

List of Tables

Table No.	Details	Page No.
2.1	Comparison of 2G and 3G mobile networks	17
6.1	MATLAB implementation of function f8-sample output	65
6.2	MATLAB implementation of function f9-sample output	65
6.3	MATLAB profile report summary for AES	68
6.4	MATLAB profile report summary for f8	69
6.5	MATLAB profile report summary for f9	71
6.6	DSP Simulator analysis without optimization	74
6.7	DSP Simulator analysis with optimization level -o3	74
6.8	Different levels of optimization for f8	74
6.9	File level optimization for f9 with variable message lengths	75
6.10	DSP Emulator analysis-optimization level -o3	75
6.11	Encryption throughput calculation based on emulator CPU cycles (speed most critical)	75
6.12	Profile Summary for Codesizetune	85
6.13	DSP/BIOS - CPU peak load	85
7.1	KASUMI test data	98
7.2	F8 test data	100
7.3	F9 test data	101
7.4	Throughput for KASUMI, f8 and f9	106
8.1	USIM Authentication and key agreements-data elements	110
8.2	USIM Authentication and key agreements-cryptographic functions	113
8.3	UE- User identity confidentiality -Data elements	114
8.4	UE -Data confidentiality -Data elements	115
8.5	UE -Data confidentiality - cryptographic functions	116
8.6	UE- Data integrity -data elements	117
8.7	UE- Data integrity -cryptographic functions	118
8.8	RNC -Data confidentiality -Data elements	119
8.9	RNC -Data confidentiality - cryptographic functions	119
8.10	RNC- Data integrity-Data elements	121
8.11	RNC- Data integrity- cryptographic functions	121
8.12	VLR- User identity confidentiality -Data elements	122
8.13	SGSN- User Identity confidentiality- Data elements	122
8.14	Composition of an Authentication vector	123
8.15	VLR/SGSN -Authentication and key agreement-Data elements	124
8.16	VLR/SGSN Authentication and Key agreement - Cryptographic functions	124
8.17	HLR/AuC - Authentication and key agreement- Data elements	125
8.18	Composition of an authentication token for synchronization failure message	126
8.19	HLR/AuC -Authentication and key agreement-cryptographic function	128