MODIFIKASI AES (*ADVANCED ENCRYPTION STANDARD*) UNTUK *LIVE CHAT* PADA *E-COMMERCE*

SKRIPSI

Diajukan untuk Memenuhi Sebagian dari Syarat untuk Memperoleh Gelar Sarjana Komputer pada Departemen Pendidikan Ilmu Komputer Program Studi Ilmu Komputer

Oleh :

Ersa Dwi Agustina

1406217

DEPARTEMEN PENDIDIKAN ILMU KOMPUTER

PROGRAM STUDI ILMU KOMPUTER

FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PENDIDIKAN INDONESIA

BANDUNG

2019

MODIFIKASI AES (*ADVANCED ENCRYPTION STANDARD*) UNTUK *LIVE CHAT* PADA *E-COMMERCE*

oleh

Ersa Dwi Agustina

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

© Ersa Dwi Agustina 2018

Universitas Pendidikan Indonesia

Januari 2019

Hak cipta dilindungi undang-undang

Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian,

Dengan dicetak ulang, difoto kopi, atau cara lainnya tanpa ijin dari penulis.

LEMBAR PENGESAHAN

MODIFIKASI AES (*ADVANCED ENCRYPTION STANDARD*) UNTUK *LIVE CHAT* PADA *E-COMMERCE*

Oleh:

Ersa Dwi Agustina

1406217

Disetujui dan Disahkan oleh :

Pembimbing I

Prof. Dr. H. Munir, M.IT.

NIP. 196603252001121001

Pembimbing II

Rizki Rachman, JP., M.Kom

NIP. 197711252006041002

Mengetahui,

Ketua Departemen Pendidikan Ilmu Komputer

Prof. Dr. H. Munir, M.IT.

NIP. 196603252001121001

PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi dengan judul "**Sistem Kriptografi *Advanced* untuk *Live Chat* pada *E-Commerce***" ini beserta seluruh isinya adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung resiko/sanksi apabila di kemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya saya ini.

Bandung, Januari 2019

Ersa Dwi Agustina

1406217

MODIFIKASI AES (*ADVANCED ENCRYPTION STANDARD*) UNTUK *LIVE CHAT* PADA *E-COMMERCE*

Oleh

Ersa Dwi Agustina – cacaeda@student.upi.edu

1406217

ABSTRAK

Penggunaan *live chat* pada *e-commerce* sebagai media komunikasi menjadi yang paling cepat pertumbuhannya dan sudah menjadi umum bagi pengguna layanan *e-commerce*. Namun, belum banyak yang mengetahui sejauh mana tingkat keamanan *live chat* pada *e-commerce*. Hal ini menjadi sangat penting, mengingat informasi yang diberikan kepada *customer service* adalah informasi yang sangat sensitif dan rahasia. Penelitian ini bertujuan untuk mengimplementasikan algoritma kriptografi Rijndael yang telah dimodifikasi ke dalam *live chat e-commerce* berbasis web, dan membandingkan tingkat keamanan kunci yang digenerate menggunakan dua teori *chaos* yang berbeda yaitu Logistic Map dan Henon Map guna memberikan perlindungan data *per-session*. Keamanan terhadap integritas data sangat penting untuk menjaga keaslian data tersebut, maka untuk menjaga keaslian data tersebut akan dienkripsi menggunakan algoritma kriptografi Rijndael 256 bits yang telah dimodifikasi dimana kunci yang akan digunakan akan di*generate* kembali oleh dua teori *chaos* yang berbeda yaitu Logistic Map dan Henon Map, dan *public key* yang digunakan akan kembali dienkripsi menggunakan algoritma kriptografi RSA guna menambah kompleksitas keamanan pesan, dan pesan yang dikirim adalah hasil *hashing* algoritma SHA-256 untuk verifikasi keaslian pesan. Hasil dari pengujian yang dilakukan menunjukkan bahwa generator kunci Henon Map memiliki nilai *Avalanche Effect* yang baik yaitu 50%, jika masukan kunci berbentuk alfanumerik. Sedangkan Logistic Map sesuai dengan penelitian terdahulu bahwa kunci yang telah di*generate* menggunakan Logistic Map memiliki tingkat keacakan yang sangat tinggi.

Kata Kunci : Kriptografi, Rijndael, SHA-256, Logistic Map, Henon Map.

MODIFICATION OF AES (ADVANCED ENCRYPTION STANDARD) FOR LIVE CHAT ON E-COMMERCE

Arrage by

Ersa Dwi Agustina – cacaeda@student.upi.edu

1406217

ABSTRACT

The use of live chat on e-commerce as a communication media has the fastest growth and common to the users of e-commerce service. This service is greatly useful to e-commerce users to exchange information about personal data. However, there are not many customers who are aware about live chat level of security on e-commerce. This is a crucial matter, as the information given to customer service on e-commerce is highly sensitive and confidential. The purpose of this research is to implement the Rijndael cryptography algorithm which has been modified into web-based live chat e-commerce, and to compare the level of security been the keys generated using two different chaos theories, which are Logistic Map and Henon Map to provide data protection in each session. Security on data integrity is fundamental to maintain the authenticity of data; therefore, to serve that purpose the data will be encrypted using 256 Rijndael cryptography algorithm which is modified in terms that the key utilized will be generated by Logistic Map and Henon Map, and the public key utilized will be encrypted using RSA algorithm to add the security complexity of the message; hence, the message delivered is the result of SHA 256 hashing algorithm. The results of the tests conducted indicate that the Henon Map key generator has a good Avalanche Effect value of 50%, if the key input is alphanumeric. While the Logistic Map is in accordance with previous research that the key that has been generated using a Logistic Map has a very high level of randomness.

Keywords: Cryptography, Rijndael, SHA-256, Logistic Map, Henon Map

DAFTAR ISI

DAFTAR PUSTAKA

Adiyasa, H., Wasito, P. S., & Adhy, S. (2014). Implementasi Algoritma Kriptografi dengan S-Box Dinamis Bergantung Pada Kunci Utama Berbasis Advanced Encryption Standard (AES). *Prosiding Seminar Nasional Ilmu Komputer Undip*.

Andrews, D. C., & Haworth, K. N. (2002). Online Customer Service Chat: Usability and Sociability Issues. *J. Internet Market*.

Arifin, Z. (2009). Studi Kasus Penggunaan Algoritma RSA sebagai Algoritma Kriptografi yang Aman. *Jurnal Informatika Mulawarman*, Vol 4 No. 3.

Arius, D. (2008). *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi.* Yogyakarta: Andi.

Ariyanto, E., Pravitasari, T. I., & Setyorini. (2008). Analisa Implementasi Algoritma Stream Cipher Sosemanuk dan Dicing dalam Proses Enkripsi Data. *Seminar Nasional Informatika*.

Arrag, S., Hamdoun, A., Abderrahim, T., & Khamlich, S. E. (2013). Implementation of Stronger AES by using Dynamic S-Box Dependent of Master Key. *Journal of Theoretical & Applied Information Technology*, Vol. 53 Issue 2, p196-204. 9p.

Chaos Theory: A Brief Introduction | IMHO. (t.thn.). Dipetik November 7, 2017, dari https://courses.seas.harvard.edu/: https://courses.seas.harvard.edu/climate/eli/Courses/EPS281r/Sources/Chaos-and-weather-prediction/1-Chaos-Theory-A-Brief-Introduction-IMHO.pdf

Elmorshidy, A., Mostafa, M. M., El-Moughrabi, I., & Al-Mezen, H. (2015). Factors Influencing Live Customer Support Chat Services: An Empirical Investigation in Kuwait. *J. theor. appl. electron. commer. res.*

Febriany, A. (2017). Protokol Keamanan Alternatif untuk Interaksi Pengguna Live Chat pada E-Commerce Berbasis Web. *Universitas Pendidikan Indonesia*.

Firdaus, H. B. (2008). Deteksi Plagiat Dokumen Menggunakan Algoritma Rabin-Karp. *Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung (ITB).*

Froehle, C. M. (2006). Service personnel, technology, and their interaction in influencing customer satisfaction. *Decision Science Institute*.

Gunawan, I. (2016). Penggunaan Brute Force Attack dalam Penerapannya pada Crypt8 dan CSA-Rainbow Tool untuk Mencari Biss. *Jurnal Nasional Informatika dan Teknologi Jaringan*, 52-55.

Hardjana, A. M. (2003). *Komunikasi Intrapersonal dan Interpersonal.* Yogyakarta: KANISIUS.

Hildamizanthi. (2011, 5 5). *http://blogs.unpad.ac.id/.* Dipetik 10 23, 2017, dari penerapan e-commerce, makalah | thumbelina: http://blogs.unpad.ac.id/hildamizanthi/2011/05/05/penerapan-e-commerce-makalah/

Ir. Rinaldi Munir, M. (2004). Advanced Encryption Standard (AES). *Bahan Kuliah ke-13 IF5054*.

Irmawati, D. (2011). Pemanfaatan Teknologi E-Commerce dalam Dunia Bisnis. *Jurnal Ilmiah Orasi Bisnis*.

Ivancevic, V. G., & Ivancevic, T. T. (2007). *High-Dimensional Chaotic and Attractor Systems.* Berlin: Springer.

Kadam, K. G., & Khaimar, P. (2015). Hybrid RSA-AES Encryption for Web Service. *International Journal of Technical Research and Applications*, 51-56.

Kumar, A., & Tiwari, N. (2012). Effective Implementation and Avanlanche Effect of AES. *International Journal of Security, Privacy and Trust Management (IJSPTM)*, Vol. 1, No 3/4.

Kurniawan, E. Y. (2014). Penerapan Teori Chaos pada Kriptografi Menggunakan Algoritma Stream Cipher dan Electronic Code Book untuk Keamanan Pesan Teks.

Kurniawan, Y. (2004). *Kriptografi Keamanan Internet dan Jaringan Komunikasi.* Bandung.

Menezes, A. J., Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Crytography.* New York: CRC Press.

Mujaddid, S. (2009). Kriptoanalisis Pada Fungsi Hash Kriptografi MD5. *Jurnal Informatika, Institut Teknologi Bandung, Bandung.*

Munir, R. (2004). Advanced Encryption Standard (AES). *Bahan Kuliah ke-13 IF5054*.

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

Munir, R., Riyanto, B., & Sutikno, S. (2006). Perancangan Algoritma Kriptografi Stream Cipher dengan Chaos.

Nugroho, E. P., Judhie Putra, R. R., & Ramadhan, I. M. (2016). SMS Authentication Code Generated by Advanced Encryption Standard (AES) 256 bits Modification Algorithm and One Time Password (OTP) to Activate New Applicant Account. *ICSITech*, 175-188.

Qiu, L., & Benbasat, I. (2005). An investigation into the effects of Text-To-Speech voice and 3D avatars on the perception of presence and flow of live help in electronic commerce. *ACM Transactions on Computer-Human Interaction (TOCHI)* .

Roskin, K. M., & Casper, J. B. (1999). From Chaos to Cryptography. http://www. gaianxaos. com/pdf/unsorted/chaos_and_cryptography. pdf.

Santoso, K. I. (2015). Metode Keamanan E-Commerce. *Jurnal Transformasi*.

Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*.

Stallings, W. (2011). *Cryptography and Network Security Principles and Practice Fifth Edition.* United States: Pearson Education, Inc.

Stallings, W. (2014). *Cryptography and Network Security.* United States: Pearson Education Inc.

Standard, N. (2001). *Announcing the Advanced Encryption Standard(AES).* Federal Information Processing Standards Publication.

Surian, D. (2006). Algoritma Kriptografi AES Rijndael. *TESLA Jurnal Teknik Elektro*, 97-101.

Susanto, A. (2016). Penerapan Teori Chaos di Dalam Kriptografi. *Jurnal Teknik Informatika*.

Syafrizal, M. (2007). ISO 17799: Standar Sistem Manajemen Keamanan Informasi. *Seminar Nasional Teknologi*.

Teddy, A. P., & Ricoida, D. I. (2016). Analisis dan Perancangan Sistem Informasi Layanan Pelanggan.