PEMBEKALAN TEKNIK ALGORITMA DALAM KEAMANAN DATA ERA REVOLUSI INDUSTRI 4.0

Nizirwan Anwar [1], Erry Yudhya Mulyani [2], Ummanah[2]
[1]Fakultas Ilmu Komputer, [2]Lembaga Penelitian dan Pengabdian Masyarakat Universitas Esa Unggul
Jalan Arjuna Utara No 9 Kebon Jeruk Jakarta 11510
nizirwan.anwar@esaunggul.ac.id

Abstract

Allah SWT created humans on earth as sosial beings to interact or communicate with each other (correspondence / collaboration). And along with the exponential development of information and communication technology, it has changed the mindset and attitude and the way of communicating in the virtual world of sosial networking pages via cyberspace. With the aim of gaining comfort, sharing ideas, calm, creative and innovative collaborations that are constructive in correspondence or user-generated content. In computer security, there are several important aspects of Confidentiality, so that the data on the device does not fall into unauthorized "hands" and which is not authorized. In general, the concept of cryptography is an information security or protection technique that is carried out by processing original information with a certain key using an encryption algorithm so as to produce new information that cannot be read directly. And to restore the integrity of the ciphertext, it can be returned to the original information through the description process. In principle, encryption is the process of randomizing or changing the initial message into other forms and structures so that the initial message cannot be recognized by other parties.

Keywords*: human, sosial-media, cryptography, cyberspace, encryption / decryption*

Abstrak

Allah SWT menciptakan manusia di muka bumi sebagai makhluk sosial untuk saling ber-interaksi atau ber-komunikasi (korespodensi/kolaborasi). Dan seiring berkembang pesat secara ekponensial teknologi informasi dan komunikasi telah mengubah pola pikir dan sikap serta cara berkomunikasi dalam dunia maya laman jejaring sosial lewat dunia maya. Dengan bertujuan memperoleh kenyamanan, bertukar pikiran dalam berbagi, ketenangan, kolaborasi kreatif dan inovatif yang bersifat konstruktif dalam berkorespodensi atau *user-generated content*. Dalam keamanan komputer terdapat beberapa aspek penting *Confidentiality*, agar data yang berada di perangkat tidak jatuh pada 'tangan' yang tidak berhak dan *which is not authorized*. Secara umum konsep kriptografi merupakan teknik pengamanan atau perlindungan informasi yang dilakukan dengan cara mengolah informasi asli dengan suatu kunci tertentu menggunakan suatu algoritma enkripsi dengan sehingga menghasilkan informasi baru yang tidak dapat dibaca secara langsung. Dan untuk mengembalikan keutuhan chipertext tersebut dapat dikembalikan menjadi informasi asli melalui proses deskripsi. Pada prinsipnya Enkripsi adalah proses mengacak atau merubah pesan awal menjadi bentuk dan susunan lain sedemikan sehingga tidak dapat dikenali pesan awal oleh pihak lain.

Kata kunci : manusia, sosial-media, kriptografi, dunia maya, enkripsi/dekripsi

Pendahuluan

Manusia diciptakan Allah SWT di muka bumi sebagai makhluk sosial yang mempunyai kecenderungan bersifat fitrah untuk saling berinteraksi atau berkomunikasi antar satu sama lain nya (*sosial a public*). Sebagaimana terkandung dalam Firman Allah SWT di Al-Qur'an "*Wahai manusia, sesungguhnya Kami menciptakan kamu dari pria dan wanita, dan membuat kamu suku-suku dan kabilah-kabilah, agar kamu saling mengenal. Sesungguhnya yang paling mulia diantara kamu adalah yang paling takwa diantara kamu.Sesungguhnya Allah itu yang maha mengetahui, yang maha waspada.* (QS. Al-Hujarat [49] Juz 26:13). Dan seiring berkembang dengan pesat secara ekponensial teknologi informasi dan komunikasi telah mengubah pola pikir dan sikap serta cara berkomunikasi (via media sosial) dalam dunia maya (virtual) yang tidak mengenal batasan wilayah (*any where, any time and no limit*). Indonesia atau Negara Kesatuan Republik Indonesia (NKRI) sebagai negara yang terdiri 16.056 kepulauan, 34 provinsi, 1 1.340 suku dan sekitar 700 bahasa daerah. Populasi suku jawa tertinggi ada sebanyak 95.2 juta (40.45%) dari total penduduk Indonesia sebanyak 260 juta(Indonesia, 2020).

Gambar 1
Peta NKRI

Gambar 2
Peta Dunia

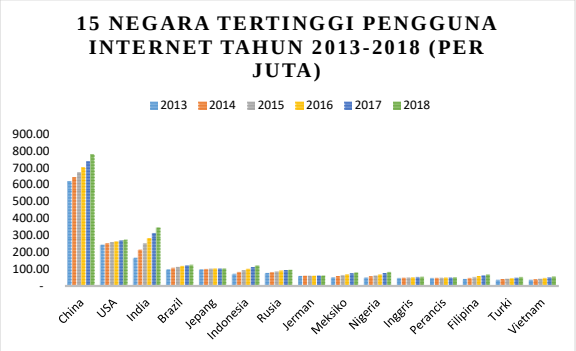
Dalam hal ini dibutuhkan oleh setiap pengguna yang terhubung pada dunia cyber (data) mempertimbang dan memperhatikan masalah keamanan data seiring dengan tumbuh pesatnya jejaring sosial daring. Laman jejaring sosial diawali oleh Classmates.com pada tahun 1995 yang berfokus pada hubungan antar mantan teman sekolah dan SixDegrees.com pada tahun 1997 (Boyd & Ellison, 2007)(Stallings, 2014) dengan feature laman tersebut sebatas membuat netizen pada zamannya pertama kali bisa meng-upload profile *picture* dan mencari teman baru lewat dunia maya. Dengan adanya jejaring ini yang saling terhubung melalui perangkat digital media teknologi menjadi, dengan bertujuan memperoleh kenyamanan, bertukar pikiran dalam berbagi, ketenangan, kolaborasi kreatif dan inovatif yang bersifat konstruktif dan *healthy* seseorang dalam berkorespodensi (saling bertukar informasi) atau *user-generated content* (Kaplan & Haenlein, 2010). Dengan kemunculan teknologi berbasis media online (daring) menjadi salah satu solusi effektif untuk saling bertukar informasi *(collaborate a networking*) dengan orang-orang di belahan dunia dengan maya. Eksistensi media sosial berdampak pada pada biaya yang lebih murah dan mudah dalam mendistribusikan informasi secara tepat dan cepat. Berdasarkan data statistic (trend dan media sosial) menunjukkan bahwa penetrasi internet sejak tahun 2016 – 2020 (gambar 1), Indonesia menempati secara rata-rata sebanyak 4% dari jumlah penetrasi di dunia ekuivalensi 1 hingga 6 individu di dunia adalah pengguna akses ke dunia maya dan waktu yang digunakan 03.26 dalam akses ber-sosial media**.** Dengan semakin tinggi para pengguna digital yang harus diperhatikan dan melakukan langkah preventif dalam menjaga informasi yang tidak diperkenankan untuk di-akses oleh pihak lain (*authorize access by other eople who do not have the authority*), pendekatan dalam pengamanan data dan jenis kejahatan dalam dunia digital serta menampilkan contoh cara mengatasi bila akun ternyata ada meng-hack (membobol akun).

Gambar 3
Poster Forum Ilmiah Dosen 2020

Hal ini menjadikan dasar bahwa tidak ada teknologi informasi yang di-rancang secara sempuran sehingga bebas dari segala bentuk attack dan kerawanan (*vulnerabilities*) berdasarkan laporan lembaga riset pengguna jasa data dan penyedia atau pengawas data menunjukkan bahwa terdapat kerawanan/ kewaspadaan pada program aplikasi semakin meningkat baik secara kuantitas dan kualitasnya.

Tabel 1
Rangking Indonesia diantara 15 Negara Pengguna Internet Tahun 2013-2018 (Kominfo, 2014)

Negara	Tahun					
	2013	2014	2015	2016	2017	2018
China	620.70	643.60	669.80	700.10	736.20	777.00
USA	246.00	252.90	259.30	264.90	269.70	274.10
India	167.20	215.60	252.30	283.80	313.80	346.30
Brazil	99.20	107.70	113.70	119.80	123.30	125.90
Jepang	100.00	102.10	103.60	104.50	105.00	105.40
Indonesia	**72.80**	**83.70**	**93.40**	**102.80**	**112.60**	**123.00**
Rusia	77.50	82.90	87.30	91.40	94.30	96.60
Jerman	59.50	61.60	62.20	62.50	62.70	62.70
Meksiko	53.10	59.40	65.10	70.70	75.70	80.40
Nigeria	51.80	57.70	63.20	69.10	76.20	84.30
Inggris	48.80	50.10	51.30	52.40	53.40	54.30
Perancis	48.80	49.70	50.50	51.20	51.90	52.50
Filipina	42.30	48.00	53.70	59.10	64.50	69.30
Turki	36.60	41.00	44.70	47.70	50.70	53.50
Vietnam	36.60	40.50	44.40	48.20	52.10	55.80



Gambar 4
Pengguna Digital Dunia dan Indonesia tahun 2016 – 2018, Penetrasi (Kemp, 2020)

Dari tabel 1 dan gambar 4, Indonesia secara rata meningkat sekitar 98.05 juta pengguna jasa data pada periode tahun 2013 hingga 2018. Dan gambar 3, Indonesia memperlihatkan adanya peningkatan yang sangat signifikasi dari tahunke tahun dalam menggunakan sosial media dalam berkorespondensi dan berkolaborasi seiring bertumbuhnya populasi penduduk rata-rat sekitar 125% (*device non-mobile*) dan 81,60% (*device mobile*). Bagaimana seharusnya orang dalam memanfaatkan jejaring sosial faktor apa saja yang mempengaruhi meningkatnya pengguna akses sosial media ? Bagaimana dampak positif dan negatif dalam membangun kepribadian seseorang yang seharusnya mem-posting status di dunia internet?

Metode Pelaksanaan

Menindaklanjuti Surat Edaran dari Menteri Pendidikan dan Kebudayaan (Kemdikbud) nomor 36962/MPK.A/HK/2020 tanggal 17 Maret 2020 perihal Pembelajaran secara Daring dan Bekerja dari Rumah dalam Rangka Pencegahan *Corona Virus Disease* (COVID-19), LLDIKTI 3 hal Kegiatan Pengabdian Kepada Masyarakat Secara Daring Nomor 2207/LL3/PT/2020 tanggal 15 Juni 2020 dan undangan Kepala LPPM Universitas Esa Unggul Nomor 06/LPPM-INT/PEN/VI/2020 tanggal 17 Juni 2020. Berdasarkan informasi diatas webinar dilaksanakan secara daring (*virtual*) dengan menggunakan aplikasi *Cloud Zoom Meeting* dan *live streaming youtube*.

Gambar 5
Jadwal Forum Ilmiah Dosen 2020

Tampilan zoom

Gambar 6
Tampilan Zoom CM Forum Ilmiah Dosen 2020

Para peserta webinar diberikan materi yang berkaitan dengan keamanann data dalam bentuk format (ppt dan atau pdf) dan e-sertifikat. Selama dan sebelum berlangsungnya seminar daring semua peserta diharuskan tata tertib yang ditentukan ;

1) Peserta yang mengikuti dan menghadiri mengisi form kepesertaan acara webinar
2) Peserta wajib mengisi absensi kehadiran
3) Peserta mendapatkan kesempatan menyampaikan pertanyaan dan dijawab narasumber.
4) Peserta 'wajib' mengisi kuesioner sebagai bahan evaluasi pelaksanaan webinar

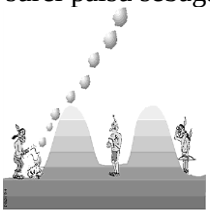
Peserta akan memperoleh e-sertifikat bila point 2 dan 4 bila telah dipeunhi, dan e-sertifikat akan dikrimkan secara otomatis ke email (surel) masing-masing peserta.

Teori Ancaman Keamanan Data

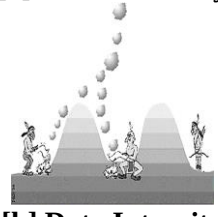
Kemajuan dan perkembangan teknologi informasi telah membawa dampak secara *massive* pada pola pikir dan perilaku orang dalam memanfaatkan informasi yang ter-hosting dalam

dunia maya. Informasi dalam bentuk dokumentasi elektronik yang dibuat, diteruskan, dikirimkan, diterima ataupun disimpan dalam bentuk/format analog, digital, elektromagnetik, optical dan atau sejenisnya. Dengan kemajuan teknologi memungkinkan semakin meningkatkan munculnya pihak yang berperilaku tidak baik/jahat melakukan ancaman (*cyber threat*) inilah yang dinamakan dengan istilah *cybercrime*, informasi yang didapatkan *cybercrime* Bareskrim Polri sejak tahun 2015(Rizki, 2018) mencatat ada 100 ribu akun di Medsos yang menyebarkan hate speech dan tahun 2016 ada sekitar 90 juta (Dakwah et al., 2018). Tahun 2016 tersebut Indonesia menempati rangking kedua setelah Jepang dalam melakukan kejahatan di dunia maya. Sebagai langkah awal sebagai pengguna internet diharuskan mengenal dan mengetahui dan memahami hal atau faktor saja dalam melakukan dan menyikapi pengamanan data yang telah di-hosting dalam dunia maya. Prinsip dalam keamanan data menurut William Stallings (Stallings, 2014)(Rahardjo, 2017) terdapat beberapa serangan yang umum terjadi pada aspek keamanan komputer antara lain;

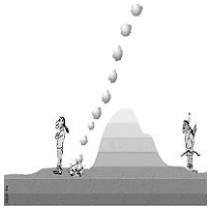
1) *Interruption*, perangkat sistem menjadi rusak atau tidak tersedia, aspek keamanan yang ditujukan adalah ketersediaan(availability) sistem. Contoh : *Denial of Service Attack*.
2) *Interception*, sistem diakses oleh orang yang tidak berhak. Contoh: Penyadapan/ *Wiretapping*.
3) *Modification*, pihak yang tidak berhak berhasil mengakses dan mengubah data. Contoh: mengubah isi laman dengan pesan-pesan yang merugikan pemilik laman.
4) *Fabrication*, pihak yang tidak berwenang menyisipkan objek palsu kedalam sistem seolah-olah sebagai pihak yang berhak. Contoh: mengirimkan surel palsu sebagai orang lain.



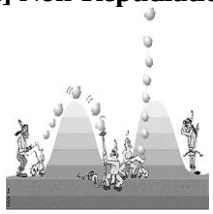
[a] Confidentiality



[b] Data Integrity



[c] Non-Repudiation



[d] Authentication

Gambar 7
Prinsip Dasar Kriptografi

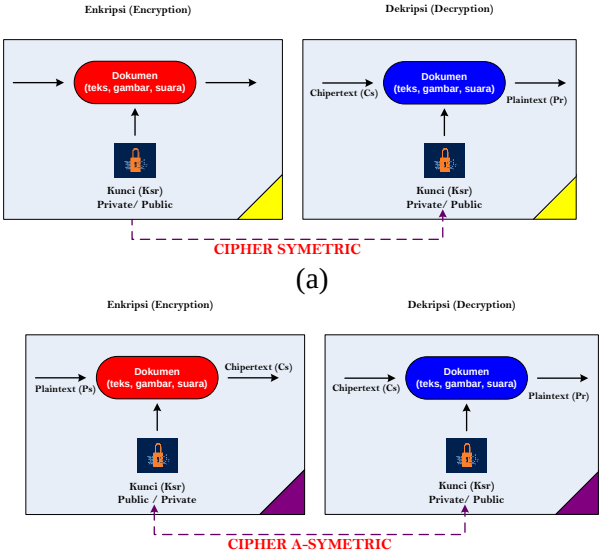
Dalam keamanan komputer (Rahardjo, 2017)(Orman, 2015)(Schneier, 1996) terdapat beberapa aspek penting (gambar 4) yang harus diperhatikan antara lain:

1) *Confidentiality*, agar data yang berada di perangkat (desktop/mobile phone) tidak jatuh pada 'tangan' yang tidak berhak dan *which is not authorized*, dan pada aspek ini digunakan teknik penyandian (kriptografi) yang terkait dengan sumber data dan pada umum menggunakan *passcode*. Akan tetapi pada teknik kriptografi jauh lebih kompleks (sophiscated) dari hanya sekedar dari *passcode*.
2) *Data Integrity*, aspek yang menjamin data/informasi tidak berubah seperti data awal (keutuhan), data dapat diubah bila dapat jin pemilik informasi.
3) *Authentication*, suatu proses validasi terhadap *user cridentials* untuk menentukan apakah seorang user's untuk dapat meng-akses jalur data atau computing services
4) *Non-Repudiation*, aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi (receiver/transmitter) bersifat elektronik digital.
5)

Kriptografi

Konsep operasional secara umum kriptografi merupakan teknik pengamanan atau perlindungan informasi yang dilakukan dengan cara mengolah informasi asli (plainteks) dengan suatu kunci tertentu (*public/private*) dengan algoritma enkripsi (simetris dan atau asimetris) dengan sehingga menghasilkan informasi baru (*chipertext*) yang tidak dapat dibaca secara langsung (*encryption*). Dan untuk proses keutuhan (data *integrity*) chipertext tersebut dapat dikembalikan menjadi informasi asli (*plaintext*) melalui proses deskripsi (*decryption*) (Anwar, Munawwar, Abduh,

& Santosa, 2018). Pada prinsipnya Enkripsi adalah proses mengacak atau merubah pesan awal menjadi bentuk dan susunan lain sedemikan sehingga tidak dapat dikenali pesan awal oleh pihak lain. Beberapa proses enkripsi menyertakan kunci didalam proses pangacakannya agar data yang dienkripsi dapat didekripsikan kembali (data utuh).Dalam proses enkripsi dan dekripsi data (plainteks/cipherteks) dikenal dengan 2 (dua) pendekatan algoritma yaitu kriptografi simetris dan kriptografi asimetris



Gambar 8
Prinsip Algoritma Kriptografi (a) Simetris (b) Asimetris

Common Vulnerabilities and Exposures (CVE) adalah sistem yang menyediakan metode referensi terkait kerentanan (*vulnerability*) dan paparan (exposure) keamanan informasi (Corporation, 2016) yang diketahui publik. National Cybersecurity FFRDC, yang dioperasikan oleh Mitre Corporation, memelihara sistem, dengan dana dari Divisi Keamanan Siber Nasional dari Departemen Keamanan Dalam Negeri Amerika Serikat. Sistem ini secara resmi diluncurkan untuk umum pada bulan September 1999(Anonymous, 2020). Menurut CERT-UK dalam penelitian mereka yang berjudul "An introduction to *Sosial Engineering (*SE*)*," dikatakan bahwa SE merupakan salah satu jenis serangan yang paling efektif dan paling produktif untuk mendapatkan informasi dengan cara masuk ke dalam suatu sistem yang memiliki mekanisme keamanan rumit. Celakanya lagi, serangan ini dapat dilakukan tanpa membutuhkan ilmu teknis yang baik (CERT-UK, 2015). Siklus penting yang sering digunakan dalam mendapatkan informasi melalui *Sosial engineering* (Christopher Hadnagy, 2011), antara lain:

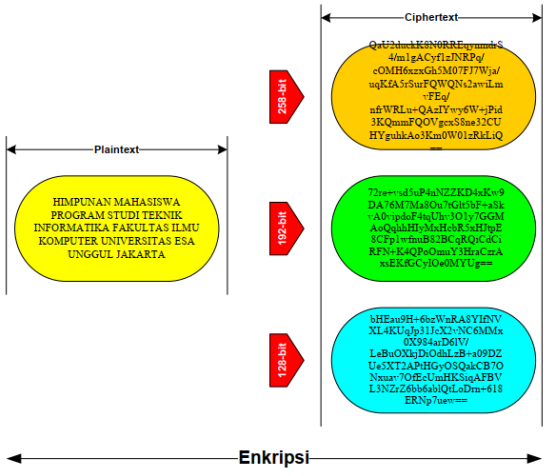
1) *Sosial engineering* mencari informasi terkait apa yang akan ia cari dan siapa yang bisa ia jadikan target eksploitasi.
2) *Sosial engineering* akan membangun hubungan dengan target yang dimaksud. Membangun hubungan tersebut dapat dilakukan dengan berbagai cara seperti bekerja pada organisasi yang ia jadikan target, membangun hubungan pertemanan ataupun persaudaraan bahkan membangun hubungan emosional.
3) *Sosial engineering* akan memanfaatkan psikis target untuk mendapatkan informasi dengan bermacam macam cara seperti rayuan, ancaman, suapan, dll.

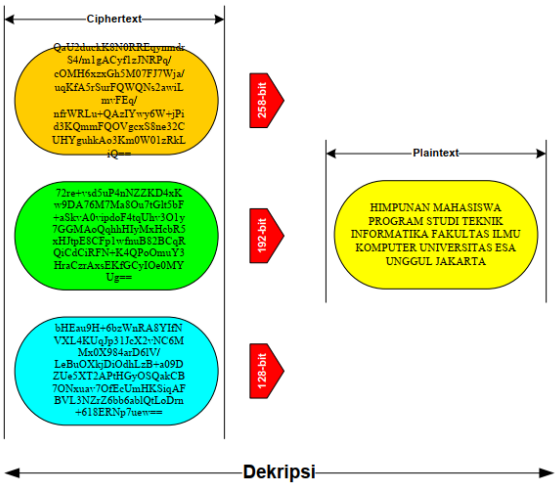
Hasil dan Pembahasan

Plaintext (sebagai sample data)

HIMPUNAN MAHASISWA PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER UNIVERSITAS ESA UNGGUL JAKARTA

dan menghasilkan ciphertext dapat dilihat dalam gambar 9(a) dan 9(b) dengan menggunakan dan mengimplementasikan kriptografi algoritma AES (Munir, 2004)(Rothke, 2007)(Stallings, 2014).





(b)

Gambar 9
Algoritma Kriptografi AES

Tabel 2
Hasil Survei Responden

Respon	Q1	Q2	Q3	Q4	Q5
Ragu	2.86%	11.43%	11.43%	2.86%	0.00%
Tidak Setuju	2.86%	45.71%	0.00%	0.00%	2.86%
Sangat Tidak Setuju	0.00%	22.86%	0.00%	0.00%	0.00%
Setuju	60.00%	8.57%	60.00%	**77.14%**	57.14%
Sangat Setuju	34.29%	11.43%	28.57%	20.00%	40.00%

Untuk mengembalikan pesan tersebut, perlu melakukan tahap dekripsi dengan menghasilkan yang tertera pada gambar 7b, sehingga dapat disimpulkan file tetap utuh sesuai dengan aslinya (plainteks) dan pada ukuran terdapat penyusutan (*compressing*) 98.31% (128 bit) serta 99.15% (192 bit dan 256 bit). Dan berdasarkan hasil survei (virtual) dalam melakukan bagaimana respon masyarakat dengan teknologi berbasis sosial media signifikasi dengan sosial engineering dengan jumlah 135 responden, dihasilkan dalam bentuk tabel di bawah ini

Keterangan ;

Q1 = [Berkembangnya "sosial engineering" akan berdampak cara berpikir dan berperilaku ke arah membangun kepribadian yang seutuhnya.

Q2 = [Berdasarkan survei Digital Indonesia tahun 2016 – 2020 potret penggunaan optimasi media sosial makin menurun tahun dari ke tahun]

Q3 = [Angka survei APJII tahun 2016 penetrasi pengguna internet di Indonesia tertinggi di pulau Jawa dan terendah di Maluku dan Papua]

Q4 = [Sosial engineering terbagi menjadi dua tipe, human based dan computer based]

Q5 = [Pembunuhan karakter atau perusakan reputasi adalah usaha untuk mencoreng reputasi seseorang merupakan salah satu dampak dari rekayasa sosial negatif]

Kesimpulan

Masifnya pergerakan data yang ada di internet patut menimbulkan kehati-hatian dalam memberikan informasi pribadi. Kemudahan akses yang diberikan bukan berarti dianggap hanya sebatas fasilitas namun juga sebagai bentuk peringatan agar informasi pribadi tidak mudah dicuri. Maka dari itu, adanya kriptografi menjadi sebuah usaha dalam meningkatkan keamanan disamping tetap dibutuhkannya kewaspadaan dari pemilik data. Meskipun tetap akan ada celah, namun diharapkan hal ini dapat mempersulit pencuri dalam mengambil data yang ada.

Daftar Pustaka

Anonymous. (2020). Common Vulnerabilities and Exposures. Retrieved March 25, 2020, from Wikipedia website: cve.mitre.org

Anwar, N., Munawwar, M., Abduh, M., & Santosa, N. B. (2018). Komparatif Performance Model Keamanan Menggunakan Metode Algoritma AES 256 bit dan RSA. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *2*(3), 783–791. https://doi.org/10.29207/resti.v2i3.606

Boyd, D., & Ellison, N. (2007). Social Network Sites: Definition, History, and Scholarship. *J. Computer-Mediated Communication.*, *13*(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Christopher Hadnagy. (2011). *Social Engineering: The Art of Human Hacking*. Retrieved from http://www.wiley.com

Corporation, T. M. (2016). Common Vulnerabilities and Exposures (CVE®). Retrieved from https://cve.mitre.org/docs/cve-intro-handout.pdf

Dakwah, J., Sosial, P., Vol, K., Syaikh, I., Siddik, A., & Belitung, B. (2018). *Hate Speech di Indonesia: Bahaya dan Solusi*. *9*(1), 3–4.

Indonesia, B. P. S. (2020). *Statistik Indonesia 2020* (1st ed.; S. P. dan K. Statistik, Ed.). Retrieved from https://www.bps.go.id/publication/2020/04/29/e9011b3155d45d70823c141f/statistik-

indonesia-2020.html

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Sosial Media. *Business Horizons*, *53*(1), 59–68.

Kemp, S. (2020). Digital 2020: 3.8 billion people use social media.

Kominfo. (2014). Pengguna Internet Indonesia Nomor Enam Dunia. Retrieved from Kementrian Komunikasi dan Informatika Republik Indonesia website: http://tekno.kompas.com/read/2014/11/24/07430087/Pengguna.Internet.Indonesia.Nomor.Enam.Dunia

Munir, R. (2004). *Advanced Encryption Standard (AES) Departemen Teknik Informatika Institut Teknologi Bandung 13 . Advanced Encryption Standard (AES)*.

Orman, H. (2015). *Encrypted Email - SPRINGER BRIEFS IN COMPUTER SCIENCE*.

Rahardjo, B. (2017). *Keamanan Informasi & Jaringan*. 47. Retrieved from http://budi.rahardjo.id/files/keamanan.pdf

Rizki, R. (2018). Polri: Indonesia Tertinggi Kedua Kejahatan Siber di Dunia. Retrieved from https://www.cnnindonesia.com/nasional/20180717140856-12-314780/polri-indonesia-tertinggi-kedua-kejahatan-siber-di-dunia

Rothke, B. (2007). A look at the Advanced Encryption Standard (AES). *Information Security Management Handbook, Sixth Edition*, 1151–1158. https://doi.org/10.1201/9781439833032.ch89

Schneier, B. (1996). *Foreword by Whitfield Diffie Preface About the Author Chapter 1 — Foundations Part I — Cryptographic Protocols Chapter 2 — Protocol Building Blocks Chapter 3 — Basic Protocols Chapter 4 — Intermediate Protocols Chapter 5 — Advanced Protocols*.

Stallings, W. (2014). *Cryptography and Network Security: Principles and Practice, International Edition: Principles and Practice*. Retrieved from https://books.google.com/books?id=q_6pBwAAQBAJ&pgis=1