-Key TDES]

COUNT = 0
Key1 = 5da89497aebc8585
Key2 = 92e9b5161367830e
Key3 = fbb96bbff4757616
DT = ca09a63118bb0111
V = e7ee96932e56e746
```

B.1.9 ANSI931_AES128VST.req

```
#  CAVS 4.3
#  "ANSI X9.31" information for "DEMO PRODUCT"
#  Generated on Tue Jan 11 12:11:44 2005

[X9.31]
[AES 128-Key]

COUNT = 0
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e922f9
V = 80000000000000000000000000000000

COUNT = 1
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e922fa
V = c0000000000000000000000000000000

COUNT = 2
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e922fb
V = e0000000000000000000000000000000
```

```
COUNT = 3
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e922fc
V = f000000000000000000000000000000

COUNT = 4
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e922fd
V = f800000000000000000000000000000

...

COUNT = 126
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e92377
V = fffffffffffffffffffffffffffffffe

COUNT = 127
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e92378
V = ffffffffffffffffffffffffffffffff
```

B.1.10 ANSI931_AES128MCT.req

```
#  CAVS 4.3
#  "ANSI X9.31" information for "DEMO PRODUCT"
#  Generated on Tue Jan 11 12:11:44 2005

[X9.31]
[AES 128-Key]

COUNT = 0
Key = 9f5b51200bf334b5d82be8c37255c848
DT = 6376bbe52902ba3b67c925fa701f11ac
V = 572c8e76872647977e74fbddc49501d1
```

B.1.11 ANSI931_AES192VST.req

```
#  CAVS 4.3
#  "ANSI X9.31" information for "DEMO PRODUCT"
#  Generated on Tue Jan 11 12:11:45 2005

[X9.31]
[AES 192-Key]

COUNT = 0
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f34b
V = 800000000000000000000000000000

COUNT = 1
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f34c
V = c00000000000000000000000000000
```

```
COUNT = 2
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f34d
V = e000000000000000000000000000000

COUNT = 3
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f34e
V = f000000000000000000000000000000

COUNT = 4
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f34f
V = f800000000000000000000000000000

...

COUNT = 126
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f3c9
V = fffffffffffffffffffffffffffffffe

COUNT = 127
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f3ca
V = ffffffffffffffffffffffffffffffff
```

B.1.12 ANSI931_AES192MCT.req

```
#  CAVS 4.3
#  "ANSI X9.31" information for "DEMO PRODUCT"
#  Generated on Tue Jan 11 12:11:45 2005

[X9.31]
[AES 192-Key]

COUNT = 0
Key = b76c34d10967ab734d5ad53498160b91bc3551166bae938a
DT = 84ce227d915aa3c9843c0ab3a9631552
V = b6afe68f999e9064ddc77ac1bb903a6d
```

B.1.13 ANSI931_AES256VST.req

```
#  CAVS 4.3
#  "ANSI X9.31" information for "DEMO PRODUCT"
#  Generated on Tue Jan 11 12:11:45 2005

[X9.31]
[AES 256-Key]

COUNT = 0
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9e88
V = 800000000000000000000000000000

COUNT = 1
```

```
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9e89
V = c0000000000000000000000000000000

COUNT = 2
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9e8a
V = e0000000000000000000000000000000

COUNT = 3
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9e8b
V = f0000000000000000000000000000000

COUNT = 4
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9e8c
V = f8000000000000000000000000000000

...

COUNT = 126
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9f06
V = fffffffffffffffffffffffffffffffe

COUNT = 127
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9f07
V = ffffffffffffffffffffffffffffffff
```

B.1.14ANSI931_AES256MCT.req

```
#  CAVS 4.3
#  "ANSI X9.31" information for "DEMO PRODUCT"
#  Generated on Tue Jan 11 12:11:45 2005

[X9.31]
[AES 256-Key]

COUNT = 0
Key = 9b05c868ff47f83aa63aa8cb4e71b2e0b87ef137b6b4f66d8632fc1f5e1d1e50
DT = 316e359ab144f0ee626d0446e0a3924c
V = 4fcdc187821f4da13e0e564459e883ca
```

B.2 Examples of *FAX* Files

B.2.1 FIPS186_VST.fax

```
#  CAVS 2.2
#  "FIPS 186" information for "Demo Product"
#  Generators selected: Xorg
#  G-Functions selected: SHA-1 DES
#  Generated on Tue Jun 03 09:18:10 2003

[Xorg - SHA1]
```

```
Q = 9eedc3fde07ed95848e3e0f0c7e690ad1327e511

COUNT = 0
b = 160
XKey = 80000000000000000000000000000000000000000
XSeed = 00000000000000000000000000000000000000000
X = 3b4bdff07dec71b4e971defecd7987e39cb021f8

COUNT = 1
b = 160
XKey = c0000000000000000000000000000000000000000
XSeed = 00000000000000000000000000000000000000000
X = 5dde2767380ae76c3a884ea4240feb11468729e7

COUNT = 2
b = 160
XKey = e0000000000000000000000000000000000000000
XSeed = 00000000000000000000000000000000000000000
X = 12098135df8852d450ee60b3fe0e368eb06f18e1

COUNT = 3
b = 160
XKey = f0000000000000000000000000000000000000000
XSeed = 00000000000000000000000000000000000000000
X = 3f87039d81ff007b02d2a4cbf1eb28be42ad9fc3

COUNT = 4
b = 160
XKey = f8000000000000000000000000000000000000000
XSeed = 00000000000000000000000000000000000000000
X = 76aae1571999ccf26fc1d8050da716fcd1d4601e

...

COUNT = 158
b = 160
XKey = fffffffffffffffffffffffffffffffffffffffffe
XSeed = 00000000000000000000000000000000000000000
X = 089fc77cf8929c246fcee00b92c27676cca08e75

COUNT = 159
b = 160
XKey = ffffffffffffffffffffffffffffffffffffffffff
XSeed = 00000000000000000000000000000000000000000
X = 2fa01580d4bf0f60509990be4e084272e95a48da

[Xorg - DES]

Q = 9eedc3fde07ed95848e3e0f0c7e690ad1327e511

COUNT = 0
b = 160
XKey = 80000000000000000000000000000000000000000
XSeed = 00000000000000000000000000000000000000000
X = 870f8a5c137c1093c7a8fd53179ff2ce7b0cf127

COUNT = 1
b = 160
XKey = c0000000000000000000000000000000000000000
XSeed = 00000000000000000000000000000000000000000
```

```
X = 218de164a97806592fb03f086a9c3c036f1e6e9d

COUNT = 2
b = 160
XKey = e000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = 98169623fa3daf298513ec5ca79ac3cac2950fdb

COUNT = 3
b = 160
XKey = f000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = 5d52a7751e05fd2af30bc9f2087084429cf5c11e

COUNT = 4
b = 160
XKey = f800000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = 34d5f9134b28785a277229ce8e1d09c6a1a76820

...

COUNT = 158
b = 160
XKey = fffffffffffffffffffffffffffffffffffffffe
XSeed = 0000000000000000000000000000000000000000
X = 14329258f79a332ae886bb9e999630b7621c31fd

COUNT = 159
b = 160
XKey = ffffffffffffffffffffffffffffffffffffffff
XSeed = 0000000000000000000000000000000000000000
X = 7fc24dcfc05cf975f702ac609f34b97d219a9f93
```

B.2.2 FIPS186_MCT.fax

```
#  CAVS 2.2
#  "FIPS 186" information for "Demo Product"
#  Generators selected: Xorg
#  G-Functions selected: SHA-1 DES
#  Generated on Tue Jun 03 09:18:10 2003

[Xorg - SHA1]

Q = 9eedc3fde07ed95848e3e0f0c7e690ad1327e511

COUNT = 0
b = 160
XKey = f6a2525581101c00a95c2c361b1036eacbde6f8c
XSeed = 0000000000000000000000000000000000000000
X = 06c18ad835835e66cd7deaef3345184e76140458

COUNT = 1
b = 168
XKey = 4a6c639722bc332d8c38ce71c6bbf42e3f8536c69e
XSeed = 0000000000000000000000000000000000000000
X = 7d08cb2a2427672ea4f6080b21cba49dd677179b
```

```
COUNT = 2
b = 176
XKey = 6972eaf9dcb2a0b73cffafe8cd1f16a022ea9b99dfff
XSeed = 000000000000000000000000000000000000000000000000
X = 389b630aa81a2099540a5fb1c691d5efef651a76

...

COUNT = 43
b = 504
XKey =
9d889fc34c474277996424711302 63a0f837545f4bcb2d55283d01995507f21a1923a23f51ceea
cac08ccf02a76cb111958dc6ab81e1c7f01631e9944e620f
XSeed =
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000
X = 96c21afc2aa2a1466e32499185e42f3af60d8b3a

COUNT = 44
b = 512
XKey =
178f92b47a9142c23ccc567b714cb5fb56ad9f55423c3ed8d9597e9183201f101d48096fee4adf
91dcc6d6a8df23c8fab77784e4daa6691fb1cd334203e11488
XSeed =
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000
X = 10a44a898faf7592035d273b2335c3e3112a469e

[Xorg - DES]

Q = 9eedc3fde07ed95848e3e0f0c7e690ad1327e511

COUNT = 0
b = 160
XKey = 996074f46f789f55e0a8c9ec1c2fc19b8f9a74e7
XSeed = 0000000000000000000000000000000000000000
X = 24026bc49010f4a2ce7d510cfbfb7497cee12e18
```

B.2.3 ANSI962_VST.fax

```
#  CAVS 2.2
#  "ANSI X9.62" information for "Demo Product"
#  Generators selected: P-192
#  G-Functions selected: SHA-1 DES
#  Generated on Tue Jun 03 09:18:15 2003

[P-192 - SHA1]

N = ffffffffffffffffffffff99def836146bc9b1b4d22831

COUNT = 0
b = 160
XKey = 8000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = 7ebf6e9c0f9828de5590fe0139c27574ae95ba3c075384c9

COUNT = 1
b = 160
```

```
XKey = c000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = f1ab3e2f58395deccaf697271e81cea97971fdc6a7444b2b

COUNT = 2
b = 160
XKey = e000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = a5a8cb5f81d6efa6ba3f7b02a677cbb8338faa8f69228fc2

COUNT = 3
b = 160
XKey = f000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = 4857d8e69abc4bdd26ee8d4821e59578e65bfc47ceec9061

COUNT = 4
b = 160
XKey = f800000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = d7c9d482b774b00f48b82569e77fe80918af87c62e748ccf

...

COUNT = 158
b = 160
XKey = fffffffffffffffffffffffffffffffffffffffe
XSeed = 0000000000000000000000000000000000000000
X = 7a9eb9d0cefb5938aa1b4c73912bc497c73a129a1099809c

COUNT = 159
b = 160
XKey = ffffffffffffffffffffffffffffffffffffffff
XSeed = 0000000000000000000000000000000000000000
X = 4e743d8ad7eb660bb44e06143344c45b7f758c2efb2c35dc

[P-192 - DES]

N = ffffffffffffffffffffffff99def836146bc9b1b4d22831

COUNT = 0
b = 160
XKey = 800000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = f4f47f39c0922d1c8fd50855e7888eb02c3a14ac0f4d3378

COUNT = 1
b = 160
XKey = c000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = f10e7d54e4c290833df478f2147aecc18cc4b68e659ab803

COUNT = 2
b = 160
XKey = e000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = 06b88cd5f46a23efb3a23e1b0b00670bd18316d72a7065b7

COUNT = 3
b = 160
```

```
XKey = f000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = 14ff126a72431e664ebd6fbf2ced6ea53bff2f883924f81c

COUNT = 4
b = 160
XKey = f800000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = f385520dbb15dde89fd3787630ddb6d0724bf48e30ccd012

...

COUNT = 158
b = 160
XKey = fffffffffffffffffffffffffffffffffffffffe
XSeed = 0000000000000000000000000000000000000000
X = 028701bdc0b422547932d71271b4ddf9af830a95853a4dcf

COUNT = 159
b = 160
XKey = ffffffffffffffffffffffffffffffffffffffff
XSeed = 0000000000000000000000000000000000000000
X = 054892327a14e4b6ef7d5c97c59688055a022cda0cf20e26
```

B.2.4 ANSI962_MCT.fax

```
#  CAVS 2.2
#  "ANSI X9.62" information for "Demo Product"
#  Generators selected: P-192
#  G-Functions selected: SHA-1 DES
#  Generated on Tue Jun 03 09:18:15 2003

[P-192 - SHA1]

N = ffffffffffffffffffffff99def836146bc9b1b4d22831

COUNT = 0
b = 160
XKey = c5d2c492698ae4947f3a44647562f133cf47ab0b
XSeed = 0000000000000000000000000000000000000000
X = 7a86414d4ee5762d5b28d19ec04a7dcb08376761cd280a38

COUNT = 1
b = 168
XKey = 3d243bfd5274dea3f50dcedc764a12603858316a1d
XSeed = 0000000000000000000000000000000000000000
X = 7ffc4672c9eb70d064c99e31021f443667f70de14addf33d

COUNT = 2
b = 176
XKey = 5ca84c37a0d41e02c3253ea9f45e72ad439c74b15839
XSeed = 0000000000000000000000000000000000000000000000000000
X = e16c91d6e2eb04dac142573d33a91d758798502cbd293cf3

...

COUNT = 43
b = 504
```

```
XKey =
798c427f180ce56f0360ee885ab42683c5a115d3b85c6b7ef52d9e2c5223d57dbc0705a07c8e59
22b9d2d8033e03420f7e5a3a6bd54faa6f110c64b3312105
XSeed =
000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000
X = cd471389238c9c1f39034531baa8b023338b781af2cfb731

COUNT = 44
b = 512
XKey =
8716e89fe11be3d607873f205655de6369c8cb123afc7b5c89c053a482a86b329a5d9228ba3892
b79f0fb592814f87a3f24bdefe0ad41813c10aa4279c71c405
XSeed =
000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000
X = feaf7968bd801f39a4b3422f631854e9bd39aab36a8254af

[P-192 - DES]

N = ffffffffffffffffffffff99def836146bc9b1b4d22831

COUNT = 0
b = 160
XKey = 98419df16f74197c100b261b197a7b7e0c8cc178
XSeed = 0000000000000000000000000000000000000000
X = 136af998090924a478cbe45d713ce405f9ae95485a9f7a57
```

B.2.5 ANSI931_TDES2VST.fax

```
#  CAVS 2.2
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jun 03 09:18:59 2003

COUNT = 0
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3c
V = 8000000000000000
R = 944dc7210d6d7fd7

COUNT = 1
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3d
V = c000000000000000
R = af1a648591bb7c2c

COUNT = 2
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3e
V = e000000000000000
R = 221839b07451e423

COUNT = 3
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
```

```
DT = c89a1d888ed12f3f
V = f000000000000000
R = eba9271e04043712

COUNT = 4
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f40
V = f800000000000000
R = 02433c9417a3326f

...

COUNT = 62
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f7a
V = fffffffffffffffe
R = 13eeb44dcba310f1

COUNT = 63
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f7b
V = ffffffffffffffff
R = e7e2b2964f36ed41
```

B.2.6 ANSI931_TDES2MCT.fax

```
#  CAVS 2.2
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jun 03 09:18:59 2003

Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3c
V = d5538f9cf450f53c
R = eedd9df4a3cce54e
```

B.2.7 ANSI931_TDES3VST.fax

```
#  CAVS 4.3
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jan 11 12:11:44 2005

[X9.31]
[3-Key TDES]

COUNT = 0
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b0e
V = 8000000000000000
R = 77df53333a5b44eb
```

```
COUNT = 1
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b0f
V = c000000000000000
R = 122a51e2a9025753

COUNT = 2
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b10
V = e000000000000000
R = b0178d244b0bbb67

COUNT = 3
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b11
V = f000000000000000
R = 1a9018f42884e9f1

COUNT = 4
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b12
V = f800000000000000
R = 47c49679d85ffd79

...

COUNT = 62
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b4c
V = fffffffffffffffe
R = 59dda16bdcedb379

COUNT = 63
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b4d
V = ffffffffffffffff
R = b7d312c46f5da339
```

B.2.8 ANSI931_TDES3MCT.fax

```
#  CAVS 4.3
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jan 11 12:11:44 2005

[X9.31]
[3-Key TDES]
```

```
COUNT = 0
Key1 = 5da89497aebc8585
Key2 = 92e9b5161367830e
Key3 = fbb96bbff4757616
DT = ca09a63118bb0111
V = e7ee96932e56e746
R = efe4b7d2c7fd6531
```

B.2.9 ANSI931_AES128VST.fax

```
#  CAVS 4.3
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jan 11 12:11:44 2005

[X9.31]
[AES 128-Key]

COUNT = 0
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e922f9
V = 80000000000000000000000000000000
R = 59531ed13bb0c05584796685c12f7641

COUNT = 1
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e922fa
V = c0000000000000000000000000000000
R = 7c222cf4ca8fa24c1c9cb641a9f3220d

COUNT = 2
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e922fb
V = e0000000000000000000000000000000
R = 8aaa003966675be529142881a94d4ec7

COUNT = 3
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e922fc
V = f0000000000000000000000000000000
R = 88dda456302423e5f69da57e7b95c73a

COUNT = 4
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e922fd
V = f8000000000000000000000000000000
R = 052592466179d2cb78c40b140a5a9ac8

...
COUNT = 126
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e92377
V = fffffffffffffffffffffffffffffffe
R = 0dd5a0367a5926bc48d938bff0858fea

COUNT = 127
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e92378
```

```
V = ffffffffffffffffffffffffffffffff
R = ae5387ee8cd912f57353ae03f9d51333
```

B.2.10 ANSI931_AES128MCT.fax

```
#  CAVS 4.3
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jan 11 12:11:44 2005

[X9.31]
[AES 128-Key]

COUNT = 0
Key = 9f5b51200bf334b5d82be8c37255c848
DT = 6376bbe52902ba3b67c925fa701f11ac
V = 572c8e76872647977e74fbddc49501d1
R = 48e9bd0d06ee18fbe45790d5c3fc9b73
```

B.2.11 ANSI931_AES192VST.fax

```
#  CAVS 4.3
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jan 11 12:11:45 2005

[X9.31]
[AES 192-Key]

COUNT = 0
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f34b
V = 80000000000000000000000000000000
R = 1707d52819791eefa50cbf25e556b493

COUNT = 1
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f34c
V = c0000000000000000000000000000000
R = 928dbe07ddc758c06f35419b17c9bd9b

COUNT = 2
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f34d
V = e0000000000000000000000000000000
R = d5def450f3b7104eb8c6f8cfe2b1caa2

COUNT = 3
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f34e
V = f0000000000000000000000000000000
R = ce290843fc3441e7478fb3662b46b1bb

COUNT = 4
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f34f
V = f8000000000000000000000000000000
R = b3260ff5d6caa8bf89b85e2f2256922f

...

COUNT = 126
```

```
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f3c9
V = fffffffffffffffffffffffffffffffe
R = 05eb1852344300436e5aa5fe7b32c42d

COUNT = 127
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f3ca
V = ffffffffffffffffffffffffffffffff
R = 153ce8d104c7ad500bf00716e7567aea
```

B.2.12 ANSI931_AES192MCT.fax

```
#  CAVS 4.3
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jan 11 12:11:45 2005

[X9.31]
[AES 192-Key]

COUNT = 0
Key = b76c34d10967ab734d5ad53498160b91bc3551166bae938a
DT = 84ce227d915aa3c9843c0ab3a9631552
V = b6afe68f999e9064ddc77ac1bb903a6d
R = fc85609a296fef21dd8620328a296f47
```

B.2.13 ANSI931_AES256VST.fax

```
#  CAVS 4.3
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jan 11 12:11:45 2005

[X9.31]
[AES 256-Key]

COUNT = 0
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9e88
V = 80000000000000000000000000000000
R = 35c7efa7784d29bc827999fbd0b33b72

COUNT = 1
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9e89
V = c0000000000000000000000000000000
R = 6cf4425dc7041a41282a78a9b012c495

COUNT = 2
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9e8a
V = e0000000000000000000000000000000
R = 1690a4ff7b7eb930db674bac2de1d175

COUNT = 3
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9e8b
V = f0000000000000000000000000000000
R = 146ff595a1466530bc57e24af7456205
```

```
COUNT = 4
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9e8c
V = f80000000000000000000000000000000
R = 96e2b41e665e0fa4c5cda207ccb79440

...

COUNT = 126
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9f06
V = fffffffffffffffffffffffffffffffe
R = 61ce1d6a487597284b41de18444f56ec

COUNT = 127
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9f07
V = ffffffffffffffffffffffffffffffff
R = 528959792daa28b3b08a3e70fa715984
```

B.2.14 ANSI931_AES256MCT.fax

```
#  CAVS 4.3
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jan 11 12:11:45 2005

[X9.31]
[AES 256-Key]

COUNT = 0
Key = 9b05c868ff47f83aa63aa8cb4e71b2e0b87ef137b6b4f66d8632fc1f5e1d1e50
DT = 316e359ab144f0ee626d0446e0a3924c
V = 4fcdc187821f4da13e0e564459e883ca
R = c887c2615bd0b9e1e7f38bd75bd5f18d
```

B.3 Examples of *RESPONSE* Files

B.3.1 FIPS186_VST.rsp

```
#  CAVS 2.2
#  "FIPS 186" information for "Demo Product"
#  Generators selected: Xorg
#  G-Functions selected: SHA-1 DES

[Xorg - SHA1]

Q = 9eedc3fde07ed95848e3e0f0c7e690ad1327e511

COUNT = 0
b = 160
XKey = 8000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = 3b4bdff07dec71b4e971defecd7987e39cb021f8

COUNT = 1
b = 160
XKey = c0000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
```

```
X = 5dde2767380ae76c3a884ea4240feb11468729e7

COUNT = 2
b = 160
XKey = e000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = 12098135df8852d450ee60b3fe0e368eb06f18e1

COUNT = 3
b = 160
XKey = f000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = 3f87039d81ff007b02d2a4cbf1eb28be42ad9fc3

COUNT = 4
b = 160
XKey = f800000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = 76aae1571999ccf26fc1d8050da716fcd1d4601e

...

COUNT = 158
b = 160
XKey = fffffffffffffffffffffffffffffffffffffffe
XSeed = 0000000000000000000000000000000000000000
X = 089fc77cf8929c246fcee00b92c27676cca08e75

COUNT = 159
b = 160
XKey = ffffffffffffffffffffffffffffffffffffffff
XSeed = 0000000000000000000000000000000000000000
X = 2fa01580d4bf0f60509990be4e084272e95a48da

[Xorg - DES]

Q = 9eedc3fde07ed95848e3e0f0c7e690ad1327e511

COUNT = 0
b = 160
XKey = 800000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = 870f8a5c137c1093c7a8fd53179ff2ce7b0cf127

COUNT = 1
b = 160
XKey = c000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = 218de164a97806592fb03f086a9c3c036f1e6e9d

COUNT = 2
b = 160
XKey = e000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = 98169623fa3daf298513ec5ca79ac3cac2950fdb

COUNT = 3
b = 160
XKey = f000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
```

```
X = 5d52a7751e05fd2af30bc9f2087084429cf5c11e

COUNT = 4
b = 160
XKey = f800000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = 34d5f9134b28785a277229ce8e1d09c6a1a76820

...

COUNT = 158
b = 160
XKey = fffffffffffffffffffffffffffffffffffffffe
XSeed = 0000000000000000000000000000000000000000
X = 14329258f79a332ae886bb9e999630b7621c31fd

COUNT = 159
b = 160
XKey = ffffffffffffffffffffffffffffffffffffffff
XSeed = 0000000000000000000000000000000000000000
X = 7fc24dcfc05cf975f702ac609f34b97d219a9f93
```

B.3.2 FIPS186_MCT.rsp

```
#  CAVS 2.2
#  "FIPS 186" information for "Demo Product"
#  Generators selected: Xorg
#  G-Functions selected: SHA-1 DES

[Xorg - SHA1]

Q = 9eedc3fde07ed95848e3e0f0c7e690ad1327e511

COUNT = 0
b = 160
XKey = f6a2525581101c00a95c2c361b1036eacbde6f8c
XSeed = 0000000000000000000000000000000000000000
X = 06c18ad835835e66cd7deaef3345184e76140458

COUNT = 1
b = 168
XKey = 4a6c639722bc332d8c38ce71c6bbf42e3f8536c69e
XSeed = 0000000000000000000000000000000000000000
X = 7d08cb2a2427672ea4f6080b21cba49dd677179b

COUNT = 2
b = 176
XKey = 6972eaf9dcb2a0b73cffafe8cd1f16a022ea9b99dfff
XSeed = 0000000000000000000000000000000000000000
X = 389b630aa81a2099540a5fb1c691d5efef651a76

...

COUNT = 43
b = 504
XKey =
9d889fc34c474277996424711302 63a0f837545f4bcb2d55283d01995507f21a1923a23f51ceea
cac08ccf02a76cb111958dc6ab81e1c7f01631e9944e620f
```

```
XSeed =
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000
X = 96c21afc2aa2a1466e32499185e42f3af60d8b3a

COUNT = 44
b = 512
XKey =
178f92b47a9142c23ccc567b714cb5fb56ad9f55423c3ed8d9597e9183201f101d48096fee4adf
91dcc6d6a8df23c8fab77784e4daa6691fb1cd334203e11488
XSeed =
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000
X = 10a44a898faf7592035d273b2335c3e3112a469e

[Xorg - DES]

Q = 9eedc3fde07ed95848e3e0f0c7e690ad1327e511

COUNT = 0
b = 160
XKey = 996074f46f789f55e0a8c9ec1c2fc19b8f9a74e7
XSeed = 0000000000000000000000000000000000000000
X = 24026bc49010f4a2ce7d510cfbfb7497cee12e18
```

B.3.3 ANSI962_VST.rsp

```
#  CAVS 2.2
#  "ANSI X9.62" information for "Demo Product"
#  Generators selected: P-192
#  G-Functions selected: SHA-1 DES

[P-192 - SHA1]

N = ffffffffffffffffffffff99def836146bc9b1b4d22831

COUNT = 0
b = 160
XKey = 8000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = 7ebf6e9c0f9828de5590fe0139c27574ae95ba3c075384c9

COUNT = 1
b = 160
XKey = c000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = f1ab3e2f58395deccaf697271e81cea97971fdc6a7444b2b

COUNT = 2
b = 160
XKey = e000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = a5a8cb5f81d6efa6ba3f7b02a677cbb8338faa8f69228fc2

COUNT = 3
b = 160
XKey = f000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
```

```
X = 4857d8e69abc4bdd26ee8d4821e59578e65bfc47ceec9061

COUNT = 4
b = 160
XKey = f800000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = d7c9d482b774b00f48b82569e77fe80918af87c62e748ccf

...

COUNT = 158
b = 160
XKey = fffffffffffffffffffffffffffffffffffffffe
XSeed = 0000000000000000000000000000000000000000
X = 7a9eb9d0cefb5938aa1b4c73912bc497c73a129a1099809c

COUNT = 159
b = 160
XKey = ffffffffffffffffffffffffffffffffffffffff
XSeed = 0000000000000000000000000000000000000000
X = 4e743d8ad7eb660bb44e06143344c45b7f758c2efb2c35dc

[P-192 - DES]

N = ffffffffffffffffffffff99def836146bc9b1b4d22831

COUNT = 0
b = 160
XKey = 800000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = f4f47f39c0922d1c8fd50855e7888eb02c3a14ac0f4d3378

COUNT = 1
b = 160
XKey = c000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = f10e7d54e4c290833df478f2147aecc18cc4b68e659ab803

COUNT = 2
b = 160
XKey = e000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = 06b88cd5f46a23efb3a23e1b0b00670bd18316d72a7065b7

COUNT = 3
b = 160
XKey = f000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = 14ff126a72431e664ebd6fbf2ced6ea53bff2f883924f81c

COUNT = 4
b = 160
XKey = f800000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = f385520dbb15dde89fd3787630ddb6d0724bf48e30ccd012

...

COUNT = 158
b = 160
```

```
XKey = fffffffffffffffffffffffffffffffffffffffe
XSeed = 0000000000000000000000000000000000000000
X = 028701bdc0b422547932d71271b4ddf9af830a95853a4dcf

COUNT = 159
b = 160
XKey = ffffffffffffffffffffffffffffffffffffffff
XSeed = 0000000000000000000000000000000000000000
X = 054892327a14e4b6ef7d5c97c59688055a022cda0cf20e26
```

B.3.4 ANSI962_MCT.rsp

```
#  CAVS 2.2
#  "ANSI X9.62" information for "Demo Product"
#  Generators selected: P-192
#  G-Functions selected: SHA-1 DES

[P-192 - SHA1]

N = ffffffffffffffffffffff99def836146bc9b1b4d22831

COUNT = 0
b = 160
XKey = c5d2c492698ae4947f3a44647562f133cf47ab0b
XSeed = 0000000000000000000000000000000000000000
X = 7a86414d4ee5762d5b28d19ec04a7dcb08376761cd280a38

COUNT = 1
b = 168
XKey = 3d243bfd5274dea3f50dcedc764a12603858316a1d
XSeed = 0000000000000000000000000000000000000000
X = 7ffc4672c9eb70d064c99e31021f443667f70de14addf33d

COUNT = 2
b = 176
XKey = 5ca84c37a0d41e02c3253ea9f45e72ad439c74b15839
XSeed = 0000000000000000000000000000000000000000
X = e16c91d6e2eb04dac142573d33a91d758798502cbd293cf3

...

COUNT = 43
b = 504
XKey =
798c427f180ce56f0360ee885ab42683c5a115d3b85c6b7ef52d9e2c5223d57dbc0705a07c8e59
22b9d2d8033e03420f7e5a3a6bd54faa6f110c64b3312105
XSeed =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000
X = cd471389238c9c1f39034531baa8b023338b781af2cfb731

COUNT = 44
b = 512
XKey =
8716e89fe11be3d607873f205655de6369c8cb123afc7b5c89c053a482a86b329a5d9228ba3892
b79f0fb592814f87a3f24bdefe0ad41813c10aa4279c71c405
```

```
XSeed =
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000
X = feaf7968bd801f39a4b3422f631854e9bd39aab36a8254af

[P-192 - DES]

N = ffffffffffffffffffffffff99def836146bc9b1b4d22831

COUNT = 0
b = 160
XKey = 98419df16f74197c100b261b197a7b7e0c8cc178
XSeed = 00000000000000000000000000000000000000000000
X = 136af998090924a478cbe45d713ce405f9ae95485a9f7a57
```

B.3.5 ANSI931_TDES2VST.rsp

```
#  CAVS 2.2
#  "ANSI X9.31" information for "Demo Product"

COUNT = 0
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3c
V = 8000000000000000
R = 944dc7210d6d7fd7

COUNT = 1
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3d
V = c000000000000000
R = af1a648591bb7c2c

COUNT = 2
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3e
V = e000000000000000
R = 221839b07451e423

COUNT = 3
Key1 = 32ad2932fd4c6202
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3f
V = f000000000000000
R = eba9271e04043712

COUNT = 4
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f40
V = f800000000000000
R = 02433c9417a3326f

...

COUNT = 62
```

```
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f7a
V = fffffffffffffffe
R = 13eeb44dcba310f1

COUNT = 63
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f7b
V = ffffffffffffffff
R = e7e2b2964f36ed41
```

B.3.6 ANSI931_TDES2MCT.rsp

```
#  CAVS 2.2
#  "ANSI X9.31" information for "Demo Product"

Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3c
V = d5538f9cf450f53c
R = eedd9df4a3cce54e
```

B.3.7 ANSI931_TDES3VST.rsp

```
#  CAVS 4.3
# ANSI931 VST

[X9.31]
[3-Key TDES]

COUNT = 0
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b0e
V = 8000000000000000
R = 77df53333a5b44eb

COUNT = 1
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b0f
V = c000000000000000
R = 122a51e2a9025753

COUNT = 2
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b10
V = e000000000000000
R = b0178d244b0bbb67

COUNT = 3
Key1 = fbf73126d0d3bf51
```

```
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b11
V = f000000000000000
R = 1a9018f42884e9f1

COUNT = 4
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b12
V = f800000000000000
R = 47c49679d85ffd79

...

COUNT = 62
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b4c
V = fffffffffffffffe
R = 59dda16bdcedb379

COUNT = 63
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b4d
V = ffffffffffffffff
R = b7d312c46f5da339
```

B.3.8 ANSI931_TDES3MCT.rsp

```
#  CAVS 4.3
# ANSI931 MCT

[X9.31]
[3-Key TDES]

COUNT = 0
Key1 = 5da89497aebc8585
Key2 = 92e9b5161367830e
Key3 = fbb96bbff4757616
DT = ca09a63118bb0111
V = e7ee96932e56e746
R = efe4b7d2c7fd6531
```

B.3.9 ANSI931_AES128VST.rsp

```
#  CAVS 4.3
# ANSI931 VST

[X9.31]
[AES 128-Key]

COUNT = 0
```

```
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e922f9
V = 80000000000000000000000000000000
R = 59531ed13bb0c05584796685c12f7641

COUNT = 1
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e922fa
V = c0000000000000000000000000000000
R = 7c222cf4ca8fa24c1c9cb641a9f3220d

COUNT = 2
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e922fb
V = e0000000000000000000000000000000
R = 8aaa003966675be529142881a94d4ec7

COUNT = 3
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e922fc
V = f0000000000000000000000000000000
R = 88dda456302423e5f69da57e7b95c73a

COUNT = 4
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e922fd
V = f8000000000000000000000000000000
R = 052592466179d2cb78c40b140a5a9ac8

...

COUNT = 126
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e92377
V = fffffffffffffffffffffffffffffffe
R = 0dd5a0367a5926bc48d938bff0858fea

COUNT = 127
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62d71d4afbb0e92378
V = ffffffffffffffffffffffffffffffff
R = ae5387ee8cd912f57353ae03f9d51333
```

B.3.10 ANSI931_AES128MCT.rsp

```
#  CAVS 4.3
# ANSI931 MCT

[X9.31]
[AES 128-Key]

COUNT = 0
Key = 9f5b51200bf334b5d82be8c37255c848
DT = 6376bbe52902ba3b67c925fa701f11ac
V = 572c8e76872647977e74fbddc49501d1
R = 48e9bd0d06ee18fbe45790d5c3fc9b73
```

B.3.11 ANSI931_AES192VST.rsp

```
#  CAVS 4.3
# ANSI931 VST

[X9.31]
[AES 192-Key]

COUNT = 0
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f34b
V = 80000000000000000000000000000000
R = 1707d52819791eefa50cbf25e556b493

COUNT = 1
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f34c
V = c0000000000000000000000000000000
R = 928dbe07ddc758c06f35419b17c9bd9b

COUNT = 2
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f34d
V = e0000000000000000000000000000000
R = d5def450f3b7104eb8c6f8cfe2b1caa2

COUNT = 3
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f34e
V = f0000000000000000000000000000000
R = ce290843fc3441e7478fb3662b46b1bb

COUNT = 4
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f34f
V = f8000000000000000000000000000000
R = b3260ff5d6caa8bf89b85e2f2256922f

...

COUNT = 126
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f3c9
V = fffffffffffffffffffffffffffffffe
R = 05eb1852344300436e5aa5fe7b32c42d

COUNT = 127
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1bf997da42478f3ca
V = ffffffffffffffffffffffffffffffff
R = 153ce8d104c7ad500bf00716e7567aea
```

B.3.12 ANSI931_AES192MCT.rsp

```
#  CAVS 4.3
# ANSI931 MCT
```

```
[X9.31]
[AES 192-Key]

COUNT = 0
Key = b76c34d10967ab734d5ad53498160b91bc3551166bae938a
DT = 84ce227d915aa3c9843c0ab3a9631552
V = b6afe68f999e9064ddc77ac1bb903a6d
R = fc85609a296fef21dd8620328a296f47
```

B.3.13 ANSI931_AES256VST.rsp

```
# ANSI931 VST

[X9.31]
[AES 256-Key]

COUNT = 0
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9e88
V = 80000000000000000000000000000000
R = 35c7efa7784d29bc827999fbd0b33b72

COUNT = 1
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9e89
V = c0000000000000000000000000000000
R = 6cf4425dc7041a41282a78a9b012c495

COUNT = 2
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9e8a
V = e0000000000000000000000000000000
R = 1690a4ff7b7eb930db674bac2de1d175

COUNT = 3
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9e8b
V = f0000000000000000000000000000000
R = 146ff595a1466530bc57e24af7456205

COUNT = 4
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9e8c
V = f8000000000000000000000000000000
R = 96e2b41e665e0fa4c5cda207ccb79440

...

COUNT = 126
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9f06
V = fffffffffffffffffffffffffffffffe
R = 61ce1d6a487597284b41de18444f56ec

COUNT = 127
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5f2a94e34748e9f07
V = ffffffffffffffffffffffffffffffff
R = 528959792daa28b3b08a3e70fa715984
```

B.3.14 ANSI931_AES256MCT.rsp

```
#  CAVS 4.3
# ANSI931 MCT

[X9.31]
[AES 256-Key]

COUNT = 0
Key = 9b05c868ff47f83aa63aa8cb4e71b2e0b87ef137b6b4f66d8632fc1f5e1d1e50
DT = 316e359ab144f0ee626d0446e0a3924c
V = 4fcdc187821f4da13e0e564459e883ca
R = c887c2615bd0b9e1e7f38bd75bd5f18d
```

B.4 Examples of *SAMPLE* Files

B.4.1 FIPS186_VST.sam

```
#  CAVS 2.2
#  "FIPS 186" information for "Demo Product"
#  Generators selected: Xorg
#  G-Functions selected: SHA-1 DES
#  Generated on Tue Jun 03 09:18:10 2003

[Xorg - SHA1]

Q = 9eedc3fde07ed95848e3e0f0c7e690ad1327e511

COUNT = 0
b = 160
XKey = 8000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = ?

COUNT = 1
b = 160
XKey = c0000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = ?

COUNT = 2
b = 160
XKey = e0000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = ?

COUNT = 3
b = 160
XKey = f0000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = ?

COUNT = 4
b = 160
XKey = f8000000000000000000000000000000000000000
```

```
XSeed = 00000000000000000000000000000000000000000000
X = ?

...

COUNT = 158
b = 160
XKey = fffffffffffffffffffffffffffffffffffffffe
XSeed = 00000000000000000000000000000000000000000000
X = ?

COUNT = 159
b = 160
XKey = ffffffffffffffffffffffffffffffffffffffff
XSeed = 00000000000000000000000000000000000000000000
X = ?

[Xorg - DES]

Q = 9eedc3fde07ed95848e3e0f0c7e690ad1327e511

COUNT = 0
b = 160
XKey = 80000000000000000000000000000000000000000000
XSeed = 00000000000000000000000000000000000000000000
X = ?

COUNT = 1
b = 160
XKey = c0000000000000000000000000000000000000000000
XSeed = 00000000000000000000000000000000000000000000
X = ?

COUNT = 2
b = 160
XKey = e0000000000000000000000000000000000000000000
XSeed = 00000000000000000000000000000000000000000000
X = ?

COUNT = 3
b = 160
XKey = f0000000000000000000000000000000000000000000
XSeed = 00000000000000000000000000000000000000000000
X = ?

COUNT = 4
b = 160
XKey = f8000000000000000000000000000000000000000000
XSeed = 00000000000000000000000000000000000000000000
X = ?

...

COUNT = 158
b = 160
XKey = fffffffffffffffffffffffffffffffffffffffe
XSeed = 00000000000000000000000000000000000000000000
X = ?

COUNT = 159
```

```
b = 160
XKey = ffffffffffffffffffffffffffffffffffffffff
XSeed = 0000000000000000000000000000000000000000
X = ?
```

B.4.2 FIPS186_MCT.sam

```
#  CAVS 2.2
#  "FIPS 186" information for "Demo Product"
#  Generators selected: Xorg
#  G-Functions selected: SHA-1 DES
#  Generated on Tue Jun 03 09:18:10 2003

[Xorg - SHA1]

Q = 9eedc3fde07ed95848e3e0f0c7e690ad1327e511

COUNT = 0
b = 160
XKey = f6a2525581101c00a95c2c361b1036eacbde6f8c
XSeed = 0000000000000000000000000000000000000000
X = ?

COUNT = 1
b = 168
XKey = 4a6c639722bc332d8c38ce71c6bbf42e3f8536c69e
XSeed = 0000000000000000000000000000000000000000
X = ?

COUNT = 2
b = 176
XKey = 6972eaf9dcb2a0b73cffafe8cd1f16a022ea9b99dfff
XSeed = 0000000000000000000000000000000000000000
X = ?

...

COUNT = 43
b = 504
XKey =
9d889fc34c4742779964247113026 3a0f837545f4bcb2d55283d01995507f21a1923a23f51ceea
cac08ccf02a76cb111958dc6ab81e1c7f01631e9944e620f
XSeed =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000
X = ?

COUNT = 44
b = 512
XKey =
178f92b47a9142c23ccc567b714cb5fb56ad9f55423c3ed8d9597e9183201f101d48096fee4adf
91dcc6d6a8df23c8fab77784e4daa6691fb1cd334203e11488
XSeed =
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000
X = ?

[Xorg - DES]
```

```
Q = 9eedc3fde07ed95848e3e0f0c7e690ad1327e511

COUNT = 0
b = 160
XKey = 996074f46f789f55e0a8c9ec1c2fc19b8f9a74e7
XSeed = 0000000000000000000000000000000000000000
X = ?
```

B.4.3 ANSI962_VST.sam

```
#  CAVS 2.2
#  "ANSI X9.62" information for "Demo Product"
#  Generators selected: P-192
#  G-Functions selected: SHA-1 DES
#  Generated on Tue Jun 03 09:18:15 2003

[P-192 - SHA1]

N = ffffffffffffffffffffff99def836146bc9b1b4d22831

COUNT = 0
b = 160
XKey = 8000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = ?

COUNT = 1
b = 160
XKey = c0000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = ?

COUNT = 2
b = 160
XKey = e0000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = ?

COUNT = 3
b = 160
XKey = f0000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = ?

COUNT = 4
b = 160
XKey = f8000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = ?

...

COUNT = 158
b = 160
XKey = fffffffffffffffffffffffffffffffffffffffe
XSeed = 0000000000000000000000000000000000000000
X = ?
```

```
COUNT = 159
b = 160
XKey = ffffffffffffffffffffffffffffffffffffffff
XSeed = 0000000000000000000000000000000000000000
X = ?

[P-192 - DES]

N = ffffffffffffffffffffff99def836146bc9b1b4d22831

COUNT = 0
b = 160
XKey = 8000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = ?

COUNT = 1
b = 160
XKey = c0000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = ?

COUNT = 2
b = 160
XKey = e0000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = ?

COUNT = 3
b = 160
XKey = f0000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = ?

COUNT = 4
b = 160
XKey = f8000000000000000000000000000000000000000
XSeed = 0000000000000000000000000000000000000000
X = ?

...

COUNT = 158
b = 160
XKey = fffffffffffffffffffffffffffffffffffffffe
XSeed = 0000000000000000000000000000000000000000
X = ?

COUNT = 159
b = 160
XKey = ffffffffffffffffffffffffffffffffffffffff
XSeed = 0000000000000000000000000000000000000000
X = ?
```

B.4.4 ANSI962_MCT.sam

```
#  CAVS 2.2
```

```
#  "ANSI X9.62" information for "Demo Product"
#  Generators selected: P-192
#  G-Functions selected: SHA-1 DES
#  Generated on Tue Jun 03 09:18:15 2003

[P-192 - SHA1]

N = ffffffffffffffffffffff99def836146bc9b1b4d22831

COUNT = 0
b = 160
XKey = c5d2c492698ae4947f3a44647562f133cf47ab0b
XSeed = 0000000000000000000000000000000000000000
X = ?

COUNT = 1
b = 168
XKey = 3d243bfd5274dea3f50dcedc764a12603858316a1d
XSeed = 000000000000000000000000000000000000000000000000
X = ?

COUNT = 2
b = 176
XKey = 5ca84c37a0d41e02c3253ea9f45e72ad439c74b15839
XSeed = 000000000000000000000000000000000000000000000000
X = ?

...

COUNT = 43
b = 504
XKey =
798c427f180ce56f0360ee885ab42683c5a115d3b85c6b7ef52d9e2c5223d57dbc0705a07c8e59
22b9d2d8033e03420f7e5a3a6bd54faa6f110c64b3312105
XSeed =
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
X = ?

COUNT = 44
b = 512
XKey =
8716e89fe11be3d607873f205655de6369c8cb123afc7b5c89c053a482a86b329a5d9228ba3892
b79f0fb592814f87a3f24bdefe0ad41813c10aa4279c71c405
XSeed =
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
X = ?

[P-192 - DES]

N = ffffffffffffffffffffff99def836146bc9b1b4d22831

COUNT = 0
b = 160
XKey = 98419df16f74197c100b261b197a7b7e0c8cc178
XSeed = 0000000000000000000000000000000000000000
X = ?
```

B.4.5 ANSI931_TDES2VST.sam

```
#  CAVS 2.2
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jun 03 09:18:59 2003

COUNT = 0
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3c
V = 8000000000000000
R = ?

COUNT = 1
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3d
V = c000000000000000
R = ?

COUNT = 2
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3e
V = e000000000000000
R = ?

COUNT = 3
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3f
V = f000000000000000
R = ?

COUNT = 4
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f40
V = f800000000000000
R = ?

...

COUNT = 62
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f7a
V = fffffffffffffffe
R = ?

COUNT = 63
Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f7b
V = ffffffffffffffff
R = ?
```

B.4.6 ANSI931_TDES2MCT.sam

```
#  CAVS 2.2
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jun 03 09:18:59 2003

Key1 = 75c71ae5a11a232c
Key2 = 40256dcd94f767b0
DT = c89a1d888ed12f3c
V = d5538f9cf450f53c
R = ?
```

B.4.7 ANSI931_TDES3VST.sam

```
#  CAVS 4.3
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jan 11 12:11:44 2005

[X9.31]
[3-Key TDES]

COUNT = 0
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b0e
V = 8000000000000000
R = ?

COUNT = 1
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b0f
V = c000000000000000
R = ?

COUNT = 2
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b10
V = e000000000000000
R = ?

COUNT = 3
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b11
V = f000000000000000
R = ?

COUNT = 4
Key1 = fbf73126d0d3bf51
```

```
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b12
V = f800000000000000
R = ?

...

COUNT = 62
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b4c
V = fffffffffffffffe
R = ?

COUNT = 63
Key1 = fbf73126d0d3bf51
Key2 = aece9d98a113c868
Key3 = b91615b91f6db926
DT = 5c8d9e2d2b619b4d
V = ffffffffffffffff
R = ?
```

B.4.8 ANSI931_TDES3MCT.sam

```
#  CAVS 4.3
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jan 11 12:11:44 2005

[X9.31]
[3-Key TDES]

COUNT = 0
Key1 = 5da89497aebc8585
Key2 = 92e9b5161367830e
Key3 = fbb96bbff4757616
DT = ca09a63118bb0111
V = e7ee96932e56e746
R = ?
```

B.4.9 ANSI931_AES128VST.sam

```
#  CAVS 4.3
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jan 11 12:11:44 2005

[X9.31]
[AES 128-Key]

COUNT = 0
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62
V = 8000000000000000
R = ?

COUNT = 1
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62
```

```
V = c000000000000000
R = ?

COUNT = 2
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62
V = e000000000000000
R = ?

COUNT = 3
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62
V = f000000000000000
R = ?

COUNT = 4
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62
V = f800000000000000
R = ?

...

COUNT = 126
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62
V = fffffffffffffffe
R = ?

COUNT = 127
Key = f3b1666d13607242ed061cabb8d46202
DT = e6b3be782a23fa62
V = ffffffffffffffff
R = ?
```

B.4.10 ANSI931_AES128McT.sam

```
#  CAVS 4.3
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jan 11 12:11:44 2005

[X9.31]
[AES 128-Key]

COUNT = 0
Key = 9f5b51200bf334b5d82be8c37255c848
DT = 6376bbe52902ba3b
V = 572c8e7687264797
R = ?
```

B.4.11 ANSI931_AES192VST.sam

```
#  CAVS 4.3
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jan 11 12:11:45 2005

[X9.31]
```

```
[AES 192-Key]

COUNT = 0
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1
V = 8000000000000000
R = ?

COUNT = 1
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1
V = c000000000000000
R = ?

COUNT = 2
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1
V = e000000000000000
R = ?

COUNT = 3
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1
V = f000000000000000
R = ?

COUNT = 4
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1
V = f800000000000000
R = ?

...

COUNT = 126
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1
V = fffffffffffffffe
R = ?

COUNT = 127
Key = 15d8780d62d3256e44641013602ba9bc4afbcaeb4c8b993b
DT = 3fd8ffe880698bc1
V = ffffffffffffffff
R = ?
```

B.4.12 ANSI931_AES192MCT.sam

```
#  CAVS 4.3
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jan 11 12:11:45 2005

[X9.31]
[AES 192-Key]

COUNT = 0
Key = b76c34d10967ab734d5ad53498160b91bc3551166bae938a
DT = 84ce227d915aa3c9
```

```
V = b6afe68f999e9064
R = ?
```

B.4.13 ANSI931_AES256VST.sam

```
#  CAVS 4.3
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jan 11 12:11:45 2005

[X9.31]
[AES 256-Key]

COUNT = 0
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5
V = 8000000000000000
R = ?

COUNT = 1
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5
V = c000000000000000
R = ?

COUNT = 2
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5
V = e000000000000000
R = ?

COUNT = 3
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5
V = f000000000000000
R = ?

COUNT = 4
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5
V = f800000000000000
R = ?

...

COUNT = 126
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5
V = fffffffffffffffe
R = ?

COUNT = 127
Key = 6d14066cb6d8212d828dfaf27a03b79f0cc73ecd76ebeeb521058c4f317a80bb
DT = da3a41ec1da3b0d5
V = ffffffffffffffff
R = ?
```

B.4.14 ANSI931_AES256MCT.sam

```
#  CAVS 4.3
#  "ANSI X9.31" information for "Demo Product"
#  Generated on Tue Jan 11 12:11:45 2005

[X9.31]
[AES 256-Key]

COUNT = 0
Key = 9b05c868ff47f83aa63aa8cb4e71b2e0b87ef137b6b4f66d8632fc1f5e1d1e50
DT = 316e359ab144f0ee
V = 4fcdc187821f4da1
R = ?
```