

Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 6: CPCM Security Test Vectors



Reference

RTR/JTC-DVB-252-6

Keywords

broadcast, DVB

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2011.

© European Broadcasting Union 2011.

All rights reserved.

DECT[™], **PLUGTESTS**[™], **UMTS**[™], **TIPHON**[™], the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPP[™] is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

LTE[™] is a Trade Mark of ETSI currently being registered for the benefit of its Members and of the 3GPP Organizational Partners.

GSM[®] and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	4
Foreword.....	4
Introduction	4
1 Scope	5
2 References	5
2.1 Normative references	5
2.2 Informative references.....	5
3 Definitions, abbreviations and notation.....	6
3.1 Definitions	6
3.2 Abbreviations	6
3.3 Notation.....	6
4 Test Vectors Cryptographic Algorithms	6
4.1 Hash Function	6
4.2 Message Authentication Code.....	6
4.3 Symmetric Cipher.....	6
4.4 Revocation Lists Digital Signature.....	7
4.5 MPEG-2 Transport Stream adaptation of the LSA.....	8
4.6 Certificate Verification.....	30
4.7 Certificate keys and digest generation.....	33
5 Test Vectors Cryptographic Protocols.....	34
5.1 Authenticated Key Exchange (AKE)	34
History	39

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://webapp.etsi.org/IPR/home.asp>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by Joint Technical Committee (JTC) Broadcast of the European Broadcasting Union (EBU), Comité Européen de Normalisation ELECTrotechnique (CENELEC) and the European Telecommunications Standards Institute (ETSI).

NOTE: The EBU/ETSI JTC Broadcast was established in 1990 to co-ordinate the drafting of standards in the specific field of broadcasting and related fields. Since 1995 the JTC Broadcast became a tripartite body by including in the Memorandum of Understanding also CENELEC, which is responsible for the standardization of radio and television receivers. The EBU is a professional association of broadcasting organizations whose work includes the co-ordination of its members' activities in the technical, legal, programme-making and programme-exchange domains. The EBU has active members in about 60 countries in the European broadcasting area; its headquarters is in Geneva.

European Broadcasting Union
CH-1218 GRAND SACONNEX (Geneva)
Switzerland
Tel: +41 22 717 21 11
Fax: +41 22 717 24 81

The Digital Video Broadcasting Project (DVB) is an industry-led consortium of broadcasters, manufacturers, network operators, software developers, regulatory bodies, content owners and others committed to designing global standards for the delivery of digital television and data services. DVB fosters market driven solutions that meet the needs and economic circumstances of broadcast industry stakeholders and consumers. DVB standards cover all aspects of digital television from transmission through interfacing, conditional access and interactivity for digital video, audio and data. The consortium came together in 1993 to provide global standardisation, interoperability and future proof specifications.

The present document is part 6 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.8].

Introduction

CPCM is a system for Content Protection and Copy Management of commercial digital content delivered to consumer products. CPCM manages content usage from acquisition into the CPCM system until final consumption, or export from the CPCM system, in accordance with the particular usage rules of that content. Possible sources for commercial digital content include broadcast (e.g. cable, satellite, and terrestrial), Internet-based services, packaged media, and mobile services, among others. CPCM is intended for use in protecting all types of content - audio, video and associated applications and data. CPCM specifications facilitate interoperability of such content after acquisition into CPCM by networked consumer devices for both home networking and remote access.

This first phase of the specification addresses CPCM for digital Content encoded and transported by linear transport systems in accordance with TS 101 154 [i.1]. A later second phase will address CPCM for Content encoded and transported by systems that are based upon Internet Protocols in accordance with TS 102 005 [i.2].

1 Scope

The present document specifies the Security Test Vectors for the Digital Video Broadcasting (DVB) Content Protection and Copy Management (CPCM) system.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <http://docbox.etsi.org/Reference>.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 101 154: "Digital Video Broadcasting (DVB); Specification for the use of Video and Audio Coding in Broadcasting Applications based on the MPEG-2 Transport Stream".

[i.2] ETSI TS 102 005: "Digital Video Broadcasting (DVB); Specification for the use of Video and Audio Coding in DVB services delivered directly over IP protocols".

[i.3] FIPS Publication 180-1 (1994): "Secure Hash Standard, National Institute of Standards and Technology".

NOTE: Available at <http://www.itl.nist.gov/fipspubs/fip180-1.htm>.

[i.4] FIPS Publication 198 (2001): "The Keyed-Hash Message Authentication Code (HMAC), National Institute of Standards and Technology".

NOTE: Available at <http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf>.

[i.5] FIPS Publication 197 (2001): "Advanced Encryption Standard, National Institute of Standards and Technology".

NOTE: Available at <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

[i.6] FIPS Special Publication 800-38A (2001): "Recommendation for Block Cipher Modes of Operation".

NOTE: Available at <http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>.

[i.7] ETSI TS 102 825-5: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 5: CPCM Security Toolbox".

[i.8] ETSI TS 102 825-1: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 1: CPCM Abbreviations, Definitions and Terms".

[i.9] PKCS #1 (V1.5): RSA Cryptography Standard, Version 2.1, RSA Laboratories, 2002.

NOTE: Available at <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf>.

3 Definitions, abbreviations and notation

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 102 825-1 [i.8] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TS 102 825-1 [i.8] apply.

3.3 Notation

The Notation used in the present document is as defined in the DVB CPCM Security Toolkit (TS 102 825-5 [i.7]). Additional Notation specific for the present document is shown in Table 1.

All numbers are represented using the big-endian convention.

Table 1: Notation

Scope	Notation	Meaning
Scrambler test vector	Block	16 bytes
	Residue	0-15 bytes partial block
	MSC	Size of MSC data
	AF	Adaptation Field size (= <code>adaptation_field_length - 1</code>)
	Payload	Size of data after MSC part
	nSB	Process n Super Blocks using RCBC
	nCBC	Process n blocks using CBC
	CS(n)	Ciphertext Stealing with n bytes
	1B	Process a single block
	SBH	Small Block Handling

4 Test Vectors Cryptographic Algorithms

4.1 Hash Function

The Test vectors for the CPCM Hash Algorithm can be found in [i.3].

4.2 Message Authentication Code

Test vectors for CPCM Message Authentication Code can be found in [i.4].

4.3 Symmetric Cipher

Test vectors for AES can be found in [i.5]. Test Vectors for CBC mode can be found in [i.6].

Table 3: RSA keys used for PKCS1.5

public exponent <i>e</i>	$2^{16} + 1 = 65537 = 0x10001$
modulus <i>n</i>	d0 bb e8 f5 9b 64 4f 1b 9a 6b 6c 44 16 1a 17 cf ff 85 4d 2b f2 c0 59 89 e8 2b b6 b7 e7 ef 19 08 8d a2 16 34 95 5b a3 96 5f cb e8 07 0b d4 a8 6a 0a 82 f2 a7 55 34 71 d6 d9 cb 2e c8 8b 1e f4 9d 4c ba 43 23 4a f8 63 a0 5b 04 44 11 cf 34 17 c4 3c 11 2c e6 52 81 44 72 f6 b1 c5 6d 7d 03 2f 13 cf 36 cc 9d 2b 26 d9 4e 8c 04 bc 17 93 bc f5 24 d6 ed e1 ab bd 0a 82 4f 4d f8 29 53 10 ba 90 f9 36 21 90 ec 97 e8 25 27 5e 7c ea a1 0a 1f 31 fc 15 01 d7 53 85 51 84 95 eb bb b6 14 ff 4a b8 b4 cf b7 f1 37 c8 61 fb 9b 88 4c 4c 19 72 84 f8 df 6a 29 0a f5 ca d3 24 04 44 d2 c1 c3 83 4f 14 af d8 b6 9d 8c 86 16 2e 0f a1 23 bf 38 32 6e 72 71 c6 30 ec bd ac 08 38 e8 17 dd 2b 6d d3 a3 67 54 d6 8c af 73 1a 9d fa ff a0 d8 1f 11 4b 21 bf 9f 6c d1 87 d2 c2 ef 66 80 20 38 d8 03 47 36 47 e7
private exponent <i>d</i>	ac 0b d6 6e 6a 90 79 6b e5 11 da 01 1c be 91 16 0e 24 cf 81 03 eb 6b 61 f2 0d e5 e3 1b b6 c5 c9 79 04 3a 8d 48 f6 69 95 ce 8c 01 49 9d 84 c0 f3 f6 8a 0c 7b c4 0d 20 2f d9 00 52 25 56 16 43 c5 4b b2 d3 17 c9 f9 86 14 6c 30 cd f2 67 f9 26 05 c7 04 d9 1f 56 ad d9 bf 70 7b 02 a1 c6 42 d3 90 de 60 ea b2 39 19 22 50 4d b4 b1 5c 35 97 af ef 97 80 27 5c 28 ca fa b1 67 30 be cf 0a a0 dc 50 30 28 4b ab a9 8f 76 1d b8 7c 55 95 6d a2 8d 62 ba ef 4b 93 a0 34 69 7e d2 d9 59 22 8a a6 42 2c e2 42 0d d9 05 2a 12 02 7f 26 4d 8d 55 39 cf 5b fc 5f 9d d9 7f b2 72 68 b7 e1 84 74 65 f7 0a 56 c2 55 83 c8 35 70 51 81 f5 bc 18 5c 17 9d 82 9e fd f7 f0 75 83 f2 83 b0 eb cb 57 24 29 68 18 6a 76 ae e7 c0 79 f5 6a a5 00 b5 64 ee 3f a6 2b 0f 87 16 6b da 95 46 38 b3 d9 69 e8 84 f0 fa bf a1

4.5 MPEG-2 Transport Stream adaptation of the LSA

This clause describes 21 test cases for the MPEG-2 Transport Stream adaptation of the LSA. For each test case a table is shown that contains 4 scrambled transport stream packets, one for each combination of MSC mode (MDI or MDD) and Chaining Mode (CBC or RCBC). For each vector the IVE is also shown.

The clear packets that are used as input for the LSA scrambling process have the following syntax:

```

TS packet := header + <adaptation field> + payload[188 - MSC]
adaptation field := af_length + payload[af_length]
MSC := 4 + <af_length + 1>
payload[n] := 00 01 02 ... n-1

```

The header is a correct 4-byte TS packet header with the `adaptation_field_control` field set according to the presence of an optional adaptation field. The payload is a sequence of bytes with ascending values from 0 up to $n-1$, with n the size of the payload: $n = 188 - \text{MSC}$. Clear packets are not shown in the tables.

All TS packets are scrambled using the following Control Word:

```
00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
```


Table 4 lists the various Test Cases.

Table 4: CPCM Scrambler Test Cases

Case	Blocks	Residue	MSC	AF	Payload	RCBC process	CBC process
1	11	8	4	0	184	5SB + CS(24)	10CBC + CS(24)
2	11	8	4	1	183	5SB + CS(23)	10CBC + CS(23)
3	11	1	11	7	177	5SB + CS(17)	10CBC + CS(17)
4	11	0	12	8	176	4SB + 1B + SB	11CBC
5	10	15	13	9	175	4SB + 1B + CS(31)	9CBC + CS(31)
6	10	13	15	11	173	MSC border case	MSC border case
7	10	12	16	12	172	MSC border case	MSC border case
8	10	11	17	13	171	MSC border case	MSC border case
9	10	1	27	23	161	4SB + 1B + CS(17)	9CBC + CS(17)
10	10	0	28	24	160	5SB	10CBC
11	9	15	29	25	159	4SB + CS(31)	8CBC + CS(31)
12	3	1	139	135	49	SB + CS(17)	2CBC + CS(17)
13	3	0	140	136	48	1B + SB	3CBC
14	2	15	141	137	47	1B + CS(31)	1CBC + CS(31)
15	2	1	155	151	33	1B + CS(17)	1CBC + CS(17)
16	2	0	156	152	32	SB	2CBC
17	1	15	157	153	31	CS(31)	CS(31)
18	1	1	171	167	17	CS(17)	CS(17)
19	1	0	172	168	16	1B	1B = 1CBC
20	0	15	173	169	15	SBH	SBH
21	0	1	187	183	1	SBH	SBH

NOTE 1: Items in Bold are the primary motivators for each test.

NOTE 2: In order to test LSA conformance, the implementer is strongly advised to test all cases for MSC Modes, MDI and MDD, and Chaining Modes:

- CBC; and
- RCBC.

NOTE 3: The correct masking of the error bit also needs to be tested for IV Mode = MDD, for CBC and RCBC. This is not explicitly shown in the present document.

Table 5: LSA Test Case 01

Context		Test Case 01											
Chaining Mode	MSC Mode		AF size	Payload	MSC	Blocks	Residue						
			000	184	004	11	08						
CBC	MDI	IVE	23 97 62 28 e2 96 6c 83 ff ae 99 4f 30 15 ff ef										
		Scrambled packet	47 60 80 91 8f 06 0d ab 07 5f 2e 9a 84 3b db 75 dc b6 76 9b 1e 5c 07 e9 4a f5 56 0b 97 91 33 3d 7d cf 21 7c 9f 6e ef 4f 14 d7 1b 0c 9e 83 c8 9b 2d d1 ca be 21 1c 73 73 cd 50 32 cd d8 58 b0 ac 9a 0a 84 40 25 59 a6 c9 92 08 c1 4d e2 20 54 94 e6 96 a0 e9 ad 37 c2 b6 2d df 80 1a 8a 7d 38 f1 fe 25 3f db 4a 86 d1 30 e1 55 13 23 ec 4e bf af 6a 1f 44 6d 5a cd 9d fa 2b 60 91 8f 6a 51 4b 0c 21 04 14 5c d9 58 63 8f 50 90 25 23 fd f1 11 f6 7c db 1a d6 ef 57 5a 30 7b 7c 8f e2 ab 61 db 57 20 71 61 cf 62 fc 80 82 51 c5 89 d8 49 10 18 d3 44 b2 71 73 ab 71 ea f8 79 f3 73 1d										
	MDD	IVE	11 d9 46 16 56 59 95 90 c0 a7 60 a2 5c ca c7 86										
		Scrambled packet	47 60 80 91 8a 2f d5 32 f8 5b 99 ac 4d 67 68 55 3f 4f c9 fc e7 bb 73 5c 0b 47 8a cf 6a 22 dc 8b 9f da 59 c6 26 93 3b 04 fb 69 c0 90 09 cd 38 b4 8e 01 3a 23 5a db 08 a8 ef ff 9e 42 0c 7f 69 e2 4f 72 0b a4 eb 61 1c f0 26 b0 58 24 af 5f 5f 23 fb 00 74 7e 54 e8 ae 7e eb 56 92 85 46 7e 56 1f 7d 7e 71 4d b2 9e 6a 5b 2a 49 22 0e 13 73 d4 ef e4 03 7e 7b 19 1f 97 da a2 b6 f3 41 ec 2b ee e9 9d ff 22 2b 29 50 5b c3 28 f6 b2 ff 1f f1 c5 f3 52 38 32 95 45 9c da fe 64 cd e8 05 6c 4c 6c 3c 3b 89 46 87 d0 b2 fe b1 06 a3 d0 cf 68 ce 0b 3a d5 87 a1 9d 88 ae f5 7a 24 25 7b 1e										
RCBC	MDI	IVE	40 81 e5 3f 73 fc 52 cc b3 2e 4a 7b a7 ab 5d 63										
		Scrambled packet	47 60 80 91 ac a2 3a b2 90 2d 50 08 56 e8 95 70 91 74 47 a8 48 43 c4 15 dd 9e 65 f9 09 e2 e7 be e2 ce c1 0f 25 30 9f 50 fc 94 af d9 a4 11 b4 53 bc c8 5a 29 1c 00 7d ad 5b b8 d4 d8 94 f7 32 1f 6f e7 53 67 42 34 6b e9 fb 8e 70 3e 97 24 aa 1c a3 61 63 e4 48 43 c4 15 dd 9e 65 f9 09 e2 e7 be e2 ce c1 0f c2 0a 5e 71 91 36 15 1b 5a 6e 56 9b 94 13 f4 c0 1c 00 7d ad 5b b8 d4 d8 94 f7 32 1f 6f e7 53 67 d0 05 97 8f 69 e4 3b 86 5f 8c b2 1c 72 c8 d5 78 48 43 c4 15 dd 9e 65 f9 09 e2 e7 be e2 ce c1 0f b1 52 51 da 39 f8 a8 f5 8f b2 53 71 ff c7 59 9c af e4 99 2d 9f 5b 33 b7										
	MDD	IVE	e4 c9 4f 03 12 31 f4 2f a2 1e f9 7a b4 49 15 17										
		Scrambled packet	47 60 80 91 b3 7a 60 9a d2 0d 0f 1e 61 11 6f f7 c6 09 e4 ab cc 69 84 e2 db 77 93 03 1b 9b 86 60 72 60 ba 28 e4 ec 7a 73 04 37 0d 17 d6 a9 8b fd 1f d1 17 74 52 01 f8 d1 ac e0 ab 3a 67 78 ea e2 ee 3f 62 99 ad a3 63 fd 80 f9 d7 8d 0e 87 a5 53 10 70 c9 69 cc 69 84 e2 db 77 93 03 1b 9b 86 60 72 60 ba 28 b5 95 a3 5d ac 96 94 16 1f 5a f3 22 76 0f 5c 65 52 01 f8 d1 ac e0 ab 3a 67 78 ea e2 ee 3f 62 99 e1 1e 48 c2 29 c2 aa ed 7c 12 9d 5e 6b 40 61 3b cc 69 84 e2 db 77 93 03 1b 9b 86 60 72 60 ba 28 59 2d 8d 3d 8e 7b 98 3f 4d 2f e1 55 bb 5e 33 e4 3d 97 eb 03 a5 84 13 0c										

Table 6: LSA Test Case 02

Context		Test Case 02											
Chaining Mode	MSC Mode		AF size	Payload	MSC	Blocks	Residue						
			001	183	005	11	07						
CBC	MDI	IVE	09 ad ed 08 a7 89 e3 ee ca 48 63 de ce 51 de 36										
		Scrambled packet	47 60 80 b1 00 57 e5 0a 1f d6 f9 86 d3 d2 84 da ef b3 1c 97 3a 70 a7 18 c5 ff f0 ac 2f e4 75 42 84 b3 08 bf 01 b2 be 71 5b 6e 4f 88 1e ea 5b 26 9b a6 21 3d 3a 70 ab 1f 79 87 70 75 ad b5 f8 40 2e 47 b1 05 3c 2e ca fd 87 69 90 d3 b0 85 5b d1 ce 48 db b0 0e 19 65 03 c6 12 7f 29 6e aa f8 ef ba ec 5a 6f 1d a2 39 e1 5d 9a 8d 0f ae a7 06 a0 43 3b 34 77 59 44 bf 73 ca ee 85 6c 1e 18 1c 08 a7 11 18 89 0b 4c e3 45 93 22 77 b9 32 32 3a aa 68 04 1f 9b a7 c4 d5 29 77 6f dd 73 d0 4e 36 b4 c1 1c 23 27 52 7d e5 d6 08 9d 07 90 c9 2b b2 2e a8 21 8e 9f 60 8a 0a ac 6a de 18 b4										
		IVE	cd 31 be e1 17 b1 08 30 00 82 23 bb a3 2b 94 8c										
		Scrambled packet	47 60 80 b1 00 66 10 9b a7 32 8f 10 d0 ac be e6 29 33 b4 ac 59 d0 9d ba 26 ce 94 47 24 f4 1d 90 18 3d 08 03 20 a2 db e1 bf d0 66 e2 f9 ea c5 24 76 63 77 b6 a5 00 3a e5 db 2c bf 23 98 f6 fa 0a d8 78 04 bb ae 71 71 33 76 13 2f 28 1f ef 15 dc 0a 71 64 da 61 94 01 7e c2 25 fe 7d 58 6a 1d 16 98 18 b7 62 8a 45 6d 89 df 48 29 0a 10 a6 45 10 e3 ae 18 c2 76 05 6a eb 1d 31 6e ad c7 b7 c4 b8 6f fe b6 a3 11 18 86 93 a5 6e 68 4b 12 07 12 38 f5 36 63 a8 fa bf 3e 96 78 d0 41 da 83 e7 92 28 ee f0 09 5c 11 0a df e7 71 d0 88 d0 9a a3 b8 55 06 6f fa 83 19 64 26 00 ee 7c 91 0b										
	MDD	IVE	40 81 e5 3f 73 fc 52 cc b3 2e 4a 7b a7 ab 5d 63										
		Scrambled packet	47 60 80 b1 00 ac a2 3a b2 90 2d 50 08 56 e8 95 70 91 74 47 a8 48 43 c4 15 dd 9e 65 f9 09 e2 e7 be e2 ce c1 0f 25 30 9f 50 fc 94 af d9 a4 11 b4 53 bc c8 5a 29 1c 00 7d ad 5b b8 d4 d8 94 f7 32 1f 6f e7 53 67 42 34 6b e9 fb 8e 70 3e 97 24 aa 1c a3 61 63 e4 48 43 c4 15 dd 9e 65 f9 09 e2 e7 be e2 ce c1 0f c2 0a 5e 71 91 36 15 1b 5a 6e 56 9b 94 13 f4 c0 1c 00 7d ad 5b b8 d4 d8 94 f7 32 1f 6f e7 53 67 d0 05 97 8f 69 e4 3b 86 5f 8c b2 1c 72 c8 d5 78 48 43 c4 15 dd 9e 65 f9 09 e2 e7 be e2 ce c1 0f 76 c5 86 f0 f4 9b ef 95 be b2 4a 38 8c c2 df f7 a7 eb 26 b6 d9 ee 90										
RCBC	MDD	IVE	5f d0 68 46 49 9f e4 7e aa fc 32 5a 6f a7 00 e7										
		Scrambled packet	47 60 80 b1 00 c4 b6 c4 a5 d1 f3 4f a4 df 59 8e 89 1e a5 98 1a e6 f9 c9 25 84 2c bf 2e 05 39 60 64 b1 9d aa 7e 7b 97 01 f9 bc fb 07 ae 95 df ad 3d 0a 12 07 62 4c ea a3 18 33 f4 61 7b c4 68 fd 2d fc ca 5a 94 21 0c 77 fb db 74 88 08 00 e0 0a 6d 29 74 18 5c e6 f9 c9 25 84 2c bf 2e 05 39 60 64 b1 9d aa 7e 30 d4 53 83 c2 6a a2 29 7a 4d 3f 08 80 d8 18 e8 4c ea a3 18 33 f4 61 7b c4 68 fd 2d fc ca 5a 94 26 66 ae 21 ee c0 bf 53 17 f0 1a fb d8 c8 ca b2 e6 f9 c9 25 84 2c bf 2e 05 39 60 64 b1 9d aa 7e 66 66 6b b1 ec 0b 8b 7a 9c 4c d7 78 c0 a2 53 3c 29 f8 d4 88 6f 70 1b										

Table 7: LSA Test Case 03

Context			Test Case 03																			
Chaining Mode	MSC Mode		AF size	Payload				MSC				Blocks				Residue						
			007	177				011				11				01						
CBC	MDI	IVE	f8 87 df 7d	15 30 42 5f	6a 83 ea 7e	05 86 12 11																
		Scrambled packet	47 60 80 b1 06 00 01 02 03 04 05 53 17 e3 70 65 e5 92 98 41 e7 30 b1 31 4f 17 71 48 07 06 cd ca 10 72 9a 33 1b ad 36 09 72 24 1a d6 28 c9 f1 97 9b 0e 0d 2b fa af eb 58 eb 0f e5 bf fd b8 a1 66 c7 81 5b 0a 90 6e 3e 0f a1 84 c2 87 eb de 46 b1 6b 1f 13 73 03 4d 92 eb 32 45 f8 58 2b 8a ed 46 32 f8 34 e5 b0 c5 74 a8 27 1f df 91 80 18 53 b5 37 63 5b b8 25 20 95 4b f0 d8 c4 95 8e 06 b9 4a b5 f0 3d f8 f6 bf 77 12 4b 8c c2 78 7c 07 5a 86 b4 4c cb cb aa 02 22 3f 5d cf 8e d7 1f cc 0a 61 49 7a 51 a4 33 e7 21 de 76 b6 c7 02 fe e7 fb b3 66 43 63 b5 ce 5c 71 a9 52 51 88 0f																			
	MDD	IVE	7d 3d 1f 81 c1 2e 9a 56 83 ee 04 00 ee b4 8a a0																			
		Scrambled packet	47 60 80 b1 06 00 01 02 03 04 05 d8 2d 3d 46 c9 9c 62 66 60 3a 96 2c 6b 4c 87 2a 85 e1 62 d4 3d 57 9b 38 1b d2 e7 0e b2 03 40 31 e5 58 80 4b 91 cc 35 b3 ae a1 2a 6c 23 85 61 b4 26 98 23 95 94 2e 3a be 61 e2 76 a0 1e 06 41 6b c4 ca 7f 74 ce 17 59 40 c6 96 cf 52 01 7f c9 0e 69 ff 22 a0 dc e0 c4 d2 95 c7 1b c6 be 09 80 7e 3f f9 58 1b 70 bf d9 fb 51 40 d5 44 e4 80 49 fd b9 bc ad 7c f3 0c 38 56 e5 88 33 bb fc 1b bb de 18 95 2a b7 af 0b 3b 4e dd ee 45 e1 b0 47 a3 80 c9 4d a1 47 8d 9c f1 9e 27 75 28 c6 fc ce 9b da 6d d5 e8 b4 7b 92 72 bc 87 3b 22 70 15 dd fa ee ea																			
	RCBC	MDI	IVE	40 81 e5 3f 73 fc 52 cc b3 2e 4a 7b a7 ab 5d 63																		
			Scrambled packet	47 60 80 b1 06 00 01 02 03 04 05 ac a2 3a b2 90 2d 50 08 56 e8 95 70 91 74 47 a8 48 43 c4 15 dd 9e 65 f9 09 e2 e7 be e2 ce c1 0f 25 30 9f 50 fc 94 af d9 a4 11 b4 53 bc c8 5a 29 1c 00 7d ad 5b b8 d4 d8 94 f7 32 1f 6f e7 53 67 42 34 6b e9 fb 8e 70 3e 97 24 aa 1c a3 61 63 e4 48 43 c4 15 dd 9e 65 f9 09 e2 e7 be e2 ce c1 0f c2 0a 5e 71 91 36 15 1b 5a 6e 56 9b 94 13 f4 c0 1c 00 7d ad 5b b8 d4 d8 94 f7 32 1f 6f e7 53 67 d0 05 97 8f 69 e4 3b 86 5f 8c b2 1c 72 c8 d5 78 48 43 c4 15 dd 9e 65 f9 09 e2 e7 be e2 ce c1 0f bf 4c c0 9e 67 19 51 2a 26 8a 12 e3 2e 98 2c 4e f0																		
MDD		IVE	5e e7 11 f1 62 31 3b 36 cf 66 c6 d7 b9 13 ab d9																			
		Scrambled packet	47 60 80 b1 06 00 01 02 03 04 05 80 e8 53 0b 01 68 9e 9b 39 86 3d ef ca e3 38 90 14 1f 77 8b 0f 67 61 4c 39 1a ef 5e 40 27 2e 6d ca 1e 16 71 b1 a4 c8 da 3b 80 cd 41 50 ed 64 eb 2c dd 25 7b 22 85 ad b6 33 84 a7 fe 9c 62 9d b8 45 b8 24 8f e6 70 38 9d 40 84 a1 fb be 93 30 fb 14 1f 77 8b 0f 67 61 4c 39 1a ef 5e 40 27 2e 6d ef 70 e9 8a 75 30 13 b6 3c 53 62 54 46 c1 b3 89 2c dd 25 7b 22 85 ad b6 33 84 a7 fe 9c 62 9d b8 b8 72 3b 28 61 31 b1 3a 4a 7a 0a 79 32 d2 75 71 14 1f 77 8b 0f 67 61 4c 39 1a ef 5e 40 27 2e 6d 3d d6 50 bf 86 6d 25 ee 2c cf f6 4d b8 9d 38 2e 6a																			

Table 9: LSA Test Case 05

Context		Test Case 05																				
Chaining Mode	MSC Mode		AF size			Payload			MSC			Blocks			Residue							
			009			175			013			10			15							
CBC	MDI	IVE	0c	2b	a0	92	1b	37	d1	5d	00	3a	de	20	09	ca	52	7b				
		Scrambled packet	47	60	80	b1	08	00	01	02	03	04	05	06	07	dd	bd	58	c7	b5	ab	d1
			96	69	d0	dc	1a	82	73	b6	a0	3c	e3	e1	09	ba	93	9c	be	d8	e8	ff
			4c	0a	c6	85	70	e1	1b	ad	ad	c1	77	72	00	be	e6	a9	c7	a7	21	e8
		84	b1	22	c5	af	df	fa	f8	14	de	e2	9f	18	8b	b4	5b	fc	19	87	5c	
		60	92	c0	69	6e	d3	89	65	74	50	a9	65	65	7c	13	1b	f6	7c	3d	80	
CBC	MDD	IVE	ac	5f	eb	97	03	2b	68	39	08	b6	66	c1	11	88	41	c9				
		Scrambled packet	47	60	80	b1	08	00	01	02	03	04	05	06	07	9c	6d	9c	0a	c0	0f	83
			7d	e6	62	2b	76	4f	3d	1b	a4	74	ab	ba	82	bd	43	5a	ad	d4	ad	10
			7a	40	89	a5	bd	85	ea	a8	22	ab	06	d5	d0	6b	55	d3	a7	7e	88	b2
		d5	b7	60	d9	db	5f	66	36	c6	7f	ab	0d	bb	4e	31	51	ba	ce	78	d7	
		52	e9	ad	2b	46	ce	66	de	86	7e	d9	eb	f3	37	15	2a	65	5a	33	54	
RCBC	MDI	IVE	40	81	e5	3f	73	fc	52	cc	b3	2e	4a	7b	a7	ab	5d	63				
		Scrambled packet	47	60	80	b1	08	00	01	02	03	04	05	06	07	ac	a2	3a	b2	90	2d	50
			08	56	e8	95	70	91	74	47	a8	48	43	c4	15	dd	9e	65	f9	09	e2	e7
			be	e2	ce	c1	0f	25	30	9f	50	fc	94	af	d9	a4	11	b4	53	bc	c8	5a
		29	1c	00	7d	ad	5b	b8	d4	d8	94	f7	32	1f	6f	e7	53	67	42	34	6b	
		e9	fb	8e	70	3e	97	24	aa	1c	a3	61	63	e4	48	43	c4	15	dd	9e	65	
RCBC	MDD	IVE	c5	3b	43	4d	e8	f2	e8	f1	82	59	69	c6	b7	47	4e	c7				
		Scrambled packet	47	60	80	b1	08	00	01	02	03	04	05	06	07	77	6e	b5	49	46	7b	20
			f5	6b	59	cf	94	6c	35	99	c4	af	51	98	f1	cc	b5	e1	71	89	a1	b7
			80	a9	12	1e	77	ff	81	6c	2d	b1	2f	41	bb	b2	cc	b4	a2	a3	cf	f6
		b2	0c	ba	4e	03	fa	f1	6b	e3	8c	01	94	72	27	8d	57	5f	f3	db	a5	
		38	69	65	db	01	b6	f7	ba	8f	3f	9a	e1	7b	af	51	98	f1	cc	b5	e1	
	71	89	a1	b7	80	a9	12	1e	77	56	32	03	89	a6	67	7c	23	97	b8	9b		
	bb	a5	86	10	45	0c	ba	4e	03	fa	f1	6b	e3	8c	01	94	72	27	8d	57		
	5f	1a	24	23	6b	7e	55	29	03	b5	34	67	6f	d3	d1	39	5f	d5	c2	9c		
	45	d5	eb	0d	d5	ff	de	bb	15	11	24	0f	b8	a6	44	f3	13	3d	28	bb		
	0b	3f	06	72	c2	0f	e3	3b														

Table 10: LSA Test Case 06

Context		Test Case 06														
Chaining Mode	MSC Mode		AF size	Payload	MSC	Blocks	Residue									
			011	173	015	10	13									
CBC	MDI	IVE	8c 39 91 1b ce c7 8d 7b 91 2b 0e e5 35 9c 22 c2													
		Scrambled packet	47 60 80 b1 0a 00 01 02 03 04 05 06 07 08 09 3d 36 0a 19 45 3c 7b 2c 8e ff 0e d0 9c 82 f3 e0 5f 11 b9 55 ed 8e 41 42 26 5c b0 2d 56 5b c9 22 0e 6a 49 15 16 28 84 c5 cc 67 18 46 35 e2 16 20 4b 0c 6a 91 84 5b d9 79 3c 2f 3b 5d 63 35 3d 4c da 49 26 a8 bc 8b ba f3 7a cb c3 ee e1 5b f9 e3 65 7e 78 f1 38 06 88 e7 3d b5 5b 8b dc 68 bc f8 cb f6 47 ad 66 9d ee 33 b6 1e 56 90 2d 4a 3d cd 9c 5b bb 7b e3 f6 29 66 4b ab f6 37 2c 8f b6 ab d4 47 ee 58 34 cc 26 12 41 7e a4 10 cd 60 5a a2 44 68 d5 30 80 07 e7 22 a4 8f 71 1c ac eb 8a 8d be fa f8 b4 96 be d3 7e 2f c9 4a 63 68													
		IVE	20 e7 e0 a5 b1 9e 40 c8 38 9e f3 04 04 15 d2 5a													
		Scrambled packet	47 60 80 b1 0a 00 01 02 03 04 05 06 07 08 09 f9 33 3a 8f 65 2d a7 bd 1d 26 1a 7a 50 a1 0f 60 22 f9 f9 97 3d cc a6 fd 7e 42 27 ef e0 00 5e 0e 83 f3 fe 6b 80 69 0a c7 24 58 60 e3 c7 bf ab 32 8b fc 8d a9 a9 6c cd 2f c7 ca 13 18 2e 99 27 0c c4 71 f7 b6 ae 47 3d ff 86 27 a2 5b 28 4a 7c 95 89 c4 bf 6f fa 5c b1 4e 1d 11 0b 6c b1 50 e8 49 2f 5b 50 37 c4 21 ae 82 3c 53 70 3f b5 e1 70 c5 6e d4 e7 e5 22 c2 0c 6e 58 ed 1b 93 45 ae 8f 24 b7 06 e1 8e f4 c9 0e 01 24 a5 ef 01 49 69 4a f0 69 cf 63 58 41 1d ff 9f ae 89 c5 d9 ce ad 60 97 d8 3e 88 b0 ae 59 34 eb 13 26 15 91 f7													
	MDD	IVE	40 81 e5 3f 73 fc 52 cc b3 2e 4a 7b a7 ab 5d 63													
		Scrambled packet	47 60 80 b1 0a 00 01 02 03 04 05 06 07 08 09 ac a2 3a b2 90 2d 50 08 56 e8 95 70 91 74 47 a8 48 43 c4 15 dd 9e 65 f9 09 e2 e7 be e2 ce c1 0f 25 30 9f 50 fc 94 af d9 a4 11 b4 53 bc c8 5a 29 1c 00 7d ad 5b b8 d4 d8 94 f7 32 1f 6f e7 53 67 42 34 6b e9 fb 8e 70 3e 97 24 aa 1c a3 61 63 e4 48 43 c4 15 dd 9e 65 f9 09 e2 e7 be e2 ce c1 0f c2 0a 5e 71 91 36 15 1b 5a 6e 56 9b 94 13 f4 c0 1c 00 7d ad 5b b8 d4 d8 94 f7 32 1f 6f e7 53 67 14 08 89 7a ca b5 ac 82 6a 33 70 c9 b2 94 86 e4 b6 78 aa 34 86 a1 63 3a a8 ab 0c 69 08 c4 e8 0f dd ea ba 79 0d a5 24 0e 8b 14 b3 b0 b8													
RCBC	MDD	IVE	c9 6d d4 aa e9 40 3e 0b ae df 58 4a 6b be d7 15													
		Scrambled packet	47 60 80 b1 0a 00 01 02 03 04 05 06 07 08 09 1e f3 58 ef ba af a6 7b 8b d0 31 57 34 f1 9d 4b a2 c7 7e 3e 2b 93 8b 11 a4 cd 2d 91 69 4e 21 2a 64 c8 7b 1d dc c7 5a b4 12 b5 60 6c a4 4c c6 74 53 ed 07 31 34 4f cc 03 a9 fe fd 5a 3b b9 66 ba 58 85 a3 09 8d 4c 38 4a 07 58 0d 50 d5 56 44 f1 a2 c7 7e 3e 2b 93 8b 11 a4 cd 2d 91 69 4e 21 2a 65 d8 ad 5b 81 e1 bd 70 6c cd 5a 21 eb 3d 46 2d 53 ed 07 31 34 4f cc 03 a9 fe fd 5a 3b b9 66 ba 48 5d bc 3a 7e 2d bb 39 b8 79 3f 39 d7 f8 ce 2d 50 f3 40 e5 11 75 88 88 16 5a ee 80 09 41 89 46 1f 21 8e 56 62 29 71 08 96 99 0d 2b 0a													

Table 11: LSA Test Case 07

Context		Test Case 07																				
Chaining Mode	MSC Mode		AF size				Payload				MSC				Blocks		Residue					
			012		172		016				10		12									
CBC	MDI	IVE	93	8e	0a	39	85	c4	d2	fb	4d	1b	c8	92	ea	9e	4b	a7				
		Scrambled packet	47	60	80	b1	0b	00	01	02	03	04	05	06	07	08	09	0a	45	ab	11	7a
		47	60	80	b1	0b	00	01	02	03	04	05	06	07	08	09	0a	45	ab	11	7a	
	MDD	IVE	27	8f	db	79	33	fa	78	c5	51	24	ee	18	22	ff	09	5a				
		Scrambled packet	47	60	80	b1	0b	00	01	02	03	04	05	06	07	08	09	0a	f6	85	a8	c9
		47	60	80	b1	0b	00	01	02	03	04	05	06	07	08	09	0a	f6	85	a8	c9	
RCBC	MDI	IVE	40	81	e5	3f	73	fc	52	cc	b3	2e	4a	7b	a7	ab	5d	63				
		Scrambled packet	47	60	80	b1	0b	00	01	02	03	04	05	06	07	08	09	0a	ac	a2	3a	b2
		47	60	80	b1	0b	00	01	02	03	04	05	06	07	08	09	0a	ac	a2	3a	b2	
	MDD	IVE	93	87	40	c3	40	70	e0	17	93	83	ce	a1	c9	fa	c5	8e				
		Scrambled packet	47	60	80	b1	0b	00	01	02	03	04	05	06	07	08	09	0a	80	1c	36	27
		47	60	80	b1	0b	00	01	02	03	04	05	06	07	08	09	0a	80	1c	36	27	

Table 12: LSA Test Case 08

Context		Test Case 08																																																																														
Chaining Mode	MSC Mode		AF size				Payload				MSC				Blocks		Residue																																																															
			013				171				017				10		11																																																															
CBC	MDI	IVE	9e 65 35 b8	6e 42 16 39	7c 72 4a c4	05 2d 46 e9																																																																										
		Scrambled packet	47 60 80 b1	0c 00 01 02	03 04 05 06	07 08 09 0a	0b 02 37 2b	72 bc 53 95	05 de a5 12	90 35 af 2b	94 31 03 c8	86 c4 6f d8	4b 2a 89 d4	fb a5 2d c0	71 ff f6 fc	05 2d 82 e7	db 0e 1f aa	c3 55 82 ec	29 40 b4	05 c7 96 56	b5 18 db 8e	40 87 78 eb	ea aa 24 3a	1d 23 6b	68 8c 1c 6a	ee 44 f1	73 75 35	7d 92 e4	15 10 a3 26	a1 0e cf	5a 69 00	2e 2e c5	4d a0 13	53 d9 ab	29 c0 05 c9	97 5d c5	4d 7c 66	d1 fc 00	fe 17 4f	9d 23 2d	69 88 be 8e e6	61 37 ae	2a 25 ff	ec 54 d4	64 94 55	81 4d a7	83 09 41 52	3c be 8a	33 4c 14	29 c3 79	1c fc c0	93 7f 07	da 40 f2	2a f4 05	74 7f 43	9f 04 2a																								
		IVE	07 40 19 24	63 51 9d 7b	4f 41 1c 75	30 d9 fd 9b																																																																										
	MDD	Scrambled packet	47 60 80 b1	0c 00 01 02	03 04 05 06	07 08 09 0a	0b 72 aa 04	54 34 c1	41 9b 4f	ac 3e 2b 44	3e 1f 79 ba	f4 23 b8	2f 53 5b 9c	ba 05 99	76 af 32 78	20 ea e2 34	26 e6 d4	f3 f6 f4	ac a6 c6	84 07 47	6e 50 16 7c	b3 a2 bd	59 5f 03	98 49 31	0e 63 fc 4d	75 02 e0	6f 10 02 a1	54 0f d8	83 ac 7c	13 c7 ca	30 71 3f 12	20 57 18	d2 4e f1	ab 01 dc	89 45 42	a6 58 78	5e f0 1d	06 20 5b	31 ab 8d	94 ac a0	2d dc a4	3b 4a 4c	76 6c 86	1c 03 27 63	35 ff 40	82 94 76	b6 9b 7c	c1 ad 2a	ef 22 c9	71 f9 f6	11 33 f4	c0 1e 62	02 6f 19	45 34 e0	73 17 58	d3 29 ef	3b 1b 15 21	a8 7f 14	5d 1d 1c	b2																				
		IVE	40 81 e5 3f	73 fc 52 cc	b3 2e 4a 7b	a7 ab 5d 63																																																																										
		Scrambled packet	47 60 80 b1	0c 00 01 02	03 04 05 06	07 08 09 0a	0b ac a2 3a	b2 90 2d	50 08 56	e8 95 70 91	74 47 a8 48	43 c4 15	dd 9e 65 f9	09 e2 e7	be e2 ce c1	0f 25 30 9f	50 fc 94 af	d9 a4 11 b4	53 bc c8	5a 29 1c	00 7d ad	5b b8 d4 d8	94 f7 32	1f 6f e7 53	67 42 34	6b e9 fb	8e 70 3e 97	24 aa 1c a3	61 63 e4	48 43 c4 15	dd 9e 65	f9 09 e2	e7 be e2	ce c1 0f	c2 0a 5e	71 91 36 15 1b	5a 6e 56	9b 94 13 f4	c0 1c 00	7d ad 5b	b8 d4 d8	94 f7 32 1f	6f e7 53 e4	6e 1f c9	49 56 4b	0a 7c d0	ef 1d 26	12 16 f2	56 cc 0f	0b 9a 19	47 6e 5e 96	91 f6																												
RCBC	MDD	IVE	30 df 50 d7	c5 1a a9 f1	90 00 ca 19	54 48 10 87																																																																										
		Scrambled packet	47 60 80 b1	0c 00 01 02	03 04 05 06	07 08 09 0a	0b 5b 50 fd	9d 09 38	2e 60 6f 80	1c ad f1 65	f9 96 d4 61	1b 57 66	d3 92 4d	88 35 32	82 ab cd	26 b9 72	b7 53 b3 7e	b4 3d 2b	ae be 36 f2	c4 32 31	2c 34 b7	5f 82 79	d5 f8 e8	ca 73 30	36 5b d3	58 6f 00	ae 4c 03	fc f9 f7	91 39 fa	4a b9 a7	0d e2 6e	d4 61 1b 57	66 d3 92	4d 88 35	32 82 ab	cd 26 b9	27 11 eb	9f e1 3a 33 b9	23 fd 0f	53 eb bc	ce af 34	b7 5f 82	79 d5 f8	e8 ca 73	30 36 5b	d3 58 57	66 d3	92 4d 88	35 32 82	ab cd 26	b9 27 11	eb 9f e1	3a 33 b9	23 fd	0f 53	eb bc ce	af 34 b7	5f 82	79 d5 f8	e8 ca	73 30 36	5b d3	58 6f	4b f7 38	8f f3 47	da be 86	0e 5a 6e	8d 2e 7b 82	85 1a f5	50 79 8b	94 78 7d	79 fc 52	c5 a9 24	96 b1 31	06 56	1c 49	af 8e 34	3e d4		
		IVE	40 81 e5 3f	73 fc 52 cc	b3 2e 4a 7b	a7 ab 5d 63																																																																										

Table 13: LSA Test Case 09

Context		Test Case 09																																																																																																																																																																																																		
Chaining Mode	MSC Mode		AF size				Payload				MSC				Blocks		Residue																																																																																																																																																																																			
			023		161		027				10		01																																																																																																																																																																																							
CBC	MDI	IVE	cd	61	3b	61	1d	77	69	ad	6b	51	41	00	76	74	45	d8																																																																																																																																																																																		
		Scrambled packet	47	60	80	b1	16	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	10	11	12	13	14	15	0f	95	94	9b	32	2d	00	4d	eb	be	29	82	41	ed	6b	57	15	b0	60	80	e7	fa	51	13	3f	56	e2	fa	12	e9	a6	0e	93	78	b2	6a	1f	6b	c8	3e	63	24	e3	6f	cc	b8	73	b5	a8	67	2b	db	a5	f2	c9	5b	31	eb	f4	89	2e	6d	90	0f	2f	c1	ee	12	c2	5f	81	72	83	e0	c5	9d	3f	9a	db	fa	c0	10	4c	27	62	92	07	30	59	c6	4c	2e	b6	fb	6b	0e	fb	c7	a4	bc	3d	25	56	b2	30	3e	18	23	f8	36	47	af	f6	c8	9d	63	de	c1	ad	48	f7	c9	80	cd	20	cc	70	a2	eb	3d	94	b5	61	2c	dd	45	a7	46	d7	14	88	fe	47	52	29	9b	6c	c6	24	4c	eb	63	21	65	bd	2b	61	30	9a	c9	63						
	IVE	64	3f	01	cd	05	0a	41	04	51	e9	96	3f	66	93	a7	37																																																																																																																																																																																			
	Scrambled packet	47	60	80	b1	16	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	10	11	12	13	14	15	f7	1a	6c	b8	36	35	5e	b8	4e	54	a9	08	4f	b9	24	70	7a	2c	a8	10	2f	e2	c5	95	30	81	ad	01	da	2b	96	f6	71	02	ab	40	99	59	7e	70	0f	75	7c	95	08	82	e2	af	c2	6b	69	b7	10	ab	bc	35	8f	18	76	0c	90	0e	4b	47	cb	f7	12	fa	64	4c	89	f4	0b	b0	cb	3d	40	51	ce	07	6b	99	8e	92	c4	66	c8	8f	41	45	32	c8	be	c9	ca	e8	ad	2c	3e	66	7c	1a	0b	18	d7	7d	3d	26	56	a9	ae	0f	cf	4b	d1	67	fe	61	8c	ce	2f	78	cf	ee	1b	fe	c5	ee	f8	8f	e9	89	4c	28	97	b1	7f	b9	d3	1b	a2	c9	32	c8	41	73	08	22	8a	36	00	a4	b7	62	95	f6	73	3c	2b	33	20							
RCBC	MDI	IVE	40	81	e5	3f	73	fc	52	cc	b3	2e	4a	7b	a7	ab	5d	63																																																																																																																																																																																		
		Scrambled packet	47	60	80	b1	16	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	10	11	12	13	14	15	ac	a2	3a	b2	90	2d	50	08	56	e8	95	70	91	74	47	a8	48	43	c4	15	dd	9e	65	f9	09	e2	e7	be	e2	ce	c1	0f	25	30	9f	50	fc	94	af	d9	a4	11	b4	53	bc	c8	5a	29	1c	00	7d	ad	5b	b8	d4	d8	94	f7	32	1f	6f	e7	53	67	42	34	6b	e9	fb	8e	70	3e	97	24	aa	1c	a3	61	63	e4	48	43	c4	15	dd	9e	65	f9	09	e2	e7	be	e2	ce	c1	0f	c2	0a	5e	71	91	36	15	1b	5a	6e	56	9b	94	13	f4	c0	1c	00	7d	ad	5b	b8	d4	d8	94	f7	32	1f	6f	e7	53	67	14	08	89	7a	ca	b5	ac	82	6a	33	70	c9	b2	94	86	e4	fa	63	7f	87	d4	03	2e	5c	24	69	d9	71	0f	4b	4d	d3	99						
	IVE	e0	7f	0e	4e	bd	04	d8	33	9d	f5	7c	c9	3d	ff	af	43																																																																																																																																																																																			
	Scrambled packet	47	60	80	b1	16	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	10	11	12	13	14	15	95	40	96	fc	ed	22	90	a3	5f	d4	7d	59	ae	8e	18	05	3a	2d	83	85	23	5d	af	8d	13	37	79	15	f9	df	db	45	fc	ee	a1	9b	14	d9	63	dd	63	0e	65	9b	a4	db	a3	5c	db	d8	61	1a	fc	21	cb	42	b0	1f	a9	e3	0e	14	b4	20	28	f5	d1	78	2f	f6	ee	b9	80	6b	29	b9	2f	dc	e7	4b	3a	2d	83	85	23	5d	af	8d	13	37	79	15	f9	df	db	45	fc	ee	a1	9b	14	d9	63	dd	63	0e	65	9b	a4	db	a3	5c	db	d8	61	1a	fc	d8	61	1a	fc	21	cb	42	b0	1f	a9	e3	0e	14	b4	20	28	f5	d1	78	2f	f6	ee	b9	80	29	ce	1d	76	18	34	79	72	23	a0	19	dc	1a	95	2f	f5	9f	9b	a9	61	13	e9	75	57	3b	63	95

Table 14: LSA Test Case 10

Context		Test Case 10																
Chaining Mode	MSC Mode		AF size	Payload	MSC	Blocks	Residue											
			024	160	028	10	00											
CBC	MDI	IVE	ee 01 86 b7 04 9b 6c 27 b6 c3 00 d0 10 da 51 b7															
		Scrambled packet	47 60 80 b1 17 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 85 9b 01 7c a4 0d 43 03 01 59 37 5b f5 87 49 a2 80 89 39 d8 22 2a 1f 64 5f a6 35 e2 d5 2b 23 0e a9 20 b0 87 f7 0c c9 28 a8 2e f8 69 1d 26 e9 a1 8f d6 a8 94 49 f1 89 c2 82 9a ab 2d 15 9c 8d b8 0a 27 40 45 27 26 fe 83 47 7c ab d2 3f 8d eb 89 b1 20 ec e2 6e 44 5e 94 b0 6f 5c 84 53 38 dc 27 cc a3 0e 18 ad 02 a7 4a 0d c7 ad d9 a9 50 f9 c1 c3 e4 a7 8b 12 de f5 36 b3 b9 f4 b5 cf a4 b5 90 93 af 52 cd 52 c0 db 25 4c 28 29 92 32 da 51 d9 2a 99 2c 4e bb ee a2 f7 5b a0 c0 d0 4a c5 8d 7c															
		IVE	05 0f 36 ee 09 6c 82 c9 2e ab 2c 5c f5 54 b9 f8															
		Scrambled packet	47 60 80 b1 17 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 1e 25 11 58 bb 53 84 fb 85 1b 65 45 10 a5 be 03 21 7d 9c ae a1 ff 51 ec b5 9e f7 e7 0b 83 25 a6 64 88 f7 fa de 0e 39 65 c9 bf a4 72 09 88 bf a2 67 29 b0 a8 67 84 ba 6e 90 2d 49 f2 f3 fa 1d f8 ce 33 4a 9d 28 b7 05 b1 a9 be 40 4c 8f fa 47 3d a2 86 30 e7 c1 43 9f 4e a9 13 40 81 44 34 f9 fe 55 c2 63 d1 56 65 87 51 9c 1e e5 09 e8 dc 4c 4c ea a0 c2 c0 f6 5f 9c 5f 84 65 34 cf 25 d2 c5 44 77 9f e1 4f 47 6c fa 44 7f 04 49 3b 38 98 8d 16 94 07 a0 36 c2 bc 3b 14 c7 61 f0 b6 07 4b e9 c6															
	MDD	IVE	40 81 e5 3f 73 fc 52 cc b3 2e 4a 7b a7 ab 5d 63															
		Scrambled packet	47 60 80 b1 17 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 ac a2 3a b2 90 2d 50 08 56 e8 95 70 91 74 47 a8 48 43 c4 15 dd 9e 65 f9 09 e2 e7 be e2 ce c1 0f 25 30 9f 50 fc 94 af d9 a4 11 b4 53 bc c8 5a 29 1c 00 7d ad 5b b8 d4 d8 94 f7 32 1f 6f e7 53 67 42 34 6b e9 fb 8e 70 3e 97 24 aa 1c a3 61 63 e4 48 43 c4 15 dd 9e 65 f9 09 e2 e7 be e2 ce c1 0f c2 0a 5e 71 91 36 15 1b 5a 6e 56 9b 94 13 f4 c0 1c 00 7d ad 5b b8 d4 d8 94 f7 32 1f 6f e7 53 67 d0 05 97 8f 69 e4 3b 86 5f 8c b2 1c 72 c8 d5 78 48 43 c4 15 dd 9e 65 f9 09 e2 e7 be e2 ce c1 0f															
RCBC	MDI	IVE	49 8d 02 fb cb 2b cc 71 92 fc 16 aa 79 46 8d 3d															
		Scrambled packet	47 60 80 b1 17 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 37 1c af 9a bf 0d 32 ea db 86 6b 65 f7 7d 95 74 01 b7 5b fd 3d a9 cc 92 2a d6 3c b3 20 90 d9 7a 7c 72 d1 f4 22 c1 55 be 7f c2 3d 95 fe 60 4f bc ef 78 f7 e6 df f2 02 99 5e 53 f1 d3 6f 0f 6b 86 23 9c a3 81 2e 54 f4 b5 c6 7d f3 67 82 7c ad 4a 01 b7 5b fd 3d a9 cc 92 2a d6 3c b3 20 90 d9 7a a4 c4 2a e9 c9 ab fa 55 32 a2 a4 9f 0e 7c ec 7c ef 78 f7 e6 df f2 02 99 5e 53 f1 d3 6f 0f 6b 86 2b 5a 6c 1f 55 30 1c 44 4b 3b 1a 20 94 e1 62 43 01 b7 5b fd 3d a9 cc 92 2a d6 3c b3 20 90 d9 7a															
	MDD	IVE	49 8d 02 fb cb 2b cc 71 92 fc 16 aa 79 46 8d 3d															
		Scrambled packet	47 60 80 b1 17 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 37 1c af 9a bf 0d 32 ea db 86 6b 65 f7 7d 95 74 01 b7 5b fd 3d a9 cc 92 2a d6 3c b3 20 90 d9 7a 7c 72 d1 f4 22 c1 55 be 7f c2 3d 95 fe 60 4f bc ef 78 f7 e6 df f2 02 99 5e 53 f1 d3 6f 0f 6b 86 23 9c a3 81 2e 54 f4 b5 c6 7d f3 67 82 7c ad 4a 01 b7 5b fd 3d a9 cc 92 2a d6 3c b3 20 90 d9 7a a4 c4 2a e9 c9 ab fa 55 32 a2 a4 9f 0e 7c ec 7c ef 78 f7 e6 df f2 02 99 5e 53 f1 d3 6f 0f 6b 86 2b 5a 6c 1f 55 30 1c 44 4b 3b 1a 20 94 e1 62 43 01 b7 5b fd 3d a9 cc 92 2a d6 3c b3 20 90 d9 7a															

Table 15: LSA Test Case 11

Context		Test Case 11																	
Chaining Mode	MSC Mode		AF size				Payload				MSC				Blocks		Residue		
			025				159				029				09		15		
CBC	MDI	IVE	6f 4c d6 e9 e0 e6 de 9c b9 48 08 53 47 a2 74 5b																
		Scrambled packet	47 60 80 b1 18 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 33 24 eb 58 e4 5f 68 f3 2a 54 ab 77 36 a1 7b ac 49 f7 45 45 cf 1e df 76 9e 2d 29 65 4d b5 6b b9 72 6a 5a a1 0b 50 cd 41 51 73 f9 86 32 13 30 2c c3 c3 61 10 e1 ea a8 26 99 06 5a 6c 85 d8 81 b3 2b ec b6 7c 36 ff 5a 8b 1e fc 5a d6 e2 0a 62 03 09 66 26 52 8e b4 59 d7 d8 69 5c 5d 28 40 68 ba 61 7d a1 a2 76 f7 3e d0 58 bf 9e ff 2c 1e 7e 69 07 dd b0 e2 b4 d4 3c 9d 93 3f cc a2 62 b0 ca e4 2d 35 e0 ca 90 ac 61 f1 cd f7 44 c8 b1 b2 9b 34 0d 64 be 43 8a bb 62 fd 85 a6 ae db 9d 06 8c																
		IVE	33 59 82 ee a1 12 cc 3b e7 cc 8e dd cd e6 ef 6d																
	MDD	Scrambled packet	47 60 80 b1 18 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 ad 26 f9 2e fc 39 00 56 41 1b d4 6c 7a 8e 61 4d f9 af af 24 7f 7b a0 d1 87 9e ed a7 e7 e7 54 2a fe 0d fb b4 18 f2 1b 67 97 32 d9 03 7c 3f 3b 57 28 15 39 8e 54 81 0b ed bc 2b 71 f9 9f 30 83 12 01 64 f2 54 85 fe de 47 37 13 48 4e 95 4c 6c ff ee 5c 43 55 44 08 bd ec 23 72 cc b7 19 23 cf 75 e3 b6 f6 de ef 81 60 d7 96 ed 98 a9 b7 34 95 04 ae 9e cd 15 88 d5 8a 88 a4 3d 4c ec c7 42 93 96 ad 47 a7 13 b7 bc d3 69 42 c2 2f cd dd 0d 26 23 a3 79 96 6a f2 ac de 90 02 a6 40 e4 c0 39 5f																
		IVE	40 81 e5 3f 73 fc 52 cc b3 2e 4a 7b a7 ab 5d 63																
		Scrambled packet	47 60 80 b1 18 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 ac a2 3a b2 90 2d 50 08 56 e8 95 70 91 74 47 a8 48 43 c4 15 dd 9e 65 f9 09 e2 e7 be e2 ce c1 0f 25 30 9f 50 fc 94 af d9 a4 11 b4 53 bc c8 5a 29 1c 00 7d ad 5b b8 d4 d8 94 f7 32 1f 6f e7 53 67 42 34 6b e9 fb 8e 70 3e 97 24 aa 1c a3 61 63 e4 48 43 c4 15 dd 9e 65 f9 09 e2 e7 be e2 ce c1 0f c2 0a 5e 71 91 36 15 1b 5a 6e 56 9b 94 13 f4 c0 1c 00 7d ad 5b b8 d4 d8 94 f7 32 1f 6f e7 53 67 92 a4 f4 2e 9f c3 df 47 52 90 79 fe c6 57 66 cf 0f 8f d0 bc c0 20 5b 0b 28 68 b1 9a 31 30 f2																
RCBC	MDI	IVE	6d 59 82 83 e2 ad 01 68 15 72 4f ba 6b f3 44 15																
		Scrambled packet	47 60 80 b1 18 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 da 5c 53 f5 9c 35 3c a8 0d 2e 74 ba 3e 7e b1 99 6b 6e bd 45 22 42 ee 77 c3 3a 73 3d fb 6e 86 f0 99 0d c0 eb 0a 71 b2 c3 2f a6 f9 e9 94 b2 f3 0c 6f 54 dd 11 aa 09 6d 3b 6b 34 65 fe 59 c2 bc 67 e7 93 c3 0e a1 46 ba 27 55 14 bd d2 d2 e9 0b d5 6b 6e bd 45 22 42 ee 77 c3 3a 73 3d fb 6e 86 f0 bf 67 c8 bf 17 1b 67 a5 e0 28 65 ca 78 fd b1 c5 6f 54 dd 11 aa 09 6d 3b 6b 34 65 fe 59 c2 bc 67 a6 01 72 2b 3a 06 79 42 a9 43 96 e6 49 54 ee 80 a2 e6 90 43 5b 51 49 93 6a 30 a5 f0 3e 8a 66																
	MDD	Scrambled packet	47 60 80 b1 18 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 da 5c 53 f5 9c 35 3c a8 0d 2e 74 ba 3e 7e b1 99 6b 6e bd 45 22 42 ee 77 c3 3a 73 3d fb 6e 86 f0 99 0d c0 eb 0a 71 b2 c3 2f a6 f9 e9 94 b2 f3 0c 6f 54 dd 11 aa 09 6d 3b 6b 34 65 fe 59 c2 bc 67 e7 93 c3 0e a1 46 ba 27 55 14 bd d2 d2 e9 0b d5 6b 6e bd 45 22 42 ee 77 c3 3a 73 3d fb 6e 86 f0 bf 67 c8 bf 17 1b 67 a5 e0 28 65 ca 78 fd b1 c5 6f 54 dd 11 aa 09 6d 3b 6b 34 65 fe 59 c2 bc 67 a6 01 72 2b 3a 06 79 42 a9 43 96 e6 49 54 ee 80 a2 e6 90 43 5b 51 49 93 6a 30 a5 f0 3e 8a 66																

Table 16: LSA Test Case 12

Context		Test Case 12																																																																																																																																																																																											
Chaining Mode	MSC Mode		AF size				Payload				MSC				Blocks		Residue																																																																																																																																																																												
			135				049				139				03		01																																																																																																																																																																												
CBC	MDI	IVE	b6	69	db	61	d0	ba	11	19	3f	70	a1	60	69	ae	81	5c																																																																																																																																																																											
		Scrambled packet	47	60	80	b1	86	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f	80	81	82	83	84	85	c5	7e	ab	49	9b	f0	d1	24	59	84	bb	9a	2b	f8	1e	9c	09	35	5e	3d	41	eb	54	e4	2c	2b	47	f9	40	3e	0d	4f	32	5f	0f	f7	d6	41	a8	64	e9	56	d2	51	60	e5	87	b5
	IVE	6e	a2	95	58	8e	74	79	69	ce	26	ad	37	8d	27	b2	be																																																																																																																																																																												
	Scrambled packet	47	60	80	b1	86	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f	80	81	82	83	84	85	1b	f9	17	45	2b	5c	c8	98	c8	9a	fc	cd	de	79	6b	11	44	46	05	ce	a9	c5	dd	5b	36	2f	ee	2b	2e	ed	8f	7d	8d	af	7a	ee	f0	7b	a2	50	a2	20	24	43	91	ed	14	74	27
RCBC	MDI	IVE	40	81	e5	3f	73	fc	52	cc	b3	2e	4a	7b	a7	ab	5d	63																																																																																																																																																																											
		Scrambled packet	47	60	80	b1	86	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f	80	81	82	83	84	85	ac	a2	3a	b2	90	2d	50	08	56	e8	95	70	91	74	47	a8	48	43	c4	15	dd	9e	65	f9	09	e2	e7	be	e2	ce	c1	0f	71	04	49	90	e4	16	6d	95	56	79	49	a0	02	cb	2e	d0
	IVE	82	a0	30	45	be	b5	75	b3	b1	93	c8	33	74	75	bc	67																																																																																																																																																																												
	Scrambled packet	47	60	80	b1	86	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f	80	81	82	83	84	85	02	b4	ab	6e	4e	2b	a2	e6	49	3d	01	a9	a1	62	9c	95	31	7e	a7	9f	b0	17	95	40	29	a4	28	25	95	23	a1	bf	37	9e	58	87	91	90	e0	87	a4	4a	67	8e	37	c6	d2	aa	bb

Table 17: LSA Test Case 13

Context		Test Case 13																				
Chaining Mode	MSC Mode		AF size	Payload				MSC				Blocks				Residue						
			136	048				140				03				00						
CBC	MDI	IVE	dc	57	bb	97	42	45	de	5a	28	5e	39	18	6b	31	5f	9a				
		Scrambled packet	47	60	80	b1	87	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e
			0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22
			23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	36
		37	38	39	3a	3b	3c	3d	3e	3f	40	41	42	43	44	45	46	47	48	49	4a	
		4b	4c	4d	4e	4f	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	
	5f	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72		
	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f	80	81	82	83	84	85	86		
	26	8d	e6	4b	97	e4	cd	e3	09	4a	ee	60	ef	ab	34	ad	3a	3e	89	8c		
	61	4d	a2	bd	20	94	60	f7	87	dc	1b	3c	0e	a5	98	53	c9	2b	5f	83		
	da	f4	e7	4d	bd	f6	73	42														
	MDD	IVE	79	87	8e	d5	ac	ca	1c	68	9d	98	cf	9f	c8	eb	7f	4e				
Scrambled packet		47	60	80	b1	87	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	
		0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	
		23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	36	
	37	38	39	3a	3b	3c	3d	3e	3f	40	41	42	43	44	45	46	47	48	49	4a		
	4b	4c	4d	4e	4f	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e		
	5f	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72		
	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f	80	81	82	83	84	85	86		
	8d	19	ba	9a	b7	ad	7b	57	93	4d	a4	44	66	b4	8a	7d	bb	72	2f	da		
	00	58	1d	3c	39	0b	24	79	7e	db	64	7b	24	63	5b	43	57	18	72	58		
	4b	48	8d	31	fc	12	85	63														
RCBC	MDI	IVE	40	81	e5	3f	73	fc	52	cc	b3	2e	4a	7b	a7	ab	5d	63				
		Scrambled packet	47	60	80	b1	87	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e
			0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22
			23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	36
		37	38	39	3a	3b	3c	3d	3e	3f	40	41	42	43	44	45	46	47	48	49	4a	
		4b	4c	4d	4e	4f	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	
	5f	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72		
	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f	80	81	82	83	84	85	86		
	52	26	fd	59	bf	94	83	e8	9b	1d	53	f6	86	21	8e	e3	6a	55	88	32		
	b0	38	10	85	19	b9	42	08	de	f6	b1	19	2f	18	f5	29	2c	a5	0a	4c		
	a6	36	a1	c0	52	21	cf	33														
	MDD	IVE	23	94	cc	e5	c0	7a	fe	15	b1	b3	f8	a1	38	c8	50	e5				
Scrambled packet		47	60	80	b1	87	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	
		0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	
		23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	36	
	37	38	39	3a	3b	3c	3d	3e	3f	40	41	42	43	44	45	46	47	48	49	4a		
	4b	4c	4d	4e	4f	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e		
	5f	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72		
	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f	80	81	82	83	84	85	86		
	e4	a4	0f	ae	55	74	79	89	eb	bc	8b	9f	0d	cf	cb	76	4d	8a	62	cf		
	8a	3b	74	cf	69	24	cd	23	f1	42	ec	b3	bc	36	cf	91	de	38	43	74		
	86	28	30	be	b0	1d	23	7d														

Table 18: LSA Test Case 14

Chaining Mode	Context		Test Case 14																
	MSC Mode		AF size	Payload	MSC	Blocks	Residue												
			137	047	141	02	15												
CBC	MDI	IVE	d9 34 21 ef 3f 8d a8 33 46 24 6f 41 ff bc 23 5c																
		Scrambled packet	47 60 80 b1 88 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 0a c5 ea e6 3c bd 37 c1 57 82 88 50 70 93 33 55 8b 1d 4c 35 9e 96 6b f5 b6 54 0e 6d 1c f5 6b 53 a2 c9 5d 04 11 d9 98 46 95 c6 1b 68 28 d1 48																
	MDD	IVE	72 b3 d9 d8 57 39 39 68 3b 23 dd b0 72 66 10 4d																
		Scrambled packet	47 60 80 b1 88 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 c0 f0 30 ad f4 28 8a 32 56 85 55 4d 2a 7e 31 24 1a 59 c5 54 b4 54 9b 9a c1 d7 e3 7d 8d 61 fd 4c e2 e4 98 f0 20 a9 51 24 5b 1a 0c 24 5f d7 e7																
RCBC	MDI	IVE	40 81 e5 3f 73 fc 52 cc b3 2e 4a 7b a7 ab 5d 63																
		Scrambled packet	47 60 80 b1 88 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 52 26 fd 59 bf 94 83 e8 9b 1d 53 f6 86 21 8e e3 16 45 2c df c5 36 6d 17 41 51 6e 7e 3b 9e 52 ab 58 cd a2 85 41 56 20 4b ba c0 61 70 67 77 b6																
	MDD	IVE	01 d5 88 0d 75 83 6c 72 c4 51 5d 70 f3 a1 a3 e0																
		Scrambled packet	47 60 80 b1 88 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 b1 d4 6a 16 71 50 18 8e 33 81 08 fe 7a 8e 8a 5e e8 c4 63 a2 89 8f e6 e7 24 71 63 84 30 5c 66 a6 a5 14 44 37 80 0a e3 e5 94 0a 5b 96 62 41 42																

Table 19: LSA Test Case 15

Chaining Mode	Context		Test Case 15																
	MSC Mode		AF size	Payload				MSC				Blocks				Residue			
			151	033				155				02				01			
CBC	MDI	IVE	6b a4 c2 31 8d 38 9f ea f8 3d b7 7c 63 cf 69 63																
		Scrambled packet	47 60 80 b1 96 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 a6 b8 5d 7d 51 49 76 bd 60 58 80 21 8c c0 c2 d2 f2 14 7e 84 a3 bf 7f 88 5f 9e aa ed c1 e0 d4 1a 27																
		IVE	51 3f 94 f2 b1 d1 5a 2b 9f f9 ae 67 50 c9 f3 9f																
	MDD	Scrambled packet	47 60 80 b1 96 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 1b 98 b0 7b 0b 85 52 5e 94 41 d6 6b 7b f2 1b 56 25 a0 18 20 49 8d bb cf 45 f1 81 50 f9 7f 4a df eb																
		IVE	40 81 e5 3f 73 fc 52 cc b3 2e 4a 7b a7 ab 5d 63																
		RCBC	MDI	IVE	47 60 80 b1 96 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 52 26 fd 59 bf 94 83 e8 9b 1d 53 f6 86 21 8e e3 4c 58 3c 12 a2 95 bd 89 ba 84 46 31 f3 57 e3 1e 28														
Scrambled packet	ca ba 16 fd 28 16 d3 40 92 f4 0f fc 1f fc 60 39																		
IVE	47 60 80 b1 96 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 27 83 78 c0 79 ea 24 c1 1c 53 54 13 ed 27 9a 59 2f e9 6c 5e ee f7 08 f7 68 7f 02 d2 06 7f 13 38 71																		
MDD	Scrambled packet		ca ba 16 fd 28 16 d3 40 92 f4 0f fc 1f fc 60 39																
	IVE		47 60 80 b1 96 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 27 83 78 c0 79 ea 24 c1 1c 53 54 13 ed 27 9a 59 2f e9 6c 5e ee f7 08 f7 68 7f 02 d2 06 7f 13 38 71																
	Scrambled packet		ca ba 16 fd 28 16 d3 40 92 f4 0f fc 1f fc 60 39																

Table 20: LSA Test Case 16

Context		Test Case 16																		
Chaining Mode	MSC Mode		AF size				Payload				MSC				Blocks		Residue			
			152				032				156				02		00			
CBC	MDI	IVE	4b 93 69 84 fe 0c 29 69 aa b4 5e 9c a8 a3 60 57																	
		Scrambled packet	47 60 80 b1 97 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 da 99 7d 71 59 ee 18 2e d7 48 9f b3 15 18 8f 3a 07 71 33 0d d8 a8 58 32 8b 6e 96 6e ee 29 0d e8																	
		IVE	77 2d f2 3f 1b 1e e8 e1 dd 61 1d b3 48 28 2f de																	
		Scrambled packet	47 60 80 b1 97 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 d9 26 6c 53 85 53 b6 41 f2 97 62 88 14 e9 69 b6 6a b5 f0 fd 2a 1f 67 0b 02 81 75 84 84 f7 3e be																	
		IVE	40 81 e5 3f 73 fc 52 cc b3 2e 4a 7b a7 ab 5d 63																	
	Scrambled packet	47 60 80 b1 97 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 ac a2 3a b2 90 2d 50 08 56 e8 95 70 91 74 47 a8 48 43 c4 15 dd 9e 65 f9 09 e2 e7 be e2 ce c1 0f																		
	RCBC	MDI	IVE	fc 8a ee af d6 3b d4 eb 83 42 c8 b4 cc a2 e1 d6																
			Scrambled packet	47 60 80 b1 97 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 f0 2a b7 8d c1 17 ac 06 7f c7 21 44 0e 27 5d fd 91 5a 71 0b 68 ff 76 7c 73 78 91 c9 07 ac 31 e3																
		MDD	IVE	fc 8a ee af d6 3b d4 eb 83 42 c8 b4 cc a2 e1 d6																
			Scrambled packet	47 60 80 b1 97 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 f0 2a b7 8d c1 17 ac 06 7f c7 21 44 0e 27 5d fd 91 5a 71 0b 68 ff 76 7c 73 78 91 c9 07 ac 31 e3																

Table 21: LSA Test Case 17

Context		Test Case 17																																																																																																																																																																																											
Chaining Mode	MSC Mode		AF size			Payload			MSC			Blocks			Residue																																																																																																																																																																														
			153			031			157			01			15																																																																																																																																																																														
CBC	MDI	IVE	f8	52	d3	9f	7e	03	f9	ad	36	af	ba	f8	13	37	82	15																																																																																																																																																																											
		Scrambled packet	47	60	80	b1	98	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f	80	81	82	83	84	85	86	87	88	89	8a	8b	8c	8d	8e	8f	90	91	92	93	94	95	96	97	8f	90	ba	d5	6a	2c	23	bc	8c	f7	f7	ea	a2	f7	45	3a	d8	fc	c0	45	67	13	6b	d2	fd	a7	9b	92	48	b3
	IVE	5c	19	74	d8	34	44	a8	97	c5	3d	16	2e	61	ec	58	19																																																																																																																																																																												
	Scrambled packet	47	60	80	b1	98	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f	80	81	82	83	84	85	86	87	88	89	8a	8b	8c	8d	8e	8f	90	91	92	93	94	95	96	97	7d	af	26	3f	49	bd	51	cb	54	59	4c	a8	17	94	0f	15	5d	0f	bd	06	3c	61	24	c1	97	a7	58	b0	5b	8b	ed
RCBC	MDI	IVE	40	81	e5	3f	73	fc	52	cc	b3	2e	4a	7b	a7	ab	5d	63																																																																																																																																																																											
		Scrambled packet	47	60	80	b1	98	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f	80	81	82	83	84	85	86	87	88	89	8a	8b	8c	8d	8e	8f	90	91	92	93	94	95	96	97	59	22	b5	fe	96	7b	7f	e1	ff	0b	1f	7e	3e	f3	9b	ee	66	36	17	95	58	eb	fe	3e	9e	f9	f9	40	ab	17
	IVE	e7	6f	a5	ef	d5	d3	33	df	f4	70	9f	ed	74	2b	80	04																																																																																																																																																																												
	Scrambled packet	47	60	80	b1	98	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f	80	81	82	83	84	85	86	87	88	89	8a	8b	8c	8d	8e	8f	90	91	92	93	94	95	96	97	35	c8	34	08	c8	dd	6e	b5	27	cc	2a	24	36	37	ca	a6	32	12	6e	ab	21	5b	8f	cb	26	c8	cf	f3	c6	96	d3

Table 22: LSA Test Case 18

Context			Test Case 18																	
Chaining Mode	MSC Mode		AF size	Payload				MSC				Blocks				Residue				
			167	017				171				01				01				
CBC	MDI	IVE	b1 08 43 14	7a cf 6f 1d	0e 51 eb 99	cb 41 22 be														
		Scrambled packet	47 60 80 b1 a6 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 4b 02 23 ab af a6 ae 25 52 3a 00 fe 40 6e a5 cb 2a																	
		IVE	cc 94 4c 72 2a 6e 25 ea 6e 71 ed 67 e1 83 cc 28																	
		Scrambled packet	47 60 80 b1 a6 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 97 1a 4c f4 d3 d4 1c c8 49 dc 1a f2 64 fc c9 2d 76																	
	MDD	IVE	40 81 e5 3f 73 fc 52 cc b3 2e 4a 7b a7 ab 5d 63																	
		Scrambled packet	47 60 80 b1 a6 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 7b 57 f3 b3 9d 91 08 cc dd 7d ac 21 52 c8 a0 4a 41																	
RCBC	MDD	IVE	ac e6 0b f2 13 8e 52 04 13 23 39 a7 75 17 c8 11																	
		Scrambled packet	47 60 80 b1 a6 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 76 3d e1 5e 14 f6 83 e2 0d 59 2a 59 4d ad b3 63 32																	

Table 23: LSA Test Case 19

Context			Test Case 19																	
Chaining Mode	MSC Mode		AF size	Payload				MSC				Blocks				Residue				
			168	016				172				01				00				
CBC	MDI	IVE	0a c1 bc 20	2e de c4 52	da 9f aa 85 58	60 ba 1f														
		Scrambled packet	47 60 80 b1 a7 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 27 7e 81 f6 13 8d cb 4f 35 1c a1 65 ab b5 d2 db																	
		IVE	95 bf fe 7a 4d e1 5f 6e	72 a9 59 13 a5	29 ee 94															
		Scrambled packet	47 60 80 b1 a7 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 1e 9f 96 3d c7 f5 a7 6b 2a 5e c9 03 a1 fe cc 81																	
	MDD	IVE	40 81 e5 3f 73 fc 52 cc b3 2e 4a 7b a7 ab 5d 63																	
		Scrambled packet	47 60 80 b1 a7 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 52 26 fd 59 bf 94 83 e8 9b 1d 53 f6 86 21 8e e3																	
RCBC	MDI	IVE	fa 3a 6b f8 e3 f3 aa 90 2b ae 91 d3 02 7b 35 51																	
		Scrambled packet	47 60 80 b1 a7 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 4c ce 55 c1 78 bf f9 2e 82 eb ff a1 0d 50 60 6a																	
	MDD	IVE	fa 3a 6b f8 e3 f3 aa 90 2b ae 91 d3 02 7b 35 51																	
		Scrambled packet	47 60 80 b1 a7 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 4c ce 55 c1 78 bf f9 2e 82 eb ff a1 0d 50 60 6a																	

Table 24: LSA Test Case 20

Chaining Mode	Context		Test Case 20																																																																																																																																																																																										
	MSC Mode		AF size	Payload				MSC				Blocks				Residue																																																																																																																																																																													
			169	015				173				00				15																																																																																																																																																																													
CBC	MDI	IVE	13	16	3e	ed	ac	b1	99	0e	77	b1	24	4d	27	c5	90	09																																																																																																																																																																											
		Scrambled packet	47	60	80	b1	a8	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f	80	81	82	83	84	85	86	87	88	89	8a	8b	8c	8d	8e	8f	90	91	92	93	94	95	96	97	98	99	9a	9b	9c	9d	9e	9f	a0	a1	a2	a3	a4	a5	a6	a7	13	17	3c	ee	a8	b4	9f	09	7f	b8	2e	46	2b	c8
	IVE	95	1f	c7	40	e7	c3	31	03	5e	1e	5b	09	f4	ed	9d	57																																																																																																																																																																												
	MDD	Scrambled packet	47	60	80	b1	a8	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f	80	81	82	83	84	85	86	87	88	89	8a	8b	8c	8d	8e	8f	90	91	92	93	94	95	96	97	98	99	9a	9b	9c	9d	9e	9f	a0	a1	a2	a3	a4	a5	a6	a7	95	1e	c5	43	e3	c6	37	04	56	17	51	02	f8	e0
RCBC	MDI	IVE	40	81	e5	3f	73	fc	52	cc	b3	2e	4a	7b	a7	ab	5d	63																																																																																																																																																																											
		Scrambled packet	47	60	80	b1	a8	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f	80	81	82	83	84	85	86	87	88	89	8a	8b	8c	8d	8e	8f	90	91	92	93	94	95	96	97	98	99	9a	9b	9c	9d	9e	9f	a0	a1	a2	a3	a4	a5	a6	a7	40	80	e7	3c	77	f9	54	cb	bb	27	40	70	ab	a6
	IVE	b2	60	ac	ec	d5	1d	a2	26	ce	af	91	3f	0a	cf	e9	52																																																																																																																																																																												
	MDD	Scrambled packet	47	60	80	b1	a8	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f	80	81	82	83	84	85	86	87	88	89	8a	8b	8c	8d	8e	8f	90	91	92	93	94	95	96	97	98	99	9a	9b	9c	9d	9e	9f	a0	a1	a2	a3	a4	a5	a6	a7	b2	61	ae	ef	d1	18	a4	21	c6	a6	9b	34	06	c2

Table 25: LSA Test Case 21

Context		Test Case 21																		
Chaining Mode	MSC Mode		AF size	payload				MSC				blocks				residue				
			183	001				187				00				01				
CBC	MDI	IVE	4b 31 21 90	f5 3f 5b c1	32 15 a7 eb	51 2d 30 aa														
		Scrambled packet	47 60 80 b1 b6 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5 4b																	
		IVE	39 c3 e7 db	17 03 2a 96	e1 51 ca cf	26 52 07 da														
		Scrambled packet	47 60 80 b1 b6 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5 39																	
		IVE	40 81 e5 3f 73 fc	52 cc b3 2e 4a 7b a7	ab 5d 63															
		Scrambled packet	47 60 80 b1 b6 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5 40																	
	MDD	IVE	cf e5 0c 34 9b 14 e6 c7	de 99 6e 65 f3 aa dd a1																
		Scrambled packet	47 60 80 b1 b6 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5 cf																	
		IVE	40 81 e5 3f 73 fc	52 cc b3 2e 4a 7b a7	ab 5d 63															
		Scrambled packet	47 60 80 b1 b6 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5 40																	
		IVE	cf e5 0c 34 9b 14 e6 c7	de 99 6e 65 f3 aa dd a1																
		Scrambled packet	47 60 80 b1 b6 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5 cf																	

4.6 Certificate Verification

This clause lists the test data for the following processes, performed in the listed order:

- 1) Verifying the hash of an unencrypted CPCM Signing Certificate, i.e. after it is recovered using RSA verification with message recovery using the public RSA key of its parent Certificate, as described in TS 102 825-5 [i.7].
- 2) Expanding the compressed modulus of the Signing Certificate using the process described in TS 102 825-5 [i.7].
- 3) Using this modulus to recover a leaf certificate that was signed with the private RSA key associated with the parent Certificate. This *RSA verification with message recovery* process is described in TS 102 825-5 [i.7].
- 4) Step 1 above, but now verifying the recovered leaf Certificate, which now contains a Diffie-Hellman public key instead of a compressed RSA modulus.

Table 26: CPCM constants used for Certificate signing and verification

Public key: e	$2^{16} + 1 = 65537$
Non-secret universal CPCM constant: C	0x243F6A8885A308D313198A2E03707344
IVCertificate	0xc0ac29b7c97c50dd3f84d5b5b5470917

Table 27 lists the body parameters used in the parent Certificate.

Table 27: Parent Certificate parameters

CPCM_version	0x01
CPCM_instance_id	0x0011223344556677
CPCM_instance_certificate_id	0xFEDCBA9876543210
issuer_id	0x0000111122223333
C and R regime mask	0x01
certificate_expiration_time	0xFFFFFFFF
generation_index	0x01
is_signer	1 (Yes)
is_revocation	0 (No)
content_handling_capability	0 (Not a device certificate, no CPCM functionality implemented)
AD_aware	0 (No)
ADM_capable	0 (No)
ADM_LM_capable	0 (No)
ADM_DC_capable	0 (No)
ADSE_countable	0 (No)
LSA_capable	0 (No)
absolute_time_aware	0 (No)
geographic_aware	0 (No)

Table 28 shows the recovered parent Certificate.

Table 28: Recovered Parent Certificate

Hash: M_1 with the MSB set to 0	1e 8c f9 03 9d 33 40 ae d5 87 11 2d 87 d0 25 8f
Certificate body: $M_2 \dots M_8$	01 00 11 22 33 44 55 66 77 fe dc ba 98 76 54 32 10 00 00 11 11 22 22 33 33 01 ff ff ff ff 01 80 00
compressed modulus: $M_9 \dots M_{16}$	7e 70 a3 f8 b9 fc 58 9d 4b 7f dc 56 0f e1 4b 49 a1 9b 6b a9 43 29 d0 ed 8d 06 98 90 33 16 c5 d7 9d d0 ef 30 7f 25 a7 5d 66 91 44 1a c2 8c a8 8a 7f 11 f3 3d ef 81 e5 d0 69 24 14 df 02 3f 12 a1 98 16 58 95 7f 7f fe 98 df a2 0b 76 e2 95 5f d3 96 dd 2b 5c 44 20 27 de f7 f1 c7 67 84 31 31 3b b6 cd f4 04 9e 83 7c 16 07 94 2b 4f 76 e8 ae a3 bb c2 96 ea 6f 67 5b 97 7c d4 ed be f2 fb 41 ef

Table 29 shows the data used in the verification process as described in step 6 in clause 4.6 in TS 102 825-5 [i.7]. Note that digest_3 thru digest_{14} are omitted and that the 127 LSBs of digest_{15} matches the hash of the Certificate as required.

Table 29: Verifying the hash of the Parent Certificate

$\text{digest}_0 = \text{IVCertificate}$	c0 ac 29 b7 c9 7c 50 dd 3f 84 d5 b5 b5 47 09 17
$\text{digest}_1 = E(\text{digest}_0)(M_2) \oplus (M_2)$	ef 58 93 fe 6f a6 f8 e8 e6 22 e1 16 c7 30 4f 58
$\text{digest}_2 = E(\text{digest}_1)(M_3) \oplus (M_3)$	97 e7 a2 dd 9d 01 82 5c 46 27 42 81 ca ac 13 8e
...	...
$\text{digest}_{15} = E(\text{digest}_{14})(M_{16}) \oplus (M_{16})$	1e 8c f9 03 9d 33 40 ae d5 87 11 2d 87 d0 25 8f
hash: M_1	1e 8c f9 03 9d 33 40 ae d5 87 11 2d 87 d0 25 8f

Table 30: Expanding the Parent Certificate's compressed modulus

$S_0 =$ padded Signing Certificate Id	fe dc ba 98 76 54 32 10 00 00 00 00 00 00 00
$S_l = E\{C\}(S_{l1}), l = 1 \dots 8$	4e b8 cf 55 05 e0 1e 46 45 ec 65 be 57 6c 74 fd
	ea 24 b4 c3 02 8b 83 fd 2a 81 87 b1 55 67 31 6d
	39 4a d3 b9 7a f8 e7 2c ac e6 06 dd 74 ba 57 06
	7b 50 a7 e3 af 62 d7 4e 37 3c 30 ad a2 23 bb 6f
	a7 c8 8e c0 9f cc 3a ea 06 38 4f ac 02 3f e2 58
	52 70 39 f3 9f 99 70 ba dc 25 a4 72 a9 30 df 19
	ad 36 c9 f0 4a 7a bf f5 b4 18 17 e3 6d ae ce 88
	25 cb 58 63 ff 71 1c d9 17 d7 c8 e6 e4 f6 df 48
uncompressed modulus: $n = S_1 \parallel M_9 \parallel \dots \parallel S_8 \parallel M_{16}$ with the MSB set to 1.	ce b8 cf 55 05 e0 1e 46 45 ec 65 be 57 6c 74 fd
	7e 70 a3 f8 b9 fc 58 9d 4b 7f dc 56 0f e1 4b 49
	ea 24 b4 c3 02 8b 83 fd 2a 81 87 b1 55 67 31 6d
	a1 9b 6b a9 43 29 d0 ed 8d 06 98 90 33 16 c5 d7
	39 4a d3 b9 7a f8 e7 2c ac e6 06 dd 74 ba 57 06
	9d d0 ef 30 7f 25 a7 5d 66 91 44 1a c2 8c a8 8a
	7b 50 a7 e3 af 62 d7 4e 37 3c 30 ad a2 23 bb 6f
	7f 11 f3 3d ef 81 e5 d0 69 24 14 df 02 3f 12 a1
	a7 c8 8e c0 9f cc 3a ea 06 38 4f ac 02 3f e2 58
	98 16 58 95 7f 7f fe 98 df a2 0b 76 e2 95 5f d3
	52 70 39 f3 9f 99 70 ba dc 25 a4 72 a9 30 df 19
	96 dd 2b 5c 44 20 27 de f7 f1 c7 67 84 31 31 3b
	ad 36 c9 f0 4a 7a bf f5 b4 18 17 e3 6d ae ce 88
	b6 cd f4 04 9e 83 7c 16 07 94 2b 4f 76 e8 ae a3
	25 cb 58 63 ff 71 1c d9 17 d7 c8 e6 e4 f6 df 48
	bb c2 96 ea 6f 67 5b 97 7c d4 ed be f2 fb 41 ef

This uncompressed modulus is used to recover a leaf certificate that was signed with the private RSA key associated with the Signing Certificate. This *RSA verification with message recovery* process is described TS 102 825-5 [i.7]. The signed leaf Certificate is shown in Table 31 and the recovered Certificate in Table 32. The hash is verified by the same process as is shown in Table 29, using the CPCM Instance Certificate Id of the leaf Certificate. This id and the Diffie-Hellman public key are the ones used for Certificate A in the AKE process described in clause 5.1. Table 33 shows the recovered leaf certificate parameters.

Table 31: Signed Leaf Certificate

Leaf Certificate RSA signed with the private RSA key associated with the Singer's Certificate.	9b 50 79 0f d1 90 a1 60 14 ac ca 08 e9 4b da 42
	b9 49 2e 8d 0d 29 a5 36 f6 1e 9d 36 93 3f e4 73
	28 28 f1 75 86 91 c7 46 f9 10 36 0d 0e b8 94 01
	5a 87 b4 5e e8 aa 3f f4 72 85 e6 96 b3 ac 3f df
	05 cf 05 81 07 ce 84 71 56 97 99 5d 79 05 22 41
	3e cf a3 b3 00 e5 26 47 b1 07 ab c6 83 84 4c 20
	ba cb 29 b8 b8 5a 87 15 41 42 9e 75 ab a5 4e 54
	1f 6c fb 22 f5 9a e9 c7 42 57 68 d1 3c 17 cc 72
	af 14 69 83 3f 65 b2 13 04 1b 25 8b 4c 91 47 79
	28 ef 80 66 7f a9 a3 72 34 25 8c b5 15 21 f6 e1
	87 fc ad c4 6c f4 79 90 2c 15 d3 eb 63 79 f5 87
	1e c7 2f 8d 0e 78 27 fd fa 60 6c 24 87 f1 9d 35
	b7 a2 ba 0f 37 b8 f9 fd 1f d3 bf 80 ce 9c d2 f7
	75 96 b3 3e 0f 50 89 d6 89 93 80 f2 2c 7c f5 c0
	fe d8 f6 54 b5 8c 70 78 45 51 cd d6 94 9e 4f 53
	1c 2f d8 21 6d 78 c9 89 4e dc 32 20 4c 3d ae bd

Table 32: Recovered Leaf Certificate

hash: M_1	25 d7 6f 98 bc 4c ca 99 ab c6 98 d9 26 f3 80 f0
Certificate body: $M_2 \dots M_8$	01 00 11 22 33 44 55 66 77 43 50 43 4d 5f 49 64 41 00 00 11 11 22 22 33 33 01 ff ff ff ff ff 01 02 00
Diffie-Hellman public key	13 72 5c e9 68 76 8c a2 a0 49 cf f0 b4 08 32 8f 0e 87 65 9c 19 1a ea 14 6b 32 8e 62 f9 fb b3 fe 25 10 bd 06 3c 85 71 42 70 9d 31 22 b8 6d 55 61 4f 08 c4 03 2d 1f d0 fd f4 35 81 e6 b1 68 53 99 ee 8a 2d e8 24 43 2f 21 2e fd f5 46 f1 2b 05 6c 30 9d 2b fa a3 c1 2e 1f 5c c5 b5 eb 09 94 f7 1f 9e 84 31 25 2f 7a 3f 56 0d 02 73 12 06 3d 17 4e 93 92 4f fa 53 8e 6f bf bc 9b fb 31 68 30 b8 d9
Verified hash: 127 LSB match M_1	a5 d7 6f 98 bc 4c ca 99 ab c6 98 d9 26 f3 80 f0

Table 33: Leaf Certificate parameters

CPCM_version	0x01
CPCM_instance_id	0x0011223344556677
CPCM_instance_certificate_id	0x4350434D5F496441
issuer_id	0x0000111122223333
C and R regime_mask	0x01
certificate_expiration_time	0xFFFFFFFFFFFF
generation_index	0x01
is_signer	0 (No)
is_revocation	0 (No)
content_handling_capability	2 (Consumption Point)
AD_aware	0 (No)
ADM_capable	0 (No)
ADM_LM_capable	0 (No)
ADM_DC_capable	0 (No)
ADSE_countable	0 (No)
LSA_capable	0 (No)
absolute_time_aware	0 (No)
geographic_aware	0 (No)

4.7 Certificate keys and digest generation

This clause lists the test data for generating Signing Certificate RSA keys and the hash used for verifying the Certificates by its child certificate. The process is described in clause 4.7 in TS 102 825-5 [i.7].

The generated Signing Certificate is also used in the previous clause. Its parameters are shown in Table 27. The CPCM constants used are shown in Table 26. The process starts with expanding the CPCM Instance Certificate Id as is shown in Table 30. This expanded id is used together with a chosen prime p , to find a suitable second prime q and modulus $n = pq$. The details of this process are beyond the scope of the present document. Table 34 shows the primes and secret RSA signing key d . The modulus is shown in Table 30. Note that the second prime q is just an example; it can be any prime that results in a modulus $n = pq$ for which, when divided in blocks of 16 bytes each, the odd blocks are made up of the expanded Signing Certificate ID. The prime q depends on the algorithm used to discover it, which is not part of the present document.

The hash of the Signing Certificate is calculated as shown in Table 29 and its MSB is set to 0. A compressed modulus is created by concatenating the blocks $M_9, M_{10}, \dots, M_{16}$ shown in Table 30. The hash, certificate body and the compressed modulus are concatenated to form the unencrypted Signing Certificate shown in Table 28.

The secret key d is used to RSA sign the Leaf Certificate shown in Table 32 as the concatenation of $M_1 \dots M_8$ and the Diffie-Hellman public key. Note that the MSB of the hash (M_1) is set to 0 prior to RSA signing. The result is the signed Leaf Certificate shown in Table 31.

Table 34: Signing Certificate's primes and secret key

chosen first prime p	e4 e6 c8 d7 17 d9 1c 71 ff 63 58 cb 25 88 ce ae 6d e3 17 18 b4 f5 bf 7a 4a f0 c9 36 ad 19 df 30 a9 72 a4 25 dc ba 70 99 9f f3 39 70 52 58 e2 3f 02 ac 4f 38 06 ea 3a cc 9f c0 8e c8 a7 6f bb 23 a2 ad 30 3c 37 4e d7 62 af e3 a7 50 7b 06 57 ba 74 dd 06 e6 ac 2c e7 f8 7a b9 d3 4a 39 6d 31 67 55 b1 87 81 2a fd 83 8b 02 c3 b4 24 ea fd 74 6c 57 be 65 ec 45 46 1e e0 05 55 cf bf 6f
discovered second prime q (Note that this is just an example)	e7 31 d6 a7 47 4a ba 15 d6 48 f5 4c d2 81 3d 0e 43 94 fa 18 17 d1 1c ee 67 08 8d cc 3c 4b 32 f0 d2 27 e2 40 19 67 bc c6 e0 df 7c 7f 34 ef 51 fa 4d d1 98 20 b0 e2 ea ff 59 34 63 8f 28 52 f0 bc b5 e0 d4 2b b0 54 f2 a8 47 19 6b 4f fa 67 3f b2 e1 b4 81 d7 d7 73 dc 26 71 bc 52 30 78 24 2c 0d 4e 0c 14 c7 a0 bb cf 1b 50 8e 50 f6 0d 4a fe 56 59 2b c0 a0 32 cf f1 b7 3b 47 c0 b0 3b b7 5f 4b 0b 65 81
private RSA key $d = \text{inverse of } e \text{ modulo } (p-1)(q-1)$:	14 59 26 b7 74 cb 99 cf 4b 04 b9 03 22 71 df 96 30 43 00 30 f4 85 bd 67 46 4e 40 af 0c 03 1e 39 19 5e 21 98 ec 80 35 2e cf 67 4e a7 0b 04 0c 5e 81 40 de 39 1c 0e 5a ad 77 6b 45 cb 33 ec 32 ef 3b 89 7d 0b cd ea 00 3f 6a 89 7d f5 80 8e f3 10 08 aa cf 50 93 c3 6e 15 08 8a 96 0c 98 47 e6 33 33 6e 3e 08 70 74 27 43 60 b6 81 08 26 64 a4 07 96 97 7a bd 06 fd 5f 54 c3 74 b4 c5 3a c9 9e ab fc d1 bc 7c ec 25 fd 75 ee 71 ea 32 65 27 63 23 1e 59 cc 60 7b be 5d 3e 23 cf 01 26 40 8d 5b 60 88 6d a6 2e 57 f4 fc 98 f0 b8 f1 7c 1b 7c d7 a7 12 97 fe 13 af d8 61 50 57 40 cd 8e a1 f4 d8 6b f4 94 71 de a5 2d 7f e2 cb be 4e e0 08 b6 84 7f 4a 84 5e 6b 8e 80 63 dc 2b 79 d2 53 92 71 e9 e4 fa 8f 5d 49 6a 3e 9c 8d 25 8c 02 4e d2 49 69 2b 58 12 53 3a 73 3b a9 1b 6f 04 4d c9 b8 39 c7 01

5 Test Vectors Cryptographic Protocols

5.1 Authenticated Key Exchange (AKE)

This clause contains the test data for the Authenticated Key Exchange protocol, which is described in clause 5.1 in TS 102 825-5 [i.7]. Table 35 shows the used CPCM public constants, which are defined in clause 6.3 in TS 102 825-5 [i.7]. Tables 36 and 37 contain the CPCM Instance Certificate Id, the chosen secret key, the derived public key and chosen random exponent for certificates A and B respectively.

Table 35: CPCM public constants for AKE

Group generator g	2
Modulus, p	da b6 b0 94 b2 c5 6a 0e d1 6b c4 6e f6 04 cf d9 ba 34 04 ca c4 bf 65 96 49 97 d0 dd c6 c5 a0 d0 75 9f af c4 67 44 45 74 57 57 8b cc 3c 70 7b f7 c2 6a 3b a9 df a5 cd 27 d2 e1 9f 60 df d3 37 d0 a0 51 ec cc 3b 82 4b 63 09 d6 fc 5c db 7e e0 41 ea 56 32 78 cb 05 4c 1b 54 25 0a c1 fb 00 d8 91 15 22 dc f6 38 c3 02 75 b3 82 46 14 69 69 35 39 fb 89 e9 fc ec 47 5a 1a f2 fd d3 9c bf b0 c8 db

Table 36: AKE values for CPCM Instance A

CPCM instance certificate id ld_A	43 50 43 4d 5f 49 64 41
Chosen secret key a	66 e4 76 cd 18 79 80 8f ff 40 c1 1c 9b 89 35 27 8c f4 ac 25 f6 c9 a0 dd f1 e2 dd 1d 87 2a 45 31 33 04 cc 74 e7 b6 26 e6 a2 00 16 35 fd b7 44 bd a5 d8 4a 95 4f 9c bb 69 bc c7 4d 35 ae ff 13 5d 39 d3 ad 0e 7a 4a 0f 10 b4 c5 f3 a4 eb 3c 3d 2b d8 b9 0c 43 56 63 1d 34 3d 45 b0 aa e9 36 77 d9 77 77 79 e6 fe 27 6b 2f dc 3c ee f5 c6 5b 3a 6d f6 54 fc a1 30 7e 43 90 c8 cc 40 7e cc c9 40 9f
Derived public key g^a	13 72 5c e9 68 76 8c a2 a0 49 cf f0 b4 08 32 8f 0e 87 65 9c 19 1a ea 14 6b 32 8e 62 f9 fb b3 fe 25 10 bd 06 3c 85 71 42 70 9d 31 22 b8 6d 55 61 4f 08 c4 03 2d 1f d0 fd f4 35 81 e6 b1 68 53 99 ee 8a 2d e8 24 43 2f 21 2e fd f5 46 f1 2b 05 6c 30 9d 2b fa a3 c1 2e 1f 5c c5 b5 eb 09 94 7f 1f 9e 84 31 25 2f 7a 3f 56 0d 02 73 12 06 3d 17 4e 93 92 4f fa 53 8e 6f bf bc 9b fb 31 68 30 b8 d9
Chosen random exponent x	45 37 81 57 a3 61 35 1b ad 03 5e 7b 75 8d 35 73 33 f3 19 97 05 13 fe e5 4f 87 7e c1 f4 d7 8e 32 2b e6 6a 55 9d ab 3a ce 16 1b 70 59 06 ee 90 05 e6 4b a8 89 ee 84 59 58 d9 eb c9 7e d3 e2 d7 e3 b7 2e 76 db 16 7c 74 d1 82 41 85 a6 23 f4 e1 ca 83 e9 5e a0 f5 69 0b cb 25 3c 54 82 22 a7 0c 20 64 0e a8 19 28 56 56 ca df e5 6b a2 d2 ef 0c 4b 8c 6a dc d0 a8 ab 5b ce f4 46 a2 55 87 e2 a2 ec

Table 37: AKE values for CPCM Instance B

CPCM instance certificate id ld_B	43 50 43 4d 5f 49 64 42
Chosen secret key b	79 69 86 57 7e de eb d3 b3 35 64 19 ac 76 1f 27 ba 04 85 cf c8 14 c1 b5 15 8c 95 8f de 02 6e 5e 8c ac 88 e7 ef 2d 9a b2 22 38 0a 8d 35 aa ad 4e 0b 11 d2 d8 83 e7 85 58 21 f1 4f 75 72 62 8c 93 b7 7f 82 9e 93 47 d2 c1 7b 36 c7 96 76 a8 fd 05 28 0a 1a 01 53 09 67 e9 c5 f3 f5 ec cf 73 1a 8e 98 9e a6 62 1e 33 e0 5f 8d ca 08 85 b2 e9 88 61 76 7f 72 3e da 78 86 a3 27 93 a8 82 eb bb f0 47
Derived public key g^b	97 64 7f 35 c3 0f 7c 74 1d d6 f2 88 1c 68 3e 55 e6 62 67 a1 8f ac 1d 16 c3 3d 9f 17 32 78 94 ad 30 5d 8c 8a 92 c0 23 85 47 bd 32 b4 ee 8b cb 73 fa b4 4b 80 64 60 4a 88 e2 31 59 44 86 be 01 a2 be c3 1c e7 f5 cd 0f 92 be 05 1b 69 90 84 37 e2 5e 80 ef 0c 49 e1 e7 3e 9a fa f5 84 fa 82 d0 70 10 6b ae d9 84 25 24 8e 92 3b 3e a6 c6 53 22 3d ac 4e 4b e0 6c 41 4b ac 22 2b 0c 68 e2 a0 60 94
Chosen random exponent y	5e ac de 5c 00 20 17 c8 20 9b f0 c5 8e 0e fd b6 bb 83 b3 70 5d 49 82 f7 d7 3d 04 32 21 13 f0 58 93 e6 ca dd f9 ec fd 24 8d 06 9b fc 27 c2 72 20 55 77 2c ea 6b 76 fd f0 a1 c0 9b f7 54 f6 2b 32 57 d0 61 55 50 d5 f9 43 37 10 7d 10 25 b3 d5 08 dd b3 b6 b5 99 db 61 a3 ca e6 d9 9a f0 95 15 b3 6a 63 65 b6 7e 13 43 60 5a cf 13 6e f1 db ad fa 5f 57 d0 1f a1 82 17 c9 65 cf fd 1f 38 d7 e2 2a

Table 38 contains the values that are exchanged unencrypted between certificate A and B.

Table 38: AKE public values used in the protocol

g^x	7c fd 98 6f c0 78 cc bb f8 df b4 f0 9c 5a 03 c5 5d e1 0a a4 52 2c 22 b0 d3 fc 38 9d 62 1d 39 7d 38 a5 e1 1f 4a 57 62 f4 c2 07 34 eb fa 53 a3 82 9a 6e 30 5c 50 ca db e4 fb 9a 71 2e fc cf 10 e6 98 e3 d9 6d fc 93 60 f0 9b 4e 5f 4d 7b cc 89 14 af 16 5b 80 76 4d 49 17 8e df 6f e3 7e 90 55 9f 5f 7e 2c c9 ef 93 8d a5 e6 9e 6e 52 b4 87 d5 22 9f 6b 79 cf e8 af 98 2d 24 13 e9 09 f9 3a 53 34
g^y	2e 79 bc 54 9f 44 cc 34 7d 12 47 b4 b9 b0 f7 31 2f c9 f5 c9 81 f2 ad 35 bb 6f 5a e9 6c 47 8a da 65 95 10 88 f9 5f 86 57 41 6b 8a 7e 9f 18 2d 49 6c 26 e7 88 2c 07 87 00 e0 c3 c1 92 b5 33 af 53 75 7b 71 6e 4b 30 f0 b3 35 8a 71 07 af 02 2b c3 0d 04 ea cd 7d 80 31 fc c7 9e 7f a3 51 f8 c9 fc 67 49 55 66 21 d3 20 eb a8 ae 34 74 c6 65 b2 da 1d da f4 4b 4e 06 ff 66 3a c4 0a a6 aa 9b d6 87
g^{xy}	38 01 75 3a 94 95 ff 38 23 7f 9a 68 ca 15 42 4c fb bb 73 49 9c 7c 2f c5 c0 bd 48 bd 40 5a 9f 6f cb ea ba 40 3a 2f 29 5a 00 8b e3 9b 28 46 cb 18 46 24 b0 5e 83 51 9f 52 4a b3 bd 5d 10 83 1a 10 26 8f 88 4b d3 db 7e 72 0a 68 bc 9a 94 f8 66 d2 6f 36 ae 5b 2b d7 c7 ed 7b ae 8b fa e9 f7 d9 10 0c c0 b9 0c 42 af 13 ac ec 17 5d 31 e4 c1 f1 9b 1e fb 23 67 ff fd 33 c3 60 06 76 5e 42 52 a9 a1
$H(g^y, g^{xy}, K_{perm}, Id_B)$	c0 8b 79 09 4e 25 2a 73 89 6c cf 4e 9c 0c 4b a6 17 69 c1 31
$H(g^x, g^{xy}, K_{perm}, Id_A)$	4b 1c f7 69 37 54 1b 78 7b f3 0f 6f 7b 4b 91 6d a3 ae 7e 34

Table 39 contains the short-term and long-term secrets agreed between CPCM Instance A and B.

Table 39: AKE derived keys

Long-term key K_{perm}	14 a2 6c 92 78 2e bb 81 da b7 c2 66 60 84 74 4b 48 8e 42 ec ff f7 a7 27 d4 d3 bb c5 34 56 dc b6 2c d7 3d 8d 9d 36 2f 59 4a a6 7a 41 00 a5 d1 8b 1f 7d b4 01 7f 61 88 56 2d 49 a9 7a a7 f8 56 39 4d e5 1c f8 88 94 d7 ae 8d 86 63 42 96 a4 d8 aa 57 62 a9 96 35 1a 4e 01 56 98 b4 9d 61 16 f5 65 c5 1a 7f f3 f7 1d ec 45 bb de 7c b2 9e a3 36 e2 17 a6 63 74 b9 15 59 f9 ad 4e 7a d2 10 f7 c6 f2
Short-term key g^{xy}	38 01 75 3a 94 95 ff 38 23 7f 9a 68 ca 15 42 4c fb bb 73 49 9c 7c 2f c5 c0 bd 48 bd 40 5a 9f 6f cb ea ba 40 3a 2f 29 5a 00 8b e3 9b 28 46 cb 18 46 24 b0 5e 83 51 9f 52 4a b3 bd 5d 10 83 1a 10 26 8f 88 4b d3 db 7e 72 0a 68 bc 9a 94 f8 66 d2 6f 36 ae 5b 2b d7 c7 ed 7b ae 8b fa e9 f7 d9 10 0c c0 b9 0c 42 af 13 ac ec 17 5d 31 e4 c1 f1 9b 1e fb 23 67 ff fd 33 c3 60 06 76 5e 42 52 a9 a1
Encryption session key K_{sess_enc}	31 10 c1 01 cc cd 9a 77 88 4c 00 a8 62 5c ef 6e
Authentication session key K_{sess_auth}	e4 c2 fc 2e 45 8d ab 6a 54 e2 14 7a e0 98 ad 07

List of tables

Table 1: Notation.....	6
Table 2: Revocation List Signing and Verification data	7
Table 3: RSA keys used for PKCS1.5.....	8
Table 4: CPCM Scrambler Test Cases	9
Table 5: LSA Test Case 01.....	10
Table 6: LSA Test Case 02.....	11
Table 7: LSA Test Case 03.....	12
Table 8: LSA Test Case 04.....	13
Table 9: LSA Test Case 05.....	14
Table 10: LSA Test Case 06.....	15
Table 11: LSA Test Case 07.....	16
Table 12: LSA Test Case 08.....	17
Table 13: LSA Test Case 09.....	18
Table 14: LSA Test Case 10.....	19
Table 15: LSA Test Case 11.....	20
Table 16: LSA Test Case 12.....	21
Table 17: LSA Test Case 13.....	22
Table 18: LSA Test Case 14.....	23
Table 19: LSA Test Case 15.....	24
Table 20: LSA Test Case 16.....	25
Table 21: LSA Test Case 17.....	26
Table 22: LSA Test Case 18.....	27
Table 23: LSA Test Case 19.....	28
Table 24: LSA Test Case 20.....	29
Table 25: LSA Test Case 21.....	30
Table 26: CPCM constants used for Certificate signing and verification	31
Table 27: Parent Certificate parameters	31
Table 28: Recovered Parent Certificate.....	31
Table 29: Verifying the hash of the Parent Certificate	31
Table 30: Expanding the Parent Certificate's compressed modulus	32
Table 31: Signed Leaf Certificate.....	32
Table 32: Recovered Leaf Certificate.....	33
Table 33: Leaf Certificate parameters	33

Table 34: Signing Certificate's primes and secret key.....	34
Table 35: CPCM public constants for AKE.....	34
Table 36: AKE values for CPCM Instance A.....	35
Table 37: AKE values for CPCM Instance B.....	35
Table 38: AKE public values used in the protocol.....	36
Table 39: AKE derived keys.....	36

History

Document history		
V1.1.1	July 2008	Publication
V1.1.2	February 2011	Publication