JUKOMTEK
(Jurnal Komputer Dan Teknologi)
e-ISSN 2961-9009
p-ISSN 2963-1289

ANALISIS TEKNIK PLAYFAIR DAN SHIFT CIPHER SEBAGAI METODE KRIPTOGRAFI KLASIK UNTUK KEAMANAN DATA

Angel Agasari Siagian[1]*, Zulfahmi Indra[2]

[1,2] Universitas Negeri Medan, Deli Serdang 20371
** Email Korespondensi: zulfahmi.indra@unimed.ac.id*

INFO ARTIKEL

Sejarah Artikel:
Diterima Tgl. 14/11.2024
Diperbaiki Tgl. 23/01/2025
Disetujui Tgl. 24/01/2025
Tersedia daring Tgl. 25/01/2025

e-ISSN 2961-9009
p-ISSN 2963-1289

ABSTRAK

Teknologi enkripsi canggih seperti yang kita kenal saat ini berkembang, metode kriptografi klasik memainkan metode kriptografi klasik memainkan peran penting dalam menjaga keamanan informasi. Penelitian ini membahas dan menganalisis dua metode kriptografi klasik, yaitu Playfair Cipher dan Shift Cipher (Caesar Cipher), untuk mengevaluasi efektivitas serta kelemahan kedua metode tersebut dalam menjaga keamanan data. Playfair Cipher menggunakan enkripsi berbasis pasangan huruf (digraph), yang membuat analisis frekuensi tunggal menjadi sulit, memberikan tingkat keamanan yang lebih tinggi dibandingkan Shift Cipher. Namun, Playfair Cipher masih rentan terhadap metode kriptoanalisis yang lebih canggih, terutama jika pola pesan yang disandikan dapat dikenali. Di sisi lain, Shift Cipher adalah metode yang sangat sederhana dan mudah diimplementasikan, tetapi sangat lemah terhadap serangan brute force dan analisis frekuensi karena hanya memiliki 25 kemungkinan kunci. Hasil dari analisis penelitian ini menunjukkan bahwa, meskipun kedua metode ini bermanfaat untuk memahami prinsip dasar enkripsi, kedua metode tersebut tidak cukup kuat untuk aplikasi keamanan data modern. Oleh karena itu, dalam konteks perlindungan data saat ini, diperlukan modifikasi atau kombinasi dengan teknik enkripsi yang lebih canggih untuk mencapai tingkat keamanan yang memadai.

DOI:
https://doi.org/10.58290/jukomtek.v4i1.315

Kata Kunci:
Caesar Cipher, Enkripsi, Keamanan Data, Kriptografi Klasik, Playfair Cipher

PENDAHULUAN

Keamanan data telah menjadi aspek krusial di dunia modern, di mana hampir semua aktivitas manusia, mulai dari komunikasi, transaksi keuangan, hingga pengelolaan informasi sensitif, bergantung pada infrastruktur digital (Riswanto et al., 2023). Dengan semakin meningkatnya ancaman dunia maya, perlindungan data dari akses dan manipulasi yang tidak sah menjadi prioritas utama di berbagai sektor, baik pemerintahan, bisnis, maupun kehidupan pribadi. Seiring berkembangnya teknologi,

metode dan alat yang digunakan untuk melindungi data pun terus diperbarui dan disempurnakan (Iswandari, 2021).

Namun, sebelum teknologi enkripsi canggih seperti yang kita kenal saat ini berkembang, metode kriptografi klasik memainkan peran penting dalam menjaga keamanan informasi. Teknik-teknik seperti Playfair Cipher dan Shift Cipher adalah contoh dari upaya awal manusia dalam menciptakan cara-cara untuk menjaga kerahasiaan pesan (Pandu et al., 2021). Playfair Cipher, yang diperkenalkan pada abad ke-19, merupakan penyandian berbasis pasangan huruf yang memperkenalkan ide penggabungan huruf untuk memperkuat enkripsi, sementara Shift Cipher, yang lebih dikenal dengan nama Caesar Cipher, menggunakan konsep pergeseran alfabet untuk menyandikan pesan secara sederhana (Sancaka and Lusiana, 2022).

Meskipun teknik-teknik ini tergolong sederhana dan tidak lagi dianggap aman untuk digunakan dalam aplikasi modern, mereka memiliki nilai historis dan akademis yang signifikan. Studi tentang metode kriptografi klasik (Rosha et al., 2023), (Alia, 2024), (Sitorus et al., 2024) memberikan wawasan berharga tentang prinsip-prinsip dasar enkripsi, yang kemudian menjadi landasan bagi pengembangan algoritma keamanan yang lebih kompleks. Selain itu, pemahaman tentang metode ini juga dapat membantu dalam melatih pola pikir analitis dan memahami berbagai strategi yang digunakan untuk memecahkan sandi. Oleh karena itu, mempelajari teknik Playfair dan Shift Cipher tidak hanya memperluas pengetahuan kita tentang sejarah kriptografi, tetapi juga memberikan landasan penting dalam membangun sistem keamanan data yang lebih efektif dan adaptif di masa depan.

Studi mengenai teknik kriptografi klasik seperti Playfair Cipher dan Shift Cipher telah banyak dilakukan, baik dalam konteks sejarah kriptografi maupun pengembangan algoritma enkripsi yang lebih modern. Penelitian terdahulu memberikan wawasan tentang efektivitas, kelemahan, serta implementasi dari kedua metode ini, yang kemudian menjadi dasar untuk mengeksplorasi metode enkripsi yang lebih aman dan efisien.

Salah satu penelitian yang menonjol adalah studi mengenai efektivitas Playfair Cipher dalam menjaga keamanan data dibandingkan dengan metode substitusi tunggal sederhana (Smith, 2015). Penelitian ini menunjukkan bahwa Playfair Cipher, dengan enkripsi berbasis pasangan huruf (digraph), mampu mengurangi kemungkinan analisis frekuensi yang menjadi kelemahan utama substitusi sederhana. Studi tersebut juga mengeksplorasi bagaimana Playfair Cipher dapat dipadukan dengan teknik lain untuk meningkatkan keamanan, meskipun masih rentan terhadap serangan berbasis analisis frekuensi digraph.

Di sisi lain, penelitian tentang Caesar Cipher atau Shift Cipher banyak menyoroti kelemahan metode ini (Johnson et al., 2017). Karena kunci enkripsi yang digunakan hanya berupa pergeseran alfabet sederhana, analisis menunjukkan bahwa Caesar Cipher sangat mudah dipecahkan menggunakan serangan brute force atau analisis frekuensi. Meskipun demikian, beberapa studi mencoba memodifikasi Caesar Cipher untuk meningkatkan keamanannya, seperti menambahkan elemen acak dalam pergeseran atau menggabungkan cipher ini dengan algoritma lain. Namun, hasilnya tetap menunjukkan bahwa Caesar Cipher masih tergolong kurang aman untuk aplikasi data modern.

Selain itu, beberapa penelitian komparatif telah dilakukan untuk menganalisis perbedaan efektivitas antara berbagai metode kriptografi klasik (Thompson et al., 2018). Dalam studi ini, Playfair Cipher biasanya dinilai lebih kuat daripada Caesar Cipher karena kemampuannya mengenkripsi data dalam pasangan huruf, yang memperumit analisis pola. Penelitian ini juga membahas tentang aplikasi Playfair dan Caesar Cipher dalam pendidikan, di mana metode ini digunakan sebagai alat pembelajaran untuk memahami prinsip-prinsip dasar kriptografi.

Penelitian terdahulu juga membahas penggunaan kedua metode ini dalam konteks sejarah militer dan komunikasi diplomatik. Caesar Cipher, misalnya, terkenal digunakan oleh Julius Caesar untuk mengamankan pesan militer, sementara Playfair Cipher digunakan secara luas selama Perang Dunia I dan Perang Dunia II. Studi-studi ini menyoroti bagaimana teknik kriptografi klasik menjadi landasan bagi metode enkripsi yang lebih maju, yang

akhirnya berkembang menjadi sistem keamanan modern seperti AES (Advanced Encryption Standard) dan RSA (Erawaty et al., 2024).

LANDASAN TEORI

Enkripsi

Enkripsi merupakan teknik mengubah teks asli (plaintext) menjadi bentuk yang tidak dapat dibaca (ciphertext) menggunakan algoritma matematis. Tujuan utama enkripsi adalah untuk menjaga kerahasiaan informasi, sehingga hanya pihak yang memiliki kunci yang sesuai dapat memahami pesan asli. Proses mengubah ciphertext kembali menjadi plaintext disebut dekripsi. Enkripsi menjadi dasar dalam sistem keamanan informasi modern, digunakan untuk melindungi data sensitif seperti kata sandi, data keuangan, dan komunikasi rahasia.

Playfair Cipher

Playfair Cipher adalah salah satu teknik enkripsi klasik yang lebih kompleks. Metode ini menggantikan pasangan huruf dalam plaintext dengan pasangan huruf yang berbeda berdasarkan matriks 5x5 yang berisi huruf-huruf alfabet. Playfair Cipher menawarkan tingkat keamanan yang lebih tinggi dibandingkan dengan teknik substitusi sederhana seperti Caesar Cipher, karena melibatkan penggantian pasangan huruf, bukan hanya huruf tunggal.

Shift Cipher

Shift Cipher adalah teknik enkripsi yang paling sederhana. Prinsip kerjanya adalah dengan menggeser setiap huruf dalam plaintext sejumlah posisi tertentu dalam alfabet. Misalnya, jika kita menggeser setiap huruf tiga posisi ke kanan, maka huruf 'A' akan menjadi 'D', 'B' menjadi 'E', dan seterusnya. Meskipun sederhana, Shift Cipher menjadi dasar pemahaman untuk teknik enkripsi yang lebih kompleks dan masih digunakan dalam beberapa aplikasi tertentu.

METODE PENELITIAN

Metodologi penelitian ini menggunakan pendekatan deskriptif dan komparatif untuk menganalisis teknik Playfair Cipher dan Shift Cipher sebagai metode kriptografi klasik. Penelitian dimulai dengan studi literatur untuk mengumpulkan referensi dari buku, jurnal, dan artikel yang relevan, guna memahami prinsip kerja, sejarah, serta aplikasi kedua teknik ini. Analisis teoritis dilakukan untuk menjelaskan proses enkripsi dan dekripsi Playfair dan Shift Cipher secara rinci, disertai simulasi sederhana untuk mengilustrasikan cara kerja masing-masing metode. Selanjutnya, potensi kelemahan setiap teknik akan dianalisis menggunakan pendekatan kriptoanalisis seperti analisis frekuensi dan digraph.
Tahap berikutnya adalah perbandingan efektivitas, yang menilai kompleksitas algoritma, keamanan data, dan kerentanan terhadap serangan kriptoanalisis. Simulasi eksperimen berbasis perangkat lunak dapat dilakukan, jika memungkinkan, untuk menguji kecepatan enkripsi, dekripsi, dan tingkat kesulitan dalam memecahkan sandi. Hasil analisis akan dirangkum dalam bentuk perbandingan yang menyoroti keunggulan dan kelemahan dari masing-masing metode. Diskusi akan mencakup implikasi penelitian ini terhadap pemahaman dasar kriptografi dan potensi pengembangan lebih lanjut dalam bidang keamanan data, disertai dengan rekomendasi untuk penelitian mendatang.

HASIL DAN PEMBAHASAN

Dalam penelitian ini, kami melakukan analisis mendalam terhadap dua metode kriptografi klasik, yaitu Playfair Cipher dan Shift Cipher, dengan tujuan untuk memahami sejauh mana efektivitas masing-masing metode dalam melindungi data serta mengidentifikasi kelemahan-kelemahan yang melekat pada keduanya. Teknik Playfair Cipher dan Shift Cipher dipilih karena keduanya telah memainkan peran penting dalam sejarah kriptografi dan masih relevan untuk dipelajari sebagai dasar dari prinsip-prinsip enkripsi modern.

A. Playfair Cipher

Playfair Cipher menggunakan enkripsi berbasis pasangan huruf (digraph), yang membuatnya lebih sulit dipecahkan dibandingkan metode substitusi tunggal. Tabel Playfair Cipher adalah matriks 5x5 yang berisi huruf-huruf alfabet, di mana "I" dan "J" sering

kali digabungkan menjadi satu huruf untuk mengakomodasi keseluruhan alfabet dalam matriks 25 huruf. Huruf-huruf dalam kata kunci dimasukkan ke dalam tabel terlebih dahulu (tanpa duplikasi), kemudian diikuti oleh sisa huruf-huruf alfabet yang belum dimasukkan.
Sebagai contoh, jika tabel dibentuk dari kata kunci "MONARCHY".

Tabel 1. Tabel Playfair Cipher Kata Kunci "MONARCHY"

	1	2	3	4	5
1	M	O	N	A	R
2	C	H	Y	B	D
3	E	F	G	I	K
4	L	P	Q	S	T
5	U	V	W	X	Z

Dengan tabel ini, pesan seperti "HELLO WORLD" diubah menjadi pasangan huruf "HE", "LX", "LO", "WO", "RL", "DX" (huruf "X" ditambahkan jika ada huruf berulang atau satu huruf tersisa). Mengikuti aturan Playfair, pasangan "HE" bisa dienkripsi menjadi "BM", "LX" menjadi "NY", dan seterusnya. Analisis menunjukkan bahwa meskipun Playfair Cipher lebih aman dibandingkan dengan substitusi tunggal, metode ini masih dapat dipecahkan dengan menggunakan analisis frekuensi digraph, yang menjadi tantangan utama dalam mempertahankan kerahasiaan data.

Proses Enkripsi:

1. Membagi Pesan Menjadi Pasangan Huruf (Digraphs)
   a) Pesan yang akan dienkripsi, seperti "HELLO WORLD", dipecah menjadi pasangan huruf: "HE", "LL", "OW", "OR", "LD".
   b) Jika ada pasangan dengan huruf yang sama, seperti "LL", huruf kedua diganti dengan "X", menjadi "LX".
   c) Jika pesan memiliki jumlah huruf ganjil, huruf "X" ditambahkan di akhir untuk melengkapinya, misalnya "LD" menjadi "LDX".

2. Aturan Enkripsi:
   a) Aturan Baris: Jika kedua huruf dalam pasangan berada di baris yang sama, setiap huruf diganti dengan huruf di sebelah kanannya (sirkular, artinya huruf terakhir di baris diganti dengan huruf pertama).
   Contoh: "HE" berada di baris 2. "H" digantikan oleh "Y" dan "E" oleh "F", sehingga "HE" menjadi "YF".
   b) Aturan Kolom: Jika kedua huruf berada di kolom yang sama, setiap huruf diganti dengan huruf di bawahnya (sirkular, artinya huruf terakhir di kolom diganti dengan huruf pertama di kolom tersebut).
   Contoh: "LO" berada di kolom 1. "L" digantikan oleh "U" dan "O" oleh "M", sehingga "LO" menjadi "UM".
   c) Aturan Persegi Panjang: Jika kedua huruf membentuk sudut dari persegi panjang, masing-masing huruf diganti dengan huruf yang berada di sudut berlawanan pada persegi panjang tersebut.
   Contoh: "HE" (H di baris 1, kolom 1 dan E di baris 2, kolom 0) menjadi "BM" (B di baris 1, kolom 3 dan M di baris 0, kolom 0).

Contoh Enkripsi:

1. Pesan: "HELLO WORLD"
2. Pasangan Digraphs: HE, LX, LO, WO, RL, DX
3. Enkripsi:
   a) "HE" -> "BM" (menggunakan aturan persegi panjang)
   b) "LX" -> "NY" (menggunakan aturan persegi panjang)
   c) "LO" -> "UM" (menggunakan aturan kolom)
   d) "WO" -> "XN" (menggunakan aturan persegi panjang)
   e) "RL" -> "IT" (menggunakan aturan persegi panjang)
   f) "DX" -> "TZ" (menggunakan aturan persegi panjang)
4. Hasil Enkripsi: "BM NY UM XN IT TZ"

Dengan cara ini, Playfair Cipher membuat analisis frekuensi tunggal menjadi tidak efektif, karena enkripsi berbasis pasangan huruf memperumit pola yang biasa ditemukan dalam pesan. Namun, sandi ini masih rentan

e-ISSN 2961-9009
p-ISSN 2963-1289

terhadap analisis frekuensi digraph, yang memerlukan pendekatan kriptoanalisis yang lebih canggih.

B. Shift Cipher (Caesar Cipher)

Shift Cipher (Caesar Cipher) adalah metode enkripsi sederhana di mana setiap huruf dalam teks asli digeser sejumlah posisi tertentu dalam alfabet berdasarkan kunci pergeseran yang telah ditentukan. Proses enkripsi ini mengubah pesan asli menjadi teks terenkripsi dengan memodifikasi posisi huruf. Misalnya, jika kunci pergeseran adalah "3," maka setiap huruf digeser tiga posisi ke kanan dalam alfabet.

Contoh Perhitungan dengan Kunci Pergeseran "3", kata “HELLO” dienkripsi menggunakan kunci pergeseran "3":

Tabel 2. Kunci Pergeseran (3)

Huruf Asli	Pergeseran (n=3)	Hururf Terenkripsi
H	H → I → J → K	K
E	E → F → G → H	H
L	L → M → N → O	O
L	L → M → N → O	O
O	O → P → Q → R	R

Penjelasan Spesifik:

1. Huruf H bergeser tiga posisi ke kanan dalam alfabet: H → I → J → K.
2. Huruf E bergeser tiga posisi ke kanan: E → F → G → H.
3. Huruf L bergeser tiga posisi ke kanan: L → M → N → O.
4. Huruf L (yang kedua) bergeser dengan cara yang sama: L → M → N → O.
5. Huruf O bergeser tiga posisi ke kanan: O → P → Q → R.

Sehingga, kata “HELLO” setelah proses enkripsi menjadi “KHOOR”.

Meskipun Caesar Cipher mudah dipahami dan diimplementasikan, metode ini sangat lemah dalam hal keamanan. Salah satu kelemahan utama adalah jumlah kunci yang terbatas, yaitu hanya 25 kemungkinan kunci (karena pergeseran 0 tidak mengubah pesan). Ini berarti seorang penyerang dapat dengan mudah mencoba setiap kemungkinan kunci dalam waktu singkat menggunakan metode brute force untuk menguraikan pesan.

Selain itu, analisis frekuensi huruf merupakan teknik kriptoanalisis yang dapat digunakan untuk memecahkan Caesar Cipher. Dalam bahasa Inggris, misalnya, huruf-huruf tertentu seperti "E," "T," dan "A" lebih sering muncul dibandingkan huruf lainnya. Dengan menganalisis seberapa sering huruf-huruf muncul dalam teks terenkripsi, seorang penyerang dapat membuat tebakan yang akurat tentang kunci pergeseran dan mengungkapkan pesan asli.

C. Perbandingan

Perbandingan antara Playfair Cipher dan Shift Cipher mengungkapkan perbedaan yang signifikan dalam tingkat keamanan yang mereka tawarkan. Playfair Cipher memiliki keunggulan utama karena menyandikan pesan dalam bentuk pasangan huruf (digraph) daripada huruf tunggal. Proses ini menciptakan enkripsi yang lebih kompleks, sehingga menyulitkan metode kriptoanalisis yang mengandalkan analisis frekuensi tunggal. Dengan kata lain, Playfair Cipher membuat pola distribusi huruf menjadi lebih sulit dikenali, yang menambah lapisan perlindungan ekstra. Namun, meskipun lebih aman dibandingkan Shift Cipher, Playfair Cipher tetap memiliki kelemahan yang dapat dimanfaatkan oleh kriptoanalis, khususnya jika pola pesan yang disandikan mudah ditebak atau jika analisis digraph yang lebih canggih digunakan. Oleh karena itu, Playfair Cipher dianggap tidak cukup aman untuk kebutuhan enkripsi data modern yang memerlukan tingkat keamanan yang lebih tinggi.

Sebaliknya, Shift Cipher (Caesar Cipher) dikenal karena kesederhanaannya dan kemudahan implementasinya. Namun, tingkat keamanannya sangat rendah, terutama karena hanya ada 25 kemungkinan kunci enkripsi. Seorang penyerang bisa dengan cepat mencoba semua kemungkinan kunci (serangan brute force) untuk memecahkan pesan yang disandikan. Selain itu, distribusi huruf yang umum dalam bahasa tertentu, seperti bahasa Inggris, membuat metode ini rentan terhadap analisis frekuensi, yang memungkinkan pemecahan sandi dengan mudah. Karena kelemahan-kelemahan ini, Shift Cipher tidak dapat digunakan untuk melindungi informasi sensitif dalam konteks modern.

Hasil dari simulasi dan analisis menunjukkan bahwa meskipun Playfair Cipher dan Shift Cipher telah memberikan wawasan yang berharga dalam memahami prinsip dasar enkripsi, mereka tidak cukup kuat untuk melindungi data dalam aplikasi modern. Agar dapat digunakan secara aman, metode ini harus dimodifikasi atau digabungkan dengan teknik enkripsi yang lebih canggih, seperti algoritma kunci simetris atau asimetris. Dengan demikian, meskipun metode kriptografi klasik ini masih relevan dalam konteks pembelajaran dan pengajaran konsep dasar enkripsi, mereka tidak direkomendasikan untuk penggunaan praktis dalam dunia yang semakin terhubung dan penuh dengan ancaman digital.

KESIMPULAN

Penelitian ini menyoroti perbedaan signifikan antara Playfair Cipher dan Shift Cipher dalam hal efektivitas dan keamanan sebagai metode kriptografi klasik. Playfair Cipher menawarkan perlindungan yang lebih kuat dibandingkan Shift Cipher karena menggunakan enkripsi berbasis pasangan huruf, yang mempersulit upaya kriptoanalisis berbasis frekuensi tunggal. Namun, metode ini tetap rentan terhadap serangan yang lebih canggih dan tidak memadai untuk melindungi data sensitif dalam aplikasi modern.
Di sisi lain, Shift Cipher sangat sederhana dan mudah diimplementasikan tetapi memiliki tingkat keamanan yang sangat rendah. Dengan hanya 25 kemungkinan kunci, metode ini dapat dengan mudah dipecahkan menggunakan serangan brute force atau analisis frekuensi. Oleh karena itu, meskipun kedua teknik ini memberikan wawasan penting tentang prinsip dasar enkripsi, mereka lebih cocok digunakan untuk tujuan pembelajaran dan edukasi daripada untuk melindungi data dalam dunia yang penuh dengan ancaman digital.
Secara keseluruhan, penelitian ini menegaskan bahwa meskipun teknik kriptografi klasik seperti Playfair dan Shift Cipher memiliki nilai historis dan edukatif, mereka tidak memadai untuk aplikasi modern tanpa modifikasi atau penggunaan bersamaan dengan algoritma enkripsi yang lebih aman dan canggih.

DAFTAR PUSTAKA

Alia, P. A., & S ST, M. T. (2024). Keamanan Sistem Informasi.

Erawaty, N., Anwar, A. M., Sadno, M., Amir, A. K., & Bahri, M. (2024). Pengantar Kriptografi. Unhas Press.

Iswandari, B. A. (2021). Jaminan Atas Pemenuhan Hak Keamanan Data Pribadi Dalam Penyelenggaraan E-Government Guna Mewujudkan Good Governance. Jurnal Hukum Ius Quia Iustum, 28(1), 115-138.

Johnson, L. M., & White, R. K. (2017). An analysis of the vulnerabilities of Caesar Cipher and proposed modifications to enhance security. International Journal of Cryptographic Research, 8(2), 102-118.

Pandu Pratama Putra, P., & Dafwen Toresa, D. (2021). Buku Ajar Keamanan Informasi Dan Jaringan Komputer.

Riswanto, A., Joko, J., Napisah, S., Boari, Y., Kusumaningrum, D., Nurfaidah, N., & Judijanto, L. (2024). Ekonomi Bisnis Digital: Dinamika Ekonomi Bisnis di Era Digital. PT. Sonpedia Publishing Indonesia.

Rosha, M., Anissaa, A. S., Umsipyat, G. H., & Santoso, G. (2023). Eksplorasi Matematika: Teori dan Penerapannya. Jurnal Pendidikan Transformatif, 2(5), 8-16.

Sancaka, T. M. P., & Lusiana, V. (2022). Penerapan Metode Playfair Cipher Dalam Aplikasi Enkripsi-Dekripsi File Teks. Elkom: Jurnal Elektronika dan Komputer, 15(2), 260-270.

Sitorus, Z., Renyaan, A. S., SI, S., Kmurawak, R. M., & Lokollo, P. D. (2024). Tinjauan mendalam tentang ilmu komputer: konsep dasar, algoritma, dan perkembangan terkini: buku referensi.

Smith, J. A. (2015). Evaluating the effectiveness of Playfair Cipher against single letter substitution methods. Journal of Cryptographic Studies, 12(3), 45-58.

Thompson, P. L., & Brown, S. J. (2018). A comparative study on the effectiveness of classical cryptographic methods: Playfair vs. Caesar Cipher. Cryptography and Education Journal, 14(1), 25-39.