3GPP TSG SA WG3 Security — S3#13 S3-000362

Technical Specification

GSM Association Specification for A5/3

Requirements Specification for the GSM A5/3 Encryption Algorithm (Version 0.5)

Contents

Foreword

This GSM Association Technical Specification has been produced by a joint working party ETSI SMG10 (also part of 3GPP TSG SA WG3) and of GSM Association Security Group, known as GSM 2000.

This specification for the so-called A5/3 algorithm is intended to be a mandatory standard for GSM, in addition to the already used A5/1 and A5/2 algorithms. A5/3 shall also be capable of use for EDGE and GPRS.

This document provides a Requirements Specification for the GSM A5/3 algorithm. The appendix A gives some other conditions that may be required, but is not part of the main specification and is non-binding.

The ALGORITHM DESIGN AUTHORITY intends the specification for use, which will be responsible for the design of the algorithm.

1 Scope

This specification constitutes a requirements specification for a cryptographic GSM A5/3 algorithm that may be used as the so-called GSM A5 algorithm.

This specification is intended to provide the ALGORITHM DESIGN AUTHORITY, which will be responsible for the design of the algorithm, with the information it requires for designing and delivering a technical specification for this algorithm. The ALGORITHM DESIGN AUTHORITY shall be the GSM2000 joint working group, open to members of the GSM Association and 3GPP(1).

The specification covers the intended use of the algorithm and use of the algorithm specification, technical requirements on the algorithm, requirements on the algorithm specification and test data, and quality assurance requirements on both the algorithm and its documentation.

2 References

[1] GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions"

3 Definitions and abbreviations

3.1 Definitions

ALGORITHM DESIGN AUTHORITY	A group known as GSM2000 to supply the specifications of the GSM A5/3 algorithm. Membership open to GSMA and 3GPP(1)
GSM A5/3 algorithm	Encryption Algorithm, which fulfils the A5 functionality in GSM and which, will be made available by the GSM Association to operators of GSM systems. It should be capable of operation as A5, GPRS and EDGE as described in 03.20.

3.2 Abbreviations

BLOCK1	1st output BLOCK of algorithm
BLOCK2	2nd output BLOCK of algorithm
COUNT	COUNTer (sometimes called TDMA)
DSP	Digital Signal Processor
GSM	Global System for Mobile communications
K_c	GSM Cipher Key

4 Use of the GSM A5/3 Algorithm

This clause defines those organisations for whom the algorithm is intended, describes the application of the algorithm, and describes the types of implementations of the algorithm that are envisaged.

4.1 Use of the algorithm

The algorithm shall only be used for GSM encryption using the A5, EDGE and GPRS function as described in [1, GSM 03.20].

More specifically the use of the algorithm is as follows:

- The algorithm is used to encrypt user and signalling data over the air interface.
- The algorithm will be used for EDGE, enhanced data in GSM.
- The algorithm will be used for GPRS packet radio service in GSM.

4.2 Types of implementation

The normal method for implementing the algorithm is in hardware or DSP.

5 Functional requirements

The ALGORITHM DESIGN AUTHORITY for the algorithm is required to design an algorithm that satisfies the functional requirements specified in this section.

5.1 Type and parameters of algorithm

The type and parameters of the algorithm are identical to those of the A5 algorithm, which are specified in [1, GSM 03.20] and are summarised here.

- The algorithm is a binary key stream generator.
- The inputs are the Key K_c and a time variant parameter COUNT.
- The outputs of the ciphering algorithm are two binary blocks BLOCK1 and BLOCK2.

Relation of the input and output parameters is illustrated in figure 1.

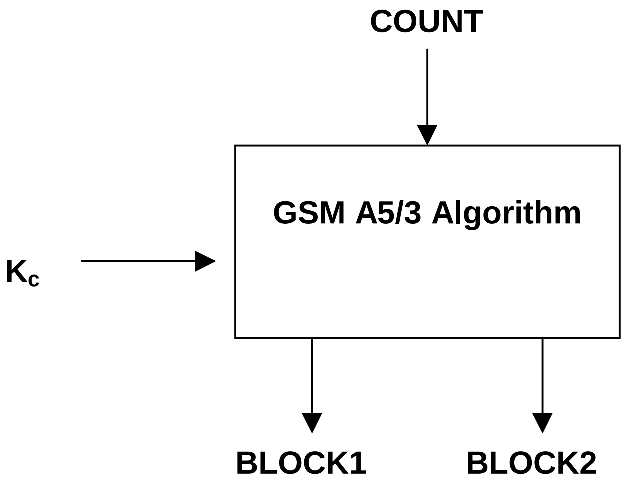

Figure 1 – Algorithm Parameters

The parameters of the algorithms are to be as follows:

K_c	64-128 bits
COUNT	22 bits 32 bits for GPRS
BLOCK1	64, 114 or 348 bits
BLOCK2	64, 114 or 348 bits

5.1.1 K_c

The encryption key (K_c) can assumed to be randomly generated unstructured data. The length of K_c is 64-128 bits. The algorithm shall thus be able to deal with variable key lengths.

5.1.2 COUNT

This input COUNT is an increasing binary counter. The length of COUNT is 22 bits and 32 bits for GPRS.

5.1.3 BLOCK1

The parameter BLOCK1 should be a random binary value with a length of 64, 114 or 348 bits. The 114 bits are in the case of regular GSM use; the 348 are in the case of use in EDGE, and 64 bits for GPRS.

5.1.4 BLOCK2

The parameter BLOCK2 should be a random binary value with a length of 64, 114 or 348 bits. The use is as in BLOCK1 above

5.1.5MODE SETTING

There may be a requirement for mode setting for the algorithm in order to instruct it to produce the appropriate output

5.2 Interfaces to the algorithm

The following interfaces to the algorithm are defined.

- **K_c:** $K_c[0]$, $K_c[1]$, ..., $K_c[k1]$ where $K_c[j]$ is the $K_c$bit with label j and $63 \leq k1 \leq 127$.
- **COUNT:** COUNT[0], COUNT[1], ..., COUNT[c1] where COUNT[j] is the COUNT bit with label and c1=21 or 31.
- **BLOCK1:** BLOCK1[0], BLOCK1[1], ..., BLOCK1[b1] where BLOCK1[j] is the BLOCK1 bit with label j and b1=64 or b1=114 or b1 =348.
- **BLOCK2:** BLOCK2[0], BLOCK2[1], ..., BLOCK2[b2] where BLOCK2[j] is the BLOCK2 bit with label j and b2=64 or b2=114 or b2=348.

5.3 Modes of operation

The mode of operation will be a key stream generation mode where, as described in the previous sections, input parameters are used to produce outputs blocks each with a length of 64 or 114 or 348 bits.

5.5 Implementation and operational considerations

Performance requirements.
The time to produce two 64 bit blocks should be max 6 msec using a 2MHz clock.
The time to produce two 114 bit blocks should be max 6 msec using a 2MHz clock.
The time to produce two 348 bit blocks should be max 10 msec using a 2MHz clock.
[Above subject to change on advice from TWG].

Implementation complexity.
It should be possible to implement the algorithm in hardware using available technology with less than 10000 gates and a layout area of less than 0.6 mm^2.

5.6 Design and evaluation principles for the algorithm

- The algorithm will be designed by the ALGORITHM DESIGN AUTHORITY shall be the GSM2000 group

- The algorithm will be openly published for public scrutiny. The DESIGN AUTHORITY will decide on the moment when to start offering and distributing the Algorithm to its members.
- A number of independent and qualified parties shall, prior to the publication, evaluate the strength of the algorithm.

The algorithm needs to be designed with a view to its continuous use for a period of at least 15 years.

The security shall be such that

- There are no known plain text attacks on the algorithm needing significantly less operations than an exhaustive key search.

6 Algorithm specification and test data requirements

The ALGORITHM DESIGN AUTHORITY are required to provide four separate deliverables: a specification of the algorithm, a set of design conformance test data, a set of algorithm input/output test data and a design and evaluation report.

6.1 Specification of the algorithm

An unambiguous specification of the algorithm needs to be provided which is suitable for use by implementers of the algorithm.

The specification shall include an annex that provides simulation code for the algorithm written in ANSI C. The specification may also include an annex containing illustrations of functional elements of the algorithm.

6.2 Design conformance test data

Design conformance test data is required to allow implementers of the algorithm to test their implementations.

The design conformance test data needs to be designed to give a high degree of confidence in the correctness of implementations of the algorithm.

The design conformance test data shall be designed so that significant points in the execution of the algorithm may be verified.

6.3 Algorithm input/output test data

Algorithm input/output test data is required to allow users of the algorithm to test the algorithm as a "black box" function.

The input/output test data shall allow users of the algorithm to perform tests for the modes of operation previously defined.

The input/output test data shall consist solely of data passed across the interfaces to the algorithm.

6.4 Format and handling of deliverables

The specification of the algorithm shall be produced on paper, and be handled according to the rules of the partners (3GPP(1) and the GSM Association).

The algorithm input/output test data shall be produced on paper and on magnetic disc.

7 Quality assurance requirements

This clause advises the ALGORITHM DESIGN AUTHORITY on measures needed to provide users of the algorithm with confidence that it is fit for purpose, and users of the algorithm specification and test data assurance that appropriate quality control has been exercised in their production.

The measures shall be recorded by the ALGORITHM DESIGN AUTHORITY in a design and evaluation report which shall be published by the as a Technical Report.

7.1 Quality assurance for the algorithm

Prior to its release, the algorithm needs to be approved as meeting the technical requirements by all members of the ALGORITHM DESIGN AUTHORITY.

7.2 Quality assurance for the specification and test data

Prior to delivery of the algorithm specification, two independent simulations of the algorithm needs to be made using the specification, and confirmed against test data designed to allow verification of significant points in the execution of the algorithm.

Design conformance and algorithm input/output test data needs to be generated using a simulation of the algorithm produced from the specification and confirmed as above. The simulation used to produce this test data needs to be identified in the test data deliverables and retained by the ALGORITHM DESIGN AUTHORITY.

7.3 Design and evaluation report

The design and evaluation report is intended to provide evidence to potential users of the algorithm, specification and test data that appropriate and adequate quality control has been applied to their production. The report shall explain the following:

- the algorithm and test data design criteria;
- the algorithm evaluation criteria;
- the methodology used to design and evaluate the algorithm;
- the extent of the mathematical analysis and statistical testing applied to the algorithm;
- the principal conclusions of the algorithm evaluation;
- the quality control applied to the production of the algorithm specification and test data.

The report shall confirm that all members of the ALGORITHM DESIGN AUTHORITY have approved the algorithm, specification and test data.

8 Summary of the ALGORITHM DESIGN AUTHORITY deliverables

- Specification of the algorithm:
    - a document for delivery only to the custodians of the algorithm;

- Design conformance test data:
    - a document for delivery only to the custodians of the algorithm;

- Algorithm input/output test data:
    - in a document and on disc for delivery to the custodians of the algorithm;

- Design and evaluation report;
    - to be published as a Technical Report.

Annex A (informative): Possible non-technical issues

Places of use

There may be possible geographical/geopolitical restrictions on the use of equipment, which embodies the algorithm, because of possible export requirements of cryptographic algorithms in some countries.

Ownership

It is expected that the algorithm will be jointly owned by 3GPP(1) and GSM Association, as in the case of the GPRS algorithms GEA-1 and GEA-2. As the GSMA is an industry partner of 3GPP(1) this issue will need to be resolved.

Intellectual Property

It is desirable that the algorithm will be free of intellectual property considerations to aid free distribution

Annex B (informative): History

Document history		
Version 0.1	January 2000	First draft for review by GSM Security 2000 group
Version 0.3	April 2000	Draft version for S3#12
Version 0.4	April 2000	Draft version produced after S3#12
Version 0.5	May 2000	Draft produced after GSM2000 No.7 in London, for presentation at S3#13 24-6 May Yokohama, Japan. Informative requirements moved to appendix.