3GPP TS 35.204 V11.0.0 (2012-09)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3G Security;
Specification of the 3GPP Confidentiality and Integrity Algorithms;
Document 4: Design Conformance Test Data
(Release 11)

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

UMTS, algorithm, KASUMI

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The 3GPP Confidentiality and Integrity Algorithms f8 & f9 have been developed through the collaborative efforts of the European Telecommunications Standards Institute (ETSI), the Association of Radio Industries and Businesses (ARIB), the Telecommunications Technology Association (TTA), the T1 Committee.

The f8 & f9 Algorithms Specifications may be used only for the development and operation of 3G Mobile Communications and services. Every Beneficiary must sign a Restricted Usage Undertaking with the Custodian and demonstrate that he fulfils the approval criteria specified in the Restricted Usage Undertaking.

Furthermore, Mitsubishi Electric Corporation holds essential patents on the Algorithms. The Beneficiary must get a separate IPR License Agreement from Mitsubishi Electronic Corporation Japan.

For details of licensing procedures, contact ETSI, ARIB, TTA or T1.

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

This specification has been prepared by the 3GPP Task Force, and gives black-box test data for the algorithm set. The test data has been selected to give a high degree of confidence that the implementation is correct. However, no claim is made that conformance with this test data guarantees a correct implementation.

This document is the last of four, which between them form the entire specification of the 3GPP Confidentiality and Integrity Algorithms:

- 3GPP TS 35.201: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: *f8* and *f9* Specification".
- 3GPP TS 35.202: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification".
- 3GPP TS 35.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 3: Implementors' Test Data".
- **3GPP TS 35.204: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 4: Design Conformance Test Data".**

This document is purely informative. The normative part of the specification of the ***f8*** (confidentiality) and the ***f9*** (integrity) algorithms is in the main body of Document 1. The normative part of the specification of **KASUMI** is found in document 2.

0 Scope

This specification gives black-box test data for the algorithm set. The test data has been selected to give a high degree of confidence that the implementation is correct. However, no claim is made that conformance with this test data guarantees a correct implementation.

1 Outline of the design conformance test data

Section 2 introduces the algorithms and describes the notation used in the subsequent sections.

Section 3 provides test data for the Confidentiality Algorithm ***f8***.

Section 4 provides test data for the Integrity Algorithm ***f9***.

1.1 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 33.102 version 3.2.0: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[2] 3GPP TS 33.105 version 3.1.0: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Cryptographic Algorithm Requirements".

[3] 3GPP TS 35.201: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: f8 and f9 Specification".

[4] 3GPP TS 35.202: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification".

[5] 3GPP TS 35.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 3: Implementors' Test Data".

[6] 3GPP TS 35.204: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 4: Design Conformance Test Data".

[7] ISO/IEC 9797-1:1999: "Information technology – Security techniques – Message Authentication Codes (MACs)".

2 Introductory information

2.1 Introduction

Within the security architecture of the 3GPP system there are two standardised algorithms; a confidentiality algorithm ***f8***, and an integrity algorithm ***f9***. These algorithms are specified in a companion document [3].

This document provides sets of input/output test data for ‘black box’ testing of physical realisations of the ***f8*** and ***f9*** algorithms.

2.2 Radix

Unless stated otherwise, all test data values presented in this document are in hexadecimal.

2.3 Bit/Byte ordering

All data variables in this specification are presented with the most significant bit (or byte) on the left hand side and the least significant bit (or byte) on the right hand side.

2.4 Presentation of input/output data

The basic data processed by the ***f8*** and ***f9*** algorithms are bit streams. In general in this document the data is presented in hexadecimal format as bytes, thus the last byte shown as part of an input or output data stream may include between 0 and 7 bits that are ignored once the **LENGTH** parameter is taken into account. (The least significant bits of the byte are ignored).

2.5 Coverage

For each of the algorithms the test data have been selected such that, provided the entire set of tests is run:

- Each key bit will have been in both the ‘1’ and the ‘0’ states.
- Each bit of the initialisation fields (COUNT, FRESH, BEARER, DIRECTION) will have been in both the ‘1’ and the ‘0’ states.
- Every entry in the internal S-boxes will have been used.

3 Confidentiality algorithm *f8*

3.1 Overview

The test data sets presented here are for the ***f8*** confidentiality algorithm.

3.2 Format

Each test set shows the various inputs to the algorithm including the plain text data stream to be encrypted/decrypted. (The length field is in decimal).

The fields are:

Key	= CK[0]…CK[127]
Count	= COUNT[0]…COUNT[31]

Bearer = BEARER[0]…BEARER[3]

Direction = DIRECTION[0]

Length = Length of data in **decimal**

Plaintext = PT[0] PT[1] ….. PT[Length-1]

This is followed by the modified input data, i.e. it is the bit-wise exclusive-or of the corresponding keystream and the input data to the algorithm.

Ciphertext = CT[0] CT[1]….CT[Length-1]

As this is a stream cipher it is purely a matter of context whether the operation is regarded as “encryption” or “decryption”. For the purposes of this document we regard the input as Plaintext and the output as Ciphertext.

The first test set is shown twice, once in binary format, once in hexadecimal format. This is to explicitly show the relationship between the binary data and the hexadecimal presentation.

The remainder of the test sets are presented in hexadecimal format only.

3.3 Test Set 1

3.3.1 Binary Representation

```
Key= 1101001111000101110101011001001000110010011111111011000 100011100
     0100000000110101110001100110100000001010111110001100011011010001

Count     = 00111001100010100101100110110100
Bearer    = 10101
Direction = 1
Length    = 253 bits
Plaintext:
1001100000011011101001101000001001001100000110111111101100011010
1011010010000101010001110010000000101001101101110001110110000000
1000110011100011001111100010110011000011110000001011010111111100
0001111100111101111010001010011011011100011001101011000111110

Ciphertext:
11001010000010100110000010110100001010011001111001 10100101010100
1101101111110111011010000110111001000110111101000100000110010000
1101110010000001101100000111010000000100010010000001001110110101
0000101010110001111111100100011001011001011110111010001100111
```

3.3.2 Hexadecimal Representation

```
Key       = D3C5D592327FB11C4035C6680AF8C6D1
Count     = 398A59B4
Bearer    = 15
Direction = 1
Length    = 253 bits
Plaintext:
981BA6824C1BFB1A B485472029B71D80 8CE33E2CC3C0B5FC 1F3DE8A6DC66B1F0

Ciphertext:
CA0A60B4299E6954 DBF7686E46F44190 DC81B074044813B5 0AB1FE46597BA338
```

3.4 Test Set 2

```
Key       = 2BD6459F82C440E0952C49104805FF48
Count     = C675A64B
Bearer    = 0C
Direction = 1
Length    = 798 bits
Plaintext:
7EC61272743BF161 4726446A6C38CED1 66F6CA76EB543004 4286346CEF130F92
922B03450D3A9975 E5BD2EA0EB55AD8E 1B199E3EC4316020 E9A1B285E7627953
59B7BDFD39BEF4B2 484583D5AFE082AE E638BF5FD5A60619 3901A08F4AB41AAB
9B134880

Cipher text:
1061793DAAACBE40 C9431E292B7FF494 96DB0D31CE24710C 01ACFF1B2C441FA9
3BB3BD65DE18027A 14CCA571A42E8B12 74AE30AC411AB6AF D88F924E65F9812D
FA80EF8E9A7EA753 391D09F480D9147C B39C23A1ACB9AC9B 2A6B4709F7E6DD84
D8FA59A4
```

3.5 Test Set 3

```
Key       = 0A8B6BD8D9B08B08D64E32D1817777FB
Count     = 544D49CD
Bearer    = 04
Direction = 0
Length    = 310 bits
Plaintext:
FD40A41D370A1F65 74509568 7D47BA1D 36D2349E23F64439 2C8EA9C49D40C132
71AFF264D0F248

Cipher text:
22B707A481F264BE 691994C2A201354D 5741A2E6B4624EE9 DF30D8D94535165B
D439223EBBD074
```

3.6 Test Set 4

```
Key       = AA1F95AEA533BCB32EB63BF52D8F831A
Count     = 72D8C671
Bearer    = 10
Direction = 1
Length    = 1022 bits
Plaintext:
FB1B96C5C8BADFB2 E8E8EDFDE78E57F2 AD81E74103FC430A 534DCC37AFCEC70E
1517BB06F27219DA E49022DDC47A068D E4C9496A951A6B09 EDBDC864C7ADBD74
0AC50C022F3082BA FD22D78197C5D508 B977BCA13F32E652 E74BA728576077CE
628C535E87DC6077 BA07D290685 90C8C B5F1088E082CFA0E C961302D69CF3D44

Ciphertext:
5C6FD2D34BE8B0F5 212600BD758881F7 6C4F11A5C3D42028 A9A029F2E0630454
829AA0A69D58D023 02E8DB3D6E9FF350 09B3595984BEB400 31271BF78727270B
9608520036125AD6 8A28213513CBA08C 7BB9EA966C0713FD 2DFFE2BADC6287CF
79B244B7236124FB 51B863684C4D89D1 940541D356809022 12081FE694DC4594
```

3.7 Test Set 5

```
Key       = 9618AE46891F86578EEBE90EF7A1202E
Count     = C675A64B
Bearer    = 0C
Direction = 1
Length    = 1245 bits
Plaintext:
8DAA17B1AE050529 C6827F28C0EF6A12 42E93F8B314FB18A 77F790AE049FEDD6
12267FECAEFC4501 74D76D9F9AA7755A 30CD90A9A5874BF4 8EAF70EEA3A62A25
0A8B6BD8D9B08B08 D64E32D1817777FB 544D49CD49720E21 9DBF8BBED33904E1
FD40A41D370A1F65 74509568 7D47BA1D 36D2349E23F64439 2C8EA9C49D40C132
71AFF264D0F24841 D6465F0996FF84E6 5FC517C53EFC3363 C38492A8

Ciphertext:
AAF8E8B349FBABB9 5C621DE6FB516744 6054AE7CFA946F99 6C26005345A1A2AF
44EEA688B759FFE3 E22D6E17BD9E7079 CC54E8D492DBFDE7 9E84043849821A24
7A67D3509BA16B49 15FDDDD638E252F4 371E471D1B39B415 8B47F14D037BBD28
37804134AD493BFC 140E437F5EBF9C29 D5D8A5816F926AA2 76E9A743A62141AD
EB653BD2963C9F54 1F5E1334B77592B1 ADED443672282801 32A747D8
```

3.8 Test Set 6

```
Key       = 54F4E2E04C83786EEC8FB5ABE8E36566
Count     = ACA4F50F
Bearer    = 0B
Direction = 0
Length    = 2837 bits
Plaintext:
40981BA6824C1BFB 4286B299783DAF44 2C099F7AB0F58D5C 8E46B104F08F01B4
1AB485472029B71D 36BD1A3D90DC3A41 B46D51672AC4C966 3A2BE063DA4BC8D2
808CE33E2CCCBFC6 34E1B259060876A0 FBB5A437EBCC8D31 C19E44543187 45E3
FA16BB11ADAE2488 79FE52DB2543E53C F445D3D828CE0BF5 C560593D97278A59
762DD0C2C9CD68D4 496A792508614014 B13B6AA51128C18C D6A90B87978C2FF1
CABE7D9F898A411B FDB84F68F6727B14 99CDD30DF0443AB4 A66653330BCBA110
5E4CEC034C73E605 B4310EAAADCFD5B0 CA27FFD89D144DF4 79275942 7C9CC1F8
CD8C87202364B8A6 87954CB05A8D4E2D 99E73DB160DEB180 AD0841E96741A5D5
9FE4189F15420026 FE4CD12104932FB3 8F735340438AAF7E CA6FD5CFD3A195CE
5ABE65272AF607AD A1BE65A6B4C9C069 3234092C4D018F17 56C6DB9DC8A6D80B
888138616B681262 F954D0E771174878 0D92291D86299972 DB741CFA4F37B8B5
B09550

Ciphertext:
BFB39672186E62B7 7FB39F9278A8AEA6 0468E05A2BB57E8B 6D6AA1B05AE83147
679207F035194553 DDF973E830C3E249 4EF6C9449FDC0735 1F8B453EEE70001D
8566B0F646394892 D443F394DA13DAC2 05D84B262819 1A0C 574E974507A9A9F3
408FCA9EC4A38869 1C513CFED22357B2 F7742FB8D5CE550E 03CAA9CFFFF54100
19590CA8D25F9AFD 5BB00FB081EAD4BD A0FAC5DC78F79771 8B6AE21BF9D0C443
B1B7F1945AEA83FA C3B2208281B30883 E590196D6499B431 7EA97E080830C204
6AFA95A3E9DB5C47 3CD054D2E0A7F080 CB5967C709DE78EC 8435CAE9B3617655
69576AA958CE5909 3ACB8A5F72096A7F E671C3717B1B514A 0AE7D7792E44F17C
48E7BAE30D5BB21D CABD217CB55B899F A7D8EA0557F672E4 36BE18350D58C65F
B6D7530E3B85FA63 1C65C3402A87D98F 3B6FB971FCCB1AF1 A6592DF2CCFE6893
A41F43ABEFD48D70 CCC9C21DDF02792B 8EE8A77988CDC317 1046C515401ABB13
2261B0
```

4 Integrity algorithm *f9*

4.1 Overview

The test data sets presented here are for the ***f9*** integrity algorithm.

Each test set shows the various inputs to the algorithm including the plain text data stream to be ‘MAC’d. The length field is in decimal.

The fields are:

Key = IK[0]…IK[127]

Count = COUNT-I[0]…COUNT-I[31]

Fresh = FRESH[0]…FRESH[31]

Direction = DIRECTION[0]

Length = Length of data in **decimal**

Message = MESSAGE[0]…MESSAGE[Length-1]

This is followed by the calculated value for MAC-I.

Output = MAC-I[0]…MAC-I[31]

The first test set is shown twice, once in binary format, once in hexadecimal format. This is to explicitly show the relationship between the binary data and the hexadecimal presentation.

The remainder of the test sets are presented in hexadecimal format only.

4.2 Test Set 1

4.2.1 Binary Representation

```
Key= 0010101111010110010001011001111110000010110001011011001100000000
     1001010100101100010010010001000001001000100000011111111101001000

Count     = 00111000101001101111000001010110
Fresh     = 10111000101011101111110110101001
Direction = 0
Length    = 88 bits
Message:
0011001100110010001101000110001001100011001110010011100001100001
001101110011010001111001

Output: 01000110111000000000110101001011
```

4.2.2 Hexadecimal Representation

```
Key       = 2BD6459F82C5B300952C49104881FF48
Count     = 38A6F056
Fresh     = B8AEFDA9
Direction = 0
Length    = 88 bits
Message:
3332346263393861 373479

Output: 46E00D4B
```

4.3 Test Set 2

```
Key       = 7E5E94431E11D73828D739CC6CED4573
Count     = 36AF6144
Fresh     = 9838F03A
Direction = 1
Length    = 254 bits
Message:
B3D3C9170A4E1632 F60F861013D22D84 B726B6A278D802D1 EEAF1321BA5929DC

Output: 2BEEF3AC
```

4.4 Test Set 3

```
Key       = D3419BE821087ACD02123A9248033359
Count     = C7590EA9
Fresh     = 57D5DF7D
Direction = 0
Length    = 511 bits
Message:
BBB057038809496B CFF86D6FBC8CE5B1 35A06B166054F2D5 65BE8ACE75DC851E
0BCDD8F07141C495 872FB5D8C0C66A8B 6DA556663E4E4612 05D84580BEE5BC7E

Output: 02158170
```

4.5 Test Set 4

```
Key       = 83FD23A244A74CF358DA3019F1722635
Count     = 36AF6144
Fresh     = 4F302AD2
Direction = 1
Length    = 768 bits
Message:
35C68716633C66FB 750C266865D53C11 EA05B1E9FA49C839 8D48E1EFA5909D39
47902837F5AE96D5 A05BC8D61CA8DBEF 1B13A4B4ABFE4FB1 006045B674BB5472
9304C382BE53A5AF 05556176F6EAA2EF 1D05E4B083181EE6 74CDA5A485F74D7A

Output: 95AE41BA
```

4.6 Test Set 5

```
Key       = 6832A65CFF4473621EBDD4BA26A921FE
Count     = 36AF6144
Fresh     = 9838F03A
Direction = 0
Length    = 383 bits
Message:
D3C5383962682071 7765667620323837 636240981BA6824C 1BFB1AB485472029
B71D808CE33E2CC3 C0B5FC1F3DE8A6DC

Output: 8B2D570F
```

4.7 Test Set 6

```
Key       = 5D0A80D8134AE19677824B671E838AF4
Count     = 7827FAB2
Fresh     = A56C6CA2
Direction = 1
Length    = 2558 bits
Message:
70DEDF2DC42C5CBD 3A96F8A0B11418B3 608D573360 4A2CD3 6AABC70CE3193BB5
153BE2D3C06DFDB2 D16E9C357158BE6A 41D6B861E491DB3F BFEB518EFCF048D7
D58953730FF30C9E C470FFCD663DC342 01C36ADDC0111C35 B38AFEE7CFDB582E
3731F8B4BAA8D1A8 9C06E81199A97162 27BE344EFCB436DD D0F096C064C3B5E2
C399993FC77394F9 E09720A811850EF2 3B2EE05D9E617360 9D86E1C0C18EA51A
012A00BB413B9CB8 188A703CD6BAE31C C67B34B1B00019E6 A2B2A690F02671FE
7C9EF8DEC0094E53 3763478D58D2C5F5 B827A0148C5948A9 6931ACF84F465A64
E62CE74007E991E3 7EA823FA0FB21923 B79905B733B631E6 C7D6860A3831AC35
1A9C730C52FF72D9 D308EEDBAB21FDE1 43A0EA17E23EDC1F 74CBB3638A2033AA
A15464EAA733385D BBEB6FD73509B857 E6A419DCA1D8907A F977FBAC4DFA35EC

Output: 3AE4BFF3
```

Annex A (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
12-1999	-	-	-	-	ETSI SAGE Publication (restricted)	-	SAGE v1.0
09-2000	SA_07				Approved by TSG SA and placed under change control	SAGE v1.0	3.1.0
07-2001	-	-	-	-	Word version received: Re-formatted into 3GPP TS format (MCC) No technical change from version 3.1.0.	3.1.0	3.1.1
08-2001	-				Addition of Mitsubishi IPR information in Foreword and correction of reference titles. No technical change from version 3.1.0.	3.1.1	3.1.2
08-2001	-	-	-	-	Release 4 version created.	3.1.2	4.0.0
06-2002	-	-	-	-	Release 5 version created.	4.0.0	5.0.0
12-2004	-	-	-	-	Release 6 version created.	5.0.0	6.0.0
06-2007	-	-	-	-	Release 7 version created.	6.0.0	7.0.0
12-2008	-	-	-	-	Release 8 version created	7.0.0	8.0.0
2009-12	-	-	-	-	Release 9 version created.	8.0.0	9.0.0
2011-03	-	-	-	-	Update to Rel-10 version (MCC)	9.0.0	10.0.0
2012-09	-	-	-	-	Update to Rel-11 version (MCC)	10.0.0	**11.0.0**