Background 3GPP/GSMA Algorithms

Algorithms for authentication and key generation:

Cipher	Proprietary	Proprietary	Proprietary	AES	Keccak
Input key size	128	128	128	128	128, 256
Output key size	54	54	64	128	128, 256
Name	COMP-128-1	COMP-128-2	COMP-128-3	MILENAGE	Tuak

Algorithms for encryption and integrity: (*A5/2 and GEA1 are export ciphers with no more than 40 bits effective security):

Cipher	Proprietary	Proprietary	KASUMI	KASUMI	KASUMI	SNOW 3G	SNOW 3G	AES	AES	ZUC	ZUC
Key size	64*	64	64	128	128	128	128	128	128	128	128
Mode	XOR	XOR	f8-mode	f8-mode	CBC-MAC	XOR	CW-MAC1	CTR	CMAC	XOR	CW-MAC2
Type	ENC	ENC	ENC	ENC	INT	ENC	INT	ENC	INT	ENC	INT
Tag size					32		32		32		32
GSM	A5/2	A5/1	A5/3	A5/4							
GPRS	GEA1	GEA2	GEA3	GEA4	GIA4	GEA5	GIA5				
UMTS				UEA1	UIA1	UEA2	UIA2				
LTE						128-EEA1	128-EIA1	128-EEA2	128-EIA2	128-EEA3	128-EIA3
NR						128-NEA1	128-NIA1	128-NEA2	128-NIA2	128-NEA3	128-NIA3