Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 4, April 2017, pg.385 – 388

Review Paper on Cryptosystems used in Cellular Networks

Basavaraj P.Halagali[1], Veena V.Desai[2]

[1]Department of Electronics and Communication, Visvesvaraya Technological University, India
[2]Department of Electronics and Communication, Visvesvaraya Technological University, India
[1] basavhp.gkk@gmail.com; [2] veenadesai@git.edu

Abstract- Nowadays, people are moving from laptop with internet connection to Mobiles for e-commerce. It may be banking transaction, online purchases, chat, SMS, MMS, recharges, file sharing or the least voice communication, they are relying on a Cellular phone or a Smart Phone. The security problems faced by cellular networks are Authenticity, Integrity and Confidentiality. This paper reviews the existing ciphers of the present cellular networks. The ciphers presented in this paper are MISTY-1, KASUMI, SNOW 3G, ZUC and AES. These ciphers are briefly explained and the necessary modifications for making them more secure are proposed. It is intended to use chaos theory for the proposed modifications.

Keywords- SMS; MMS; KASUMI; SNOW 3G; ZUC; AES; MISTY-1

I. INTRODUCTION

A variety of cellular networks were developed over the years consisting of 1G, 2G, 2.5G, 3G & 4G. Different technologies like TDMA, CDMA, GSM, EDGE, HSPDA, UTMS and the new technology LTE were designed for cellular networks. The overall aim is to increase the data rate for high speed communication. All these technologies use one or other security system for their protection. Several of these security systems are attacked using Sandwich cryptanalysis, Sliding property technique, Differential cryptanalysis, Biclique cryptanalysis etc. It is required to solidify these security systems (Cryptosystems) to enhance their strength against cryptanalysis. The present cryptosystems of cellular networks are briefed below.

II. MISTY-1 CIPHER

The block cipher MISTY1 was designed by Matsui and published in 1997. MISTY-1 is a block cipher with 128 bit key and 64 bit input and output. The core of MISTY-1 is an eight-round Feistel network built around a 32-bit nonlinear Boolean function FO. FO is a round function which itself uses 3 round Feistel network containing a 16-bit nonlinear function FI. The function FI, on its turn, consists of a similar 3-round ladder network, using 7 ×7-bit and 9 ×9-bit S-boxes called S_7 and S_9.

It became a CRYPTREC e-government recommended cipher in 2002, and a NESSIE selected block cipher in 2003, and was adopted as an ISO international standard in 2005 and 2010. The cryptanalysis attack on MISTY-1 is through related-key differential and related-key amplified boomerang attacks under certain weak key assumptions

III. KASUMI CIPHER

KASUMI cipher is a minor modification to the original cipher MISTY-1. KASUMI is a block cipher used in UMTS, GSM and GPRS mobile communication systems. In UMTS, KASUMI is used in the confidentiality (f8) and integrity algorithms (f9) with names UEA1 and UIA1 respectively. In GSM, KASUMI is used in the A5/3 key stream generator and in GPRS in the GEA3 key stream generator. KASUMI was designed for 3GPP to be used in UMTS security system by the Security Algorithms Group of Experts (SAGE), a part of the European standards body ETSI. The original MISTY-1 algorithm was slightly modified for easier hardware implementation and to meet other requirements set for 3G mobile communications security.

KASUMI is a block cipher with 128-bit key and 64-bit input and output. The core of KASUMI is an eight-round Feistel network. The round functions in the main Feistel network are irreversible Feistel-like network transformations. In each round the round function uses a round key which consists of eight 16-bit sub keys derived from the original 128-bit key using a fixed key schedule.

Difference between MISTY-1 and KASUMI is the expansion of the key. The key schedule consists of cyclical network of nonlinear FI-functions in the case of MISTY-1, but is completely linear in KASUMI.

IV. SNOW 3G CIPHER

SNOW 3G is a stream cipher algorithm that had been conceived and chosen in 2006 as the heart of the second set of UMTS condentiality and integrity algorithms. It has been kept as the engine of the rst set of LTE cryptographic algorithms as well.

SNOW 3G stream cipher is a two components stream cipher with an internal state of 608 bits initialized by a 128-bit key and a 128-bit initialization vector IV. SNOW 3G consists of two interacting modules, a Linear Feedback Shift Register (LFSR) and a Finite State Machine (FSM). The LFSR is constructed from 16 stages, each holding 32 bits and the feedback is defined by a primitive polynomial over the finite field $GF(2^{32})$. The FSM is based upon three 32-bit registers R1, R2 and R3 and uses two substitution box ensembles S1 and S2. The mixing operations are exclusive OR and addition modulo 2^{32}.

V. ZUC CIPHER

ZUC is a stream cipher designed by the Data Assurance and Communication Security Research Center (DACAS) of the Chinese Academy of Sciences. The cipher forms the core of the 3GPP mobile standards 128-EEA3 (for encryption) and 128-EIA3 (for message integrity). It was proposed for inclusion in the Long Term Evolution (LTE) or the 4th generation of cellular wireless standards (4G). ZUC is LFSR-based and uses a 128-bit key and a 128-bit initialization vector (IV).

The algorithm has three parts or "layers" – a linear feedback shift register (LFSR) layer, a bit-reorganisation ("BR") layer and a nonlinear function F. The execution of the algorithm proceeds in two stages – an initialization stage and a "working" stage. Each iteration of the algorithm in the working stage generates 32 bits of keystream output.

ZUC is a word-oriented stream cipher. It takes a 128-bit initial key and a 128-bit initial vector (IV) as input, and outputs a keystream of 32-bit words (where each 32-bit word is hence called a key-word). This keystream can be used

for encryption/decryption. The 32×32 S-box S is composed of 4 juxtaposed 8×8 S-boxes, i.e., S=(S0,S1,S2,S3), where S0=S2, S1=S3.

The execution of ZUC has two stages: initialization stage and working stage. In the first stage, a key/IV initialization is performed, i.e., the cipher is clocked without producing output. The second stage is a working stage. In this stage, with every clock pulse, it produces a 32-bit word of output.

The vulnerability in ZUC is due to the non-injective property in the initialization, which results in the difference in the initialization vector being cancelled.

VI. AES CIPHER

AES is based on a design principle known as a substitution-permutation network, a combination of both substitution and permutation. AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.

AES operates on a 4 × 4 column-major order matrix of bytes, termed the *state*. Most AES calculations are done in a particular finite field.

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The number of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key. There are four different rounds used by AES viz.,

1. SubBytes - a non-linear substitution step where each byte is replaced with another according to a lookup table.
2. ShiftRows - a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
3. MixColumns - a mixing operation which operates on the columns of the state, combining the four bytes in each column.
4. AddRoundKey - each byte of the state is combined with a block of the round key using bitwise XOR.

The only successful published attacks against the full AES were side-channel attacks on some specific implementations. Side channel attacks do not attack the cipher as a black box, and thus are not related to cipher security as defined in the classical context, but are important in practice. They attack implementations of the cipher on hardware or software systems that inadvertently leak data.

VII. CHAOS THEORY

Chaos theory incepted in 1960 by Lorenz has not been utilized till today in generating randomness in cryptosystems. Lorenz equations define a three-dimensional system of ordinary differential equations that depends on three real positive parameters. As we vary the parameters, we change the behavior of the flow determined by the equations. For some parameter values, numerically computed solutions of the equations oscillate, apparently forever, in the pseudo-random way we now call "chaotic".

In addition, there are some parameter values for which we see "preturbulence", a phenomenon in which trajectories oscillate chaotically for long periods of time before finally settling down to stable stationary or stable periodic behaviour, others in which we see "intermittent chaos", where trajectories alternate between chaotic and apparently stable periodic behaviours, and yet others in which we see "noisy periodicity", where trajectories appear chaotic though they stay very close to a non-stable periodic orbit.

VIII. PROPOSED WORK

As we have seen from the above discussion, for the cryptosystems to work they rely on diffusion, confusion and permutation properties. They use key schedule, sub key generation and substitution boxes. Most of them use fiestel structures, LFSRs etc. to generate randomness. Here we propose chaos equations for randomness generation. The existing cryptosystems in cellular networks will be envisaged and the flaws in the system are picked and if necessary suitable modifications will be made using chaos theory. After developing the modified system, it is benchmarked against the existing algorithms on suitable parameters. The modified algorithms are put to cryptanalysis for performance evaluation. Further the study aims at developing a new cryptosystem of our own and comparing with the existing systems on different parameters and as well as put to cryptanalysis for betterment in security systems.

REFERENCES

[1] Van der Arend, P. J. C., *Security Aspects and the Implementation in the GSM System*, Proceedings of the Digital Cellular Radio Conference, Hagen, Westphalia, Germany, October, 1988.
[2] Biala, J., *Mobilfunk und Intelligente Netze*, Friedr., Vieweg & Sohn Verlagsgesellschaft, 1994.
[3] Cooke, J.C.; Brewster, R.L., *Cyptographic Security Techniques for Digital Mobile Telephones*, Proceedings of the IEEE International Conference on Selected Topics in Wireless Communications, Vancouver, B.C., Canada, 1992.
[4] European Telecommunications Standards Institute, Recommendation GSM 02.09, "Security Aspects".
[5] European Telecommunications Standards Institute, Recommendation GSM 02.17, "Subscriber Identity Module".
[6] European Telecommunications Standards Institute, Recommendation GSM 03.20, "Security Related Network Functions".
[7] Hodges, M.R.L., *The GSM Radio Interface*, British Telecom Technology Journal, Vol. 8, No. 1, January 1990
[8] Hudson, R.L., *Snooping versus Secrecy*, Wall Street Journal, February 11, 1994
[9] Schneier, B., *Applied Cryptography*, J. Wiley & Sons, 1994.
[10] Williamson, J., *GSM Bids for Global Recognition in a Crowded Cellular World*, Telephony, vol. 333, no. 14, April 1992
[11] 3GPP, 2009. *Security architecture*. 3GPP TS 33.102, Version 9.1.0.
[12] 3GPP2, 2008. *Enhanced cryptographic algorithms*. 3GPP2 S.S0055-A, Version 4.0. Qualcomm Incorporated, USA.
[13] 3GPP2, 2010. *Over-the-air service provisioning of mobile stations in spread spectrum standards*. 3GPP2 C.S0016-D, Version 1.0.
[14] Barker, E., W. Barker, W. Burr, W. Polk and M. Smid, 2007. *Recommendation for key management-part 1*: General (Revised). NIST, Special Publication 800-57, March, 2007.
[15] Blumenthal, U., M. Marcovici, S. Mizikovsky, S. Patel, G.S. Sundaram and M. Wong, 2002. *Wireless network security architecture*. Bell Labs Technical Journal.
[16] Chou, W., 2003. *Elliptic curve cryptography and its applications to mobile devices*. University of Maryland, College Park.
[17] De Vriendt, J., P. Laine, C. Lerouge and X. Xu, 2002. *Mobile network evolution: A revolution on the move*. Wireless Communication
[18] Harte, L., M. Hoenig, D. McLaughlin and R. Kta, 1999. *CDMA IS-95 for Cellular and PCS*. 1st Edn., McGraw-Hill Publisher, New York, ISBN: 978-0070270701
[19] Kalra, S. and S.K. Sood, 2011. *Elliptic curve cryptography: Survey and its security applications*. Proceedings of the International Conference on Advances in Computing and Artificial Intelligence, Rajpura/Punjab, India, July 21-22, 2011, ACM, New York, USA.,
[20] Lauter, K., 2004. *The advantages of elliptic curve cryptography for wireless security*. IEEE Wireless Communication
[21] Law, L., A. Menezes, M. Qu, J. Solinas and S. Vanstone, 1998. *An efficient protocol for authenticated key agreement.* Technical Report, CORR 98-05, Department of CO., University of Waterloo.
[22] Mun, H., K. Han and K. Kim, 2009. *3G-WLAN interworking: Security analysis and new authentication and key agreement based on EAP-AKA*. Proceedings of the Wireless Telecommunications Symposium, April 22-24, 2009, Prague, Taiwan.
[23] Perez, F.A., 2004. *Security in current commercial wireless networks: A survey*. School of Electrical and Computer Engineering, Purdue University West Lafayette.
[24] Rohini, P.P., 2004. *Over-the-air provisioning in CDMA*. Gemplus Technologies, October 2004.

