3GPP TS 55.218 V6.1.0 (2002-12)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the A5/3 Encryption Algorithms for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 3: Design conformance test data (Release 6)

Keywords
GSM, GPRS, security, algorithm, testing

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 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.

0 Scope

This specification has been prepared by the 3GPP Task Force, and gives a detailed specification of the **A5/3** encryption algorithms for GSM and ECSD, and of the **GEA3** encryption algorithm for GPRS.

This document is the third of three, which between them form the entire specification of the **A5/3** and **GEA3** algorithms:

- Specification of the A5/3 Encryption Algorithms for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 1: A5/3 and GEA3 Specifications.
- Specification of the A5/3 Encryption Algorithms for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 2: Implementors' Test Data.
- **Specification of the A5/3 Encryption Algorithms for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 3: Design Conformance Test Data.**

The normative part of the specification of the **A5/3** and **GEA3** algorithms is in the main body of Document 1. The annexes to this document are purely informative. Documents 2 and 3 (this document) are also purely informative.

The normative part of the specification of the block cipher **(KASUMI)** on which the **A5/3** and **GEA3** algorithms are based can be found in TS 35.202 [5].

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 encryption algorithm A5/3 for GSM.

Section 4 provides test data for the encryption algorithm A5/3 for ECSD.

Section 5 provides test data for the encryption algorithm GEA3 for GPRS.

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] TS 55.216: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the A5/3 Encryption Algorithms for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 1: A5/3 and GEA3 Specifications".

[2] TS 55.217: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the A5/3 Encryption Algorithms for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 2: Implementors' Test Data".

[3] TS 55.218: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the A5/3 Encryption Algorithms for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 3: Design Conformance Test Data".

[4] 3GPP TS 35.201 version 4.1.0: "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".

[5] 3GPP TS 35.202 version 4.0.0: "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".

[6] 3GPP TS 35.203 version 4.0.0: "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".

2 Introductory information

2.1 Introduction

In this document black box test data are given for three ciphering algorithms: **A5/3** for GSM, **A5/3** for ECSD, and **GEA3** for GPRS (including EGPRS). The algorithms are stream ciphers that are used to encrypt/decrypt blocks of data under a confidentiality key $\mathbf{K_C}$. Each of these algorithms is based on the **KASUMI** algorithm that is specified in reference TS 35.202 [5]. **KASUMI** is a block cipher that produces a 64-bit output from a 64-bit input under the control of a 128-bit key. The algorithms defined in TS 55.216 [1] use **KASUMI** in a form of output-feedback mode as a keystream generator. No test data will be given for **KASUMI**, as these can be found in TS 35.203 [6].

2.2 Notation

2.2.1 Radix

We use the prefix **0x** to indicate **hexadecimal** numbers.

2.2.2 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. Where a variable is broken down into a number of sub-strings, the left most (most significant) sub-string is numbered 0, the next most significant is numbered 1 and so on through to the least significant.

For example an n-bit **STRING** is subdivided into 64-bit substrings $\mathbf{SB_0,SB_1…SB_i}$ so if we have a string:

0x0123456789ABCDEFFEDCBA98765432l086545381AB594FC28786404C50A37…

we have:

$\mathbf{SB_0}$ = 0x0123456789ABCDEF
$\mathbf{SB_1}$ = 0xFEDCBA9876543210
$\mathbf{SB_2}$ = 0x86545381AB594FC2
$\mathbf{SB_3}$ = 0x8786404C50A37…

In binary this would be:

000000010010001101000101011001111000100110101011110011011110111111111110…

with $\mathbf{SB_0}$ = 00000001001000110100010101100111100010011010101111001101111011111
$\mathbf{SB_1}$ = 11111110110111001011101010011000011101100101010000110010000100000
$\mathbf{SB_2}$ = 10000110010101000101001110000001101010110101100101001111111000010
$\mathbf{SB_3}$ = 10000111100001100100000001001100010100001010001101110…

2.2.3 Presentation of input/output data

The basic data processed by the algorithm A5/3 are blocks of two times 114 bits (GSM) resp. 348 bits (ECSD). 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 block may include 0 to 6 bits that are ignored once the block size has been reached (the least significant bits of the byte are ignored).

2.3 List of Variables

BLOCK1	a string of keystream bits output by the **A5/3** algorithm — 114 bits for GSM, 348 bits for ECSD.
BLOCK2	a string of keystream bits output by the **A5/3** algorithm — 114 bits for GSM, 348 bits for ECSD.
COUNT	a 22-bit frame dependent input to both the GSM and ECSD **A5/3** algorithms.
DIRECTION	a 1-bit input to the **GEA3** algorithm, indicating the direction of transmission (uplink or downlink).
INPUT	a 32-bit frame dependent input to the **GEA3** algorithm.
K_C	the cipher key that is an input to each of the three cipher algorithms defined here. Although at the time of writing the standards specify that K_C is 64 bits long, the algorithm specifications here allow it to be of any length between 64 and 128 inclusive, to allow for possible future enhancements to the standards.
KLEN	the length of K_C in bits, between 64 and 128 inclusive (see above).
M	an input to the **GEA3** algorithm, specifying the number of octets of output to produce.
OUTPUT	the stream of output octets from the **GEA3** algorithm.

2.4 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, DIRECTION) will have been in both the '1' and the '0' states.
- Every entry in the internal S-boxes of **KASUMI** will have been used.

The **KASUMI** coverage is already being reached with the 64 bit test sets of each algorithm.

3 Algorithm A5/3 for GSM

3.1 Overview

The test data sets presented here are for the algorithm A5/3 for GSM. For GSM, the DIRECTION bit is not applicable and is set to zero.

3.2 Format

Each test starts by showing the various inputs (K_C, COUNT) to the function. Thereafter both keystream blocks are shown. The first test set will also list all values in their binary representations.

3.3 Test Set 1

3.3.1 Binary Representation

KLEN	64
Kc	0010101111010110010110011111100000101100010110111110000000000
COUNT	100100111100100000111

BLOCK1:
1000100010011111011101010101011111001111011010001101110100001101010111011111011000010000110110001000110010110001

BLOCK2:
0101110010100011010000000110101010100010010001001100111101101001110011111000001000111101010101101101000101101111101

3.4 Test Set 2

KLEN	64
Kc	0x952C49104881FF48
COUNT	0x061527

BLOCK1: 0xAB7DB38A573A325DAA76E4CB800A40

BLOCK2: 0x4C4B594FEA9D00FE8978B7B7BC1080

3.5 Test Set 3

KLEN	64
Kc	0xEFA8B2229E720C2A
COUNT	0x33FD3F

BLOCK1: 0x0E4015755A336469C3DD8680E30340

BLOCK2: 0x6F10669E2B4E18B042431A28E47F80

3.6 Test Set 4

KLEN	64
Kc	0x3451F23A43BD2C87
COUNT	0x0E418C

BLOCK1: 0x75F7C4C51560905DFBA05E46FB54C0

BLOCK2: 0x192C95353CDF979E054186DF15BF00

3.7 Test Set 5

KLEN	64
Kc	0xCAA2639BE82435CF
COUNT	0x2FF229

BLOCK1: 0x301437E4D4D6565D4904C631606EC0

BLOCK2: 0xF0A3B8795E264D3E1A82F684353DC0

3.8 Test Set 6

KLEN	64
Kc	0x7AE67E87400B9FA6
COUNT	0x2F24E5

BLOCK1: 0xF794290FEF643D2EA348A7796A2100

BLOCK2: 0xCB6FA6C6B8A705AF9FEFE975818500

3.9 Test Set 7

KLEN	64
Kc	0x58AF69935540698B
COUNT	0x05446B

BLOCK1: 0x749CA4E6B691E5A598C461D5FE4740

BLOCK2: 0x31C9E444CD04677ADAA8A082ADBC40

3.10 Test Set 8

KLEN	64
Kc	0x017F81E5F236FE62
COUNT	0x156B26

BLOCK1: 0x2A6976761E60CC4E8F9F52160276C0

BLOCK2: 0xA544D8475F2C78C35614128F1179C0

3.11 Test Set 9

KLEN	64
Kc	0x1ACA8B448B767B39
COUNT	0x0BC3B5

BLOCK1: 0xA4F70DC5A2C9707F5FA1C60EB10640

BLOCK2: 0x7780B597B328C1400B5C74823E8500

3.12 Test Set 10

KLEN	80
Kc	0x5ACB1D644C0D512041A5
COUNT	0x1D5157

BLOCK1: 0x8EFAEC49C355CCD995C2BF649FD480

BLOCK2: 0xF3A2910CAEDF587E976171AAF33B80

3.13 Test Set 11

KLEN	80
Kc	0x9315819243A043BEBE6E
COUNT	0x2E196F

BLOCK1: 0xAA08DB46DD3DED78A612085C529D00

BLOCK2: 0x0250463DA0E3886F9BC2E3BB0D73C0

3.14 Test Set 12

KLEN	128
Kc	0x3D43C388C9581E337FF1F97EB5C1F85E
COUNT	0x35D2CF

BLOCK1: 0xA2FE3034B6B22CC4E33C7090BEC340

BLOCK2: 0x170D7497432FF897B91BE8AECBA880

3.15 Test Set 13

KLEN	128
Kc	0xA4496A64DF4F399F3B4506814A3E07A1
COUNT	0x212777

BLOCK1: 0x89CDEE360DF9110281BCF57755A040

BLOCK2: 0x33822C0C779598C9CBFC49183AF7C0

4 Algorithm A5/3 for ECSD

4.1 Overview

The test data sets presented here are for the algorithm A5/3 for ECSD.

For ECSD, the DIRECTION bit is not applicable and is set to zero. ECSD allows block sizes up to 348 bits for BLOCK1 and BLOCK2. As A5/3 for ECSD always produces two times 348 bits, the superfluous bits of each output block have to be discarded.

4.2 Format

Each test starts by showing the various inputs (K_C, COUNT) to the function. Thereafter both keystream blocks are shown. The first test set will also list all values in their binary representations.

4.3 Test Set 1

4.3.1 Binary Representation

KLEN	64
Kc	0010101111010110010110011111100000101100010110111100000000000
COUNT	100100111100100000111 1

BLOCK1:
1111011101011110011001100011101011001110101000100001111011001001110100001011110111101001100010110110
1100001100111011100000011001001010011001111010000011000010100001101000101110001011111001000101000011
0010011010111110111101010001010100001000100110110110110110110000111100100111000110101111101110010110
000010011111100100000101001000000010110011011100

BLOCK2:
1111010100010100001001101101000101110010110110110100011110111111111011010011111001101101100000111101
0001010011110100100001110110001101100110110011001100110101011011111110101110100001011011001001111100
1001101101001001111100101111011101110111010110110000101101010000010010010000010111110010011110110101
101011100110001010111000001001101001111010101001

4.3.2 Hexadecimal Representation

KLEN	64
Kc	0x2BD6459F82C5BC00
COUNT	0x24F20F

BLOCK1: 0xF75E663ACEA21EC9D0BDE98B6C33B819299E830A1A2E2F914326BEF515089B6DB0F271AFB9609F905202CDC0

BLOCK2: 0xF51426D172DB47BFED3E6D83D14F4876366CCCD5BFAE85B27C9B49F2F7775B0B504905F27B5AE62B8269EA90

4.4 Test Set 2

KLEN	64
Kc	0x952C49104881FF48
COUNT	0x061271

BLOCK1: 0x7A48E94F5949D6145C6A8918C9136ABEF03D44EF8815F01981999A06E1D24A324EE2553879B85F88CF8A5A70

BLOCK2: 0x056D9F4C43D82878A6EA70C6007DF5BC27FF134A06889E5164AFCEE6ED99D2DEF25BC0DDB25B7C77E9210910

4.5 Test Set 3

KLEN	64
Kc	0xEFA8B2229E720C2A
COUNT	0x33FD3F

BLOCK1: 0x09B49CE620E4A36B7956186C8F248B6150DC2362B3F41F6F28F486D9A80BB879DA4FE349E72EF9755A501590

BLOCK2: 0x02B17EE1DF32D9302567E470EA3A26B0FFCDE60DFB8A28C10609AEC74CA1EEDF3BAA3334C28E7E4DDA38A4A0

4.6 Test Set 4

KLEN	64
Kc	0x3451F23A43BD2C87
COUNT	0x0041BC

BLOCK1: 0x1257046374CDC415B8B920FBBA0B5AC14165A157704F0C0ADB14F457708BF71B2B19291C796395AECE0512C0

BLOCK2: 0xFBE2DE7861EBDD918FB450E4AA66C4405B8A90C80A1F94F07316A60EC4299E1DB5CBEE1A900344914F194EF0

4.7 Test Set 5

KLEN	64
Kc	0xCAA2639BE82435CF
COUNT	0x1FF209

BLOCK1: 0x1640244FFF0A22021A3B8B7604661B518ADEACE830191F024D16E18081687799129E37466C67B4805E71D4E0

BLOCK2: 0xE62268E32C9A61FF2386849D6330A09D4A8AB99D9D905D0E4191B8D6DFAD3E924FBB026B214D5AC5E3D9CCC0

4.8 Test Set 6

KLEN	80
Kc	0x5ACB1D644C0D512041A5
COUNT	0x156B26

BLOCK1: 0xAE630E6400A71DD02B24789C13157DE0B89525B040EF772341E3F5B5E3533C488998C5904A47C399874CC120

BLOCK2: 0x1995B34B89FB53BF9278FED919EE8CCE20AE54E2EF295D92DD74D871D34482A40ECE60ECB9ED15CCD9337C90

4.9 Test Set 7

KLEN	80
Kc	0x9315819243A043BEBE6E
COUNT	0x2E196F

BLOCK1: 0xB4AF6C69B33BD7A3921BDE4C7780FADDE7B169D82D63DC969577588C37BAC61E5C07C10B18F4E466E244AB70

BLOCK2: 0x376F8B04E7F675844CD704F207D5D60ACD2050D4D4A94E37C3E911758735419894BF2213F910D8F3DCCBE970

4.10 Test Set 8

KLEN	128
Kc	0x3D43C388C9581E337FF1F97EB5C1F85E
COUNT	0x35D2CF

BLOCK1: 0x566A5690468114D018FC796FAA1C58EA96BC49BA3CCC426E19F3E800D508BBC65608B97CD5F1AA7DCE0510B0

BLOCK2: 0x1418CD8B91E369BD363ECF2C70644AD0819E33DACF33925AAE31A6BDCEA26391F918DFDEB60ECDF66AC603D0

4.11 Test Set 9

KLEN	128
Kc	0xA4496A64DF4F399F3B4506814A3E07A1
COUNT	0x212777

BLOCK1: 0x9440D02F6267722222FF55767A15679A446A9F1BB84EE1B25792BC6E2EFC0A3D7A423C506808021AB401E020

BLOCK2: 0x8266AA6D07CE062AB6DB85F53B9244052093BDAD7A9D06DBEF9C1FB73959CFC5BFE4F25062429873E7DB5000

5 Algorithm GEA3 for GPRS

5.1 Overview

The test data sets presented here are for the algorithm GEA3 for GPRS.

5.2 Format

Each test starts by showing the various inputs (K_C, COUNT, DIRECTION, M) to the function. Thereafter both keystream blocks are shown. The first test set will also list all values in their binary representations.

5.3 Test Set 1

5.3.1 Binary Representation

KLEN	64
Kc	0010101111010110010110011111100000101100010110111110000000000
INPUT	10001110100101000010000110100011
DIRECTION	0
M	59

OUTPUT:

```
01011111001101011001011100001001110111110100101010000110100000001000001011011000101111011011011001001
00000001100101000010100000001111100010000000101101001000110111001100110111000010101011111111011101101
01000001010111011011111011110100001101010100111011101011101100100001110100000111001111001100101110111
11111011001011010111000001101011110101111010111111111101001101110001111111001001011011100011100101111
00001101000101000011110111001011001001100010010000000101010010000010011 0
```

5.3.2 Hexadecimal Representation

KLEN	64
Kc	0x2BD6459F82C5BC00
INPUT	0x8E9421A3
DIRECTION	0
M	59

OUTPUT:

```
0x5F359709DE950D0105B17B6C90194280F880B48DCCDC2AFEED415DBEF4354EEBB21D073CCBBFB2D706BD7AFFD371FC96E3
970D143DCB2624054826
```

5.4 Test Set 2

KLEN	64
Kc	0x952C49104881FF48
INPUT	0x5064DB71
DIRECTION	0
M	59

OUTPUT:

```
0xFDC03D738C8E14FF0320E59AAF75760799E9DA78DD8F888471C4AEAAC1849633A26CD84F459D265B83D7D9B9A0B1E54F4D
75E331640DF19E0DB0E0
```

5.5 Test Set 3

KLEN	64
Kc	0xEFA8B2229E720C2A
INPUT	0x4BDBD5E5
DIRECTION	1
M	59

OUTPUT:

0x4718A2ADFC90590949DDADAB406EC3B925F1AF1214673909DAAB96BB4C18B1374BB1E99445A81CC856E47C6E49E9DBB987
3D0831B2175CA1E109BA

5.6 Test Set 4

KLEN	64
Kc	0x3451F23A43BD2C87
INPUT	0x893FE14F
DIRECTION	0
M	59

OUTPUT:

0xB46B1E284E3F8B63B86D9DF0915CFCEDDF2F061895BF9F82BF2593AE4847E94A4626C393CF8941CE15EA7812690D8415B8
8C5730FE1F5D410E16A2

5.7 Test Set 5

KLEN	64
Kc	0xCAA2639BE82435CF
INPUT	0x8FE17885
DIRECTION	1
M	59

OUTPUT:

0x9FEFAF155A26CF35603E727CDAA87BA067FD84FF98A50B7FF0EC8E95A0FB70E79CB93DEE2B7E9AB59D050E1262401571F3
49C68229DDF0DECC4E85

5.8 Test Set 6

KLEN	64
Kc	0x1ACA8B448B767B39
INPUT	0x4F7BC3B5
DIRECTION	0
M	59

OUTPUT:

0x514F6C3A3B5A55CA190092F7BB6E80EF3EDB738FCDCE2FF90BB387DDE75BBC32A04A67B898A3DFB8198FFFC37D437CF69E
7F9C13B51A868720E750

5.7 Test Set 7

KLEN	80
Kc	0x5ACB1D644C0D512041A5
INPUT	0xF0A7F9D0
DIRECTION	1
M	59

OUTPUT:

0x1CC337BCFA4E339713BD8B4C42C2E7571BE86B6B7C56EDB662199B1705BACB692D377DB61812B31B58A923F7F13AEFD21A
AFBB28739979124A3EE5

5.10 Test Set 8

KLEN	80
Kc	0x9315819243A043BEBE6E
INPUT	0x0B5B6901
DIRECTION	0
M	59

OUTPUT:

0x23D335BE02460D89AB609C32E2DF8CB04F336FB358FB74778AC0331EBE00FFAE8D218EEE5CD181B3BC1580B6D0D7FD6DAC
2DFF34654AD9545EB293

5.11 Test Set 9

KLEN	128
Kc	0x3D43C388C9581E337FF1F97EB5C1F85E
INPUT	0x48571AB9
DIRECTION	0
M	59

OUTPUT:

0xFC7314EF00A63ED0116F236C5D25C54EEC56A5B71F9F18B4D7941F84E422ACBDE5EEA9A204679002D14F312F3DEE2A1AC9
17C3FBDC3696143C0F5D

5.12 Test Set 10

KLEN	128
Kc	0xA4496A64DF4F399F3B4506814A3E07A1
INPUT	0xEB04ADE2
DIRECTION	1
M	59

OUTPUT:

0x2AEB5970FB06B718027D048488AAF24FB3B74EA4A6B1242FF85B108FF816A303C72757D9AAD862B835D1D287DBC141D0A2
8D79D87BB137CD1198CD

Annex A:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2002-05	-	-	-	-	ETSI SAGE first publication		SAGE V1.0
2002-07	-	-	-	-	Agreed at SA WG3 #24 for presentation to TSG SA #17 for approval. Converted into 3GPP TS format (TS 55.218) (Technically equivalent to SAGE V1.0)	SAGE V1.0	1.0.0
2002-09	SP-17	SP-020506	-	-	Approved for Release 6 - version 6.0.0	1.0.0	6.0.0
2002-12	SP-18	SP-020721	001	-	EGPRS algoritm	6.0.0	6.1.0