Verifikasi *Quick Response Code* dengan Vigenere *Cipher* dan *Multi-Factor* RSA

Quick Response Code Verification using Vigenere Cipher and Multi-Factor RSA

Bagas Dwi Yulianto[1], Said Hirzi Hadi[2]
[1]Program Studi S1 Informatika, Universitas Pignatelli Triputra
[2]Program Studi S1 Rekayasa Perangkat Lunak, Universitas Pignatelli Triputra
E-mail: [1]bagas19.yulianto@gmail.com, [2]hirzihadi01@gmail.com

Abstrak

Data personal merupakan hal yang sensitif bagi pemiliknya. Kelalaian dari penggunaan teknologi terkini seperti *QR Code* yang kurang tepat dapat mengakibatkan kebocoran data atau informasi. Pada hakikatnya *QR Code* hanya mengubah informasi menjadi gambar dua dimensi yang pembacaannya menggunakan sistem pindai, sehingga informasi yang didalamnya belum terlindungi dan informasi tersebut dapat langsung dibaca oleh semua orang. Penelitian ini berfokus pada kombinasi kriptografi simetris *Vigenere Cipher* serta kriptografi asimetris RSA yang ditingkatkan lagi menjadi *Multi-factor* RSA. Kombinasi tersebut untuk meningkatkan keamanan suatu informasi/data sebelum dirubah menjadi *QR Code*. Metode yang diusulkan membuktikan bahwa *QR Code* yang dipindai langsung dari berbagai perangkat akan menghasilkan kode enkripsi sehingga pihak tidak bertanggungjawab tidak dapat membaca nilai pesan asli. Pesan asli hanya bisa dibaca dari dari *scanner* dengan metode yang diusulkan sehingga keamanan *QR Code* terverifikasi. Serta hasil uji dengan *Avalanche effect* memenuhi standar baik dengan nilai 53,671875%.

Kata kunci: *QR Code, Vigenere Cipher, Multi-factor RSA*

Abstract

Personal data is sensitive to its owner. Negligence to use the latest technology such as an inappropriate QR Code can result in data or information leaks. In essence, a QR Code only changes information into a two-dimensional image that can be read using a scanning system, so that the information contained therein is not protected and the information can be read directly by everyone. This research focuses on a combination of Vigenere Cipher symmetric cryptography and RSA asymmetric cryptography which has been further upgraded to Multi-factor RSA. This combination is to increase the security of information/data before it is converted into a QR Code. The proposed method proves that QR Codes scanned directly from various devices will produce encryption so that irresponsible parties cannot read the original message value. The original message can only be read from the scanner with the proposed method so that the security of the QR Code is verified. Avalanche effect test results meet good standards with a value of 53.671875%.

Keywords: QR Code, Vigenere Cipher, Multi-factor RSA

1. PENDAHULUAN

Data personal merupakan hal yang sensitif bagi pemiliknya. Pertukaran data sebagai informasi di masa ini tidak dapat dihindarkan lagi karena teknologi informasi yang selalu bergerak dengan cepat [1]. Informasi tersebut jelas rentan terhadap berbagai serangan dari berbagai pihak untuk mendapatkan, merubah, mencuri isi dari informasi tersebut [2]. Informasi dari Kementrian Komunikasi dan Informatika pada siaran pers no 138/HM/KOMINFO/07/2023 terdapat ±90 kasus kegagalan perlindungan data sepanjang tahun 2019 – 2023, dengan 86,7% merupakan kasus

kebocoran data pribadi [3]. Berkaca dari kasus tersebut, data personal milik pribadi sangat mudah untuk diserang. Kelalaian serta penggunaan teknologi terkini seperti *Quick Response Code (QR Code)* yang kurang tepat dapat pula mengakibatkan kebocoran data atau informasi.

Data atau informasi saat ini telah banyak menggunakan teknologi *QR Code* [4], teknologi tersebut merubah informasi menjadi bentuk kode dua dimensi dengan visual berbentuk gambar kotak-kotak [5]. Popularitas *QR Code* meningkat drastis dibandingkan dengan *barcode* dikarenakan konversi karakternya yang lebih besar serta varisai serta visualnya yang lebih bagus [6] namun seringkali *QR Code* digunakan hanya untuk merubah informasi secara langsung, sehingga semua orang yang memiliki wewenang ataupun tidak dapat memindai kode tersebut dan melihat informasi didalamnya, sehingga informasi didalamnya dapat terancam keamanannya. Maka perlu penggunaan metode kriptografi untuk menyamarkan kode, sehingga terverifikasi hanya pihak yang memiliki akses yang dapat melihat informasi didalamnya.

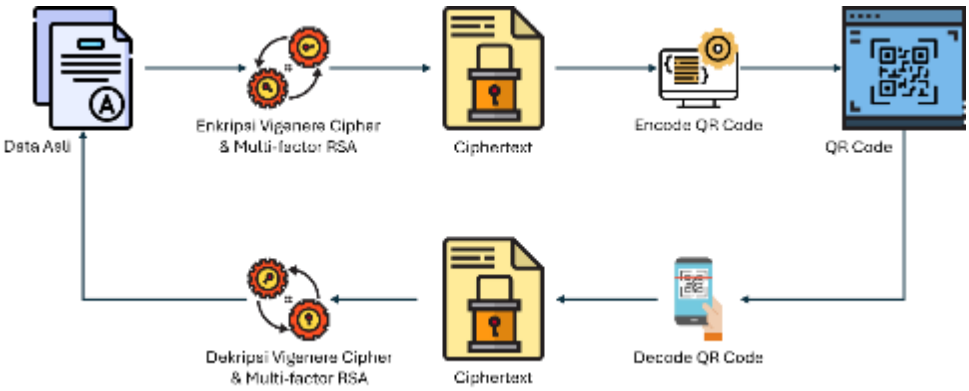
Penggunaan kriptografi kunci simetris yaitu *Vigenere Cipher* yang telah teruji tidak dapat dipecahkan serta kerahasiaannya yang mumpuni, algoritma tersebut telah digunakan untuk memenuhi kasus kriptografi dan standar keamanan modern [7]. *Vigenere Cipher* menggunakan teknik penyandian subtitusi *monoalphabetic* yang berbeda-beda pada *ciphertext* sehingga pesan dapat disembunyikan [8]. Untuk lebih meningkatkan keamanan digunakan kriptografi kunci asimetris memiliki kunci publik dan kunci privat, salah satunya adalah algoritma RSA yang memiliki waktu eksekusi enkripsi maupun dekripsi paling cepat dibandingkan DSA dan ElGamal [9]. Peningkatan RSA ke *Multi-factor* RSA menjamin kualitas keamanan [10] karena menggunakan lebih banyak bilangan prima [11]. Bilangan prima pada Multi-factor RSA selaras dengan peningkatan keamanan [12] serta dapat juga dapat mengurangi ukuran data [13].

Penelitian dari E. H. Rachmawanto, dkk. [14], menyatakan pengujian enkripsi *Vigenere Cipher* berjalan dengan baik sehingga dapat menyembunyikan informasi dan dapat disimpan dengan baik di dalam QR Code. Lalu A. M. S. Pangan, dkk. [15], berhasil membuat sistem berbasis web untul layanan Covid-19 terpusat dengan mengotentikasi *QR Code* menggunakan algoritma RSA asimetris untuk melindungi privasi penggunanya. Dari dua penelitian yang telah berhasil maka fokus penelitian ini adalah mengkombinasikan kriptografi *Vigenere Cipher* dan *Multi-factor* RSA menjadi super enkripsi.

Diharapkan kombinasi tersebut memverifikasi *QR Code* dengan lebih baik dengan pengujian *Avalanche Effect*, sehingga informasi dalam *QR Code* hanya dapat diakses oleh pihak tertentu dan meningkatkan keamanannya. Sehingga menyelesaikan permasalahan mendasar berkaitan langsung dengan data personal yang merupakan informasi vital dimiliki oleh setiap individu [16]. Dengan adanya teknik pengamanan data yaitu kriptografi diharapkan keamanan data dan informasi yang dimiliki tiap individu meningkat. Kemudian permasalahan yang ada pada penggunaan teknologi *QR Code* yang digunakan secara langsung, memiliki kerentanan terhadap kebocoran data [17]. Pada hakikatnya *QR Code* hanya mengubah informasi menjadi gambar dua dimensi yang pembacaannya menggunakan sistem pindai [18], sehingga informasi yang didalamnya belum terlindungi dan informasi tersebut dapat langsung dibaca oleh semua orang.

2. METODE PENELITIAN

Penelitian ini berfokus pada kombinasi kriptografi simetris *Vigenere Cipher* serta kriptografi asimetris RSA yang ditingkatkan lagi menjadi *Multi-factor* RSA. Kombinasi tersebut untuk meningkatkan keamanan suatu informasi/data sebelum dirubah menjadi QR Code [14] dengan mengenkripsinya. Sehingga verifikasi keamanannya terjaga dan akses informasi diberikan kepada pihak yang memiliki kewenangan.



Gambar 1 Skema Proses Penelitian

Skema proses penelitian dijelaskan secara rinci pada poin-poin dibawah ini:

2.1 Data uji

Data uji diperoleh dengan menggunakan pemrograman *random text* sehingga terkumpul data-data privat yang nantinya diolah dengan algoritma usulan dan diubah dalam bentuk *Qr Code*.

2.2 Proses enkripsi data

Enkripsi data menggunakan kombinasi algoritma usulan, yang pertama *Vigenere Cipher*, merupakan algoritma simetris dengan satu kunci privat [19] dengan persamaan (1), dikarenakan data uji di cari nilai ASCII yang terdiri dari 256 karakter, maka modulo yang digunakan ialah 255 (0-255).

$$CV_i = (P_i + K_i)\ mod\ 255 \quad (1)$$

Setiap pesan ke-n (P_i) akan ditambahkan dengan Kunci ke-n (K_i) sehingga membentuk *Ciphertext* ke-n (CV_i). Setelah terbentuk keseluruhan *ciphertext* dari *Vigenere Cipher* dilanjutkan enkripsi dengan *Multi-factor* RSA.

RSA merupakan salah satu kriptografi asimetris dengan kunci privat dan kunci publik, dibentuk dengan aturan-aturan bilangan prima dan modulo yang disebut sebagai pembangkitan kunci [20], *multi-factor* pada RSA merupakan jumlah faktor bilangan prima yang digunakan dalam proses penyandian, penelitian ini akan menggunakan tiga faktor bilangan prima sesuai persamaan (2) lalu nilai n yang merupakan hasil kali jumlah bilangan prima untuk di persamaan (3), n digunakan untuk perhitungan modulo setiap kunci, berikutnya φn dengan φ (totien) merupakan fungsi inti dari algoritma RSA disebut juga sebagai fungsi totien Carmichael dijabarkan dalam persamaan (4), kemudian nilai e merupakan eksponensial dengan aturan dalam persamaan (5), dan nilai d yang merupakan nilai invers dari e dengan modulo φn sesuai dengan persamaan (6).

$$p_1, p_2, p_3 = Prima, p_1 \neq p_2 \neq p_3 \quad (2)$$

$$n = p_1 \times p_2 \times p_3 \quad (3)$$

$$\varphi_n = KPK(p_1 - 1, p_2 - 1, p_3 - 1) \quad (4)$$

$$e > 1, FPB(e, \varphi_n) = 1 \quad (5)$$

$$d = e^{-1}\ mod\ \varphi_n \quad (6)$$

Hasil akhir enkripsi (enc) merupakan enkripsi dari *ciphertext Vigenere Cipher* (CV) dengan *Multi-factor* RSA sesuai dengan persamaan (7). Hasil akhir enkripsi kemudian di *encode* kedalam *QR Code*.

$$enc_i = CV_i^{\,e} \bmod n \quad (7)$$

2.3 Proses dekripsi data

Dekripsi data dilakukan dengan *decode QR Code* lalu proses dibalik dari dekripsi algortima *Multi-factor* RSA (DR) sesuai persamaan (8), dengan nilai-nilai pembangkitan kunci yang sama dengan proses enkripsi.

$$DR_i = enc_i^{\,d} \bmod n \quad (8)$$

Setelah itu dilanjutkan dengan dekripsi dari algoritma *Vigenere Cipher* sehingga menghasilkan data/pesan aslinya (M) dengan persamaan (9).

$$M_i = (DR_i - K_i) \bmod 255 \quad (9)$$

2.4 Pengujian

Metode usulan kombinasi algoritma akan diuji dengan pengujian *Avalanche effect* (AE) yang mana akan menguji tingkat ketahanan dari kombinasi algoritma dengan membandingkan jumlah bit yang berbeda (x) dari total bit (n) yang terbentuk, dapat dilihat pada persamaan (10), hasil AE dikatakan baik sesuai standar adalah yang memiliki nilai lebih dari 50% [21].

$$AE = \frac{x}{n} \times 100\% \quad (10)$$

3. HASIL DAN PEMBAHASAN

Data uji yang terbentuk dari program *text random* adalah text dengan panjang 16 karakter atau setara dengan 128 bit. Kunci yang digunakan pada *Vigenere Cipher* adalah **P1gN4t3Lli**, lalu pembangkitan kunci *Multi-factor* RSA menggunakan variabel berikut p_1=5, p_2=17, p_3=3 dan nilai eksponensial e=83. Lalu tabel 1 merupakan data uji, hasil enkripsi serta *encode QR Code*.

Tabel 1 Data Uji, Enkripsi dan *Qr Code*

No	Data Uji	Enkripsi	*QR Code*
1	l 4 k g 3 9 e v 0 u u s z 9 u o	89 65 a5 e2 34 c5 cb e0 e7 12 da d1 1e 87 a9 e9	
2	v y v 1 o n 2 3 x 8 o d e h p 0	c0 aa dd df 52 5b 65 df cf ce fb 59 cc 71 d1 d1	
3	r 8 a 1 9 m c 7 a 3 m e n 0 v p	e0 b4 8c df 8b 1e 4b 0b cd e7 90 4b 75 9c aa cf	
4	v c h l d u p f w r b n r 0 7 z	c0 e8 4e ba cb 3e 52 ac e9 09 ac 72 d0 9c 17 bb	
5	q p r v c 4 p h n d u 9 g v m 9	e6 a6 4e 87 a8 8f a6 71 cd be 7b 3b dc ee c5 a0	

No	Data Uji	Enkripsi	*QR Code*
6	1 7 l e y 5 g c 8 a u 7 g 3 j m	63 3b f1 86 c5 a9 9a 28 d1 2b da 3b a1 63 e3 1e	
7	k c w u w p y h v 1 x z v f t v	ee e8 12 f0 ab cf b2 96 5b 9a 8c ab dd 96 a2 ae	
8	x q b u p n c g h k 8 t y c l 8	8c a8 7e f0 d1 5b 4b 86 35 35 88 2d 2c 03 be b2	
9	m u 7 e t t 2 z a 8 4 p c k n q	90 6a e3 86 a2 49 65 c0 cd ce 7b ce 2b e6 a8 13	
10	v k c 7 d w y w h 1 w k n f o z	c0 e7 2b 07 cb a0 b2 f0 35 9a 4f e7 75 96 52 bb	

QR Code yang dipindai langsung dari berbagai perangkat akan menghasilkan kode enkripsi sehingga pihak yang tidak bertanggungjawab tidak dapat membaca nilai pesan asli. Pesan asli hanya bisa dibaca dari aplikasi scanner yang telah dibuat dengan menambahkan algoritma dekripsi *Multi-factor* RSA serta *Vigenere Cipher*. Sehingga terbukti dapat memverifikasi keabsahan *QR Code*. Lalu tabel 2 merupakan hasil verifikasi *QR Code*.

Tabel 2 Hasil Verifikasi

No	*QR Code*	Pindai Langsung	Dekripsi	Keterangan
1		89 65 a5 e2 34 c5 cb e0 e7 12 da d1 1e 87 a9 e9	l 4 k g 3 9 e v 0 u u s z 9 u o	Terverifikasi
2		c0 aa dd df 52 5b 65 df cf ce fb 59 cc 71 d1 d1	v y v 1 o n 2 3 x 8 o d e h p 0	Terverifikasi
3		e0 b4 8c df 8b 1e 4b 0b cd e7 90 4b 75 9c aa cf	r 8 a 1 9 m c 7 a 3 m e n 0 v p	Terverifikasi
4		c0 e8 4e ba cb 3e 52 ac e9 09 ac 72 d0 9c 17 bb	v c h l d u p f w r b n r 0 7 z	Terverifikasi

No	*QR Code*	Pindai Langsung	Dekripsi	Keterangan
5		e6 a6 4e 87 a8 8f a6 71 cd be 7b 3b dc ee c5 a0	q p r v c 4 p h n d u 9 g v m 9	Terverifikasi
6		63 3b f1 86 c5 a9 9a 28 d1 2b da 3b a1 63 e3 1e	1 7 l e y 5 g c 8 a u 7 g 3 j m	Terverifikasi
7		ee e8 12 f0 ab cf b2 96 5b 9a 8c ab dd 96 a2 ae	k c w u w p y h v 1 x z v f t v	Terverifikasi
8		8c a8 7e f0 d1 5b 4b 86 35 35 88 2d 2c 03 be b2	x q b u p n c g h k 8 t y c l 8	Terverifikasi
9		90 6a e3 86 a2 49 65 c0 cd ce 7b ce 2b e6 a8 13	m u 7 e t t 2 z a 8 4 p c k n q	Terverifikasi
10		c0 e7 2b 07 cb a0 b2 f0 35 9a 4f e7 75 96 52 bb	v k c 7 d w y w h 1 w k n f o z	Terverifikasi

Dari seluruh percobaan pemindaian pesan asli berhasil disembunyikan dan hanya bisa dilihat dengan *scanner* yang telah memiliki kode algoritma sehingga keamanan *QR Code* terverifikasi. Kemudian hasil pengujian *Avalanche effect* dapat dilihat pada tabel 3.

No	Pesan Asli	Hasil Metode Usulan	Bit Data	*Avalanche effect*
1	l 4 k g 3 9 e v 0 u u s z 9 u o	89 65 a5 e2 34 c5 cb e0 e7 12 da d1 1e 87 a9 e9	71 / 128	55,46875%
2	v y v 1 o n 2 3 x 8 o d e h p 0	c0 aa dd df 52 5b 65 df cf ce fb 59 cc 71 d1 d1	74 / 128	57,8125%
3	r 8 a 1 9 m c 7 a 3 m e n 0 v p	e0 b4 8c df 8b 1e 4b 0b cd e7 90 4b 75 9c aa cf	72 / 128	56,25%
4	v c h l d u p f w r b n r 0 7 z	c0 e8 4e ba cb 3e 52 ac e9 09 ac 72 d0 9c 17 bb	63 / 128	49,21875%
5	q p r v c 4 p h n d u 9 g v m 9	e6 a6 4e 87 a8 8f a6 71 cd be 7b 3b dc ee c5 a0	69 / 128	53,90625%
6	1 7 l e y 5 g c 8 a u 7 g 3 j m	63 3b f1 86 c5 a9 9a 28 d1 2b da 3b a1 63 e3 1e	65 / 128	50,78125%
7	k c w u w p y h v 1 x z v f t v	ee e8 12 f0 ab cf b2 96 5b 9a 8c ab dd 96 a2 ae	74 / 128	57,8125%
8	x q b u p n c g h k 8 t y c l 8	8c a8 7e f0 d1 5b 4b 86 35 35 88 2d 2c 03 be b2	59 / 128	46,09375%
9	m u 7 e t t 2 z a 8 4 p c k n q	90 6a e3 86 a2 49 65 c0 cd ce 7b ce 2b e6 a8 13	75 / 128	58,59375%
10	v k c 7 d w y w h 1 w k n f o z	c0 e7 2b 07 cb a0 b2 f0 35 9a 4f e7 75 96 52 bb	65 / 128	50,78125%
Rata-Rata			**68,7 / 128**	**53,671875%**

Hasil rata-rata menunjukan persentase 53,671875% sehingga tergolong baik dan memenuhi standar keamanan *Avalanche effect*.

4. KESIMPULAN DAN SARAN

Penggunaan metode gabungan *Vigenere Cipher* dan *Multi-factor* RSA sebagai super enkripsi terbukti dapat memverfikasi pesan yang telah diubah menjadi *QR Code*. Hasil pindaian

secara langsung tidak dapat memperoleh pesan asli sehingga kerahasiaannya terjamin. Hasil uji *Avalanche effect* dari metode tersebut mendapatkan nilai rata-rata 53,671875% sehingga memenuhi standar baik karena memiliki nilai lebih dari 50%.

UCAPAN TERIMA KASIH

Penulis berterimakasih atas dukungan penuh dan pendanaan penelitian yang dilaksanakan kepada Universitas Pignatelli Triputra melalui Lembaga Penelitian dan Pengabdian Masyarakat. Terimakasih atas kesempatan yang diberkan, semoga tercapai kontribusi positif dari hasil penelitian untuk kemajuan ilmu pengetahuan dan peningkatan akademik di Universitas Pignatelli Triputra.

DAFTAR PUSTAKA

[1] S. Vatshayan, R. A. Haidri, dan J. Kumar Verma, "Design of Hybrid Cryptography System based on Vigenère Cipher and Polybius Cipher," dalam *2020 International Conference on Computational Performance Evaluation (ComPE)*, Jul 2020, hlm. 848–852. doi: 10.1109/ComPE49325.2020.9199997.

[2] K. Pavani dan P. Sriramya, "Enhancing Public Key Cryptography using RSA, RSA-CRT and N-Prime RSA with Multiple Keys," dalam *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, Feb 2021, hlm. 1–6. doi: 10.1109/ICICV50876.2021.9388621.

[3] Biro Humas Kementerian Kominfo, "Perkembangan Penanganan Dugaan Kebocoran Data Paspor 34,9 Juta Warga Indonesia." [Daring]. Tersedia pada: https://www.kominfo.go.id/content/detail/50065/siaran-pers-no-138hmkominfo072023-tentang-perkembangan-penanganan-dugaan-kebocoran-data-paspor-349-juta-warga-indonesia/0/siaran_pers

[4] C. Bhardwaj, H. Garg, dan S. Shekhar, "An Approach for Securing QR code using Cryptography and Visual Cryptography," dalam *2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*, Mei 2022, hlm. 284–288. doi: 10.1109/CISES54857.2022.9844332.

[5] T. Wang dan F. Jia, "The impact of health QR code system on older people in China during the COVID-19 outbreak," *Age and Ageing*, vol. 50, no. 1, hlm. 55–56, Jan 2021, doi: 10.1093/ageing/afaa222.

[6] A. Averin dan N. Zyulyarkina, "Malicious Qr-Code Threats and Vulnerability of Blockchain," dalam *2020 Global Smart Industry Conference (GloSIC)*, Nov 2020, hlm. 82–86. doi: 10.1109/GloSIC50886.2020.9267840.

[7] N. Uniyal, G. Dobhal, A. Rawat, dan A. Sikander, "A Novel Encryption Approach Based on Vigenère Cipher for Secure Data Communication," *Wireless Pers Commun*, vol. 119, no. 2, hlm. 1577–1587, Jul 2021, doi: 10.1007/s11277-021-08295-5.

[8] A. Al-Sabaawi, "Cryptanalysis of Vigenère Cipher: Method Implementation," dalam *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, Des 2020, hlm. 1–4. doi: 10.1109/CSDE50874.2020.9411383.

[9] S. Ahmed dan T. Ahmed, "Comparative Analysis of Cryptographic Algorithms in Context of Communication: A Systematic Review," *International Journal of Scientific and Research Publications*, vol. 12, no. 7, Art. no. 7, Jul 2022, doi: 10.29322/IJSRP.12.07.2022.p12720.

[10] T. S. Putra, M. A. Budiman, dan S. Suwilo, "Signcryption Techniques For Digital File Security Using the RSA Multi-Factor Algorithm and the ESIGN Algorithm," dalam *2023 International Conference of Computer Science and Information Technology (ICOSNIKOM)*, Nov 2023, hlm. 1–6. doi: 10.1109/ICoSNIKOM60230.2023.10364520.

[11] N. W. Nasution, S. Efendi, dan Sawaluddin, "Analysis of RSA variants in securing message," *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 725, no. 1, hlm. 012131, Jan 2020, doi: 10.1088/1757-899X/725/1/012131.

[12] A. Dash, A. Sarkar, A. Chatterjee, S. Darshana, M. Pandey, dan R. K. Barik, "Multi-Factor Analysis of RSA Based on Variations in Primes Used for Modulus Generation," dalam *2023 3rd International Conference on Innovative Sustainable Computational Technologies (CISCT)*, Sep 2023, hlm. 1–6. doi: 10.1109/CISCT57197.2023.10351432.

[13] M. A. Budiman, P. Sihombing, dan I. A. Fikri, "A cryptocompression system with Multi-Factor RSA algorithm and Levenstein code algorithm," *J. Phys.: Conf. Ser.*, vol. 1898, no. 1, hlm. 012040, Jun 2021, doi: 10.1088/1742-6596/1898/1/012040.

[14] E. H. Rachmawanto, R. S. Gumelar, Q. Nabila, C. A. Sari, dan R. R. Ali, "Testing Data Security Using a Vigenere Cipher Based on the QR Code," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, Nov 2023, doi: 10.22219/kinetik.v8i4`.1734.

[15] A. M. S. Pangan, I. L. Lacuesta, R. C. Mabborang, dan F. P. Ferrer, "Authenticating Data Transfer Using RSA-Generated QR Codes," *European Journal of Information Technologies and Computer Science*, vol. 2, no. 4, Art. no. 4, Agu 2022, doi: 10.24018/compute.2022.2.4.73.

[16] V. B. Savant dan R. D. Kasar, "A Review on Network Security and Cryptography," *Research Journal of Engineering and Technology*, vol. 12, no. 4, hlm. 110-114., Des 2021, doi: 10.52711/2321-581X.2021.00019.

[17] F. Hu, Y. Yao, W. Li, dan N. Yu, "A Novel Visual Cryptography Scheme Shared with Edge Information Embedded QR Code," dalam *Artificial Intelligence and Security*, X. Sun, J. Wang, dan E. Bertino, Ed., Cham: Springer International Publishing, 2020, hlm. 86–97. doi: 10.1007/978-3-030-57881-7_8.

[18] A. Mohammed Ali dan A. K. Farhan, "Enhancement of QR Code Capacity by Encrypted Lossless Compression Technology for Verification of Secure E-Document," *IEEE Access*, vol. 8, hlm. 27448–27458, 2020, doi: 10.1109/ACCESS.2020.2971779.

[19] D. I. R. Munir, *Kriptografi*, 2 ed. Bandung: INFORMATIKA, 2019.

[20] S. Rubinstein-Salzedo, "The RSA Cryptosystem," dalam *Cryptography*, S. Rubinstein-Salzedo, Ed., Cham: Springer International Publishing, 2018, hlm. 113–126. doi: 10.1007/978-3-319-94818-8_12.

[21] R. Verma dan A. K. Sharma, "Cryptography: Avalanche effect of AES and RSA," *IJSRP*, vol. 10, no. 4, hlm. p10013, Apr 2020, doi: 10.29322/IJSRP.10.04.2020.p10013.