3GPP TS 55.217 V1.0.0 (2002-07)

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 EDGE, and the GEA3 Encryption Algorithm for GPRS; Document 2: Implementors' Test Data (Release 6)

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

Keywords
3GPP, GPRS, security, algorithm

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 4

0 Scope 5

1 Outline of the implementors' test data 5
1.1 References 5

2 Introductory information 6
2.1 Introduction 6
2.2 Notation 6
2.2.1 Radix 6
2.2.2 Conventions 6
2.2.3 Bit/Byte ordering 6
2.2.4 Presentation of input/output data 7
2.3 List of Variables 7

3 Algorithm A5/3 for GSM 8
3.1 Overview 8
3.2 Format 8
3.3 Test Set 1 8
3.4 Test Set 2 9
3.5 Test Set 3 9
3.6 Test Set 4 10
3.7 Test Set 5 10

4 Algorithm A5/3 for EDGE 11
4.1 Overview 11
4.2 Format 11
4.3 Test Set 1 11
4.4 Test Set 2 12
4.5 Test Set 3 13
4.6 Test Set 4 14
4.7 Test Set 5 15

5 Algorithm GEA3 for GPRS 15
5.1 Overview 15
5.2 Format 15
5.3 Test Set 1 16
5.4 Test Set 2 17
5.5 Test Set 3 18
5.6 Test Set 4 19
5.7 Test Set 5 20

Annex A: Change history 21

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 EDGE, and of the **GEA3** encryption algorithm for GPRS.

This document is the second 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 EDGE, and the GEA3 Encryption Algorithm for GPRS; Document 1: A5/3 and GEA3 Specifications.
- **Specification of the A5/3 Encryption Algorithms for GSM and EDGE, and the GEA3 Encryption Algorithm for GPRS; Document 2: Implementors' Test Data.**
- Specification of the A5/3 Encryption Algorithms for GSM and EDGE, 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 (this document) and 3 above 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 implementors' test data

Section 2 introduces the algorithm 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 EDGE.

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 EDGE, 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 EDGE, 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 EDGE, 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 the implementors'test data are given for three ciphering algorithms: **A5/3** for GSM, **A5/3** for EDGE, and **GEA3** for GPRS. 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.

The three algorithms are all very similar. In Document 1 (TS 55.216 [1]) they are specified in terms of a core function **KGCORE** (section 3); The implementors'test data will reflect this as it will show the input/output data of **KGCORE** as well as important steps in the calculation inside **KGCORE**.

2.2 Notation

2.2.1 Radix

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

2.2.2 Conventions

We use the assignment operator '=', as used in several programming languages. When we write

<*variable*> = <*expression*>

we mean that <*variable*> assumes the value that <*expression*> had before the assignment took place. For instance,

x = x + y + 3

means

(new value of *x*) becomes (old value of *x*) + (old value of *y*) + 3.

2.2.3 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. 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:

0x0123456789ABCDEFFEDCBA98765432108654538 1AB594FC28786404C50A37…

we have:

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

In binary this would be:

00000000100100011010001010110011110001001101010111100110111101111111111110…

with $\mathbf{SB_0}$ = 00000000100100011010001010110011110001001101010111100110111101111
$\mathbf{SB_1}$ = 11111110110111001011101010011000011101100101010000110010000010000
$\mathbf{SB_2}$ = 10000110010101000101001110000001101010110101100101001111111000010
$\mathbf{SB_3}$ = 10000111100001100100000001001100010100001010001101 10111…

2.2.4 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 (EDGE). 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

A	a 64-bit register that is used within the **KGCORE** function to hold an intermediate value.
BLKCNT	a 64-bit counter used in the **KGCORE** function.
BLOCK1	a string of keystream bits output by the **A5/3** algorithm — 114 bits for GSM, 348 bits for EDGE.
BLOCK2	a string of keystream bits output by the **A5/3** algorithm — 114 bits for GSM, 348 bits for EDGE.
CA	an 8-bit input to the **KGCORE** function.
CB	a 5-bit input to the **KGCORE** function.
CC	a 32-bit input to the **KGCORE** function.
CD	a 1-bit input to the **KGCORE** function.
CE	a 16-bit input to the **KGCORE** function reserved for future use. This input will not be shown in this document.
CK	a 128-bit input to the **KGCORE** function.
CL	an integer input to the **KGCORE** function, in the range $1…2^{19}$ inclusive, specifying the number of output bits for **KGCORE** to produce.
COUNT	a 22-bit frame dependent input to both the GSM and EDGE **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.

3 Algorithm A5/3 for GSM

3.1 Overview

The test data sets presented here are for the algorithm A5/3 for GSM. No detailed data of internal states of Kasumi are presented here as these are covered in section 3 of document TS 35.203 [6].

For GSM, the DIRECTION bit is not applicable and is set to zero. The COUNT variable is 22 bits in length.

3.2 Format

Each test set starts by showing the various inputs to the function and their mapping to KGCORE inputs. Thereafter the input/output values of the initial KASUMI operation are shown. Finally the feedback and the resulting keystream block is shown in a table.

The first test set will also give the results in binary format to explicitly show the relationship between the hexadecimal and binary format.

3.3 Test Set 1

Input A5/3		
KLEN	64 Bits	
Kc	0x2BD6459F82C5BC00	
COUNT	0x24F20F	
Input KGC		
Key	0x2BD6459F82C5BC002BD6459F82C5BC00	
CA	0x0F	
CB	0	
CC	0x0024F20F	
CD	0	
CL	228	
Init		
Initial A	0x0024F20F000F0000	
Key used	0x7E8310CAD790E9557E8310CAD790E955	
Modified A	0x91B5F53F0EFCA154	
Key now	0x2BD6459F82C5BC002BD6459F82C5BC00	
Feedback		
BLKCNT	KASUMI Input	Keystream
0	0x91B5F53F0EFCA154	0x889EEAAF9ED1BA1A
1	0x192B1F90902D1B4F	0xBBD8436232E45728
2	0x2A6DB65D3C18F67E	0xD01AA89133DA73C1
3	0x41AF5DAE3D26D296	0x1EAB68B7D89BC841

BLOCK1: 0x889EEAAF9ED1BA1ABBD8436232E440
10001000100111101110101010101111100111101101000110111010000110101011101111011000010000110110001000110010101110010001

BLOCK2: 0x5CA3406AA244CF69CF047AADA2DF40
01011100101000110100000001101010101000100100010011001111011010011100111100000100011110101010110110100010101101000

3.4 Test Set 2

Input A5/3		
KLEN	64 Bits	
Kc	0x952C49104881FF48	
COUNT	0x061272	
Input KGC		
Key	0x952C49104881FF48952C49104881FF48	
CA	0x0F	
CB	0	
CC	0x00061272	
CD	0	
CL	228	
Init		
Initial A	0x00061272000F0000	
Key used	0xC0791C451DD4AA1DC0791C451DD4AA1D	
Modified A	0x3E6A82C79F192DC7	
Key now	0x952C49104881FF48952C49104881FF48	
Feedback		
BLKCNT	KASUMI Input	Keystream
0	0x3E6A82C79F192DC7	0xFB4D5FBCEE13A333
1	0xC527DD7B710A8EF5	0x89285686E9A5C942
2	0xB742D44176BCE487	0x40DE38150115F15F
3	0x7EB4BAD29E0CDC9B	0x8D9D98B91A94B296

BLOCK1: 0xFB4D5FBCEE13A33389285686E9A5C0

BLOCK2: 0x25090378E0540457C57E367662E440

3.5 Test Set 3

Input A5/3		
KLEN	64 Bits	
Kc	0xEFA8B2229E720C2A	
COUNT	0x33FD3F	
Input KGC		
Key	0xEFA8B2229E720C2AEFA8B2229E720C2A	
CA	0x0F	
CB	0	
CC	0x0033FD3F	
CD	0	
CL	228	
Init		
Initial A	0x0033FD3F000F0000	
Key used	0xBAFDE777CB27597FBAFDE777CB27597F	
Modified A	0x46C50F2C98B65D25	
Key now	0xEFA8B2229E720C2AEFA8B2229E720C2A	
Feedback		
BLKCNT	KASUMI Input	Keystream
0	0x46C50F2C98B65D25	0x0E4015755A336469
1	0x48851A59C285394D	0xC3DD8680E3035BC4
2	0x851889AC7BB506E3	0x19A78AD3862C1090
3	0x5F6285FF1E9A4DB6	0xC68A391FE8A6ADEB

BLOCK1: 0x0E4015755A336469C3DD8680E30340

BLOCK2: 0x6F10669E2B4E18B042431A28E47F80

3.6 Test Set 4

Input A5/3		
KLEN	80 Bits	
Kc	0x5ACB1D644C0D51204EA5	
COUNT	0x156B26	
Input KGC		
Key	0x5ACB1D644C0D51204EA55ACB1D644C0D	
CA	0x0F	
CB	0	
CC	0x00156B26	
CD	0	
CL	228	
Init		
Initial A	0x00156B26000F0000	
Key used	0x0F9E4831195804751BF00F9E48311958	
Modified A	0x3071F1EC67B203EB	
Key now	0x5ACB1D644C0D51204EA55ACB1D644C0D	
Feedback		
BLKCNT	KASUMI Input	Keystream
0	0x3071F1EC67B203EB	0xE095306AD5086E2E
1	0xD0E4C186B2BA6DC4	0xAC7F3107DE4FA22D
2	0x9C0EC0EBB9FDA1C4	0xC1DFC97D5BC5661D
3	0xF1AE38913C7765F5	0xD6096F476AEDC64B

BLOCK1: 0xE095306AD5086E2EAC7F3107DE4F80

BLOCK2: 0x88B7077F25F56F1598775825BD1D80

3.7 Test Set 5

Input A5/3		
KLEN	128 Bits	
Kc	0xD3C5D592327FB11C4035C6680AF8C6D1	
COUNT	0x0A59B4	
Input KGC		
Key	0xD3C5D592327FB11C4035C6680AF8C6D1	
CA	0x0F	
CB	0	
CC	0x000A59B4	
CD	0	
CL	228	
Init		
Initial A	0x000A59B4000F0000	
Key used	0x869080C7672AE4491560933D5FAD9384	
Modified A	0x0CAAEC5C175B5A03	
Key now	0xD3C5D592327FB11C4035C6680AF8C6D1	
Feedback		
BLKCNT	KASUMI Input	Keystream
0	0x0CAAEC5C175B5A03	0xDCE64362AB5F89C1
1	0xD04CAF3EBC04D3C3	0x1EF0B305166570F4
2	0x125A5F59013E2AF5	0x889D5511E9E3575D
3	0x8437B94DFEB80D5D	0x062B5CED6039506A

BLOCK1: 0xDCE64362AB5F89C11EF0B305166540

BLOCK2: 0xC3D222755447A78D5D7418AD73B580

4 Algorithm A5/3 for EDGE

4.1 Overview

The test data sets presented here are for the algorithm A5/3 for EDGE. No detailed data of the internal states of Kasumi are presented here as these are covered in section 4 of document TS 35.203 [6].

For EDGE, the DIRECTION bit is not applicable and is set to zero. The COUNT variable is 22 bits in length. EDGE allows block sizes up to 348 bits for BLOCK1 and BLOCK2. As A5/3 for EDGE 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 to the function and their mapping to KGCORE inputs. Thereafter the input/output values of the initial KASUMI operation are shown. Finally the feedback and the resulting keystream block is shown in a table.

The first test set will also give the results in binary format to explicitly show the relationship between the hexadecimal and binary format.

4.3 Test Set 1

Input A5/3		
KLEN	64 Bits	
Kc	0x2BD6459F82C5BC00	
COUNT	0x24F20F	
Input KGC		
Key	0x2BD6459F82C5BC002BD6459F82C5BC00	
CA	0xF0	
CB	0	
CC	0x0024F20F	
CD	0	
CL	696	
Init		
Initial A	0x0024F20F00F00000	
Key used	0x7E8310CAD790E9557E8310CAD790E955	
Modified A	0xF3B3A9E4CDB3EA39	
Key now	0x2BD6459F82C5BC002BD6459F82C5BC00	
Feedback		
BLKCNT	KASUMI Input	Keystream
0	0xF3B3A9E4CDB3EA39	0xF75E663ACEA21EC9
1	0x04EDCFDE0311F4F1	0xD0BDE98B6C33B819
2	0x230E406FA1805222	0x299E830A1A2E2F91
3	0xDA2D2AEED79DC5AB	0x4326BEF515089B6D
4	0xB0951711D8BB7150	0xB0F271AFB9609F90
5	0x4341D84B74D375AC	0x5202CDCF51426D17
6	0xA1B1642B9CF18728	0x2DB47BFED3E6D83D
7	0xDE07D21A1E553203	0x14F4876366CCCD5B
8	0xE7472E87AB7F276A	0xFAE85B27C9B49F2F
9	0x095BF2C30407751F	0x7775B0B504905F27
10	0x84C61951C923B514	0xB5AE62B8269EA9BB

```
BLOCK1: 0xF75E663ACEA21EC9D0BDE98B6C33B819299E830A1A2E2F914326BEF515089B6DB0F271AFB9609F905202CDC0
11110111010111100110011000111010110011101010001000011110110010011101000010111101111010011000010110110
11000011001110111000000110010010100110011111010000011000010100001101000101110001011111001000101000011
00100110101111101111010100010101000010001001101101101101101100001111001001110001101011111011100101100
00001001111110010000010100100000001011001101100
```

```
BLOCK2: 0xF51426D172DB47BFED3E6D83D14F4876366CCCD5BFAE85B27C9B49F2F7775B0B504905F27B5AE62B8269EA90
11110101000101000010011011010001011100101101101101000111101111111111011010011111100110110110000011110100
00010100111101001000011101100011011001101100110011001101010110111111101011101000010110110010011111100
```

100110110100100111110010111101110111011101011011000010110101000001001001000001011111001001111011010110111001100010101110000010011010011110101010010

4.4 Test Set 2

Input A5/3		
KLEN	64 Bits	
Kc	0x952C49104881FF48	
COUNT	0x061272	
Input KGC		
Key	0x952C49104881FF48952C49104881FF48	
CA	0xF0	
CB	0	
CC	0x00061272	
CD	0	
CL	696	
Init		
Initial A	0x0006127200F00000	
Key used	0xC0791C451DD4AA1DC0791C451DD4AA1D	
Modified A	0x50736152B21A65A1	
Key now	0x952C49104881FF48952C49104881FF48	
Feedback		
BLKCNT	KASUMI Input	Keystream
0	0x50736152B21A65A1	0xE1876AA5B250B2B8
1	0xB1F40BF7004AD718	0xD58ADE52844E84E1
2	0x85F9BF003654E142	0x09A38FF6A87FCC7B
3	0x59D0EEA41A65A9D9	0x72FC8387494086DB
4	0x228FE2D5FB5AE37E	0xA2D2A1EE189DB569
5	0xF2A1C0BCAA87D0CD	0xA9245157CDD323EA
6	0xF95730057FC9464D	0x3518270A162C054E
7	0x656B4658A43660E8	0x120F5C703AE0AB32
8	0x427C3D2288FACE9B	0x4498D40D56268745
9	0x14EBB55FE43CE2ED	0xC41BC58D71DD255C
10	0x9468A4DFC3C740F7	0xCAC6BDA3B244397E

BLOCK1: 0xE1876AA5B250B2B8D58ADE52844E84E109A38FF6A87FCC7B72FC8387494086DBA2D2A1EE189DB569A9245150

BLOCK2: 0x7CDD323EA3518270A162C054E120F5C703AE0AB324498D40D56268745C41BC58D71DD255CCAC6BDA3B244390

4.5 Test Set 3

Input A5/3		
KLEN	64	
Kc	0xEFA8B2229E720C2A	
COUNT	0x33FD3F	
Input KGC		
Key	0xEFA8B2229E720C2AEFA8B2229E720C2A	
CA	0xF0	
CB	0	
CC	0x0033FD3F	
CD	0	
CL	696	
Init		
Initial A	0x0033FD3F00F00000	
Key used	0xBAFDE777CB27597FBAFDE777CB27597F	
Modified A	0x0950A4B18725EF90	
Key now	0xEFA8B2229E720C2AEFA8B2229E720C2A	
Feedback		
BLKCNT	KASUMI Input	Keystream
0	0x0950A4B18725EF90	0x09B49CE620E4A36B
1	0x00E43857A7C14CFA	0x7956186C8F248B61
2	0x7006BCDD080164F3	0x50DC2362B3F41F6F
3	0x598C87D334D1F0FC	0x28F486D9A80BB879
4	0x21A422682F2E57ED	0xDA4FE349E72EF975
5	0xD31F47F8600B16E0	0x5A5015902B17EE1D
6	0x5300B121AC32018B	0xF32D9302567E470E
7	0xFA7D37B3D15BA899	0xA3A26B0FFCDE60DF
8	0xAAF2CFBE7BFB8F47	0xB8A28C10609AEC74
9	0xB1F228A1E7BF03ED	0xCA1EEDF3BAA3334C
10	0xC34E49423D86DCD6	0x28E7E4DDA38A4AEE

BLOCK1: 0x09B49CE620E4A36B7956186C8F248B6150DC2362B3F41F6F28F486D9A80BB879DA4FE349E72EF9755A501590

BLOCK2: 0x02B17EE1DF32D9302567E470EA3A26B0FFCDE60DFB8A28C10609AEC74CA1EEDF3BAA3334C28E7E4DDA38A4A0

4.6 Test Set 4

Input A5/3		
KLEN	80	
Kc	0x5ACB1D644C0D51204EA5	
COUNT	0x156B26	
Input KGC		
Key	0x5ACB1D644C0D51204EA55ACB1D644C0D	
CA	0xF0	
CB	0	
CC	0x00156B26	
CD	0	
CL	696	
Init		
Initial A	0x00156B2600F00000	
Key used	0x0F9E4831195804751BF00F9E48311958	
Modified A	0x4653A8F67463F66B	
Key now	0x5ACB1D644C0D51204EA55ACB1D644C0D	
Feedback		
BLKCNT	KASUMI Input	Keystream
0	0x4653A8F67463F66B	0x0E5874E1CB66E2C0
1	0x480BDC17BF0514AA	0x438D49C5744C966F
2	0x05DEE133002F6006	0x001845E736CF365E
3	0x464BED1142ACC036	0xF842FAFFE4D28733
4	0xBE11520990B1715C	0x7C4A5FE5ACB03A39
5	0x3A19F713D8D3CC57	0x52810E30BB4AEDC7
6	0x14D2A6C6CF291BAA	0xA066C740F8D8A862
7	0xE6356FB68CBB5E0E	0x157E2A18F7E35173
8	0x532D82EE8380A710	0x6DF7CC7728172CA1
9	0x2BA464815C74DAC3	0xFE2736DE2DB08FBE
10	0xB8749E2859D379DF	0x14A0FF88C1AF790A

BLOCK1: 0x0E5874E1CB66E2C0438D49C5744C966F001845E736CF365EF842FAFFE4D287337C4A5FE5ACB03A3952810E30

BLOCK2: 0x0BB4AEDC7A066C740F8D8A862157E2A18F7E351736DF7CC7728172CA1FE2736DE2DB08FBE14A0FF88C1AF790

4.7 Test Set 5

Input A5/3		
KLEN	128	
Kc	0xD3C5D592327FB11C4035C6680AF8C6D1	
COUNT	0x0A59B4	
Input KGC		
Key	0xD3C5D592327FB11C4035C6680AF8C6D1	
CA	0xF0	
CB	0	
CC	0x000A59B4	
CD	0	
CL	696	
Init		
Initial A	0x000A59B400F00000	
Key used	0x869080C7672AE4491560933D5FAD9384	
Modified A	0x4278E040B3401A23	
Key now	0xD3C5D592327FB11C4035C6680AF8C6D1	
Feedback		
BLKCNT	KASUMI Input	Keystream
0	0x4278E040B3401A23	0x9887368E48257E17
1	0xDAFFD6CEFB656435	0x2EFF14BABC114DB5
2	0x6C87F4FA0F515794	0x159C2E3D0521AFCD
3	0x57E4CE7DB661B5ED	0x04487995989C35F8
4	0x463099D52BDC2FDF	0xF26C005D4CBDE2E3
5	0xB014E01DFFFDF8C5	0x9F18572D6DD0D2FA
6	0xDD60B76DDE90C8DF	0x85CF7C5FF04CDEC1
7	0xC7B79C1F430CC4E5	0x2318F01D418F4BBB
8	0x6160105DF2CF5190	0xF5FAFF8DFEA66C92
9	0xB7821FCD4DE676B8	0x47A8F64DEBF71A36
10	0x05D0160D58B7001F	0x4FBB36F39161ECB9

BLOCK1: 0x9887368E48257E172EFF14BABC114DB5159C2E3D0521AFCD04487995989C35F8F26C005D4CBDE2E39F185720

BLOCK2: 0xD6DD0D2FA85CF7C5FF04CDEC12318F01D418F4BBBF5FAFF8DFEA66C9247A8F64DEBF71A364FBB36F39161EC0

5 Algorithm GEA3 for GPRS

5.1 Overview

The test data sets presented here are for the algorithm GEA3 for GPRS. No detailed data of the internal states of Kasumi are presented here as these are covered in section 3 of document TS 35.203 [6].

5.2 Format

Each test starts by showing the various inputs to the function and their mapping to KGCORE inputs. Thereafter the input/output values of the initial KASUMI operation are shown. Finally the feedback and the resulting keystream block is shown in a table.

The first test set will also give the results in binary format to explicitly show the relationship between the hexadecimal and binary format.

5.3 Test Set 1

Input GEA3		
KLEN	64 Bits	
Kc	0x2BD6459F82C5BC00	
INPUT	0x5124F20F	
DIRECTION	1	
M	51	
Input KGC		
Key	0x2BD6459F82C5BC002BD6459F82C5BC00	
CA	0xFF	
CB	0	
CC	0x5124F20F	
CD	1	
CL	408	
Init		
Initial A	0x5124F20F04FF0000	
Key used	0x7E8310CAD790E9557E8310CAD790E955	
Modified A	0xDF1F9CA88B8F3248	
Key now	0x2BD6459F82C5BC002BD6459F82C5BC00	
Feedback		
BLKCNT	KASUMI Input	Keystream
0	0xDF1F9CA88B8F3248	0xF0270AAF26851D2A
1	0x2F389607AD0A2F63	0x4E88CC48CBFC740D
2	0x919750E040734647	0x94ACAB8495D27A7E
3	0x4BB3372C1E5D4835	0x154F5DA9E991EF8A
4	0xCA50C101621EDDC6	0x4198C7369655E5B9
5	0x9E875B9E1DDAD7F4	0x72DA2B05CF4CD394
6	0xADC5B7AD44C3E1DA	0xB132EBAD0F8F793E

OUTPUT:
0xF0270AAF26851D2A4E88CC48CBFC740D94ACAB8495D27A7E154F5DA9E991EF8A4198C7369655E5B972DA2B05CF4CD394B1
32EB

11110000001001110000101010111100100110100001010001110100101010010011101000100011001100010010001100
10111111110001110100000011011001010010101100101010111000010010010101110100100111101001111110000101 01
01001111010111011010100111101001100100011110111110001010010000011001100011000111001101101001011001 01
01011110010110111001011100101110110100010101100000101110011111010011001101001110010100101100010011001 0
11101011

5.4 Test Set 2

Input GEA3		
KLEN	64 Bits	
Kc	0x952C49104881FF48	
INPUT	0xD3861272	
DIRECTION	0	
M	51	
Input KGC		
Key	0x952C49104881FF48952C49104881FF48	
CA	0xFF	
CB	0	
CC	0xD3861272	
CD	0	
CL	408	
Init		
Initial A	0xD386127200FF0000	
Key used	0xC0791C451DD4AA1DC0791C451DD4AA1D	
Modified A	0x619D4068C2D10D43	
Key now	0x952C49104881FF48952C49104881FF48	
Feedback		
BLKCNT	KASUMI Input	Keystream
0	0x619D4068C2D10D43	0x9B7B516B15FB65E2
1	0xFAE61103D72A68A0	0x83B722DBE3A2CFCB
2	0xE22A62B32173C28A	0x0B255CFB38D529B9
3	0x6AB81C93FA0424F9	0x61BC04129D5C6565
4	0x0021447A5F8D6822	0xAA25C31E63D10A04
5	0xCBB88376A1000742	0x8191BC1F17E67ECA
6	0xE00CFC77D537738F	0xAA509A78B1A8ABEF

OUTPUT:
0x9B7B516B15FB65E283B722DBE3A2CFCB0B255CFB38D529B961BC04129D5C6565AA25C31E63D10A048191BC1F17E67ECAAA
509A

5.5 Test Set 3

Input GEA3		
KLEN	64 Bits	
Kc	0xEFA8B2229E720C2A	
INPUT	0x4AB3FD3F	
DIRECTION	0	
M	51	
Input KGC		
Key	0xEFA8B2229E720C2AEFA8B2229E720C2A	
CA	0xFF	
CB	0	
CC	0x4AB3FD3F	
CD	0	
CL	408	
Init		
Initial A	0x4AB3FD3F00FF0000	
Key used	0xBAFDE777CB27597FBAFDE777CB27597F	
Modified A	0x3A06D4477FA3DF28	
Key now	0xEFA8B2229E720C2AEFA8B2229E720C2A	
Feedback		
BLKCNT	KASUMI Input	Keystream
0	0x3A06D4477FA3DF28	0x0306B1F1E6286F27
1	0x390065B6998BB00E	0x148FF4F081164EA3
2	0x2E8920B7FEB59189	0x05E3296121F56491
3	0x3FE5FD265E56BBBA	0xA3BBEAB48EF824B3
4	0x99BD3EF3F15BFB9F	0x64D304946DCA4677
5	0x5ED5D0D31269995A	0x3F3A548642C68545
6	0x053C80C13D655A6B	0xC0FEE047AA50EBDF

OUTPUT:
0x0306B1F1E6286F27148FF4F081164EA305E3296121F56491A3BBEAB48EF824B364D304946DCA46773F3A548642C68545C0
FEE0

5.6 Test Set 4

Input GEA3	
KLEN	80 Bits
Kc	0x5ACB1D644C0D51204EA5
INPUT	0xA1056B26
DIRECTION	1
M	51
Input KGC	
Key	0x5ACB1D644C0D51204EA55ACB1D644C0D
CA	0xFF
CB	0
CC	0xA1056B26
CD	1
CL	408
Init	
Initial A	0xA1056B2604FF0000
Key used	0x0F9E4831195804751BF00F9E48311958
Modified A	0xA4B67C463FF7B4D5
Key now	0x5ACB1D644C0D51204EA55ACB1D644C0D

Feedback		
BLKCNT	KASUMI Input	Keystream
0	0xA4B67C463FF7B4D5	0xAA7906987B717A55
1	0x0ECF7ADE4486CE81	0xD58DA45465C74030
2	0x713BD8125A30F4E7	0xDA5AB70DAD711ECA
3	0x7EECCB4B9286AA1C	0x119EE76FFAA8D228
4	0xB5289B29C55F66F9	0x7EEE1314CD5E5333
5	0xDA586F52F2A9E7E3	0xCAB78DF6DACE4B86
6	0x6E01F1B0E539FF55	0x2814AD2CB44D715F

OUTPUT:
0xAA7906987B717A55D58DA45465C74030DA5AB70DAD711ECA119EE76FFAA8D2287EEE1314CD5E5333CAB78DF6DACE4B8628
14AD

5.7 Test Set 5

Input GEA3		
KLEN	128 Bits	
Kc	0xD3C5D592327FB11C4035C6680AF8C6D1	
INPUT	0x0A3A59B4	
DIRECTION	0	
M	51	
Input KGC		
Key	0xD3C5D592327FB11C4035C6680AF8C6D1	
CA	0xFF	
CB	0	
CC	0x0A3A59B4	
CD	0	
CL	408	
Init		
Initial A	0x0A3A59B400FF0000	
Key used	0x869080C7672AE4491560933D5FAD9384	
Modified A	0x5AEE7A85947015B1	
Key now	0xD3C5D592327FB11C4035C6680AF8C6D1	
Feedback		
BLKCNT	KASUMI Input	Keystream
0	0x5AEE7A85947015B1	0x6E217CE41EBEFB5E
1	0x34CF06618ACEEEEE	0xC8094C1597429006
2	0x92E73690033285B5	0x5E42BABC9AE35654
3	0x04ACC0390E9343E6	0xA53085CE68DFA442
4	0xFFDEFF4BFCAFB1F7	0x6A2FF0AD4AF33410
5	0x30C18A28DE8321A4	0x06A3F84B7613ACB4
6	0x5C4D82CEE263B903	0xFBDC342DCFF787DA

OUTPUT:
0x6E217CE41EBEFB5EC8094C15974290065E42BABC9AE35654A53085CE68DFA4426A2FF0AD4AF3341006A3F84B7613ACB4FB
DC34

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 55.217) (Technically equivalent to SAGE V1.0)	SAGE V1.0	1.0.0