PETIR: Jurnal Pengkajian dan Penerapan Teknik Informatika
Vol. 15, No. 1, Maret 2022, P-ISSN 1978-9262, E-ISSN 2655-5018
DOI: https://doi.org/10.33322/petir.v15i1.1333

Implementasi Algoritma AES untuk Keamanan Data Rekam Medis

Oktaria Gina Khoirunnisa[1]; Djuniadi[2]

[1,2] Universitas Negeri Semarang
[1] oktariagina@students.mail.ac.id
[2] djuniadi@mail.unnes.ac.id

ABSTRACT

The rapid development of technology certainly greatly affects various fields. Various daily tasks are also helped by technology. In addition to the positive impacts, the negative impacts also need to be alerted for, one of which is the issue of document security. The health sector is an example of a field related to privacy, one of which is medical record documents. There are not a few cases of patient data leakage occurred. This unwanted event can be avoided by securing it with Cryptography. There are various kinds of cryptography, one of which is AES (Advanced Encryption Standard). Based on this description, this study aims to simulate the security of medical record documents at a clinic using the AES method. The simulation results show that the AES algorithm can be a recommendation for data protection. By going through the encryption process the data will be converted into a form that is not understood and must be processed using a decryption process so that it can be understood again. The advantage is that not everyone can access the document.

Keywords: *cryptography, AES Algorithm, medical record*

ABSTRAK

Pertumbuhan teknologi yang sangat pesat tentunya sangat mempengaruhi berbagai bidang. Berbagai pekerjaan sehari hari pun juga terbantu dengan adanya teknologi. Selain dampak positif yang diperhatikan dampak negatif pun juga perlu diwaspadai yaitu perihal keamanan dokumen. Bidang kesehatan merupakan contoh yang bidang berhubungan dengan privasi. Salah satunya yaitu dokumen rekam medis. Tidak sedikit kasus kebocoran data pasien yang terjadi. Peristiwa yang kurang diinginkan seperti ini dapat terhindarkan dengan melakukan pengamanan dengan Kriptografi. Terdapat berbagai macam kriptografi salah satunya yaitu AES (Advanced Encryption Standard). Berdasarkan uraian tersebut penelitian ini bertujuan untuk melakukan simulasi pengamanan dokumen rekam medis pada salah satu klinik dengan menggunakan metode AES. Hasil simulasi menunjukan bahwa algoritma AES dapat menjadi rekomendasi bagi perlindungan data. Dengan melalui proses enkripsi data akan diubah menjadi bentuk yang tidak dimengerti dan harus diproses menggunakan proses dekripsi agar bisa kembali dimengerti. Keuntungannnya adalah tidak semua orang bisa mengakses dokumen tersebut.

Kata kunci: *Cryptography, algoritma AES, data rekam medis*

Vol. 15, No. 1, Maret 2022, P-ISSN 1978-9262, E-ISSN 2655-5018
DOI: https://doi.org/10.33322/petir.v15i1.1333

1. PENDAHULUAN

Perkembangan teknologi sangat mempengaruhi kehidupan. Pemanfaataannya pun sudah diterapkan diberbagai bidang mengingat adanya perkembangan yang sangat pesat. Dimulai dari pekerjaan yang sederhana hingga perkejaan yang rumit sekalipun. Pemanfaat teknologi memanglah sangat diperlukan, namun terdapat hal yang juga tidak bisa kita lupakan yaitu kemanan privasi dokumen karna pada dasarnya setiap dokumen mempunyai privasinya tersendiri [1].

Bidang kesehatan adalah salah satu bidang yang tentunya berhubungan dengan privasi, salah satunya yaitu rekam medis, yang merupakan bentuk dari dokumentasi yang dimiliki oleh setiap pasen yang dimiliki setiap sarana layanan kesehatan yang didalamnya terdapat keterangan tentang data probadi, riwayat pemeriksaan, perawatan, tindakan serta layanan yang pernah pasien terima [2]. Tujuan dari adanya rekam medis sendiri tak lain guna menunjang tercapainya administrasi yang tertib agar dapat meningkatkan pelayanan kesehatan pada instansi pelayanan kesehatan [3]. Dokumen rekam medis selain disimpan oleh klinik atau rumah sakit terkait, dokumen tersebut juga terkadang dikirimkan pada klinik atau rumah sakit lain sebagai data rujukan pasien. Adanya hal hal tersebut tentunya menimbulkan adanya kemungkinan data tersebar atau dipergunakan tidak semestinya[4]. Dampak negatif tersebut hanyalah satu dari sekian banyak dampak yang diwaspadai oleh pengguna teknologi informasi saat ini[5]. Melihat adanya kemungkinan tersebut diperlukan adanya antisipasi berupa perlindungan dokumen guna mengurangi hal yang tidak semestinya. Metode yang dapat digunakan tak lain adalah kriptografi.

Kriptografi merupakan satu dari beberapa algoritma yang dimanfaatkan dalam menjaga kerahasian data[6]. Sesuai dengan pengertian tersebut, kriptografi ini dapat menjamin bahwa data yang dikirim dilindungi dengan maksud agar penerima pesan dapat memperoleh informasi yang benar benar asli[7]. Proses pada kriptografi sendiri terdapat dua yaitu enkripsi dan dekripsi. Enkripsi sendiri merupakan teknik mengonversikan teks asli atau *plaintext* menjadi *ciphertex*t[8]. Berbanding terbalik dengan dekripsi yang merupakan teknik pegembalian *ciphertext* menjadi teks asli atau *plaintext*[9]. Kriptografi sendiri dapat dikategorikan lebih lanjut berdasarkan jenis *security key* yang digunakan, yaitu menjadi *symmetric key* dan *asymmetric key* [8]. Pemilihan pengguanaan juga mempengaruhi tingkat keamanan. Fakta tersebut berkaitan dengan semakin semakin panjang kunci yang dipakai maka semakin lama pula waktu yang diperlukan pihak yang tidak bertanggung jawab untuk membuka dokumen tersebut dengan kata lain semakin rumit kunci yang digunakan akan semakin aman.

Terdapat berbagai macam algoritma kriptografi dengan masing masing kegunaannya, salah satunya yaitu AES. Enkripsi AES (*Advanced Encryption Standard*) sendiri merupakan satu dari beberapa teknik kriptografi yang dimanfaatkan guna mengatasi keamanan data dengan cara mengenskrip data sehingga tidak memngetahui *key* pada dokumen tidak bisa membuka dokumen tersebut[10]. AES sendiri merupakan algoritma perkembangan dari algoritma DES, dimana jika keduanya dibandingkan AES sendiri memerlukan waktu yang jauh lebih singkat ketika melakukan enkripsi dan dekripsi[11].

Berdasarkan uraian diatas, penelitian ini bertujuan untuk melakukan simulasi pengamanan dokumen rekam medis pada salah satu klinik dengan menggunakan metode AES. Penggunaan metode AES dinilai tepat karena seperti yang sudah disebutkan sebelumnya bahwa metode ini lebih unggul dibandingkan DES. Dengan adanya simulasi pengamanan data ini diharapkan dapat menjadi solusi untuk pengamanan dokumen rekam medis, sehingga data pasien tidak disalahgunakan oleh pihak yang tidak bertanggung jawab.

Vol. 15, No. 1, Maret 2022, P-ISSN 1978-9262, E-ISSN 2655-5018
DOI: https://doi.org/10.33322/petir.v15i1.1333

2. METODE/PERANCANGAN PENELITIAN

2.1. Kriptografi

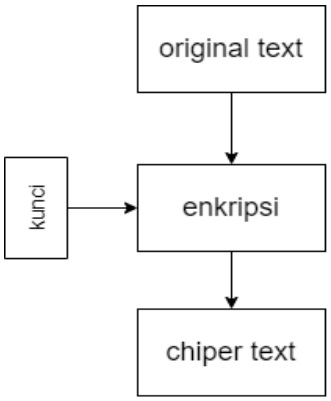
Kriptografi sendiri adalah bidang yang mempelajari tentang bagaimana ilmu praktek pada matematika yang memiliki kesinambungan dengan aspek aspek kemaanan sistem informasi seperti kerahasiaan data, kebenaran data, serta pemrosesan data[12]. Singkatnya, kriptografi merupakan suatu ilmu yang digunakan dalam menjaga keamanan suatu file. Tahap awal pada kriptografi akan mengubah text asli menjadi kode-kode terlebih dahulu atau yang lebih dikenal dengan proses enkripsi[13]. Metode enkripsi sendiri merupakan tahap ditranformasikan suatu data yang akan digunakan kedalam bentuk yang hampir tidak *familiar* oleh pihak ketiga. Setelah data atau informasi yang nantinya diterima oleh penerima, penerima akan melakukan dekripsi.

2.2. AES (Advanced Encryption Standart)

AES merupakan algoritma kriptografi *cipher block* yang termasuk dalam kategori simetris. Kunci pada algoritma ini pun dapat dibagi menjadi tiga, yaitu 128, 192, serta 256 [14]. Pada seri kunci 128 sendiri nantinya dapat dibagi menjadi empat blok dasar operasional yang berbentuk matirks 4x4 [15].

Penerapan metode AES. Proses penyelesaian dari *framework* pada algoritma AES :

1) Proses Enkripsi

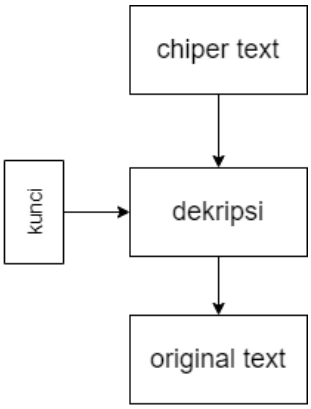


Gambar 1. Proses Enkripsi

Dalam proses enkripsi, pertama peneliti akan menggunakan tools cryptool 2.1 untuk melakukan praktik enkripsi dan dekripsi. Pada langkah awal setelah memasuki cryptol 2.1 peneliti akan menentukan *key* yang akan diguakan dalam melakukan enkripsi serta dekripsi. Setelah menentukan *key* maka *key* tersebut diubah dalam bentuk hex yang kemudian akan dimasukan ke dalam box *key*. Selanjutnya peniliti akan memasukkan pesan singkat yang dikirimkan ke dalam *box message to encryp* setelah itu klik next. Kemudian akan muncul hasil dari proses enkripsi tersebut berupa kode hex pada box yang bertuliskan AES Output.

Vol. 15, No. 1, Maret 2022, P-ISSN 1978-9262, E-ISSN 2655-5018
DOI: https://doi.org/10.33322/petir.v15i1.1333

2) Proses Dekripsi

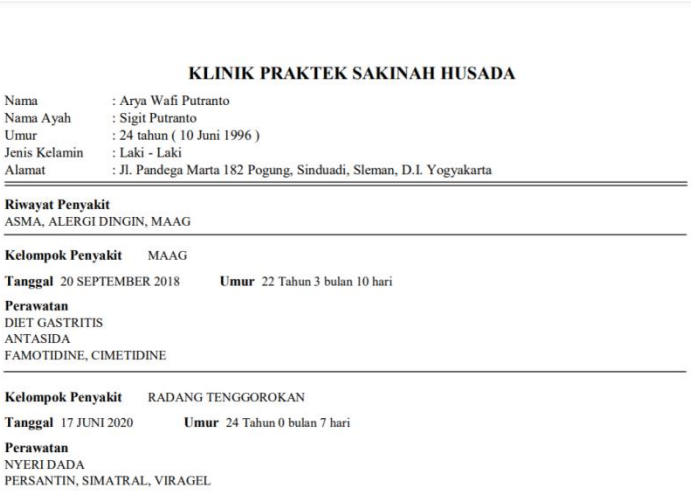


Gambar 2. Proses Dekripsi

Proses dekripsi terhadap cipher teks merupakan oponen dari proses enkripsi. Setelah mendapatkan hex text pada proses enkripsi, hex text tersebut kita masukkan dalam kolom *Message to Decrypt*. Selain itu *key* yang digukana juga masih sama seperti pada proses enkripsi sebelumnya. Selanjutnya peniliti akan memasukkan kode hex yang tadi didapatkan pada proses enkripsi yang dikirimkan ke dalam *box message to decryp* setelah itu klik next. Kemudian akan muncul hasil dari proses dekripsi tersebut berupa pesan yang tadinya dimasukan pada proses enkripsi pada box yang bertuliskan AES Output.

3. HASIL DAN PEMBAHASAN

Langkah pertama yang kita lakukan yaitu menyiapkan dokumen yang akan kita gunakan dalam proses simulasi ini. Dokumen yang digunakan pada penelitian ini merupakan dokumen rekam medis pada salah satu klinik praktek yang dimana didalamnya terdapat berbagai data pribadi milik pasien yang bersifat rahasia.



KLINIK PRAKTEK SAKINAH HUSADA

Nama : Arya Wafi Putranto
Nama Ayah : Sigit Putranto
Umur : 24 tahun (10 Juni 1996)
Jenis Kelamin : Laki - Laki
Alamat : Jl. Pandega Marta 182 Pogung, Sinduadi, Sleman, D.I. Yogyakarta

Riwayat Penyakit
ASMA, ALERGI DINGIN, MAAG

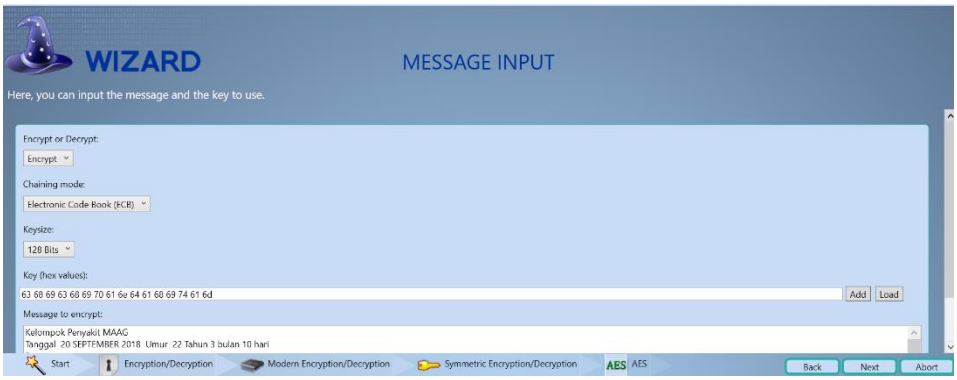
Kelompok Penyakit MAAG
Tanggal 20 SEPTEMBER 2018 **Umur** 22 Tahun 3 bulan 10 hari
Perawatan
DIET GASTRITIS
ANTASIDA
FAMOTIDINE, CIMETIDINE

Kelompok Penyakit RADANG TENGGOROKAN
Tanggal 17 JUNI 2020 **Umur** 24 Tahun 0 bulan 7 hari
Perawatan
NYERI DADA
PERSANTIN, SIMATRAL, VIRAGEL

Gambar 3. Dokumen Rekam Medis Pasien

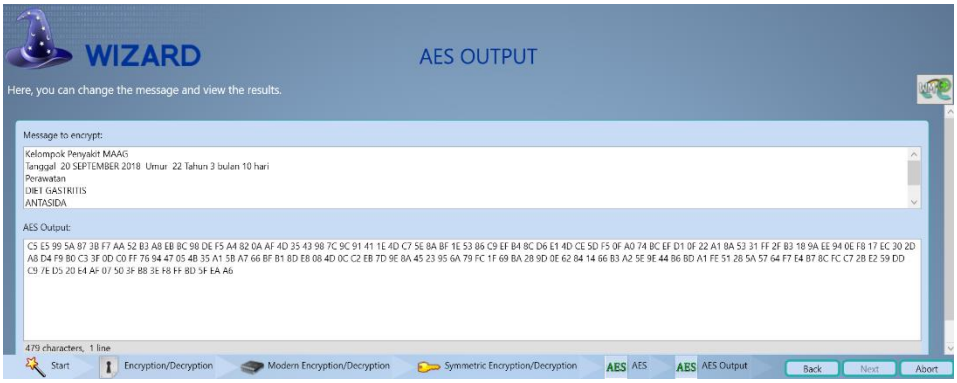
Simulasi ini menggunakan salah satu bagian pada dokumen tersebut yaitu salah satu catatan riwayat pemeriksaan pasien seperti gambar 3. Data tersebut sebagai contoh *plaintext* yang diproses enkripsi dan dekripsi.

Vol. 15, No. 1, Maret 2022, P-ISSN 1978-9262, E-ISSN 2655-5018
DOI: https://doi.org/10.33322/petir.v15i1.1333



Gambar 4. Proses Input Enkripsi

Pada gambar 4, peneliti memasukan kode yang sudah berbentuk hex kedalam kolom *key*. Dalam penelitian ini, peneliti menggunakan kunci yang sudah diubah kedalam kode hex yaitu, 63 68 69 63 68 69 70 61 6e 64 61 68 69 74 61 6d atau jika diterjemahkan chichipandahitam. Selanjutnya, peneliti memasukkan data rekam medis. Setelah proses itu sudah selesai diisi, selanjutnya dienkripsikan. Hasilnya tampak pada gambar 5.



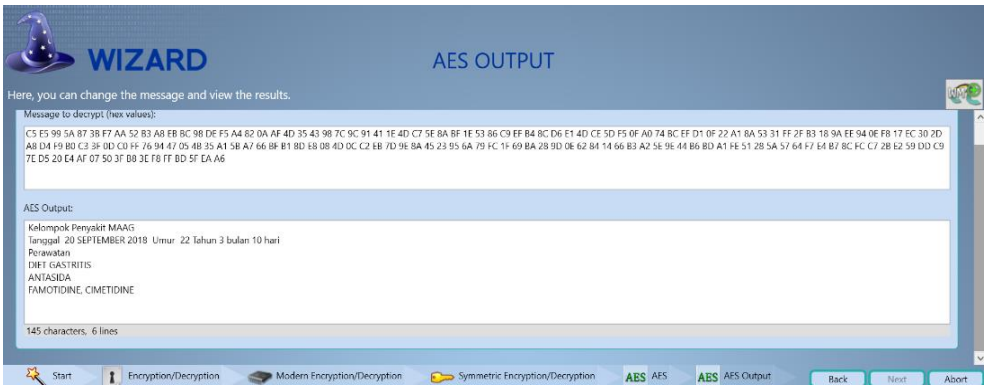
Gambar 5. Output Enkripsi

Setelah proses enkripsi selesai, maka akan muncul hasil dari enkripsi berupa *chipertext* yang akan tampil pada kolom AES Output. Dimana, *Chipertext* merupakan text yang susah dibaca dan kurang dimengerti oleh kebanyakan orang awam.

Gambar 6. Proses Input Dekripsi

PETIR: Jurnal Pengkajian dan Penerapan Teknik Informatika
Vol. 15, No. 1, Maret 2022, P-ISSN 1978-9262, E-ISSN 2655-5018
DOI: https://doi.org/10.33322/petir.v15i1.1333

Setelah melakukan enkripsi kita akan mendapatkan *chipertext* yang nantinya akan kita masukan kedalam proses dekripsi. *Chipertext* yang didapatkan dimasukan pada kolom Message to decrypt. Selain itu peneliti juga memasukkan kode yang sama yaitu 63 68 69 63 68 69 70 61 6e 64 61 68 69 74 61 pada kolom *key*s. Lalu klik next guna melanjutkan proses tersebut.



Gambar 7. Output Dekripsi

Setelah proses dekripsi selesai, maka akan muncul hasil dari dekripsi berupa plaintext atau *original text* yang akan tampil pada kolom AES Output. Hasil yang diperoleh dari proses dekripsi ini merupakan salah satu bagian dari dokumen rekam medis berupa riwayat pemeriksaan pasien yang digunakan pada proses enkripsi. Dengan munculnya *plaintext* yang sama dengan text yang dipakai ketika proses enkripsi tersebut maka proses dekripsi sudah berhasil. Berhasilnya proses dekripsi ini membuktikan bahwa algoritma AES merupakan algoritma yang simetris, yaitu dengan menggunakan kode hex yang sama 63 68 69 63 68 69 70 61 6e 64 61 68 69 74 61 6d. Selain itu dengan penggunaan kode hex yang tidak banyak orang mengerti akan meningkatkan kemanan dari pengamanan ini. Simulasi ini juga membuktikan bahwa algoritma AES dapat membantu dalam proses pengamanan dokumen sehimgga dapat meminimalisir adanya penyalahgunaan data.

4. KESIMPULAN DAN SARAN

AES merupakan salah satu algoritma kriptografi yang digunakan untuk mengamankan data. Salah satunya yaitu bisa digunakan untuk proses pengamanan dokumen medis. Sebagai sampel adalah data diri serta riwayat penyakit suatu pasien yang merupakan suatu privasi. Hasil simulasi menunjukan bahwa algoritma AES dapat menjadi rekomendasi bagi perlindungan data. Dengan melalui proses enkripsi, data medis diubah menjadi bentuk yang tidak dimengerti sehingga aman. Apabila data tersebut mau diperlukan maka harus diproses menggunakan proses dekripsi agar bisa kembali dimengerti. Simulasi ini juga membuktikan bahwa algoritma AES merupakan algoritma yang simetris dimana kode hex 63 68 69 63 68 69 70 61 6e 64 61 68 69 74 61 6d dapat digunakan pada proses enkripsi dan juga dekripsi.

DAFTAR PUSTAKA

[1] T. S. Alasi, R. Wanto, and V. H. J. J. I. K. L. Sitanggang, "IMPLEMENTASI KRIPTOGRAFI ALGORITMA IDEA PADA KEAMANAN DATA TEKS BERBASIS ANDROID," vol. 2, no. 1, 2020.

[2] J. S. Pasaribu and J. J. J. I. T. I. T. Sihombing, "Perancangan Sistem Informasi Rekam Medis Pasien Rawat Jalan Berbasis Web Di Klinik Sehat Margasari Bandung," vol. 3, no. 3, 2017.

Vol. 15, No. 1, Maret 2022, P-ISSN 1978-9262, E-ISSN 2655-5018
DOI: https://doi.org/10.33322/petir.v15i1.1333

[3] H. M. Ulfa, D. Wahyuni, R. Amalia, and F. J. A. J. A. R. K. M. Edigan, "Penerapan Rekam Medis Di Puskesmas Senapelan Kota Pekanbaru," vol. 1, no. 2, pp. 83-86, 2021.

[4] A. F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, J. M. R. Tavares, and V. H. C. J. C. S. R. de Albuquerque, "A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform," vol. 52, pp. 1-11, 2018.

[5] A. J. J. Rahman, "Perancangan Aplikasi Pengamanan File Pada Memory Card Handphone Menggunakan Algoritma Kunci Asimetris Elgamal," vol. 6, no. 5, pp. 531-537, 2019.

[6] J. Clawdia, N. Khairina, and M. K. J. K. Harahap, "Implementasi Algoritma Kriptografi One Time Pad (OTP) Dengan Dynamic Key Linear Congruential Generator (LCG)," vol. 1, no. 1, 2017.

[7] D. K. Sharma, N. C. Singh, D. A. Noola, A. N. Doss, and J. J. M. T. P. Sivakumar, "A review on various cryptographic techniques & algorithms," 2021.

[8] M. F. Mushtaq *et al.*, "A survey on the cryptographic encryption algorithms," vol. 8, no. 11, pp. 333-344, 2017.

[9] A. J. C. Abdullah and N. Security, "Advanced encryption standard (AES) algorithm to encrypt and decrypt data," vol. 16, pp. 1-11, 2017.

[10] A. Prameshwari and N. P. J. J. E. I. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," vol. 8, no. 1, pp. 52-58, 2018.

[11] H. H. Ali and S. H. Shaker, "Modified Advanced Encryption Standard algorithm for fast transmitted data protection," in *IOP Conference Series: Materials Science and Engineering*, 2020, vol. 928, no. 3, p. 032011: IOP Publishing.

[12] M. M. J. P. Amin, "Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks," vol. 3, no. 2, pp. 129-136, 2016.

[13] Y. D. Putri, R. Rosihan, and S. J. J. Lutfi, "Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance," vol. 2, no. 2, pp. 87-94, 2019.

[14] K. Muttaqin, J. J. J. o. A. E. Rahmadoni, and T. Science, "Analysis And Design of File Security System AES (Advanced Encryption Standard) Cryptography Based," vol. 1, no. 2, pp. 113-123, 2020.

[15] P. Patil, P. Narayankar, D. Narayan, and S. M. J. P. C. S. Meena, "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish," vol. 78, pp. 617-624, 2016.