{tag} {/tag}
International Journal of Computer Applications

Volume 85 - Number 2

Year of Publication: 2014

Authors:
Hazem M. El Bakry

Ali E. Taki_el_deen

Ahmed Hussein Ali El Tengy

10.5120/14810-2635
{bibtex}pxc3892635.bib{/bibtex}

Abstract

SMS/Multimedia messages are one of the popular ways of communication. Sending an SMS/MMS is cheap, fast and simple. Because of mobile networks attack or smartphones hackers, the GSM networks are not secure, so that all information or SMS/MMS messages are vulnerable. This paper describe an android application that helps the user to encrypt the message (SMS/Multimedia files) before it is transmitted over the mobile network. The new idea of the program is to transmit encrypted messages and multimedia files via mobile networks or the internet as an alternative mean. To maintain intensive security, the program uses a Hybrid encryption algorithm based on Blowfish and S-Boxes of DES encryption. Moreover, it uses a private key encrypts the files and another private key encrypts file name. The transferring media is maintained online in the absence of mobile network coverage.

References

- Chin, E. , Felt, A. P. , Greenwood, K. , and Wagner, D. "Analyzing

Inter-Application Communication in Android". In Proc. of the Annual International Conference on Mobile Systems, Applications, and Services (2011).

- Marko Hassinen, "SafeSMS - End-to-End Encryption for SMS Messages", IEEE International Conference on Telecommunications, 2008, 359-365.
- S. Jahan, M. M. Hussain,M. R. Amin and S. H. Shah Newaz, "A Proposal for Enhancing the Security System of Short Message Service in GSM", IEEE International Conference on Anti-counterfeiting Security and Identification, 2008, 235-240.
- Mary Agoyi and Devrim Seral, "SMS Security: An Asymmetric Encryption Approach", IEEE International Conference on Wireless and Mobile Communications, 2010, 448-452.
- P. Traynor, W. Enck, P. McDaniel and T. La Porta. "Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks", IEEE/ACM Transactions on In Networking, 17(1):40-53, 2009.
- Mary Agoyi, Devrim Seral, "SMS Security: An Asymmetric Encryption Approach", Sixth International Conference on Wireless and Mobile Communications, 2010 IEEE, pp 448-452.
- Ferguson, N. , Schneier, B. and Kohno, "Cryptography Engineering: Design Principles and Practical Applications", T. Indianapolis: Wiley Publishing, Inc. 2010.
- Roland Schloglhofer, "Secure and Usable Authentication on Mobile Devices", MoMM2012, 3-5 December, 2012, Bali, Indonesia. ACM 978-1-4503-1307-0/12/12 (pp 257-262).
- M. Toorani and A. A. Behesti, "SSMS – A Secure SMS Messaging Protocol for the M-Payment Systems", IEEE Symposium on Computers and Communications, 2012, 700-705.
- Marko Hassinen, "SafeSMS- End-to-End Encrption for SMS Messages", IEEE International Conference on Telecommunications, 2008, 359-365.
- Kuo-Tsang Huang, Jung-Hui Chiu, and Sung-Shiou Shen, "A Novel Structure with Dynamic Operation Mode for Symmetric-Key Block Ciphers". International Journal of Network Security & Its Applications (IJNSA) 5 (1): 19, (January 2013).
- Mary Agoyi and Devrim Seral, "SMS Security: An Asymmetric Encyrption Approach", IEEE International Conference on Wireless and Mobile Communication, 2010, 448-452.
- Jawahar Thakur and Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, (ISSN 2250-2459, Volume 1, Issue 2, December 2011)
- Dripto Chatterjee, Joyshree Nath, Soumitra Mondal, Suvadeep Dasgupta and Asoke Nath, " Advanced Symmetric key Cryptography using extended MSA method: DJSSA symmetric key algorithm", Jounal of Computing, Vol 3, issue-2, Page 66-71, Feb(2011).
- Trisha Chatterjee, Tamodeep Das, Joyshree Nath, Shayan Dey and Asoke Nath, "Symmetric key cryptosystem using combined cryptographic algorithms- generalized modified vernam cipher method, MSA method and NJJSAA method: TTJSA algorithm", Proceedings of IEEE International conference: World Congress WICT-2011 t held at Mumbai University 11-14 Dec, 2011, Page 1179-1184(2011).
- Somdip Dey, Asoke Nath, "Modern Encryption Standard (MES) Version-I: An Advanced Cryptographic Method", Proceedings of IEEE 2nd World Congress on

Information and Communication Technologies (WICT- 2012), pp. 242-247.

- Dripto Chatterjee, Joyshree Nath, Sankar Das, Shalabh Agarwal and Asoke Nath, "Symmetric key Cryptography using modified DJSSA symmetric key algorithm", Proceedings of International conference Worldcomp 2011 held at LasVegas 18-21 July 2011, Page-306-311, Vol 1(2011).
- E. Barker and A. Roginsky, "Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes", NIST SP 800-131, 2010, Technical Report.
- Somdip Dey, Joyshree Nath, Asoke Nath, "An Integrated Symmetric Key Cryptographic Method - Amalgamation of TTJSA Algorithm, Advanced Caeser Cipher Algorithm, Bit Rotation and reversal Method : SJA Algorithm", International Journal of Modern Education and Computer Science (IJMECS), ISSN: 2075- 0161 (Print), ISSN: 2075-017X (Online), Vol 4, No 5, Page 1- 9, 2012.
- Debanjan Das, Joyshree Nath, Megholova Mukherjee, Neha Chaudhury and Asoke Nath, "An Integrated symmetric key cryptography algorithm using generalized vernam cipher method and DJSA method: DJMNA symmetric key algorithm", Proceedings of IEEE International conference: World Congress WICT-2011 to be held at Mumbai University 11-14 Dec, 2011, Page 1203-1208(2011).
- Jiao Wentao, "Cloud computing environments cryptographic applications", Chinese Association for Cryptologic Research, vol. 5, no. 1, pp. 20-29, 2011.
- Satyaki Roy, Navajit Maitra, Joyshree Nath, Shalabh Agarwal and Asoke Nath, "Ultra Encryption Standard(UES) Version-I: Symmetric Key Cryptosystem using generalized modified Vernam Cipher method, Permutation method and Columnar Transposition method", Proceedings of IEEE sponsored National Conference on Recent Advances in Communication, Control and Computing Technology-RACCCT 2012, 29-30 March held at Surat, Page 81- 88(2012).
- Asoke Nath, Saima Ghosh, Meheboob Alam Mallik, "Symmetric Key Cryptography using Random Key generator", Proceedings of International conference on security and management (SAM'10) held at Las Vegas, USA Jull 12-15, 2010, Vol 2, Page: 239-244(2010).
- Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C",(2011).
- William E. Burr, "Data Encryption Standard", in NIST's anthology",A Century of Excellence in Measurements, Standards, and Technology: A Chronicle of Selected NBS/NIST Publications,(2000).

Index Terms

Computer Science Communications

Keywords

Cryptography Blowfish Encryption Mobile System SMS