

Mobile Phone Communication

Hoang Vo
Billy Ngo

Wireless Network

•Analog Network

- Advance Mobile Phone System (AMPS)
- Nordic Mobile Telephone (NMT)
- Total Access Communication System (TACS).

•Digital Network

- GSM
- 3GPPP Protocol

Analog Authentication

- MIN/ESN Protocol
 - MIN: Mobile Identify Number, 10 digits
 - ESN: Electronic Serial Number, 32 bits
 - Clear transmission
- Attack
 - Simple police frequency scanner.
 - Prone to eavesdropping
 - Cloning

Cellular Phone Cloning

- The “cloning” of a cellular telephone occurs when the account number of a victim telephone user is stolen and reprogrammed into another cellular telephone.
- Each cellular phone has a unique pair of identifying numbers: the electronic serial number (“ESN”) and the mobile identification number (“MIN”).
- The ESN/MIN pair can be cloned in a number of ways without the knowledge of the carrier or subscriber through the use of electronic scanning devices.

Cellular Phone Cloning Cont.

- After the ESN/MIN pair is captured, the cloner reprograms or alters the microchip of any wireless phone to create a clone of the wireless phone from which the ESN/MIN pair was stolen.
- The entire programming process takes ten-15 minutes per phone.
- After this process is completed, both
- phones (the legitimate and the clone) are billed to the original, legitimate account.

Analog (cont.)

• Counter Measures

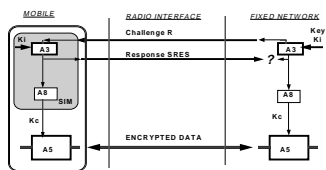
- Duplicate Detection
- Velocity trap
- RF fingerprinting
- Usage profiling
- Call counting
- Pin code

Eavesdropping

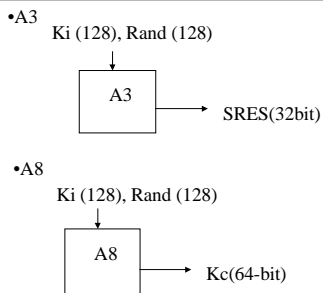
- Eavesdropping means to overhear, record, amplify or transmit any part of the private discourse of others without the permission of all persons engaged in the discourse.
- Use of cellular phone ESN readers or police scanners can be used for eavesdropping on cell phone conversations.

GSM Authentication

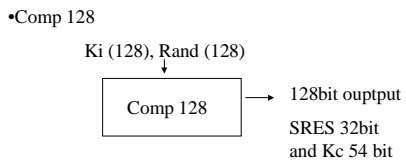
- Encryption algorithms:
 - A3 - Authentication algorithm.
 - A5 - Encryption and Decryption
 - A8 - Key generator
- Currently COMP 128 algorithm is used as the A3/A8 implementation in most GSM network



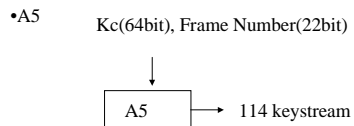
GSM authentication



GSM (cont.)



GSM(cont..)



GSM(cont.)

- A5(cont.)
 - consist of three LFSRs of length 19, 22, and 23, which are clocked based on the middle bits of the register
 - Output of Three LFSRs are XOR
- Attacks on A5
 - Brute-Force - time complexity 2^{64}
 - Divide and conquer attack- reduce the complexity to 2^{45}

Cell Phone Tracking

- Every cellular telephone is a physical locating device!
- This is generally true even when the user is not in a call. The phone need merely be switched on.
- Location tracking is inherent in the way cellular telephones work. The network needs to know (approximately) where you are in order to do its job.
- There is no known way to avoid revealing your location when you use a cell phone.

3GPP (3rd Generation Partnership Project)

- In the last few years, GSM took a lot of flak for their approach to crypto algorithm design, which relied on keeping the algorithms secret.
- 3GPP has chosen a superior approach to their crypto requirements.
- They are making open to the public all of their drafts, standards and recommendations, and rely on their algorithms withstanding the scrutiny of any interested researchers.

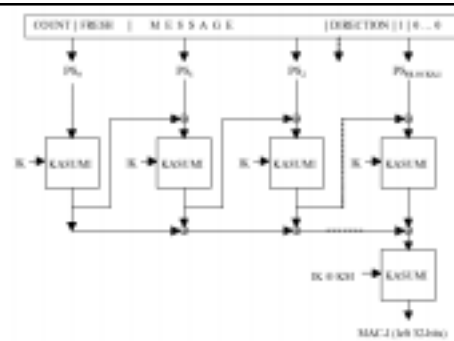


Figure 2: Integrity function

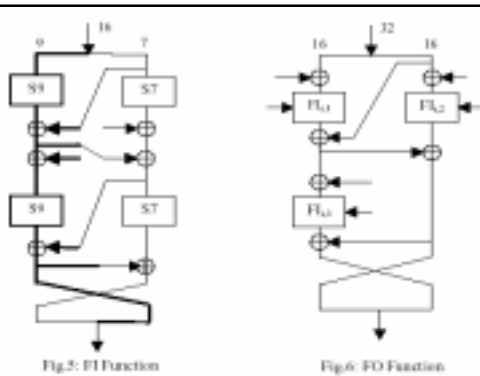


Fig.5: FI Function

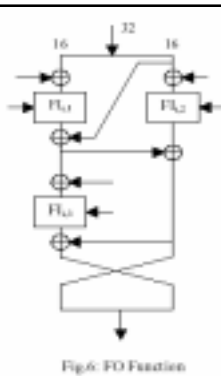


Fig.6: FO Function

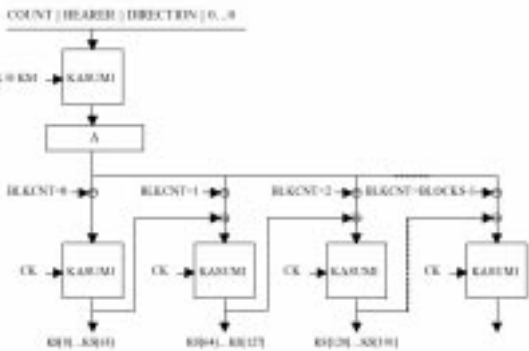


Figure 1: Keystream Generator