ETSI/SAGE Specification

Version: 1.1
Date: 25th October 2012

Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2

Document 3: Implementors' Test Data

Document History		
V1.0	**10-01-2006**	**Publication**
1.1	**25-10-2012**	**Correction to mis-edited IV in section 5.5**

PREFACE

This specification has been prepared by the 3GPP Task Force, and gives detailed test data for implementors of the algorithm set. It provides visibility of the internal state of the algorithm to aid in the realisation of the algorithms.

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

- Specification of the 3GPP Confidentiality and Integrity Algorithms ***UEA2*** & ***UIA2***.
  Document 1: Algorithm Specifications.

- Specification of the 3GPP Confidentiality and Integrity Algorithms ***UEA2*** & ***UIA2***.
  Document 2: SNOW 3G Algorithm Specification.

- Specification of the 3GPP Confidentiality and Integrity Algorithms ***UEA2*** & ***UIA2***.
  Document 3: Implementors' Test Data.

- Specification of the 3GPP Confidentiality and Integrity Algorithms ***UEA2*** & ***UIA2***.
  Document 4: Design Conformance Test Data.

This document is purely informative. The normative part of the specification of the ***UEA2*** (confidentiality) and the ***UIA2*** (integrity) algorithms is in the main body of document 1. The normative part of the specification of **SNOW 3G** is found in document 2.

Blank Page

TABLE OF CONTENTS

REFERENCES

[1] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (3G TS 33.102 version 6.3.0)

[2] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Cryptographic Algorithm Requirements; (3G TS 33.105 version 6.0.0)

[3] Specification of the 3GPP Confidentiality and Integrity Algorithms ***UEA2*** & ***UIA2***. Document 1: ***UEA2*** and ***UIA2*** specifications.

[4] Specification of the 3GPP Confidentiality and Integrity Algorithms ***UEA2*** & ***UIA2***. Document 2: **SNOW 3G** specification.

[5] Specification of the 3GPP Confidentiality and Integrity Algorithms ***UEA2*** & ***UIA2***. Document 3: Implementors' Test Data.

[6] Specification of the 3GPP Confidentiality and Integrity Algorithms ***UEA2*** & ***UIA2***. Document 4: Design Conformance Test Data.

[7] P. Ekdahl and T. Johansson, "A new version of the stream cipher SNOW", in Selected Areas in Cryptology (SAC 2002), LNCS 2595, pp. 47–61, Springer-Verlag,

1. OUTLINE OF THE IMPLEMENTORS' TEST DATA

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

Section 3 provides test data for **SNOW 3G**.

Section 4 provides test data for the Confidentiality Algorithm ***UEA2***.

Section 5 provides test data for the Integrity Algorithm ***UIA2***.

2. INTRODUCTORY INFORMATION

2.1. Introduction

Within the security architecture of the 3GPP system there are two standardised algorithms; a confidentiality algorithm ***UEA2***, and an integrity algorithm ***UIA2***. These algorithms are specified in a companion document [3]. Each of these algorithms is based on the **SNOW 3G** algorithm that is specified in [4].

To assist implementors with their realisation of the algorithm set this document provides test data for these algorithms along with extensive detail of the internal states of the algorithms as they process the given input data.

Final testing of the algorithms should be performed using the test data sets given in the "Design Conformance" companion document [6].

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. 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 the 128-kit key $\boldsymbol{K}$ is subdivided into four 32-bit substrings $\boldsymbol{K}_0$, $\boldsymbol{K}_1$, $\boldsymbol{K}_2$, $\boldsymbol{K}_3$ so if we have a key

$$\boldsymbol{K} = 0123456789ABCDEFFEDCBA9876543210$$

we have:

$$\boldsymbol{K}_0 = 01234567, \boldsymbol{K}_1 = 89ABCDEF, \boldsymbol{K}_2 = FEDCBA98, \boldsymbol{K}_3 = 76543210.$$

2.4. Presentation of input/output data

The basic data processed by the ***UEA2*** and ***UIA2*** 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).

3. SNOW 3G

3.1. Overview

The test data sets presented here are for the **SNOW 3G** stream cipher algorithm.

3.2. Format

Each test set starts by showing the input and output data values.

This is followed by a table showing the state of the LFSR at the beginning of the computation.

Then for the first 8 steps of the initialisation the content of s_0, s_2, s_5, s_{11}, s_{15}, R1, R2, R3 is given in a table.

Then the state of the LFSR and the FSM at the end of the initialisation is given.

For the first 3 steps of keystream generation s_0, s_2, s_5, s_{11}, s_{15}, R1, R2, R3 are given in a table.

Finally the output $\mathbf{z}_1$, $\mathbf{z}_2$, … is given.

3.3. Test Set 1

```
input:
   Key:   2B D6 45 9F 82 C5 B3 00 95 2C 49 10 48 81 FF 48
   IV:    EA 02 47 14 AD 5C 4D 84 DF 1F 9B 25 1C 0B F4 5F
output:
   z1: AB EE 97 04
   z2: 7A C3 13 73
```

K_0	K_1	K_2	K_3
2B D6 45 9F	82 C5 B3 00	95 2C 49 10	48 81 FF 48

IV_0	IV_1	IV_2	IV_3
EA 02 47 14	AD 5C 4D 84	DF 1F 9B 25	1C 0B F4 5F

Initialisation Mode
LFSR-state at the beginning:

i	s_{0+i}	s_{1+i}	s_{2+i}	s_{3+i}	s_{4+i}	s_{5+i}	s_{6+i}	s_{7+i}
0	D429BA60	7D3A4CFF	6AD3B6EF	B77E00B7	2BD6459F	82C5B300	952C4910	4881FF48
8	D429BA60	6131B8A0	B5CC2DCA	B77E00B7	868A081B	82C5B300	952C4910	A283B85C

	s_0	s_2	s_5	s_{11}	s_{15}	R1	R2	R3
0	D429BA60	6AD3B6EF	82C5B300	B77E00B7	A283B85C	00000000	00000000	00000000
1	7D3A4CFF	B77E00B7	952C4910	868A081B	97DF2884	82C5B300	63636363	25252525
2	6AD3B6EF	2BD6459F	4881FF48	82C5B300	311BA301	136CCF98	486C5BC4	93939393
3	B77E00B7	82C5B300	D429BA60	952C4910	A69FCBCB	237EC89F	EAEBC424	4B7815EA
4	2BD6459F	952C4910	6131B8A0	A283B85C	E76F0ADA	8A3D73AE	21A4385B	E662EC27
5	82C5B300	4881FF48	B5CC2DCA	97DF2884	A52DCD12	A8F78CE2	63A7F600	BC3F3A8D
6	952C4910	D429BA60	B77E00B7	311BA301	1A349A62	6D9B0D47	20712A2D	391D0883

7	4881FF48	6131B8A0	868A081B	A69FCBCB	2A2A44DB	AED43261	401B1511	45A6ED60

LFSR-state after completion of the initialisation mode:

i	S_{0+i}	S_{1+i}	S_{2+i}	S_{3+i}	S_{4+i}	S_{5+i}	S_{6+i}	S_{7+i}
0	8F1215A6	E003A052	9241C929	68D7BF8C	16BF4C2A	8DEF9D70	32381704	11DD346A
8	E18B81EA	77EBD4FE	57ED9505	0C33C0EF	1A037B59	97591E82	A91CCB44	7B48E04F

FSM-state after completion of the initialisation mode:
R1 = 61DA9249
R2 = 427DF38C
R3 = 0FB6B101

Keystream mode

	S_0	S_2	S_5	S_{11}	S_{15}	R1	R2	R3
0	E003A052	68D7BF8C	32381704	1A037B59	1646644C	C4D71FFD	90F0B31F	CC612008
1	9241C929	16BF4C2A	11DD346A	97591E82	52E43190	8F49EA2B	0AACC1E1	3367438C
2	68D7BF8C	8DEF9D70	E18B81EA	A91CCB44	B737110E	2D6739C7	5295DA23	5293E49E

Output:
$\mathbf{z}_1$ = AB EE 97 04
$\mathbf{z}_2$ = 7A C3 13 73

3.4. Test Set 2

input:
Key: 8C E3 3E 2C C3 C0 B5 FC 1F 3D E8 A6 DC 66 B1 F3
IV: D3 C5 D5 92 32 7F B1 1C DE 55 19 88 CE B2 F9 B7
output:
$\mathbf{z}_1$: EF F8 A3 42
$\mathbf{z}_2$: F7 51 48 0F

K_0	K_1	K_2	K_3
8C E3 3E 2C	C3 C0 B5 FC	1F 3D E8 A6	DC 66 B1 F3

IV_0	IV_1	IV_2	IV_3
D3 C5 D5 92	32 7F B1 1C	DE 55 19 88	CE B2 F9 B7

Initialisation Mode
LFSR-state at the beginning:

i	S_{0+i}	S_{1+i}	S_{2+i}	S_{3+i}	S_{4+i}	S_{5+i}	S_{6+i}	S_{7+i}
0	731CC1D3	3C3F4A03	E0C21759	23994E0C	8CE33E2C	C3C0B5FC	1F3DE8A6	DC66B1F3
8	731CC1D3	F28DB3B4	3E970ED1	23994E0C	BE9C8F30	C3C0B5FC	1F3DE8A6	0FA36461

	S_0	S_2	S_5	S_{11}	S_{15}	R1	R2	R3
0	731CC1D3	E0C21759	C3C0B5FC	23994E0C	0FA36461	00000000	00000000	00000000
1	3C3F4A03	23994E0C	1F3DE8A6	BE9C8F30	EF81E474	C3C0B5FC	63636363	25252525
2	E0C21759	8CE33E2C	DC66B1F3	C3C0B5FC	7A554815	9D7C30E6	F878FA8B	93939393
3	23994E0C	C3C0B5FC	731CC1D3	1F3DE8A6	53E0AE66	486E1CEB	2148E845	098F198B
4	8CE33E2C	1F3DE8A6	F28DB3B4	0FA36461	9A1EE9B8	9BDCC09D	87A622BB	EFFA4239
5	C3C0B5FC	DC66B1F3	3E970ED1	EF81E474	2390FE04	A51E1448	F6CFB4FB	2087DC1D
6	1F3DE8A6	731CC1D3	23994E0C	7A554815	6FB8C36C	14E087C7	72462DC5	0B8BF471
7	DC66B1F3	F28DB3B4	BE9C8F30	53E0AE66	BA5DB98F	9A58E842	481D2AB5	5C8EE565

LFSR-state after completion of the initialisation mode:

i	S_{0+i}	S_{1+i}	S_{2+i}	S_{3+i}	S_{4+i}	S_{5+i}	S_{6+i}	S_{7+i}
0	04D6A929	942E1440	82ABD3FE	5832E9F4	5F9702A0	08712C81	644CC9B9	DBF6DE13
8	BAA5B1D0	92E9DD53	A2E2FA6D	CE6965AA	02C0CD4E	6E6D984F	114A90E7	5279F8DA

FSM-state after completion of the initialisation mode:
R1 = 65130120
R2 = A14C7DBD
R3 = B68B551A

Keystream mode

	S_0	S_2	S_5	S_{11}	S_{15}	R1	R2	R3
0	942E1440	5832E9F4	644CC9B9	02C0CD4E	C1E93B6B	6046F758	59E685C1	7DCBC989
1	82ABD3FE	5F9702A0	DBF6DE13	6E6D984F	CEB99926	736D85F1	37DD84E6	A9BECBB1
2	5832E9F4	08712C81	BAA5B1D0	114A90E7	E34F6919	AA259A88	56C45F48	C3546A61

Output:
$\mathbf{z}_1$ = EF F8 A3 42
$\mathbf{z}_2$ = F7 51 48 0F

3.5. Test Set 3

input:
Key: 40 35 C6 68 0A F8 C6 D1 A8 FF 86 67 B1 71 40 13
IV: 62 A5 40 98 1B A6 F9 B7 45 92 B0 E7 86 90 F7 1B
output:
$\mathbf{z}_1$: A8 C8 74 A9
$\mathbf{z}_2$: 7A E7 C4 F8

K_0	K_1	K_2	K_3
40 35 C6 68	0A F8 C6 D1	A8 FF 86 67	B1 71 40 13

IV_0	IV_1	IV_2	IV_3
62 A5 40 98	1B A6 F9 B7	45 92 B0 E7	86 90 F7 1B

Initialisation Mode
LFSR-state at the beginning:

i	S_{0+i}	S_{1+i}	S_{2+i}	S_{3+i}	S_{4+i}	S_{5+i}	S_{6+i}	S_{7+i}
0	BFCA3997	F507392E	57007998	4E8EBFEC	4035C668	0AF8C6D1	A8FF8667	B1714013
8	BFCA3997	7397CE35	1292C97F	4E8EBFEC	5B933FDF	0AF8C6D1	A8FF8667	D3D4008B

	S_0	S_2	S_5	S_{11}	S_{15}	R1	R2	R3
0	BFCA3997	57007998	0AF8C6D1	4E8EBFEC	D3D4008B	00000000	00000000	00000000
1	F507392E	4E8EBFEC	A8FF8667	5B933FDF	EE2CABF5	0AF8C6D1	63636363	25252525
2	57007998	4035C668	B1714013	0AF8C6D1	667356A3	F13E06A5	79A1E99D	93939393
3	4E8EBFEC	0AF8C6D1	BFCA3997	A8FF8667	6410181D	9C84BD1D	8EEEB4AE	E5995CC4
4	4035C668	A8FF8667	7397CE35	D3D4008B	241A7790	E9421A01	75196F5C	C83E1776
5	0AF8C6D1	B1714013	1292C97F	EE2CABF5	C485B826	30C3489F	36A44937	0F317420
6	A8FF8667	BFCA3997	4E8EBFEC	667356A3	A211C1E9	54480696	02D90971	3D982023
7	B1714013	7397CE35	5B933FDF	6410181D	6E8AE7E6	75EFA940	D63B98F8	883F13A7

LFSR-state after completion of the initialisation mode:

i	S_{0+i}	S_{1+i}	S_{2+i}	S_{3+i}	S_{4+i}	S_{5+i}	S_{6+i}	S_{7+i}
0	FEAFBAD8	1B11050A	23708014	AC8494DB	ED97D431	DBBB59B3	6CD30005	7EC36405
8	B20F02AC	EB407735	50E41A0E	FFA8ABC1	EB4800A7	D4E6749D	D1C452FE	A92A3153

```
FSM-state after completion of the initialisation mode:
R1 = 6599AA50
R2 = 5EA9188B
R3 = F41889FC
```

Keystream mode

	S_0	S_2	S_5	S_{11}	S_{15}	R1	R2	R3
0	1B11050A	AC8494DB	6CD30005	EB4800A7	0FE91C6F	8E4CE8DA	2DEF74EA	42B4B0A3
1	23708014	ED97D431	7EC36405	D4E6749D	C3CB3734	5C572590	79B51828	2496A1E1
2	AC8494DB	DBBB59B3	B20F02AC	D1C452FE	739AB29C	D40ADE0C	5037B990	32D1FAE0

Output:

$\mathbf{z}_1$ = A8 C8 74 A9

$\mathbf{z}_2$ = 7A E7 C4 F8

3.6. Test Set 4

This test ensures that all entries in the tables S_R, T0, T1, T2, T3, S2_T0, S2_T1, S2_T2, S2_T3 and MUL_α, DIV_α are correct. For a fixed key and IV the algorithm is clocked 2500 times in keystream mode. With the given data every entry will be used at least once.

```
Iterated test for full tables coverage
input:
   Key:   0D ED 72 63 10 9C F9 2E 33 52 25 5A 14 0E 0F 76
   IV:    6B 68 07 9A 41 A7 C4 C9 1B EF D7 9F 7F DC C2 33
output:
```

z_1: D7 12 C0 5C

z_2: A9 37 C2 A6

z_3: EB 7E AA E3

…

z_{2500}: 9C 0D B3 AA

4. CONFIDENTIALITY ALGORITHM *UEA2*

4.1. Overview

The test data sets presented here are for the ***UEA2*** confidentiality algorithm. No detailed data is presented for the internal states of **SNOW 3G** as that is covered in section 3.

4.2. Format

Each test set starts by showing the various inputs to the algorithm including the data stream to be encrypted/decrypted. (The length field is in decimal). This is followed by:

the key words $\mathbf{K}_0$, $\mathbf{K}_1$, $\mathbf{K}_2$, $\mathbf{K}_3$

the Initialisation Variables $\mathbf{IV}_0$, $\mathbf{IV}_1$, $\mathbf{IV}_2$, $\mathbf{IV}_3$.

Thereafter three columns of data are shown.

Word number shows the number of the current 32-bit word.

Keystream shows the 32-bit output from **SNOW 3G**.

Enc/dec data shows the modified input data, i.e. it is the bitwise exclusive-or of the corresponding keystream and the input data to the algorithm. As this is a bitwise stream cipher it is purely a matter of context whether the operation is regarded as "encryption" or "decryption".

4.3. Test Set 1

```
Count-C    = 72A4F20F
Bearer     = 0C
Direction  = 1
CK         = 2B D6 45 9F 82 C5 B3 00 95 2C 49 10 48 81 FF 48
Length     = 798 bits
Plaintext:
7EC61272 743BF161 4726446A 6C38CED1
66F6CA76 EB543004 4286346C EF130F92
922B0345 0D3A9975 E5BD2EA0 EB55AD8E
1B199E3E C4316020 E9A1B285 E7627953
59B7BDFD 39BEF4B2 484583D5 AFE082AE
E638BF5F D5A60619 3901A08F 4AB41AAB
9B134880
```

K_0	K_1	K_2	K_3
48 81 FF 48	95 2C 49 10	82 C5 B3 00	2B D6 45 9F

IV_0	IV_1	IV_2	IV_3
64 00 00 00	72 A4 F2 0F	64 00 00 00	72 A4 F2 0F

Wordnumber	Keystream	enc/dec data
0	F22DB45B 37E71C5B	8CEBA629 43DCED3A
2	4EB6F404 CD886C15	0990B06E A1B0A2C4
4	9DCA27B1 F062AF46	FB3CEDC7 1B369F42
6	F8E2F587 8976E8B8	BA64C1EB 6665E72A
8	33E2B848 E798969D	A1C9BB0D EAA20FE8

10	85E5961A 057983F1	6058B8BA EE2C2E7F
12	10F55076 71185285	0BECCE48 B52932A5
14	D53CED16 FD580500	3C9D5F93 1A3A7C53
16	7BEE12BE 1C5C52EC	2259AF43 25E2A65E
18	78C12E8A C5B1B9D5	3084AD5F 6A513B7B
20	3BF90900 DF06DF63	DDC1B65F 0AA0D97A
22	3C3C15D5 C270DE52	053DB55A 88C4C4F9
24	FB4D09C0	605E4140

4.4. Test Set 2

```
Count-C     = E28BCF7B
Bearer      = 18
Direction   = 0
CK          = EF A8 B2 22 9E 72 0C 2A 7C 36 EA 55 E9 60 56 95
Length      = 510 bits
Plaintext:
10111231 E060253A 43FD3F57 E37607AB
2827B599 B6B1BBDA 37A8ABCC 5A8C550D
1BFB2F49 4624FB50 367FA36C E3BC68F1
1CF93B15 10376B02 130F812A 9FA169D8
```

K_0	K_1	K_2	K_3
E9 60 56 95	7C 36 EA 55	9E 72 0C 2A	EF A8 B2 22

IV_0	IV_1	IV_2	IV_3
C0 00 00 00	E2 8B CF 7B	C0 00 00 00	E2 8B CF 7B

Wordnumber	Keystream	enc/dec data
0	F0CB07FB 6E4571CF	E0DA15CA 8E2554F5
2	A691AB3F 3F1A7BB9	E56C9468 DC6C7C12
4	B4713F3C B592AC3A	9C568AA5 032317E0
6	79AF82A8 3627BAAB	4E072964 6CABEFA6
8	927D6308 49000249	89864C41 0F24F919
10	D0619E91 196B16A7	E61E3DFD FAD77E56
12	114992D8 26F421E6	0DB0A9CD 36C34AE4
14	0B1B1198 00FECB24	181490B2 9F5FA2FC

4.5. Test Set 3

```
Count-C     = FA556B26
Bearer      = 03
Direction   = 1
CK          = 5A CB 1D 64 4C 0D 51 20 4E A5 F1 45 10 10 D8 52
Length      = 120 bits
Plaintext:
AD9C441F 890B38C4 57A49D42 1407E8
```

K_0	K_1	K_2	K_3
10 10 D8 52	4E A5 F1 45	4C 0D 51 20	5A CB 1D 64

IV_0	IV_1	IV_2	IV_3
1C 00 00 00	FA 55 6B 26	1C 00 00 00	FA 55 6B 26

Wordnumber	Keystream	enc/dec data
0	1793752F 8A3FFDAF	BA0F3130 0334C56B

2	0503D43E AEC7AE	52A7497C BAC046

4.6. Test Set 4

```
Count-C     = 398A59B4
Bearer      = 05
Direction   = 1
CK          = D3 C5 D5 92 32 7F B1 1C 40 35 C6 68 0A F8 C6 D1
Length      = 253 bits
Plaintext:
981BA682 4C1BFB1A B4854720 29B71D80
8CE33E2C C3C0B5FC 1F3DE8A6 DC66B1F0
```

K_0	K_1	K_2	K_3
0A F8 C6 D1	40 35 C6 68	32 7F B1 1C	D3 C5 D5 92

IV_0	IV_1	IV_2	IV_3
2C 00 00 00	39 8A 59 B4	2C 00 00 00	39 8A 59 B4

Wordnumber	Keystream	enc/dec data
0	0080D71E 902835AD	989B719C DC33CEB7
2	7BA22D72 ABCBF214	CF276A52 827CEF94
4	298F7EEC 685D340B	A56C40C0 AB9D81F7
6	BD945260 D2777540	A2A9BAC6 0E11C4B0

4.7. Test Set 5

```
Count-C     = 72A4F20F
Bearer      = 09
Direction   = 0
CK          = 60 90 EA E0 4C 83 70 6E EC BF 65 2B E8 E3 65 66
Length      = 837 bits
Plaintext:
40981BA6 824C1BFB 4286B299 783DAF44
2C099F7A B0F58D5C 8E46B104 F08F01B4
1AB48547 2029B71D 36BD1A3D 90DC3A41
B46D5167 2AC4C966 3A2BE063 DA4BC8D2
808CE33E 2CCCBFC6 34E1B259  60876A0
FBB5A437 EBCC8D31 C19E4454 318745E3
98764598 7A986F2C B0
```

K_0	K_1	K_2	K_3
E8 E3 65 66	EC BF 65 2B	4C 83 70 6E	60 90 EA E0

IV_0	IV_1	IV_2	IV_3
48 00 00 00	72 A4 F2 0F	48 00 00 00	72 A4 F2 0F

Wordnumber	Keystream	enc/dec data
0	180AA00E 09F7D155	5892BBA8 8BBBCAAE
2	ECF02839 1355927E	AE769AA0 6B683D3A
4	3BC59BD9 D97D9BCB	17CC04A3 69881697
6	CD18F5FA 25709B41	435E44FE D5FF9AF5
8	612A0C4A 6D75D36D	7B9E890D 4D5C6470
10	AE38CEB7 74DAAAAD	9885D48A E40690EC
12	B056FB8E 5A935F82	043BAAE9 705796E4
14	93D4BA28 57C0FE05	A9FF5A4B 8D8B36D7
16	7372B4F2 4031D316	F3FE57CC 6CFD6CD0
18	312C8A0B AE56E26E	05CD3852 A85E94CE
20	907834E7 3BB4B4FF	6BCD90D0 D07839CE
22	C8ED7110 FB0970EB	09733544 CA8E3508
24	DB52C0C8 E8B2AE04	43248550 922AC128

26	A8	18

5. INTEGRITY ALORITHM *UIA2*

5.1. Overview

The test data sets presented here are for the ***UIA2*** integrity algorithm. No detailed data is presented for the internal states of **SNOW 3G** as that is covered in section 3.

5.2. Format

The test data set shows the input values to the algorithm.

This is followed by:

the key words $\mathbf{K}_0$, $\mathbf{K}_1$, $\mathbf{K}_2$, $\mathbf{K}_3$

the Initialisation Variables $\mathbf{IV}_0$, $\mathbf{IV}_1$, $\mathbf{IV}_2$ and $\mathbf{IV}_3$

the keystream words $\mathbf{z}_1$, $\mathbf{z}_2$, $\mathbf{z}_3$,, $\mathbf{z}_4$, $\mathbf{z}_5$.

the value $\mathbf{P} = \mathbf{z}_1 \| \mathbf{z}_2$

the value $\mathbf{Q} = \mathbf{z}_3 \| \mathbf{z}_4$.

Then for each message word M_i, $0 \le i \le \mathbf{D}\text{-}1$ this word M_i and the intermediate value EVAL are given. After that the result of the multiplication of EVAL by **Q** is displayed.

Finally the output **MAC-I** of the ***UIA2***-algorithm is shown.

5.3. Test Set 1

```
COUNT-I     = 38A6F056
FRESH       = 05D2EC49
DIRECTION   = 0
IK          = 2B D6 45 9F 82 C5 B3 00 95 2C 49 10 48 81 FF 48
LENGTH      = 189 bits
MESSAGE:
6B227737296F393C 8079353EDC87E2E8 05D2EC49A4F2D8E0
```

K_0	K_1	K_2	K_3
48 81 FF 48	95 2C 49 10	82 C5 B3 00	2B D6 45 9F

IV_0	IV_1	IV_2	IV_3
05 D2 EC 49	38 A6 F0 56	05 D2 EC 49	38 A6 F0 56

$\mathbf{z}_1$	$\mathbf{z}_2$	$\mathbf{z}_3$	$\mathbf{z}_4$	$\mathbf{z}_5$
DC 0D 53 25	2A 5D 31 90	7E 1B 8E 28	25 EC 4C AA	63 D9 C7 7C

```
P= DC 0D 53 25  2A 5D 31 90
Q= 7E 1B 8E 28  25 EC 4C AA
```

i	Mi	EVAL

0	6B227737 296F393C	8BA78DCD 0D8C242D
1	8079353E DC87E2E8	7559CCE4 3F4DCEB5
2	05D2EC49 A4F2D8E0	8C108081 F386B04E
3	00000000 000000BD	8C108081 F386B0F3

Multiply by Q: EVAL= 4817DF5C 251B5E20

MAC-I: 2BCE1820

5.4. Test Set 2

```
COUNT-I     = 3EDC87E2
FRESH       = A4F2D8E2
DIRECTION   = 1
IK          = D4 2F 68 24 28 20 1C AF CD 9F 97 94 5E 6D E7 B7
LENGTH      = 254 bits
MESSAGE:
B5924384328A4AE0 0B737109F8B6C8DD 2B4DB63DD533981C EB19AAD52A5B2BC0
```

K_0	K_1	K_2	K_3
5E 6D E7 B7	CD 9F 97 94	28 20 1C AF	D4 2F 68 24

IV_0	IV_1	IV_2	IV_3
A4 F2 58 E2	BE DC 87 E2	A4 F2 D8 E2	3E DC 87 E2

$\mathbf{z}_1$	$\mathbf{z}_2$	$\mathbf{z}_3$	$\mathbf{z}_4$	$\mathbf{z}_5$
67 0E 29 DE	2A D6 DE 7E	A4 2A D0 48	40 7A 24 AC	20 F8 60 70

P= 67 0E 29 DE 2A D6 DE 7E
Q= A4 2A D0 48 40 7A 24 AC

i	Mi	EVAL
0	B5924384 328A4AE0	E7354091 E1B57157
1	0B737109 F8B6C8DD	655CA81A A179F483
2	2B4DB63D D533981C	E6E0FD58 B1B4BA89
3	EB19AAD5 2A5B2BC0	9BC353AA 5FE30866
4	00000000 000000FE	9BC353AA 5FE30898

Multiply by Q: EVAL= DC8378CD FD41FE17

MAC-I: FC7B18BD

5.5. Test Set 3

```
COUNT-I     = 36AF6144
FRESH       = 9838F03A
DIRECTION   = 1
IK          = FD B9 CF DF 28 93 6C C4 83 A3 18 69 D8 1B 8F AB
LENGTH      = 319 bits
MESSAGE:
5932BC0ACE2B0ABA 33D8AC188AC54F34 6FAD10BF9DEE2920 B43BD0C53A915CB7
DF6CAA72053ABFF2
```

K_0	K_1	K_2	K_3
D8 1B 8F AB	83 A3 18 69	28 93 6C C4	FD B9 CF DF

IV_0 IV_1 IV_2 IV_3

```
98 38 70 3A      B6 AF 61 44      98 38 F0 3A      36 AF 61 44
```

z_1	z_2	z_3	z_4	z_5
B3 9A FB 5D	53 AA 27 D4	56 A1 C4 AE	CB 68 F9 1A	BF 27 34 7B

```
P= B3 9A FB 5D  53 AA 27 D4
Q= 56 A1 C4 AE  CB 68 F9 1A
```

i	Mi	EVAL
0	5932BC0A CE2B0ABA	6E988791 F4F8ADD7
1	33D8AC18 8AC54F34	39723954 579492CB
2	6FAD10BF 9DEE2920	EEEAC385 C4D5E0C0
3	B43BD0C5 3A915CB7	EB79B071 CBAECF56
4	DF6CAA72 053ABFF2	32114B23 317FA002
5	00000000 0000013F	32114B23 317FA13D

```
Multiply by Q: EVAL= BDD6CED4 C458544C

MAC-I: 02F1FAAF
```

5.6. Test Set 4

```
COUNT-I     = 14793E41
FRESH       = 0397E8FD
DIRECTION   = 1
IK          = C7 36 C6 AA B2 2B FF F9 1E 26 98 D2 E2 2A D5 7E
LENGTH      = 384 bits
MESSAGE:
D0A7D463DF9FB2B2 78833FA02E235AA1 72BD970C1473E129 07FB648B6599AAA0
B24A038665422B20 A499276A50427009
```

K_0	K_1	K_2	K_3
E2 2A D5 7E	1E 26 98 D2	B2 2B FF F9	C7 36 C6 AA

IV_0	IV_1	IV_2	IV_3
03 97 68 FD	94 79 3E 41	03 97 E8 FD	14 79 3E 41

z_1	z_2	z_3	z_4	z_5
45 89 8E 82	8F 27 EB 98	E3 23 07 09	A0 0C B7 0A	8F 75 AC 4B

```
P= 45 89 8E 82  8F 27 EB 98
Q= E3 23 07 09  A0 0C B7 0A
```

i	Mi	EVAL
0	D0A7D463 DF9FB2B2	9E80B47B 98010914
1	78833FA0 2E235AA1	5EA34890 532D5FFB
2	72BD970C 1473E129	0EAE8E55 95661FCF
3	07FB648B 6599AAA0	7EA00D6D 65C8F93F
4	B24A0386 65422B20	BEC91666 B07F7551
5	A499276A 50427009	689EF151 53554DC2
6	00000000 00000180	689EF151 53554C42

```
Multiply by Q: EVAL= B7C0F88B 24B5417C

MAC-I: 38B554C0
```

5.7. Test Set 5

```
COUNT-I      = 296F393C
FRESH        = 6B227737
DIRECTION    = 1
IK           = F4 EB EC 69 E7 3E AF 2E B2 CF 6A F4 B3 12 0F FD
LENGTH       = 1000 bits
MESSAGE:
10BFFF839E0C7165 8DBB2D1707E14572 4F41C16F48BF403C 3B18E38FD5D1663B
6F6D900193E3CEA8 BB4F1B4F5BE82203 2232A78D7D75238D 5E6DAECD3B4322CF
59BC7EA84AB18811 B5BFB7BC553F4FE4 4478CE287A148799 90D18D12CA79D2C8
55149021CD5CE8CA 0371CA04FCCE143E 3D7CFEE94585B588 5CAC46068B
```

K_0	K_1	K_2	K_3
B3 12 0F FD	B2 CF 6A F4	E7 3E AF 2E	F4 EB EC 69

IV_0	IV_1	IV_2	IV_3
6B 22 F7 37	A9 6F 39 3C	6B 22 77 37	29 6F 39 3C

$\mathbf{z}_1$	$\mathbf{z}_2$	$\mathbf{z}_3$	$\mathbf{z}_4$	$\mathbf{z}_5$
99 14 88 47	1C 79 03 08	66 2D 90 AA	FA C5 92 D2	05 8B EA 75

```
P= 99 14 88 47  1C 79 03 08
Q= 66 2D 90 AA  FA C5 92 D2
```

i	Mi	EVAL
0	10BFFF83 9E0C7165	012195E9 7A42A6A9
1	8DBB2D17 07E14572	AA21E590 9BF9218F
2	4F41C16F 48BF403C	9102FF2C FA4C4906
3	3B18E38F D5D1663B	5243F583 1D672845
4	6F6D9001 93E3CEA8	18BC08D1 186CA669
5	BB4F1B4F 5BE82203	31D2F689 B033849E
6	2232A78D 7D75238D	33E9FCFC 7BFA4A8E
7	5E6DAECD 3B4322CF	0305A650 808ECF4E
8	59BC7EA8 4AB18811	923C4E45 E2F6BD66
9	B5BFB7BC 553F4FE4	4DEE3814 18B4C03B
10	4478CE28 7A148799	705DF239 099FB08B
11	90D18D12 CA79D2C8	AD00C27B 09065FA0
12	55149021 CD5CE8CA	52079A4B 3518C204
13	0371CA04 FCCE143E	392E7593 A8C1E40F
14	3D7CFEE9 4585B588	692A55BE F50F6B7F
15	5CAC4606 8B000000	1D034F2B EAADE93F
16	00000000 000003E8	1D034F2B EAADEAD7

```
Multiply by Q: EVAL= 039CAFDB C799E383

MAC-I: 061745AE
```

5.8. Test Set 6

This test ensures that all entries in the tables PM0, PM1, …, PM7 are correct. The message is chosen such that every entry of every table PM0, PM1, …, PM7 is used once.

```
COUNT-I      = 296F393C
FRESH        = 6B227737
DIRECTION    = 1
IK           = B3 12 0F FD B2 CF 6A F4 E7 3E AF 2E F4 EB EC 69
LENGTH       = 16448 bits
```

```
MESSAGE:
0000000000000000 0101010101010101 E0958045F3A0BBA4 E3968346F0A3B8A7
C02A018AE6407652 26B987C913E6CBF0 83570016CF83EFBC 61C082513E21561A
427C009D28C298EF ACE78ED6D56C2D45 05AD032E9C04DC60 E73A81696DA665C6
C48603A57B45AB33 221585E68EE31691 87FB0239528632DD 656C807EA3248B7B
46D002B2B5C7458E B85B9CE95879E034 0859055E3B0ABBC3 EACE8719CAA80265
C97205D5DC4BCC90 2FE1839629ED7132 8A0F0449F588557E 6898860E042AECD8
4B2404C212C9222D A5BF8A89EF679787 0CF50771A60F66A2 EE62853657ADDF04
CDDE07FA414E11F1 2B4D81B9B4E8AC53 8EA30666688D881F 6C348421992F31B9
4F8806ED8FCCFF4C 9123B89642527AD6 13B109BF75167485 F1268BF884B4CD23
D29A0934925703D6 34098F7767F1BE74 91E708A8BB949A38 73708AEF4A36239E
50CC08235CD5ED6B BE578668A17B58C1 171D0B90E813A9E4 F58A89D719B11042
D6360B1B0F52DEB7 30A58D58FAF46315 954B0A8726914759 77DC88C0D733FEFF
54600A0CC1D0300A AAEB94572C6E95B0 1AE90DE04F1DCE47 F87E8FA7BEBF77E1
DBC20D6BA85CB914 3D518B285DFA04B6 98BF0CF7819F20FA 7A288EB0703D995C
59940C7C66DE57A9 B70F82379B70E203 1E450FCFD2181326 FCD28D8823BAAA80
DF6E0F4435596475 39FD8907C0FFD9D7 9C130ED81C9AFD9B 7E848C9FED38443D
5D380E53FBDB8AC8 C3D3F06876054F12 2461107DE92FEA09 C6F6923A188D53AF
E54A10F60E6E9D5A 03D996B5FBC820F8 A637116A27AD04B4 44A0932DD60FBD12
671C11E1C0EC73E7 89879FAA3D42C64D 20CD1252742A3768 C25A901585888ECE
E1E612D9936B403B 0775949A66CDFD99 A29B1345BAA8D9D5 400C91024B0A6073
63B013CE5DE9AE86 9D3B8D95B0570B3C 2D391422D32450CB CFAE96652286E96D
EC1214A934652798 0A8192EAC1C39A3A AF6F15351DA6BE76 4DF89772EC0407D0
6E4415BEFAE7C925 80DF9BF507497C8F 2995160D4E218DAA CB02944ABF83340C
E8BE1686A960FAF9 0E2D90C55CC6475B ABC3171A80A36317 4954955D7101DAB1
6AE8179167E21444 B443A9EAAA7C91DE 36D118C39D389F8D D4469A846C9A262B
F7FA18487A79E8DE 11699E0B8FDF557C B48719D453BA7130 56109B93A218C896
75AC195FB4FB0663 9B3797144955B3C9 327D1AEC003D42EC D0EA98ABF19FFB4A
F3561A67E77C35BF 15C59C2412DA881D B02B1BFBCEBFAC51 52BC99BC3F1D15F7
71001B7029FEDB02 8F8B852BC4407EB8 3F891C9CA733254F DD1E9EDB56919CE9
FEA21C174072521C 18319A54B5D4EFBE BDDF1D8B69B1CBF2 5F489FCC98137254
7CF41D008EF0BCA1 926F934B735E090B 3B251EB33A36F82E D9B29CF4CB944188
FA0E1E38DD778F7D 1C9D987B28D132DF B9731FA4F4B41693 5BE49DE30516AF35
78581F2F13F561C0 663361941EAB249A 4BC123F8D15CD711 A956A1BF20FE6EB7
8AEA2373361DA042 6C79A530C3BB1DE0 C99722EF1FDE39AC 2B00A0A8EE7C800A
08BC2264F89F4EFF E627AC2F0531FB55 4F6D21D74C590A70 ADFAA390BDFBB3D6
8E46215CAB187D23 68D5A71F5EBEC081 CD3B20C082DBE4CD 2FACA28773795D6B
0C10204B659A939E F29BBE1088243624 429927A7EB576DD3 A00EA5E01AF5D475
83B2272C0C161A80 6521A16FF9B0A722 C0CF26B025D5836E 2258A4F7D4773AC8
01E4263BC294F43D EF7FA8703F3A4197 463525887652B0B2 A4A2A7CF87F00914
871E25039113C7E1 618DA34064B57A43 C463249FB8D05E0F 26F4A6D84972E7A9
054824145F91295C DBE39A6F920FACC6 59712B46A54BA295 BBE6A90154E91B33
985A2BCD420AD5C6 7EC9AD8EB7AC6864 DB272A516BC94C28 39B0A8169A6BF58E
1A0C2ADA8C883B7B F497A49171268ED1 5DDD2969384E7FF4 BF4AAB2EC9ECC652
9CF629E2DF0F08A7 7A65AFA12AA9B505 DF8B287EF6CC9149 3D1CAA39076E28EF
1EA028F5118DE61A E02BB6AEFC3343A0 50292F199F401857 B2BEAD5E6EE2A1F1
91022F9278016F04 7791A9D18DA7D2A6 D27F2E0E51C2F6EA 30E8AC49A0604F4C
13542E85B68381B9 FDCFA0CE4B2D3413 54852D360245C536 B612AF71F3E77C90
95AE2DBDE504B265 733DABFE10A20FC7 D6D32C21CCC72B8B 3444AE663D65922D
17F82CAA2B865CD8 8913D291A6589902 6EA1328439723C19 8C36B0C3C8D085BF
AF8A320FDE334B4A 4919B44C2B95F6E8 ECF73393F7F0D2A4 0E60B1D406526B02
2DDC331810B1A5F7 C347BD53ED1F105D 6A0D30ABA477E178 889AB2EC55D558DE
AB2630204336962B 4DB5B663B6902B89 E85B31BC6AF50FC5 0ACCB3FB9B57B663
297031378DB47896 D7FBAF6C600ADD2C 67F936DB037986DB 856EB49CF2DB3F7D
A6D23650E438F188 4041B013119E4C2A E5AF37CCCDFB6866 0738B58B3C59D1C0
248437472ABA1F35 CA1FB90CD714AA9F 635534F49E7C5BBA 81C2B6B36FDEE21C
A27E347F793D2CE9 44EDB23C8C9B914B E10335E350FEB507 0394B7A4A15C0CA1
20283568B7BFC254 FE838B137A2147CE 7C113A3A4D65499D 9E86B87DBCC7F03B
BD3A3AB1AA243ECE 5BA9BCF25F82836C FE473B2D83E7A720 1CD0B96A72451E86
3F6C3BA664A6D073 D1F7B5ED990865D9 78BD3815D06094FC 9A2ABA5221C22D5A
B996389E3721E3AF 5F05BEDDC2875E0D FAEB39021EE27A41 187CBB45EF40C3E7
```

```
3BC03989F9A30D12 C54BA7D2141DA8A8 75493E65776EF35F 97DEBC2286CC4AF9
B4623EEE902F840C 52F1B8AD658939AE F71F3F72B9EC1DE2 1588BD35484EA444
36343FF95EAD6AB1 D8AFB1B2A303DF1B 71E53C4AEA6B2E3E 9372BE0D1BC99798
B0CE3CC10D2A596D 565DBA82F88CE4CF F3B33D5D24E9C083 1124BF1AD54B7925
32983DD6C3A8B7D0
```

K_0	K_1	K_2	K_3
F4 EB EC 69	E7 3E AF 2E	B2 CF 6A F4	B3 12 0F FD

IV_0	IV_1	IV_2	IV_3
6B 22 F7 37	A9 6F 39 3C	6B 22 77 37	29 6F 39 3C

$\mathbf{z}_1$	$\mathbf{z}_2$	$\mathbf{z}_3$	$\mathbf{z}_4$	$\mathbf{z}_5$
EC 81 B3 C2	3C CF 81 87	61 F7 63 FF	4B A3 D3 7A	12 C6 F4 AC

P= EC 81 B3 C2 3C CF 81 87
Q= 61 F7 63 FF 4B A3 D3 7A

i	Mi	EVAL
0	00000000 00000000	00000000 00000000
1	01010101 01010101	E1948144 F2A1BAA5
2	E0958045 F3A0BBA4	E1948144 F2A1BAA5
3	E3968346 F0A3B8A7	C3290289 E5437551
4	C02A018A E6407652	22BD83CD 17E2CFF4

…

255	1124BF1A D54B7925	CD67C229 3C57482F
256	32983DD6 C3A8B7D0	2CF3436D CEF6F28A
257	00000000 00004040	2CF3436D CEF6B2CA

Multiply by Q: EVAL= 0559DB0A B7D8E5A3

MAC-I: 179F2FA6

<End of Document>