PURWARUPA SISTEM KEAMANAN SEPEDA MOTOR MENGGUNAKAN ALGORITMA RSA, DIFFIE-HELLMAN DAN AES BERBASIS MIKROKONTROLER ARDUINO UNO

SKRIPSI

Diajukan untuk memenuhi bagian dari
syarat memperoleh gelar Sarjana Komputer
pada Departemen Pendidikan Ilmu Komputer
Program Studi Ilmu Komputer

Oleh
Andrian Anugrah Putra
1400626

PROGRAM STUDI ILMU KOMPUTER
DEPARTEMEN PENDIDIKAN ILMU KOMPUTER
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA
2019

PURWARUPA SISTEM KEAMANAN SEPEDA MOTOR MENGGUNAKAN ALGORITMA RSA, DIFFIE-HELLMAN DAN AES BERBASIS MIKROKONTROLER ARDUINO UNO

Oleh Andrian Anugrah Putra

Skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

Universitas Pendidikan Indonesia

Agustus 2019

ANDRIAN ANUGRAH PUTRA

1400626

PURWARUPA SISTEM KEAMANAN SEPEDA MOTOR MENGGUNAKAN ALGORITMA RSA, DIFFIE-HELLMAN DAN AES BERBASIS MIKROKONTROLER ARDUINO UNO

DISETUJUI DAN DISAHKAN OLEH PEMBIMBING:

Pembimbing I,

Rizky Rachman JP., M.Kom.

NIP. 197711252006041002

Pembimbing II,

Dr. Muhammad Nursalman, M.T.

NIP. 197909292006041002

Mengetahui

Ketua Departemen Pendidikan Ilmu Komputer

Lala Septem Riza, M.T., Ph.D.

NIP. 197809262008121001

PURWARUPA SISTEM KEAMANAN SEPEDA MOTOR MENGGUNAKAN ALGORITMA RSA, DIFFIE-HELLMAN DAN AES BERBASIS MIKROKONTROLER ARDUINO UNO

Oleh

Andrian Anugrah Putra — andriananugrahputra@student.upi.edu

1400626

ABSTRAK

Di Indonesia terutama di kawasan perkotaan, kendaraan merupakan salah satu alat transportasi yang tidak lepas dari kebutuhan sehari-hari, salah satu kendaraan terbanyak yaitu sepeda motor. Sepeda motor difungsikan sebagai media transportasi sehari-hari baik untuk perjalanan ketempat kerja, pasar, sekolah ataupun untuk hiburan. Sehingga sepeda motor merupakan kendaraan yang lazim atau hampir dimiliki setiap keluarga. Dengan banyaknya jumlah sepeda motor yang ada di Indonesia, jumlah pencurian sepeda motor pun bisa dibilang tinggi dibandingkan dengan kendaraan bermotor yang lainnya. Hal ini disebabkan oleh perkembangan teknologi sepeda motor yang belum maksimal dalam hal sistem keamanannya. Biasanya sistem keamanan yang disediakan pabrikan hanya terfokus pada penggunaan kunci kontak dan kunci stang. Untuk meminimalisir kasus pencurian, peneliti merancang sistem keamanan tambahan berupa mikrokontroler Arduino Uno yang dikendalikan melalui *smartphone* dengan jaringan Bluetooth. Algoritma yang digunakan pada rancangan ini yaitu RSA dan Diffie-Hellman yang merupakan *hybrid cryptosystem* berfungsi sebagai pembangkit kunci *public* dan *private*, sedangkan algoritma AES berfungsi untuk enkripsi dekripsi *password* yang dikirim oleh *smartphone* dan diterima oleh Arduino. Untuk mengetahui tingkat keamanan pada algoritma AES dilakukan beberapa pengujian antara lain *Avalanche Effect* yang dibagi menjadi dua bagian, yaitu *confusion* sebesar 50,51% dan *diffusion* sebesar 49,75%, dan pengujian *Randomness* dengan hasil yang menyatakan lolos uji keacakan. Untuk Mengetahui keamanan dari sistem yang telah dibuat maka dilakukan pengujian dengan *password guessing attack* yang menunjukan bahwa sistem yang telah dibuat tahan terhadap serangan-serangan tersebut. Untuk pengujian Bluetooth dilakukan dengan cara mengukur setiap jarak dalam satuan meter. Dengan pengujian tanpa hambatan, Bluetooth dapat mengirim dan menerima data sejauh 12 meter, sedangkan pengujian dengan hambatan hanya dapat mengirim dan menerima data kurang dari 7 meter.

Kata Kunci : Arduino Uno, Bluetooth, AES, Diffie-Hellman, RSA, *Hybrid cryptosystem*.

SECURITY SYSTEM PROTOTYPE MOTORCYCLE USING MICROCONTROLLER ARDUINO UNO BASED RSA, DIFFIE-HELLMAN AND AES ALGORITHM

Arranged by

Andrian Anugrah Putra — andriananugrahputra@student.upi.edu

1400626

ABSTRACT

In Indonesia, especially in urban areas, the vehicle is a form of transportations that can not be separated from daily needs, one of the most used vehicles are motorbikes. Motorbikes are used as daily transportation whether for travel to work, markets, schools or for entertainment. Therefore, a motorbike is a common vehicle that almost owned by every family. With a large number of motorbikes in Indonesia, the number of motorbike thefts can be considered high compared to the other forms of vehicles. This is due to the development of motorcycle technology that has not yet been maximized in terms of its security system. Usually, the security systems provided by the manufacturer only focuses on the use of ignition keys and handlebar locks. To minimize the theft cases, the researcher designed an additional security system in the form of an Arduino Uno microcontroller that is controlled via a smartphone with Bluetooth network. The algorithm used in this design is RSA and Diffie-Hellman which is a hybrid cryptosystem that functions as a public and private key generator, while the AES algorithm serves to encrypt password decryption sent by a smartphone and received by Arduino. To find out the level of security in the AES algorithm, several tests were carried out including Avalanche Effect which was divided into two parts, namely confusion by 50.51% and diffusion by 49.75%, and Randomness testing with the results that passed the randomness test. To find out the security of the system that has been created, it is tested with a guessing attack password that shows that the system has been made resistant to these attacks. Bluetooth testing was carried out by measuring each distance in meters. Test without obstacles shows that Bluetooth can send and receive the data as far as 12 meters, while test with obstacles shows that it can only send and receive data less than 7 meters.

Keywords : Arduino Uno, Bluetooth, AES, Diffie-Hellman, RSA, Hybrid cryptosystem.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

Abdel-Rehim, W. M., Ismail, I. A., & Morsy, E. (2015). Testing randomness: the original poker approach acceleration using parallel MATLAB with OpenMP. *Computer Science and Engineering*, *5*(2), 25-29.

Abdul Zabar, A. (2016). Rancang Bangun Alat Pengukur Luas Tanah Berbasis Mikrokontroler Dan Android User Interface.

Abdullah, A. M. (2017). Advanced encryption standard (aes) algorithm to encrypt and decrypt data. *Cryptography and Network Security*.

Abomhara, M., Khalifa, O. O., Zakaria, O., Zaidan, A. A., Zaidan, B. B., & O Alanazi, H. (2010). Suitability of Using Symmetric Key to Secure Multimedia Data: An Overview. *Journal of Applied Sciences*, *10*, 1656 1661.

Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman,J.A., ... & VanderSloot, B. (2015, October). Imperfect forward secrecy: How Diffie Hellman fails in practice. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 5-17). ACM.

Alani, M. M. (2010). Testing randomness in ciphertext of block-ciphers using DieHard tests. *Int. J. Comput. Sci. Netw. Secur*, *10*(4), 53-57.

Alliance, O. H. (2011). Android overview. *Open Handset Alliance*, *8*, 88-91.

Andriotis, P., Oikonomou, G., & Tryfonas, T. (2012, December). Forensic analysis of wireless networking evidence of android smartphones. In *Information forensics and security (WIFS), 2012 IEEE international workshop on* (pp. 109-114). IEEE.

Arduino, S. A. (2015). Arduino. Obtenido de Arduino Mega: http://arduino.cc/en/Main/arduinoBoardMega.

Arifin, Z. (2016). Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman. *Jurnal Informatika Mulawarman (JIM)*, *4*(3), 7 14.

Ariyus, D. (2008). *pengantar ilmu kriptografi: teori analisis & implementasi*. Penerbit Andi.

Banzi, M., & Shiloh, M. (2014). *Getting started with Arduino: the open source electronics prototyping platform*. Maker Media, Inc.

Benvenuto, C. J. (2012). Galois field in cryptography. *University of Washington*.

Bisdikian, C. (2001). An overview of the Bluetooth wireless technology. *IEEE Commun Mag*, *39*(12), 86-94.

Boehm, B. W. (1988). A spiral model of software development and enhancement. *Computer*, *21*(5), 61-72.

Briggs, M. E. (1998). An introduction to the general number field sieve.

Budiyanto, A. (2012). Pengantar Cloud Computing. *Komunitas Cloud Computing Indonesia*.

Budmar, P. (2012). Why Japanese smartphones never went global. PC World, 11.

Chandramohan, J., Nagarajan, R., Satheeshkumar, K., Ajithkumar, N., Gopinath, P. A., & Ranjithkumar, S. (2017). Intelligent Smart Home Automation and Security System Using Arduino and Wi-fi. *International Journal of Engineering And Computer Science (IJECS)*, *6*(3), 20694-20698.

Daemen, J., & Rijmen, V. (1999). AES proposal: Rijndael.

Das, S., Ganguly, S., Ghosh, S., Sarker, R., & Sengupta, D. (2016, October). A bluetooth based sophisticated home automation system using smartphone. In *Intelligent Control Power and Instrumentation (ICICPI), International Conference on* (pp. 236-240). IEEE.

Developers, A. (2015). Application fundamentals. *Accessed on March30*.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, *22*(6), 644-654.

Elgin, B. (2005). Google buys Android for its mobile arsenal. *Bloomberg Businessweek*, *16*.

El-Rabbany, A. (2002). Introduction to GPS: the global positioning system. Artech house.

Gadre, D. V. (2000). *Programming and customizing the AVR microcontroller*. McGraw-Hill Professional.

Gu, G., & Peng, G. (2010, December). The survey of GSM wireless communication system. In *Computer and Information Application (ICCIA), 2010 International Conference on* (pp. 121-124). IEEE.

Gupta, A., & Walia, N. K. (2014). Cryptography algorithms: A review. Van Tilborg, H. C., & Jajodia, S. (Eds.). (2014). *Encyclopedia of cryptography and security*. Springer Science & Business Media.

Haartsen, J. C. (2003). Bluetooth radio system. *Wiley Encyclopedia of Telecommunications*.

Haartsen, J. C., & Mattisson, S. (2000). Bluetooth-a new low-power radio interface providing short-range connectivity. *Proceedings of the IEEE*, *88*(10), 1651 1661.

Hartadi, L., & Sasmoko, D. (2015). Sistem Keamanan Kendaraan Suzuki Smash Menggunakan Atmega 8 Dengan Sensor Bluetooth HC-6 Berbasis Android. *ELKOM*, *8*(1).

Indartono, K., & Kusuma, B. A. Sistem Keamanan Kendaraan Bermotor Menggunakan Quick Response Code Berbasis Android dan Arduino.

Jobusch, D. L., & Oldehoeft, A. E. (1989). A survey of password mechanisms: Weaknesses and potential improvements. Part 2. *Computers & Security*, *8*(8), 675-689.

Katz, J., Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.

Kholilah, I., & Al Tahtawi, A. R. (2017). Aplikasi Arduino-Android untuk Sistem Keamanan Sepeda Motor. *JTERA-Jurnal Teknologi Rekayasa*, *1*(1), 53-58.

Kretzschmar, U. (2009). Aes128–ac implementation for encryption and decryption. *TI-White Paper*.

Kumar, A., & Tiwari, M. N. (2012). effective implementation and avalanche effect of AES. *International Journal of Security, Privacy and Trust Management (IJSPTM)*, *1*(3/4), 31-35.

Lee, H., Lee, K., & Shin, Y. (2009). Aes implementation and performance evaluation on 8-bit microcontrollers. *arXiv preprint arXiv:0911.0482*.

Lengkong, H. N., Sinsuw, A. A., & Lumenta, A. S. (2015). Perancangan Penunjuk Rute Pada Kendaraan Pribadi Menggunakan Aplikasi Mobile GIS Berbasis Android Yang Terintegrasi Pada Google Maps. *E-journal Teknik Elektro dan Komputer*, *4*(2), 18-25.

Liu, S., Jiang, Y., & Striegel, A. (2014). Face-to-face proximity estimationusing bluetooth on smartphones. *IEEE Transactions on Mobile Computing*, *13*(4), 811 823.

Lusiana, V. (2011). Implementasi Kriptografi pada File Dokumen Menggunakan Algoritma AES-128. *Jurnal Dinamika Informatika*, *3*(2).

Mahmoud, E. M., Abd, A., Hafez, E., & Elgarf, T. A. (2013). Dynamic AES-128 with key-dependent S-box.

Mohamed, A. A., & Madian, A. H. (2010, December). A Modified Rijndael Algorithm and it's Implementation using FPGA. In *2010 17th IEEE International Conference on Electronics, Circuits and Systems* (pp. 335 338). IEEE.

Muhammad, R. H., & Adi, R. S. (2017). Rancang Bangun Sistem Pengamanan Mobil Menggunakan ID Card Dengan Metode Radio Frequency Identification. *KOPERTIP: Jurnal Ilmiah Manajemen Informatika dan Komputer*, *1*(1), 39-44.

Munir, R. (2006). Kriptografi. *Informatika, Bandung*.

Nalwan, P. A. (2003). Panduan Praktis Teknik Antarmuka dan Pemrograman Mikrokontroler AT89C51. *Jakarta: Elex Media Komputindo Gramedia*.

Ni, X., Shi, W., & Fook, V. F. S. (2007, April). Aes security protocol implementation for automobile remote keyless system. In *2007 IEEE 65th Vehicular Technology Conference-VTC2007-Spring* (pp. 2526-2529). IEEE.

Parab, J., Shelake, V. G., Kamat, R. K., & Naik, G. M. (2007). *Exploring C for microcontrollers: A hands on approach*. Springer Science & Business Media.

Patel, R., & Kamboj, P. (2016, August). Security Enhancement of Blowfish Block Cipher. In *International Conference on Smart Trends for Information Technology and Computer Communications* (pp. 231-238). Springer, Singapore.

Patil, A. N., Tripathi, A., & Fanan, S. A. (2017). Intelligent Street-Light System using Arduino UNO. *International Journal of Engineering Science*, *10919*.

Pham, H. D., Drieberg, M., & Nguyen, C. C. (2013, December). Development of vehicle tracking system using GPS and GSM modem. In *Open Systems (ICOS), 2013 IEEE Conference on* (pp. 89-94). IEEE.

Pramstaller, N., Gurkaynak, F. K., Haene, S., Kaeslin, H., Felber, N., & Fichtner, W. (2004, September). Towards an AES crypto-chip resistant to differential power analysis. In *Proceedings of the 30th European Solid State Circuits Conference* (pp. 307-310). IEEE.

Primartha, R. (2014). Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES). *Jurnal Sistem Informasi*, *3*(2).

Ramanujam, S., & Karuppiah, M. (2011). Designing an algorithm with high Avalanche Effect. *IJCSNS International Journal of Computer Science and Network Security*, *11*(1), 106-111.

Rangaraju, S., De Vroey, L., Messagie, M., Mertens, J., & Van Mierlo, J. (2015). Impacts of electricity mix, charging profile, and driving behavior on the emissions performance of battery electric vehicles: A Belgian case study. *Applied energy*, *148*, 496-505.

Raza, M., Iqbal, M., Sharif, M., & Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. *World Applied Sciences Journal*, *19*(4), 439-444.

Reisinger, D. (2012). Worldwide smartphone user base hits 1 billion. CNET, October, 17, 8301-1035.

Rivest, D. R., Shamir, A., & Adleman, L. RSA (cryptosystem). *ArithmeticAlgorithmsAndApplications*, 19.

Sadikin, R. (2012). Kriptografi untuk keamanan jaringan. *Penerbit ANDI, Yogyakarta*.

Safaat, N. (2012). Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android. *Bandung: informatika*.

Samara, G., & Al-Raba'nah, Y. (2017). Security Issues in Vehicular Ad Hoc Networks (VANET): a survey. *arXiv preprint arXiv:1712.04263*.

Saranya, K., Mohanapriya, R., & Udhayan, J. (2014). A review on symmetric key encryption techniques in cryptography. *International Journal of Science, Engineering and Technology Research (IJSETR)*, *3*(3), 539-544.

Sasi, S. B., Dixon, D., Wilson, J., & No, P. (2014). A general comparison of symmetric and asymmetric cryptosystems for WSNs and an overview of location based encryption technique for improving security. *IOSR Journal of Engineering*, *4*(3), 1.

Sasongko, J. (2005). Pengamanan Data Informasi menggunakan Kriptografi Klasik. *Dinamik-Jurnal Teknologi Informasi*, *10*(3).

Selmane, N., Guilley, S., & Danger, J. L. (2008, May). Practical setup time violation attacks on AES. In *2008 Seventh European Dependable Computing Conference* (pp. 91-96). IEEE.

Sipayung, T. A., Khairunnisa, K., & Muslih, M. (2017). Konvergensi Rasio Keuangan Terhadap Rata-rata Industri (studi Kasus Pada Sektor Industri Otomotif Dan Komponen Yang Terdaftar Pada Bursa Efek Indonesia Periode 2013 2015). *eProceedings of Management*, *4*(3).

Sonjaya, I. (2007). Uji Homogenitas Data Iklim di Stasiun Klimatologi Banjarbaru. Stasiun Klimatologi Banjarbaru.

Stallings, W., & Tahiliani, M. P. (2014). *Cryptography and network security: principles and practice* (Vol. 6). London: Pearson.

Suryani, K. N. (2009). Algoritma RC4 Sebagai Metode Enkripsi. *Program Studi Teknik Informatika Institut Teknologi Bandung*.

Svensson, P. (2013). Smartphones now outsell ‘dumb’phones. News NZ, April.

Wahyuni, A. (2011). Keamanan Pertukaran Kunci Kriptografi dengan Algoritma Hybrid: Diffie-Hellman dan RSA. *Majalah Ilmiah Informatika*, *2*(2).

Walpole, R. E., & Myers, R. H. (1995). Ilmu peluang dan statistika untuk insinyur dan ilmuwan. *Bandung: ITB*.

Westlund, H. B. (2002). NIST reports measurable success of Advanced Encryption Standard. *Journal of Research of the National Institute of Standards and Technology*, *107*(3), 307.

Yan, J. J. (2001, September). A note on proactive password checking. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 127 135). ACM.

Zainuri, A., Wibawa, U., & Maulana, E. (2015). Implementasi *Bluetooth* HC–05 untuk Memperbarui Informasi Pada Perangkat Running Text Berbasis Android. *Jurnal EECCIS Vol*, *9*(2).