

Working of A5/1 Algorithm







Introduction

- A5/1 is a stream cipher used to provide over-the-air communication privacy in the GSM cellular telephone standard.
- A GSM transmission is organized as sequences of *bursts*.
- In a typical channel and in one direction, one burst is sent every 4.615 milliseconds and contains 114 bits available for information.
- A5/1 is based around a combination of three linear feedback shift registers (LFSRs) with irregular clocking.
- A5/1 uses symmetric cryptography.



Initialization Phase

- It uses three linear shift registers (LFSR) that are initialized to zero.
- LFSR 1 (R1):
 - Length 19 bits
 - Clocking bit: 8
 - Tapped bits: 13, 16, 17, 18
- LFSR 2 (R2):
 - Length 22 bits
 - Clocking bit: 10
 - Tapped bits: 20, 21
- LFSR 1 (R3):
 - Length 23 bits
 - Clocking bit: 10
 - Tapped bits: 7, 20, 21, 22

- 
- 
- Registers are clocked $64 + 22$ times ignoring irregular clocking.
 - Key bits of a 64 bits session key followed by 22 bit frame counter are consecutively XORed in parallel to the feedback of all three registers which is generated by XORing the tapped bits of respective registers.
 - The session key is generated by an algorithm that is saved on SIM.
 - Frame counter indicates number of the actual frame that is being ciphered. One frame is 228 bits long.



Warm-Up Phase

- Registers are clocked 100 times with irregular clocking.
- Irregular clocking follows the majority rule.
- Maj function:- This function determines from three binary inputs whether 1's are more or 0's are more. As there are three values no chances of a tie.
- Majority bit is determined based on clocking bits of the registers.
- If the clocking bit of the register is same as the majority bit, the register is clocked.
- Output of the registers is ignored.



Key Stream Generation

- Initialization of registers is complete.
- Registers are clocked with irregular clocking.
- Irregular clocking follows the same majority rule.
- Output of each register(MSBs) is XORed to produce key Stream.
- The key stream that was produced in previous step is now XORed with bits of plain text to create cipher text.