3GPP Cipher

Report to 3GPP PCG

Sophia Antipolis

7th July 1999

Professor Michael Walker

Chairman 3GPP SA3 (Security)

vodafone

Why do we need a new Cipher?

- Key length of GSM A5 (54 bits) is no longer adequate - for example DES keys of 56 bits can be found using exhaustive search in a few hours
- A5 parameters are not appropriate for UTRAN - different message key (frame count), variable length of bit stream output
- Additional functionality needed - integrity mode
- More future proof - newer design techniques

How should we design the Cipher?

- SA 3 considered the design process and reported in *Criteria for cryptographic algorithm design process*
- Strong demand for a more open process than that adopted for GSM - some would like an entirely independent & open design and evaluation process
- Compromise position taken - takes account of time scale & export issues, uses process that has served us well, introduces independence and openness

Cipher Algorithm Design, 1

- SA3 to generate algorithm requirements
- Requirements to ETSI SAGE
- SAGE to establish design and internal evaluation team - individuals from outside core SAGE group to be co-opted where they enhance expertise (foreseen in SAGE TOR)
- SAGE design or select algorithm and perform their evaluation - security, implementation, exportability

Cipher Algorithm Design, 2

- As part of design process SAGE will consult with national authorities who are responsible for export approval (UK, D, NL, F, SE) - they always do this
- I propose to re-join SAGE to help with export approval issues, especially US (who are always involved), Japan, Korea & (if possible) China
- *Initial indications are that national authorities in Europe are more relaxed about the cipher strength than they were for GSM - the world moves on*

Cipher Algorithm Design, 3

- SA 3 commission a private external expert evaluation of the SAGE algorithm
- External experts report back directly to SAGE
- SAGE complete design and evaluation
- Design and evaluation report prepared by SAGE for SA3 - this will not address design principles but demonstrate that the design and evaluation was properly undertaken

Cipher Algorithm Design, 4

- Algorithm specification and test data (needed for implementation) completed by SAGE and delivered to ETSI for release to manufacturers - this is the *definitive* specification (subject to version control)
- Publish description for public *scrutiny* - this will run in parallel with implementation phase
- Process for responding to public criticism needed

Status of Algorithm Design

- Process for algorithm design approved at SA # 3
- PCG informed of process by letter 24 May, and funding (Euro 330,000) requested
- SAGE able to start work in principle in July & deliver at end of year - candidate algorithms already under consideration, but urgent to start officially
- Two new co-opted members of SAGE being considered - strong candidate from Japan

Open Issues

- Provision of funds
- Ownership, liability and licensing in a quasi-open environment - not a first (IBM did the same with DES) but ETSI (?) legal department needs to get involved now

vodafone