KEAMANAN DATA MENGGUNAKAN GABUNGAN KRIPTOGRAFI AES DAN RSA

Candra Irawan[1], Eko Hari Rachmawanto[2]
[1]Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro [2]
Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
e-mail: [1]candra.irawan@dsn.dinus.ac.id, [2]eko.hari@dsn.dinus.ac.id

ABSTRAK

Kriptografi menggunakan algoritma Advamce Encryption Standard (AES) maupun Rivest Shamir Adleman (RSA) secara individual sudah sering digunakan baik dalam proses pengamanan pesan berupa teks maupun citra digital. Pada penelitian ini akan digunakan gabungan AES dan RSA. Tujuan gabungan ini adalah meningkatkan nilai Avalanche Effect pada hasil implementasi serta untuk menganalisa waktu kebutuhan untuk proses enkripsi dan dekripsi. Pada penelitian ini, digunakan sejumlah data teks, audio dan video dengan jumlah byte antara 100 smapai 4000 bytes. Telah dilakukan perbandingan hasil perhitungan Avalanche effect (AE) pada AES, modified AES dan AES-RSA melalui 15 kali percobaan. Hasil perbandingan menunjukkan bahwa AES-RSA menghasilkan AE paling tinggi yaitu 44,74%.

***Kata Kunci**: Kriptografi, Algoritma AES, algoritma RSA, Enkripsi, Dekripsi*

1. PENDAHULUAN

Ada banyak aspek keamanan dan banyak aplikasi, mulai dari transmisi data yang aman, perlindungan kata sandi, keamanan online, perbankan online, dan banyak lagi. Salah satu aspek penting untuk komunikasi yang aman adalah kriptografi yang dapat didefinisikan sebagai konversi data menjadi kode sandi yang dapat diuraikan dan juga dapat dengan aman dikirim melalui jaringan publik atau pribadi. Para pelaku atau praktisi kriptografi disebut cyrptographers. Sebuah algoritma kriptografik (cryptographic algorithm), disebut cipher, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Biasanya persamaan kedua matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat. Algoritma kriptografi digunakan pada proses enkripsi maupun deskripsi. Pada umumnya algoritma kriptografi dibedakam menjadi dua jenis, yaitu kriptografi kunci simetris (symmetric key cryptography) dan kriptografi kunci tidak simetris (asymmetric key cryptgraphy). Contoh kriptografi simetris adalah vigenere cipher sedangkan contoh kriptografi asimetris adalah Advanced Encryption Standard (AES). Enkripsi adalah proses mengubah data plaintext menjadi ciphertext untuk menyembunyikan maknanya dan dengan demikian mencegah penerima yang tidak sah mengambil data asli. Oleh karena itu, tugas utama enkripsi adalah memastikan kerahasiaan [1], [2]. Perusahaan biasanya mengenkripsi data mereka sebelum transmisi untuk memastikan bahwa data tersebut aman selama transit. Data terenkripsi di kirim melalui jaringan publik dan di dekripsi oleh penerima yang dituju [3], [4].

Advanced Encryption Standard (AES) adalah algoritma kriptografi enkripsi yang standart untuk digunakan system keamanan pada semua data. AES tersebut diimplementasikan dalam berbagai macam perangkat lunak dan perangkat keras. Algoritma Aes juga memiliki standart keamanan yang sangat tinggi. AES menggantikan Algoritma Data Enrkripsi standart (DES) [4]–[6]. AES juga dapat memilih beberapa kunci, yaitu memliki panjang 128,192, atau 256 bit. Algoritma AES menggunakan kunci yang sama untuk enkripsi dan dekripsi dan menggunakan 4 struktur panggung dalam satu putaran untuk membentuk teks sandi untuk setiap putaran.

Selain Algoritma AES, penulis juga menambahkan metode Algoritma RSA. Algoritma RSA yaitu teknik kriptografi asimetris yang populer. Algottma RSA memiliki tingkat keamanan yang sangat baik, dimana algoritma tersebut penfaktoran yang sulit terhadap sebuah bilangan besar menjadi faktor faktor prima. Keamanan RSA tergantung pada waktu yang diperlukan untuk menemukan kunci privat [7]–[9]. Untuk memaksimalkan keamanan, RSA membutuhkan sejumlah besar angka. Namun, nilai piksel gambar dibatasi, misalnya 0 hingga 255, ini pasti akan membuat kunci variasi RSA menjadi terbatas. Batasan ini memerlukan modifikasi agar RSA berfungsi lebih optimal untuk enkripsi beberapa data. Algoritma yang memiliki panjang kunci dalam bit yang dapat diatur sehingga semakin lama semakin sulit memecahkan karena kesulitan anjak dua angka yang sangat besar, tetapi butuh waktu lama untuk proses dekripsi. Algoritma AES berfungsi untuk menyembunyikan data yang akan dikirim ke penerima sementara untuk pertukaran kunci akan disembunyikan menggunakan algoritma RSA [10]. Algoritma RSA tidak digunakan untuk mengenkripsi data, tetapi mengenkripsi kunci simetris dengan kunci publik penerima pesan karena cara kerja algoritma RSA lebih lambat daripada kriptografi simetris seperti DES atau AES [11]. Oleh karena itu pesan akan dienkripsi dengan algoritma kunci simetris, yaitu algoritma AES, sedangkan kuncinya akan dienkripsi dengan algoritma asimetris yaitu algoritma RSA.

Penelitian ini menggunakan kombinasi algoritma kriptografi asimetris dan simetris, yaitu algoritma RSA dan algoritma AES. Algoritma RSA adalah kriptografi asimetris. Algoritma yang memiliki panjang kunci dalam bit yang dapat diatur sehingga semakin lama semakin sulit memecahkan karena kesulitan anak dua angka yang sangat besar, tetapi butuh waktu lama untuk proses dekripsi, sedangkan algoritma AES adalah algoritma simetris yang menggunakan block cipher. Selama proses enkripsi dan dekripsi, algoritma AES-128 melakukan sepuluh fungsi transformasi siklus,mis. Tambahkan Round Key, Sub Byte, Shift Rows dan Mix Column. Penelitian dilakukan untuk melihatpengaruh kombinasi tanda tangan digital dengan algoritma RSA dan AES ke sistem disposisitujuan kriptografi berbasis surat, yaitu Kerahasiaan, Integritas Data, Otentikasi, dan Nonrepudiasi.

2. METODE PENELITIAN

Kriptografi

Kriptografi adalah logika manipulasi matematis data (ciphertext) dengan beberapa teks (Key). Untuk mengkonversi teks biasa ke teks sandi diterapkan algoritma enkripsi pada teks biasa menggunakan kunci [1]. Dan untuk mengubah cipher text menjadi plain text diterapkan algoritma dekripsi pada cipher text menggunakan kunci. Sebelum algoritma enkripsi dan dekripsi diperlukan beberapa algoritma untuk membangkitkan kunci terlebih dahulu. Selama kriptografi, ada tiga proses dasar pembuatan kunci, enkripsi dan proses dekripsi. Setiap sistem keamanan harus menyediakan sekumpulan fungsi keamanan yang menjamin kerahasiaan sistem. Fungsi-fungsi ini biasanya disebut sebagai tujuan dari sistem keamanan. Tujuan-tujuan ini dapat didaftar sebagai berikut [12] :

1. Otentikasi: Sebelum mengirim dan menerima data menggunakan sistem, identitas penerima dan pengirim harus diverifikasi. Kerahasiaan atau Kerahasiaan: Biasanya fungsi ini adalah cara kebanyakan orang mengidentifikasi sistem yang aman. Ini berarti bahwa hanya orang yang diautentikasi yang dapat menafsirkan isi pesan dan tidak ada orang lain.
2. Integritas: Integritas berarti bahwa konten data yang dikomunikasikan dijamin bebas dari segala jenis modifikasi antara titik akhir (pengirim dan penerima). Bentuk dasar dari integritas adalah jumlah cek paket dalam paket IPv4.
3. Non-Repudiation: Fungsi ini menyiratkan bahwa baik pengirim maupun penerima tidak dapat secara salah menyangkal bahwa mereka telah mengirim pesan tertentu.
4. Keandalan dan Ketersediaan Layanan: Karena sistem yang aman biasanya diserang oleh penyusup, yang dapat memengaruhi ketersediaan dan jenis layanannya kepada penggunanya. Sistem tersebut harus menyediakan cara untuk memberikan pengguna mereka kualitas layanan yang mereka harapkan.

Untuk mencapai tujuan sistem keamanan, algoritma enkripsi harus memberikan kekuatan yang cukup dengan keamanan tinggi yang diimplementasikan dalam batasan kecepatan yang dapat diterima. Oleh karena itu, evaluasi kinerja menjadi sangat penting untuk algoritma enkripsi yang ada.

Algoritma AES

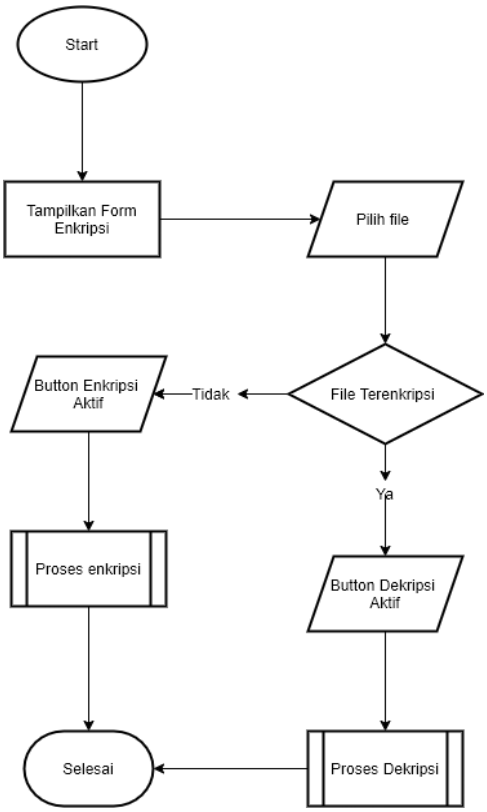
AES (Advanced Encryption Standard) juga disebut varian dari Algoritma Rijndael, memiliki ukuran blok 128 bit dengan 128 (dengan 10 siklus pengulangan), 192 (dengan 12 siklus pengulangan) atau 256 (dengan 14 siklus pengulangan) bit ukuran kunci. Serangan brute force dapat membuka kunci algoritma AES. Dalam algoritma serangan ini penyerang menggunakan kamus kata-kata dalam bahasa Inggris dan mencari tahu kata-kata yang digunakan sebagai kunci. Algoritma AES menggunakan ciphertext untuk mengenkripsi data. Setiap data yang enkripsi pada aes tersebut tidak akan terbaca oleh pengguna yang tidak tau key nya, karena algoritma aes tersebut diberi key oleh pengguna yang mempunyai file [11], [13]. AES dipilih karena sifat keamanan yang kuat dan implementasi sederhana baik dalam perangkat lunak dan perangkat keras. Penggunaan ukuran kunci yang lebih besar meningkatkan kekuatan kriptografi tetapi mensyaratkan bahwa jumlah yang lebih besar dari putaran berulang dilakukan [4]. Algoritma AES juga digunakan karena karena keuntungan untuk mengamankan dokumen dan terbukti aman berdasarkan NIST Standard. Pada proses enkripsi diatas, data akan diencryption key, data tersebut akan berubah menjadi aes dan akan keluar outputnya menjadi ciphertext. Algoritma AES digunakan untuk keamanan selama proses pengkodean pesan yang akan dikirim ke penerima. Algoritma AES digunakan dalam penelitian ini untuk memenuhi tujuan kriptografi yaitu kerahasiaan dan integritas data, sehingga konten pesan dilindungi dari tindakan seperti mengetuk data [14]. Kecepatan komputer yang sangat pesat dianggap sangat membahayakan DES, sehingga ditetapkanlah algoritma baru Rijndael sebagai AES.

Algoritma RSA

Algoritma Rsa menggunakan dua kunci atau yang disebut dengan sandi asimetris untuk mengenkripsi data pada rsa tersebut. Tingkat keamanan pada algoritma RSA sangat bergantung pada asimetris yang ada pada algoritma tersebut [8]. Maka disaat besaran ukuran kunci akan tambah semakin sulit untuk ditembus pada algoritma tersebut.

Algoritma RSA digunakan untuk mengamankan kunci ketika proses enkripsi pada dokumen yang telah dienkripsi oleh algoritma Aes. Algoritma RSA digunakan untuk memenuhi tujuan otentikasi kriptografi yaitu dannon-repudiation [15]. Pada kelebihan algoritma RSA yaitu mempunyai Kekuatan pada proses eksponensial, dan jumlah factorials menjadi 2 bilangan prima yang sampai sekarang sulit untuk melakukan dikenal. Di Algoritma RSA, dua nomor algoritma yang digunakan untuk membuat dua kunci publik dan swasta. Sulit untuk mengetahui pesan asli dari kunci sinyal sehingga aman dari brute force attack.

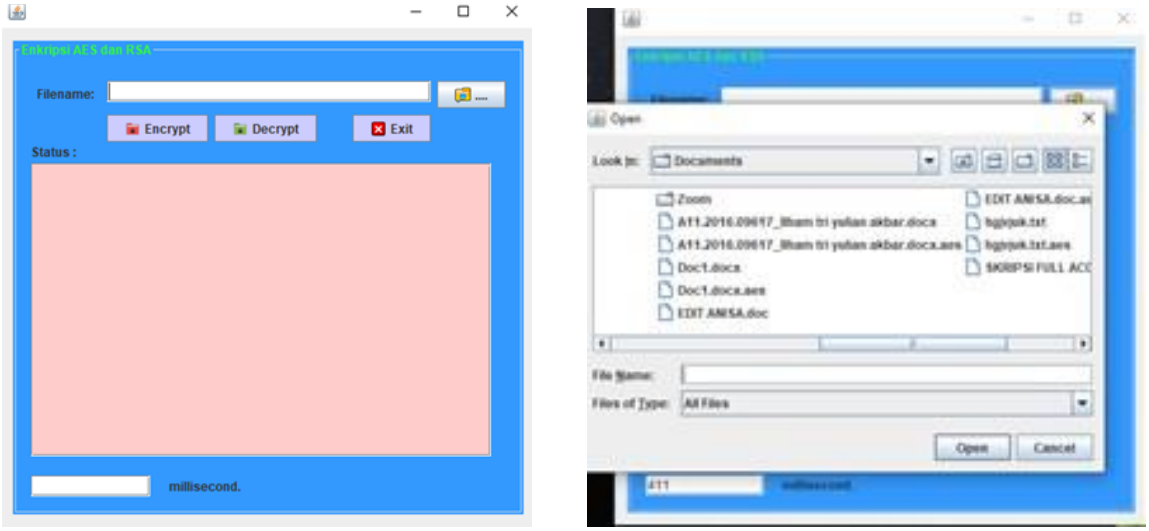
Pemodelan Proses



Gambar 1. Pemprosessan Enkrispsi dan Dekripsi Algoritma AES dan RSA

3. HASIL DAN PEMBAHASAN

Pada penelitian ini penulis mencoba untuk menggabungkan antara algoritma keduanya. Dan tidak hanya menggabungkan antara kedua algoritma tersebut, penulis juga mencoba untuk menenkripsi file. Dan mendekripsi kan file tersebut. Penggunaan aplikasi ini menggunakan java dan aplikasinya menggunakan NetBeans.



(a) (b)

Gambar 2. (a) Tampilan Awal Aplikasi, (b) Pemilihan File

Pada Gambar 2 (a) di atas merupakan gambaran hasil program sebelum melakukan sebuah proses pemprosessan file pada enkripsi dan dekripsi. Digambar tersebut ada yang filename, Encypt, Decrypt, Exit, status, dan waktu (*millisecond*) yang akan menunjukkan pemprosessan terjadinya enkripsi dan dekripsi dan tekan tombol yang sejajar pada file name. Gambar 2 (b) menunjukkan, setelah itu masukan sebuah file, contoh yang diatas akan melakukan sebuah enkripsi sebuah file gambar yang berformat file .jpg yang sudah dipilih dahulu pada menu yang disediakan sebelumnya, pada hal tersebut button pada decrypt otomatis akan menghilang, dikarenakan akan terjadi proses pada enkripsi pada file-file tersebut.

(a) (b)

Gambar 3. (a) Hasil Enkripsi, (b) Hasil dekripsi

Gambar 3 (a) menunjukkan, Setelah memasukan file, tekan button Encrypt, dan status pada file yang telah terenkripsi sukses, dan waktu proses program enkripsi akan keluar yaitu 339. Output filenya berubah namanya bertambah format bernama .aes yang menandakan itu sebuah file yang terenkripsi. Tetap kalau format .aes dihapus secara manual tidak akan mempengaruhi pada file yang telah terenkripsi. Gambar 3 (b) menunjukkan proses pada enkripsi tersebut, untuk membuka pada file yang sudah terenkripsi. Lakukan proses yang bernama dekripsi. Pada proses dekripsi akan membuka kunci dari enkripsi tersebut. Gambar diatas menunjukkan perbedaan antara hasil enkripsi dan dekripsi yaitu pada button. Enkripsi akan menghilang atau tidak bisa ditekan, sedangkan untuk dekripsi akan muncul dengan sendirinya. Setelah ditekan pada button dekryptnya, akan keluar dari status kalau proses pada dekripsi sudah selesai dan file akan kembali seperti semula lagi. Dan perbedaan pada waktunya yaitu antara enkripsi dan dekripsi lebih cepat dekripsi. Pada Gambar 3 diatas menunjukkan, perbedaan file yang sesudah terenkripsi dan sebelum terenkripsi. Pada gambar tersebut terlihat file yang sesudah terenkripsi tidak bisa dibuka atau tidak bisa dibaca oleh system. Dan untuk membuka lagi pada file tersebut maka harus melalui proses dekripsi.

Tabel 1. Hasil proses Enkripsi

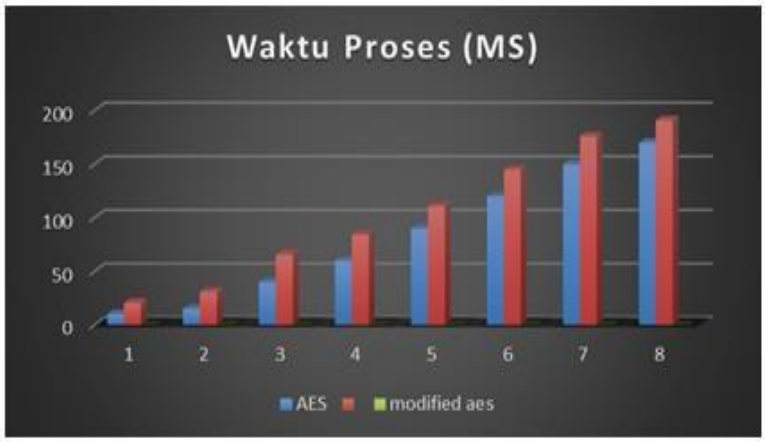
Jenis File	Sebelum Dienkripsi (bytes)	Setelah Dienkripsi (bytes)	Waktu enkripsi (millisecond)	Selisihh bytes	Perbedaan (%)
WORD	2.794.898	2.794.936	789	38	0,00136
PDF	986.303	986.328	277	25	0,002535
PPT	850.005	850.040	204	35	0,004118
EXCEL	23.552	23.592	105	40	0,169837
MP3	4.559.256	4.559.288	681	32	0,000702
GAMBAR	77.997	78.024	513	27	0,034617
VIDEO	31.389.103	31.389.128	3953	25	0,00008

Berdasarkan pada Tabel 1, Metode algoritma AES dan RSA enkripsi file mengalami sedikit kenaikan dalam ukuran tersebut, rata rata 0,030463878%, dan selisih dari ukuran bytes sebelum dan sesudah dienkripsi kenaikannya hampir tinggi dan waktu enkripsi juga lama.

Tabel 2. Avalanche Effect dari AES

Parameter		AES	Modified AES	AES – RSA
Avalanche Effect	1 Bit of Plaintext Changed	50,00%	12,04%	44,74%
	1 Bit of Cipherkey Changed	49,24%	48,56%	45,55%
Robustness Text		43,50%	20,55%	23,44%

Tabel 2 di atas menjelaskan pengujian Robusiness test performansi pada sebuah system yang menggunakan algoritma AES termodifikasi tereferensi lebih baik dengan menghasilkan nilai BER (bit error Rate) yang lebih kecil yakni sebesar 20,55%. Pengujian robustnes mengambil sampel sebanyak 15 kali, dengan jumlah bit error meningkat secara linear.



Gambar 4. Grafik Waktu Pemrosesan

Pada Gambar 4 menjelaskan waktu sebuah komputasi yang dibutuhkan kedua system untuk melakukan enkripsi file. Berdasarkan pada data tersebut diperoleh bahwa proses enkripsi menggunakan algoritma AES lebih cepat dibandingkan oleh algoritma algoritma AES yang termodifikasi. Dan panjang data file yang di enkripsi sangat berpengaruh terhadap waktu yang semakin lama dibutuhkan oleh kedua system tersebut.

Tabel 3. Avalanche Effect RSA

Percobaan	Plaintext	Kunci Private	CipherText	Prosentase
1	Bus	7	32 39 80	11,11%
	Bis		32 118 80	
2	Kawan	7	68 59 37 59 33	6,06%
	Kawat		68 59 37 59 129	
3	Makro	7	21 59 68 49 45	12,90%
	Mikro		21 118 68 49 45	
4	Peta	7	18 62 129 59	15,38%
	Peti		18 62 129 118	
5	Karapan	7	68 59 49 59 18 59 33	11,90%
	Harapan		91 59 49 59 18 59 33	

Dari pengujian pada Tabel 3, inputan pada plaintext yang berbeda dengan 1 karakter tiap percobaan menggunakan kunci yang sama akan menghasilkan chipertext yang berbeda-beda. Kemudian pada percobaan tersebut menghasilkan rata-rata presentase Avalanche effect yaitu sebesar 10,35%.

4. KESIMPULAN

Dari hasil perancangan dan pembuatan aplikasi Enkrispi dan deskripsi dengan Kriptografi menggunakan Algoritma AES dan algoritma RSA maka didapatkan beberapa hasil. Dari hasil percobaan yang telah dilakukan pada aplikasi ini dapat mengenkripsi dan mendekripsi file file pdf, word, ppt, excel, mp3, gambar dan video dengan sempurna. Setelah file pdf, word, ppt, excel, mp3, gambar dan video dienkripsi terdapat kenaikan besar file rata-rata mencapai 0,030463878% dari file asli. Setelah file pdf, word, ppt, excel, mp3, gambar dan video yang terenkripsi didekripsi maka file kembali ke ukuran semula. Semakin besar ukuran file yang dienkripsi semakin lama juga waktu yang dienkripsi.

5. SARAN

Adapun saran untuk pengembangan selanjutnya adalah menggunakan hardware yang lebiih baru untuk mercepat proses enkripsi dan dekripsi. File yang dapat dienkripsi dan dekripsi tidak hanya file pdf, word, ppt, excel, mp3, gambar dan video tetapi dapat dikembang untuk file yang lain.

DAFTAR PUSTAKA

[1] P. Bindlish, "Study of RSA, DES and Cloud Computing," *Int. J. Adv. Res. Comput. Sci.*, vol. 7, no. 3, pp. 211–215, 2016.

[2] C. Mahalle, M. Kulkarni, T. Nangude, and P. G. Navale, "Digital Signature Authentication and Verification on Smart Phones using CR PT Algorithm," *Int. Res. J. Eng. Technol.*, vol. 4, no. 5, pp. 332–338, 2017.

[3] S. Sitinjak and Y. Fauziah, "Aplikasi Kriptografi File Menggunakan Algoritma Blowfish," in *Seminar Nasional Informatika 2010*, 2010, vol. 2010, pp. 78–86.

[4] D. P. Joseph and M. Krishna, "Cognitive Analytics and Comparison of Symmetric and Asymmetric Cryptography Algorithms," *Int. J. Adv. Res. Comput. Sci.*, vol. 6, no. 3, pp. 51–56, 2015.

[5] Sangeeta and E. A. Kaur, "A Review on Symmetric Key Cryptography Algorithms," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 4, pp. 358–362, 2017.

[6] D. Nilesh and M. Nagle, "The new cryptography algorithm with high throughput," in *2014 International Conference on Computer Communication and Informatics*, 2014, pp. 1–5.

[7] N. Sharma, Prabhjot, and H. Kaur, "A Review of Information Security using Cryptography Technique.," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 4, pp. 323–326, 2017.

[8] R. Mathur, S. Agarwal, and V. Sharma, "Solving security issues in mobile computing using cryptography techniques — A Survey," in *International Conference on Computing, Communication & Automation*, 2015, pp. 492–497.

[9] S. K, "An Optimal RSA Encryption Algorithm for Secret Images," *Int. J. Pure Appl. Math.*, vol. 118, no. 20, pp. 2491–2500, 2018.

[10] Ali, "Comparison and Evaluation of Digital Signature Schemes Employed in NDN Network," *Int. J. Embed. Syst. Appl.*, vol. 5, no. 2, pp. 15–29, Jun. 2015.

[11] E. Setyaningsih, C. Iswahyudi, and N. Widyastuti, "Image Encryption on Mobile Phone using Super Encryption Algorithm," *Telkomnika*, vol. 10, no. 4, pp. 837–845, 2012.

[12] K. R. Ilaga and C. A. Sari, "Analysis of Secure Image Crypto-Stegano Based on Electronic Code Book and Least Significant Bit," *J. Appl. Intell. Syst.*, vol. 3, no. 1, pp. 28–38, 2018.

[13] G. Prasetyadi, R. Refianti, and A. B. Mutiara, "File Encryption and Hiding Application Based on AES and Append Insertion Steganography," *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 16, no. 1, p. 361, Feb. 2018.

[14] M. Vanitha and R. Mangayarkarasi, "Comparative study of different cryptographic algorithms," *Int. J. Pharm. Technol.*, vol. 8, no. 4, pp. 26433–26438, 2016.

[15] E. B. Setiawan and Y. S. Nugraha, "Kriptografi Citra Menggunakan Metode Rivest-Shamir-Adleman Chinese Remainder Theorem Di Konsultan XYZ," *J. Ultim.*, vol. 7, no. 2, pp. 82–90, 2016.

TRANSFORMASI DIGITAL DI MASA PANDEMI COVID-19

Kristophorus Hadiono[1], Hari Murti[2], Rina Candra Nur Santi[3]
[1,2]Program Studi Sistem Informasi, Fakultas Teknologi Informasi, Universitas Stikubank
[3]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Stikubank
e-mail: [1]kristophorus.hadiono@edu.unisbank.ac.id, [2]harimurti@edu.unisbank.ac.id,
[3]r_candra_ns@edu.unisbank.ac.id

ABSTRAK

Era digital merupakan era yang sudah tidak dapat dihindari. Kondisi pandemi covid-19 dan banyak negara berjuang untuk meminimalkan dampaknya yang masih berlangsung. Digitalisasi merupakan salah satu andalan disaat pandemi seperti ini. Digitalisasi datang dan dipercepat, tetapi memiliki dampak yang cukup berat untuk mereka yang tidak siap.

Diawali dari proses digitalisasi, perubahan informasi analog menjadi informasi digital, transformasi digital mulai menggelinding. Organisasi harus siap untuk bermetamorfosis dalam menyambut transformasi digital. Proses transformasi digital biasanya didahului oleh digitalisasi, dimana proses tersebut merujuk kepada penggunaan menggunakan informasi yang sudah dalam bentuk digital untuk menciptakan dan mendapatkan nilai baru dengan cara yang baru. Proses tranformasi digital memunculkan kematangan digital yang dapat dilihat dari dua sisi, dampak digital dan kesiapan digital. Pada 2 dimensi tersebut, organisasi ditantang dan diberikan dua pilihan, yaitu berubah atau tergilas.

Organisasi harus siap melakukan perubahan fundamental dan memiliki kesigapan yang cukup dalam menjawab dampak digital dan mempersiapkan dirinya untuk menyambut transformasi digital. Akibat yang ditimbulkan oleh tranformasi digital terhadap organisasi akan berbeda-beda dan tidak menjadi masalah pada titik mana organisasi dapat berubah dan bertahan dalam lingkup kematangan digital.

Kata Kunci*: transformasi digital, kematangan digital, digitalisasi*

1. PENDAHULUAN

Era sekarang merupakan era digital. Era digital saat ini sudah bukan merupakan impian, tetapi menjadi sebuah kenyataan yang harus dijalani terlebih disaat pandemi Covid-19 melanda seluruh negara di dunia. Pandemi Covid-19 membuat perubahan yang sudah tajam, menjadi lebih tajam. Perubahan sebelumnya dipicu oleh kompetisi, permintaan pasar, munculnya teknologi baru, dan peraturan / regulasi baru dari otoritas. Perubahan yang terjadi sekarang selain dipicu oleh hal-hal yang sudah dikenal sebelumnya, sekarang ditambah faktor pandemi Covid-19. Perubahan saat ini menjadi lebih berat karena kondisi pandemi menyebabkan pergerakan fisik manusia terbatas.

Kondisi di era digital saat ini menuntut semua aktor dalam kehidupan ekonomi dan sektor lainnya tidak gagap dengan teknologi, terutama teknologi informasi / digital. Hal ini dapat dilihat dari berita yang dipublikasi di media online surat kabar nasional kompas di tahun 2019. Pada tahun tersebut, tingkat daya saing Indonesia berada pada posisi 32 diantara 63 negara dunia. Posisi tersebut naik 11 poin bila dibandingkan dengan tahun lalu (Tahun 2018, Indonesia berada di posisi 43 dunia). Naiknya posisi tersebut disebabkan karena ada peningkatan efisiensi di sektor pemerintahan, perbaikan infrastruktur, dan kemudahan berusaha [1]. Tetapi di tahun 2020 lalu, posisi Indonesia turun ke peringkat 40. Turunnya peringkat Indonesia ke posisi 40 dipengaruhi oleh beberapa hal, seperti laju pertumbuhan ekonomi yang melambat karena pandemi covid-19 melanda Indonesia. Pelambatan laju pertumbuhan ekonomi memberikan dampak yang cukup kuat. Dampak tersebut mengakibatkan ketidakpastian ekonomi yang menyebabkan naiknya angka pengangguran sehingga masyarakat miskin bertambah, serta menurunnya kegiatan ekspor dan impor karena penurunan permintaan ataupun penurunan pasokan dari negara lain [2].

Dari laporan berjudul IMD World Digital Competitiveness Ranking 2020, dibuat oleh Institute for Management Development (IMD) yang berkedudukan di Swiss, dan terbit di tahun 2020; terdapat beberapa faktor penilaian. Faktor penilaian tersebut adalah Knowledge, Technology, dan Future Readiness [3]. Masing-masing faktor tersebut memiliki 3 (tiga) sub faktor lagi. Dimana, faktor Knowledge memiliki sub faktor Talent, Training & Education, dan Scientific concentration. Faktor Technology memiliki sub faktor Regulatory framework, Capital, dan Technological framework; sedangkan faktor Future Readiness memiliki sub faktor Adaptive attitudes, Business agility, dan IT integration. Faktor Knowledge merupakan faktor yang memiliki tujuan untuk menangkap apakah sebuah negara memiliki kemampuan, kesadaran, pemahaman atas sesuatu (biasanya disebut sebagai intangible/tidak terlihat) yang dibutuhkan untuk belajar dan menemukan teknologi baru. Faktor Technology merupakan faktor yang memiliki tujuan untuk menilai kesiapan sebuah negara untuk masuk dalam fase pengembangan / pembangunan transformasi digital. Istilah umum yang dapat digunakan adalah kesiapan lingkungan dari negara tersebut untukmasuk ke dalam fase transformasi digital. Faktor terakhir, *Future readiness*, merupakan faktor yang memiliki tujuan untuk menilai tingkat kesiapan ekonomi sebuah negara dalam mencapai transformasi digital.