Penerapan Kriptografi Caesar Cipher Dan Hill Cipher dalam Pengiriman Pesan Rahasia Sebagai Media Pembelajaran Matematika Realistik Pada Materi Modulo

Rosi Widia Asiani[1)], Ili Yanti[2)]

[1,2] Fakultas Tarbiyah dan Keguruan, Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi
[1]Jalan Jambi – Muaro Bulian Km.16, Muaro Jambi, 36363
e-mail: rosiwidia@uinjambi.ac.id[1)] iliyanti124@gmail.com[2)]

ABSTRACT

Cryptography is a branch of applied mathematics that has many benefits in technological developments. In its application, cryptography is used for sending secret messages, Automatic Teller Machine (ATM), the use of ATM for banking, even starting to increase to internet banking, mobile banking, electronic communication such as fixed telephone, cellular, sms, and mms. On the other hand, Realistic Mathematics Learning in schools is expected to be applied considering the importance of the results of the learning in everyday life. Modulo material is one of the topics in algebraic mathematics which in understanding the concept can be helped by applying Hill Cipher and Ceasar Cipher cryptography. Thus, realistic mathematics learning can be realized in the classroom with simple media, namely sending secret messages or cryptography.

***Keywords**: Cryptography, Caesar Cipher, Hill Cipher, PMR, Modulo*

ABSTRAK

Kriptografi merupakan salah satu cabang ilmu bidang matematika terapan memiliki banyak manfaat dalam perkembangan teknologi. Dalam penerapannya, kriptografi digunakan untuk pengiriman pesan rahasia, Automatis Teller Machine (ATM), penggunaan ATM untuk banking, bahkan mulai meningkat menjadi internet banking, mobile banking, komunikasi elektronik seperti telepon tetap, seluler, sms, dan mms. Di sisi lain, Pembelajaran Matematika Realistik di sekolah sangat diharapkan untuk dapat diterapkan mengingat pentignya hasil dari pembelajaran tersebut dalam kehidupan sehari-hari. Materi Modulo merupakan salah satu topik dalam bidang matematika aljabar yang dalam memahami konsepnya dapat dibantu dengan menerapkan kriptografi Hill Cipher dan Ceasar Cipher. Dengan demikian pembelajaran matematika realistik dapat tereallisasi di kelas dengan media yang sederhana, yaitu pengiriman pesan rahasia atau kriptografi

Kata Kunci: Kriptografi, Ceasar Cipher, Hill Cipher, PMR, Modulo

A. PENDAHULUAN

Manusia merupakan makhluk hidup yang diciptakan dengan membawa dua fungsi utama, yakni sebagai makhluk yang dapat berpikir dan makhluk yang melakukan reproduksi. Menilik pada fungsi utamanya sebagai makhluk berpikir tentunya manusia tidak terlepas daripada pengetahuan yang didapatkan dari melihat, mendengar, mengamati dan mempelajari segala sesuatu yang ada di lingkungannya. Dalam pembahasan formalnya, manusia adalah makhluk yang akan melakukan pembelajaran seumur hidup (*long life education*), dimanapun ia mendapatkannya.

Mengingat pembelajaran sangat berkaitan dalam bidang kehidupan manusia, bahkan dewasa ini kebutuhan dalam belajar banyak tersebar pada jenjang Pendidikan. Dimulai dari Pendidikan informal, nonformal dan formal. Hal ini dijelaskan dalam UU RI. No. 20 Tahun 2003 tentang SISDIKNAS pada pasal 13 ayat 1 yang menyebutkan tentang tiga jalur lingkungan pendidikan; yaitu pendidikan formal, nonformal dan informal yang saling melengkapi dan memperkaya termasuk dalam hal membentuk sikap dan perilaku (UNDANG-UNDANG TENTANG SISTEM PENDIDIKAN NASIONAL, 2003, p. 6).

Tujuan dari Pendidikan adalah untuk menciptakan masyarakat yang memiliki kemampuan dalam berpikir kritis, kemampuan dalam membuka jaringan, menemukan konsep-konsep baru, mampu menganalisis, berpikir logis, dan memiliki strategi pemecahan masalah (Yanti: 2022). Hal ini juga sesuai dengan kompetensi yang dibutuhkan di abad ke-21. Kompetensi tersebut meliputi: 1) memiliki karakter yang baik (religius, nasionalis, integritas, gotong-royong dan mandiri), 2) memiliki kemampuan 4C (*critical thingking, creativity, collaboration, and communication)*, dan 3) menguasi literasi (Wayan Widaya, dkk, 2019).

Mengingat tujuan-tujuan yang dihharapkan dari Pendidikan tersebut, maka dibutuhkan pembelajaran yang tidak hanya mengutamakan kegiatan mengingat, menghafal dan memahami sebuah teori, akan tetapi juga dibutuhkan kegiatan-kegiatan paradigma baru yang meliputi pemecahan masalah, membuat konsep baru, menciptakan dan menganalisis. Kegiatan-kegiatan pembelajaran tersebut salah satunya dapat ditemukan pada sang ratu ilmu, yaitu matematika. Matematika selain sebagai

sebuah mata pelajaran yang diajarkan di sekolah juga memiliki peran penting dalam kemajuan peradaban umat manusia. Mengingat matematika memuat substansi penalaran logis yang bermula dari definisi-definisi yang disepakati menuju implikasi-implikasi yang bersifat pasti. Dengan demikian, sangat mudah diterima bahwa kebutaan manusia terhadap matematika berimplikasi pada hilangnya kemampuan berpikir secara disipliner dalam menyikapi masalah-masalah nyata (Ibrahim, 2012).

Matematika bahkan tidak hanya terbatas pada angka-angka abstrak, matematika sangat bermanfaat dalam berbagai bidang kehidupan. Matematika yang terlibat dalam kehidupan merupakan realistiknya matematika. Sehingga, ciri utama matematika yang hanya berupa angka terasa hidup ketika dikaitan dengan dunia nyata. Selain dapat mengetahui hakikat manfaat belajar matematika juga dapat menumbuhkan kemampuan dalam memecahkan masalah. Matematika realistik merupakan kegiatan matematika di dunia nyata. Matematika bukan tempat untuk memindahkan ide dari guru ke siswa, melainkan tempat bagi siswa untuk menemukan kembali ide dan konsep matematika melalui eksplorasi dunia nyata.

Dalam matematika realistik dikenal dengan istilah matematisasi. Matematisasi diartikan sebagai proses mematematikakan dunia nyata. Treffer mengelompokkan matematisasi menjadi dua, yaitu matematisasi horizontal dan vertical (Hartono: tanpa tahun). Matematisasi horizontal merupakan proses penyelesaian soal-soal kontekstual dari dunia nyata. Dalam hal ini siswa mencoba menyelesaikan soal-soal dunia nyata dengan cara mereka sendiri, menggunkan bahasa dan symbol mereka sendiri. Sementara matematisasi vertical merupakan proses formalisasi konsep matematika. Dalam hal ini siswa mencoba menyusun prosedur umum yang dapat digunakan untuk menyelesaikan soal-soal sejenis tanpa bantuan konteks.

Seiring perkembangan teknologi yang begitu pesat kegunaan matematika realistic tidak hanya berkaitan dengan penyelesaian soal-soal matematika, akan tetapi juga berkaitan dengan kegiatan berkomunikasi dan saling bertukar informasi atau data secara jarak jauh yang tidak terbatas lagi pada antar daerah dan kota, akan tetapi sudah melintasi berbagai benua dan samudera. Pertukaran informasi atau data yang meningkat tajam tersebut memungkinkan terjadinya kebocoran data atau diretas oleh

pihak yang tidak bertanggung jawab. Mengingat hal tersebut tuntutan akan keamanan terhadap kerahasiaan data dan informasi dalam pertukaran harus menjadi pokok serius agar tidak terjadi kebocoran data. Begitu banyak pengguna seperti departemen pertahanan, suatu perusahaan atau bahkan individu-individu tidak ingin informasi yang mereka sampaikan di ketahui oleh orang lain atau kompetitornya atau negara lain. Oleh karena dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah kriptografi (Halim: 2018).

Algoritma kriptografi telah banyak sekali diciptakan untuk menyembunyikan pesan. Algoritma kriptografi saat ini dapat dikelompokan menjadi algoritma klasik dan algoritma modern. Bentuk umum algoritma klasik yaitu cipher subtitusi dan cipher transposisi. Cipher subtitusi dilakukan dengan mengganti (substitusi) suatu huruf pada plaintext menjadi huruf lain pada chipertext. Jenis substitusi dalam kriptografi antara lain Cipher Abjad Tunggal, Cipher Substitusi Homofonik, Cipher Abjad Majemuk, dan Polygram Substitution Cipher. Contoh algoritma kriptografi klasik dengan bentuk cipher substitusi yaitu Vigenere Cipher, Caesar Cipher, dan Hill Cipher (Arrijal, dkk: 2016).

Pada algoritma Caesar cipher, setiap huruf pada plaintext digantikan huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Dalam caesar cipher pergeseran pada tiap karakter dilakukan sesai dengan kunci yang diberikan (Puspita, K., &Wayahdi, M. R. (2015). *Hill Cipher* merupakan penerapan aritmatika pada Kriptografi. Teknik Kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang diguanakan untuk melakukan enkripsi dan dekripsi (Sasongko,2005). *Hill Cipher* diciptakan oleh Lesier S. Hill pada tahun 1992.Teknik Kriptografi ini diciptakan dengan maksud untuk dapat menciptakan kode (*Cipher*) yang tidak dapat dipecahkan dengan teknik analisis frekuensi. *Hill Cipher* tidak mengganti setiap abjad yang sama pada *plainteks* dengan abjad lainnya yang sama pada *cipherteks* karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya (Sasongko,2005).

Metode Hill Cipher merupakan satu dari beberapa metode dalam kriptografi. Metode ini tidak berdasarkan pada penggantian setiap abjad yang sama pada plaintext dengan abjad lainnya yang sama pada ciphertext. Metode ini menggunakan kunci

dengan suatu matriks ordo $m \times m$. Banyak hal yang dapat dilakukan pada sebuah matriks. Diantaranya perkalian matriks, mencari determinan matriks, menentukan invers matriks, trace matriks, dan lain sebagainya (F. Aryani and Yulianis : 2018). Teori aritmatika modulo yang diterapkan terhadap matriks nxn merupakan dasar dari konsep kerja Hill Chiper (Endaryono, dkk, 2021: 42).

Modulo merupakan salah satu daripada penjabarannya. Modulo memaikan peranan penting dalam komputasi integer, khususnya pada aplikasi kriptorafi. Adapun operator yang digunakan adalah **mod** atau singkatan dari modulo itu sendiri. Operator modulo memberikan sisa pembagian (Ginting, 2010: 48-49).

Modulo didefiniskan "Misalkan a adalah bilangan bulat dan m adalah bilangan bulat positif. Operasi $a \ mod \ m$ memberikan sisa jika a dibagi dengan m. Dengan kata lain $a \ mod \ m = r$ sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$." Bilangan m disebut modulus atau modulo. Dalam hasil aritmatika modulo m terletak dalam himpunan $\{0,1,2, \dots, m-1\}$. Misalnya 23 dibagi 3 memberikan hasil dengan sisa 2, dapat ditulis $23 \ mod \ 3 = 2$.

Implementasi dari kriptografi sangat banyak bisa kita temui dalam kehidupan sehari – sehari, seperti *Automatis Teller Machine (*ATM), penggunaan ATM untuk *banking*, bahkan mulai meningkat menjadi internet *banking*, *mobile banking*, komunikasi elektronik seperti telepon tetap, seluler, sms, mms. Komunikasi via internet seperti *email, messaging, chatting, voice call, e-goverment* dan *e-commerce.* Dalam konteks sederhannya, terlebih lagi dalam dunia Pendidikan yang subjeknya adalah siswa sekolah menengah dibutuhkan implementasi yang sederhana dan dekat dengan lingkungan belajarnya. Dalam hal ini pemanfaatan media pembelajaran berbasis realistik (matematika realistik) sangat diperlukan. Pengimplentasian dari kriptografi ini dapat diterapkan dengan memberikan *games* berupa penyampaian pesan kata dari beberapa kelompok siswa.

Pemanfaatan penyampaian pesan ini merupakan media yang paling sederhana. Untuk itu, penelitian ini menghubungkan bagaimana keterkaiatan aplikasi kriptografi dalam media pembelajaran matematika realistik.

B. TINJAUAN PUSTAKA

1. Kriptografi

Secara bahasa, kriptografi berasal dari bahasa Yunani yang tersusun dari dua kata yaitu *cryptos* yang berarti rahasia dan *graphien* yang berarti menulis (Schneier, 1996). Sedangkan secara istilah, kriptografi dapat diartikan sebagai ilmu pengetahuan tentang penulisan pesan rahasia dengan tujuan untuk menyembunyikan makna pesan tersebut (Paar, C., & Pelzl, 2009) dalam Mubarak (2019). Menilik pada sejarah bahwa kriptografi sudah dikenalkan oleh bangsa Mesir sejak 4000 tahun yang lalu yang digunakan untuk mengirimkan pesan ke pasukan militer yang berada di lapangan supaya pesan yang dibawa tidak ketahui oleh pihak musuh.

Sasangko (2005) dalam Sianturi (2019: 3) disebutkan bahwa kriptograpi (*Cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. "*Crypto"* berarti "*secret"* (rahasia), dan *"Graphy"* berarti "*writing*" (tulisan). Dalam hal ini kriptografi disebut juga dengan ilmu dan seni, karena sejak jaman dahulu orang-orang mempelajari dan memperdalam sistem pengamanan pesan ini, sehingga menghasilkan berbagai algoritma yang sudah banyak dikenal saat ini (Ariyus, 2006).

Terdapat istilah yang sering digunakan atau komponen dalam kriptografi yang terdiri atas:

a. *Plaintext*, pesan asli, dapat dipahami.
b. *Ciphertext*, pesan acak, sulit atau tak bisa dipahami.
c. *Key*, kunci yang digunakan dalam kriptografi
d. Algorithma atau *cipher* berupa urutan kerja pada aturan enkripsi (*enchipering*) dan dekripsi (*dechipering*) (A. Prayitno and N. Nurdin: 2017) dalam Endaryono, dkk (2021).

Adapun proses dasar dari kriptografi yaitu:

a. Enkripsi, proses penyandian, mengubah kode atau pesan yang dimengerti (*plaintext*) menjadi kode atau pesan yang tidak bisa dipahami *(chipertext*)

b. Proses kebalikannya disebut deskripsi, mengubah cipherteks menjadi *plainteks*.
c. Proses enkripsi dan dekripsi membutuhkan mekanisme dan kunci (key) dalam suatu sistem yang disebut cipher. (B. Solihin Hasugian: 2019) dalam Endaryono, dkk (2021).

Terdapat beberapa jenis kriptografi diantaranya Caesar Chiper dan Hill Chiper yang akan dibahas sebagai berikut

1. Kriptograpi *Ceaser Cipher*

Widya Teffani Putri (2018) menjelaskan bahwa Caesar cipher merupakan salah satu algoritma cipher tertua dan paling diketahui dalam perkembangan ilmu kriptografi. Caesar cipher merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan cara melakukan penukaran karakter pada plainteks menjadi tepat satu karakter pada cipherteks. Teknik seperti ini disebut juga sebagai cipher abjad tunggal.

Adapun langkah-langkah yang dilakukan untuk membentuk cipherteks dengan Caesar cipher adalah:

a. Besarnya pergeseran karakter yang digunakan dalam membentuk cipherteks ke plainteks.
b. Menukarkan karakter pada plainteks menjadi cipherteks dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya. Misalnya diketahui bahwa pergeseran = 3, maka huruf A akan digantikan oleh huruf D, huruf B menjadi huruf E, dan seterusnya.

Susunan alphabet setelah digeser sejauh 3 huruf membentuk sebuah table substitusi sebagai berikut :

Tabel 2.1 Table substitusi ROT3

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12
P	A	B	C	D	E	F	G	H	I	J	K	L	M
C	D	E	F	G	H	I	J	K	L	M	N	O	P
Indeks	13	14	15	16	17	18	19	20	21	22	23	24	25
P	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Untuk menyandikan sebuah pesan, cukup mencari setiap huruf yang hendak disandikan di alfabet biasa, lalu tuliskan huruf yang sesuai pada alfabet sandi. Untuk memecahkan sandi tersebut gunakan cara sebaliknya. Contoh penyandian sebuah pesan adalah sebagai berikut : Plainteks : SURATDIBERIKANKEPADADILA Cipherteks : VXUDWGLEHULNDQNHSDGDGLOD

2. Kriptografi *Hill Cipher*

Hill Cipher merupakan aritmetika modulo terhadap matriks yang dalam penerapannya menggunakan Teknik perkalian matriks dan Teknik invers terhadap matriks. Kunci pada *Hill Cipher* adalah matriks ordo $m \times m$ dengan m merupakan ukuran blok. Kunci matriks harus memiliki invers, hal ini karena invers kunci atau yang biasa dilambangkan dengan K^{-1} merupakan kunci yang digunakan dalam melakukan deskripsi (Nisak, 2015: 18-19).

Matriks K yang menjadi kunci ini harus merupakan matriks yang invertible (yaitu memiliki invers K^{-1} sehingga :

$K.K^{-1} = I$……..(1)

Keterangan :

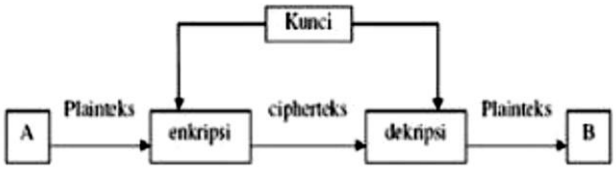
K : Kunci

K^{-1} : Invers Kunci

I : Matriks Identitas

Kunci harus memiliki invers matriks K yaitu K^{-1} akan dipakai melakukan dekripsi (Sansani: 2008) dalam Sianturi (2019: 41).

Kriptografi *Hill Cipher* yang disebut sebagai kriptografi simetris merupakan salah satu algoritma kriptografi kunci simetris dan merupakan salah satu *kriptopolyalphabetic*. *Hill cipher* diciptakan oleh *Lester S. Hill* pada tahun 1929. Teknik Kriptografi ini diciptakan dengan maksud untuk dapat menciptakan cipher yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. Berbeda dengan *caesar cipher*, *hill cipher* tidak mengganti setiap abjad yang sama pada plainteks dengan abjad yang sama dengan cipherteks karena menggunakan perkalian matriks pada dasar enkripsi dan deskripsinya (Siregar, 2018: 12-13). *Hill cipher* atau kode *hill* merupakan algoritma krptografi yang sangat kuat dilihat dari segi kemanannya dengan matriks kunci *hill cipher* harus merupakan matriks yang *invertible*, karena disitulah letak keunikan sekaligus kesulitan *hill cipher* tersebut. Berikut ini proses Kriptografi *Hill Cipher*.



Gambar 2. Kriptografi *Hill Cipher*

2. Media Pembelajaran Berbasis Matematika Realistik

Pembelajaran Matematika Realistik diadopsi dari RME (*Realistic Mathematic Education*) yang merupakan teori pembelajaran dalam Pendidikan matematika. RME pertama kali diperkenalkan dan dikembangkan di Belanda sejak tahun 1970 oleh Institut Freudental. RME dipandang sangat berhasil dalam mengembangkan pengertian siswa (Suharta: 2001) dalam Musrikah (2016).

Menurut Gravemeijer (1994) terdapat tiga prinsip pokok RME, yaitu:

a) *Guided reinvention and progresive mathematizing*, yaitu memberi kesempatan kepada siswa untuk menemukan konsep atau algoritma sebagaimana ditemukannya konsep itu secara matematis;
b) *Didactical Phenomenology*, yaitu fenomena pembelajaran harus menekankan bahwa masalah kontekstual yang diajukan kepada siswa memenuhi kriteria:

memperlihatkan beberapa macam aplikasi yang telah diantisipasi, dan sesuai dengan dampak pada matematisasi progresif;

c) *Self developed models* yaitu model yang dikembangkan siswa harus menjembatani pengetahuan informal ke pengetahuan matematika formal (Khabibah: 2001) dalam Musrikah (2016).

Salah satu karakteristik Pembelajaran Matematika Realistik menurut Treffers (1993) dan Van den Heuvel Panhuizen (1998) adalah *Used of Context (menggunakan dunia "nyata"),* yaitu belajar matematika adalah aktifitas konstruktif (Yuwono I: 2006). Siswa dikenalkan pada konsep dan abstraksi melalui hal-hal konkrit dan diawali dari pengalaman siswa serta berasal dari lingkungan sekitar siswa. Sedangkan menurut Suharta yang dimaksud dengan menggunakan konteks adalah pembelajaran diawali dengan masalah kontekstual (dunia nyata), sehingga memungkinkan mereka menggunakan pengalaman sebelumnya secara langsung (Markinah: 2016).

Pada penelitian ini pendekatan Matematika Realistik menjadi sebuah media dalam pelajaran materi Modulo yang dikaitakan dengan matriks. Sehingga setelah siswa diberikan penjelasan secara abstraksi mengenai materi tersebut siswa diarahkan langsung pada contoh nyatanya dimana siswa itu sendiri yang terlibat. Pelajaran Modulo dapat direalistiknya menjadi sebuah permaianan menyampaikan pesan dari siswa pertama yang ditunjuk sampai kepada siswa yang paling terakhir. Penyampaian pesan tersebut dapat dibuktikan secara matematis menggunakan konsep kriptografi *Ceaser Cipher* dan *Hill Cipher* yang menggunakan operasi modulo dan matriks.

Matematika realistik dapat menjadi sebuah media pembelajaran yang menjadikan matematika abstraksi ke matematika konkret dalam kehidupan siswa. Dengan terpenuhinya pembelajaran dengan matematika realistik tentunya memiliki manfaat bagi siswa dalam mengenali permasalahan dan dunia nyata ke simbol matematika atau sebaliknya.

C. METODE PENELITIAN

Jenis penelitian yang digunakan dalam penelitian ini adalah studi kepustakaan *(library research)*. Studi kepustakaan merupakan jenis penelitian yang dilakukan dengan mengumpulkan data-data yang diperlukan dari buku, jurnal, atau hasil-hasil penelitian sebelumnya (T, Konseling, Pendidikan, & Surabaya, 2018).

Dalam penelitian ini, dipilih beberapa artikel dan/atau jurnal tentang kriptografi, Modulo, Matriks dan matematika realistik. Artikel yang berjudul *Penyandian Kriptografi Metode Hill Cipher dan Ceasar Chipher dengan Menggunakan Appiventor* karay Kahoirun Nisak (2015) merupakan rujukan utama dalam memahami tentang kriptografi Ceaser Copher dan Hill Chipher. Jurnal yang berjudul *Implementasi Algoritma Kriptografi Enigma Termodifikasi Sebagai Media Pembelajaran Matematika Berbasis Pmri Untuk Materi Komposisi Fungsi Dan Fungsi Invers* oleh Najib Mubarak (2019) menjadi rujukan dalam menelaah pembelajaran matematika realistik.

Jurnal yang berjudul *Peranan Aritmetika Modulo dan Bilangan Prima pada Algoritma Kriptografi RSA (Rivest-Shamir-Adleman)* karya Dahlia Br Ginting (2010) digunakan dalam memahami materi modulo. Serta jurnal-jurnal lainnya yang berkaitan dengan judul penelitian ini.

D. HASIL PENELITIAN

Matematika realistik bukan sesuatu yang baru dalam dunia pendidikan terkhusus matematika. Sejak tahun 80-an, pendekatan pembelajaran berbasis matematika realistik mulai dikenalkan dan diajarkan kepada pendidik. Sejauh ini, matematika realistik makin dikenal, meskipun tidak sedikit yang memiliki pemahaman yang mendalam. Meskipun demikian media pembelajaran berbasis matematika realistik memberikan pengaruh yang lebih baik terhadap kemampuan siswa.

Hal ini sebagaimana penelitian yang dilakukan Najib Mubarak (2019) tentang implementasi kriptografi dalam Pembelajaran Matematika Realistik Indonesia (PMRI). Disimpulkan bahwa pembelajaran matematika lebih mampu dimaknai siswa dengan pendekatan realistik. Dalam (Lismareni, N., Somakim., Kesumawati, 2014), disimpulkan bahwa pendekatan PMRI untuk materi aritmatika sosial telah mampu

meningkatkan pemahaman peserta didik kelas VII. Melihat dari penelitian terdahulu terlihat bahwa media pembelajaran berbasis realistik sangat baik digunakan dalam proses pembelajaran. Adapun tulisan ini akan fokus membahas penerapan kriptografi *Ceaser Cipher* dan *Hill Cipher* sebagai media pembelajaran matematika realistik pada materi modulo.

Penerapan kriptografi sebagai media pembelajaran matematika realistik dapat dilakukan dalam proses pembelajaran materi pokok modulo dengan menggunakan metode *Caesar Cipher* dan *Hill Cipher* yang dapat dikemas dalam bungkus permainan kriptografi yang merupakan permainan *role play* pengiriman pesan rahasia. Permainan pengiriman pesan rahasia dilakukan dengan memposisikan sebagian peserta didik sebagai pengirim pesan dan sebagaian lain sebagai penerima pesan.

1. *Caesar Cipher*

   Langkah pertama guru membagi siswa menjadi 2 kelompok, misal kelompok A dan kelompok B. Kemudian guru memberikan pesan rahasia pada kelompok A, misal isi pesan tersebut adalah MATEMATIKA REALISTIK. Kelompok A diminta mengubah pesan tersebut menjadi kode rahasia dengan langkah enkripsi sebagai berikut.

   Proses enskripsi:

   a. Guru meminta siswa mengubah pesan dari bentuk karakter huruf menjadi bilangan seperti berikut.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
S	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**										
18	**19**	**20**	**21**	**22**	**23**	**24**	**25**										

   Diketahui:

   Pesan: **MATEMATIKA REALISTIK**

   Dikodekan menjadi *plainteks* $P =$

   12 0 19 4 12 0 19 8 10 0 17 4 0 11 8 18 19 8 10

b. Langkah kedua guru memberi kunci misal 12, dengan aturan siswa menambahkan masing-masing bilangan pada P dengan bilangan 12, kemudian jika bilangan hasil penjumlahan tersebut lebih dari 25, guru meminta kurangi bilangan tersebut dengan bilangan 26. Secara matematis, proses enkripsi pada *Caesar Cipher* yang dilakukan adalah sebagai berikut:

$C = (K + P)\ mod\ 26$

C = Cipherteks | K = Kunci | P = Plainteks

Kunci: 12

$C_1 = (K + P_1) mod\ 26 = (10 + 12) mod\ 26 = 22\ mod\ 26 = 22 = W$

$C_2 = (10 + 0) mod\ 26 = 10\ mod\ 26 = 10 = K$

$C_3 = (10 + 19) mod\ 26 = 29\ mod\ 26 = 3 = D$

$C_4 = (10 + 4) mod\ 26 = 14\ mod\ 26 = 14 = O$

$C_5 = (10 + 12) mod\ 26 = 22\ mod\ 26 = 22 = W$

$C_6 = (10 + 0) mod\ 26 = 10\ mod\ 26 = 10 = K$

$C_7 = (10 + 19) mod\ 26 = 29\ mod\ 26 = 3 = D$

$C_8 = (10 + 8) mod\ 26 = 18\ mod\ 26 = 18 = S$

$C_9 = (10 + 10) mod\ 26 = 20\ mod\ 26 = 20 = U$

$C_{10} = (10 + 0) mod\ 26 = 10\ mod\ 26 = 10 = K$

$C_{11} = (10 + 17) mod\ 26 = 27\ mod\ 26 = 1 = B$

$C_{12} = (10 + 4) mod\ 26 = 14\ mod\ 26 = 14 = O$

$C_{13} = (10 + 0) mod\ 26 = 10\ mod\ 26 = 10 = K$

$C_{14} = (10 + 11) mod\ 26 = 21\ mod\ 26 = 21 = V$

$C_{15} = (10 + 8) mod\ 26 = 18\ mod\ 26 = 18 = S$

$C_{16} = (10 + 18) mod\ 26 = 28\ mod\ 26 = 2 = C$

$C_{17} = (10 + 19) mod\ 26 = 29\ mod\ 26 = 3 = D$

$C_{18} = (10 + 8) mod\ 26 = 18\ mod\ 26 = 18 = S$

$C_{19} = (10 + 10) mod\ 26 = 20\ mod\ 26 = 20 = U$

c. Pesan $P =$ **MATEMATIKAREALISTIK** dienskripsikan menjadi:

$C =$ WKDOWKDSUKBOKVSCDSU

Proses deskripsi:

Setelah proses enkripsi oleh kelompok A guru meminta kelompok B menerjemahkan isi pesan rahasia tersebut. Langkah-langkah yang dilakukan adalah sebagai berikut:

a. Pertama isi pesan tersebut pertama diubah ke bentuk suatu bilangan sama seperti proses awal enkripsi.

   $C =$ **WKDOWKDSUKBOKVSCDSU**

   Diintegerkan menjadi: $C =$

   22 10 3 14 22 10 3 18 20 10 1 14 10 21 18 2 3 18 20

b. Kemudian guru memberitahu kalau kuncinya adalah 12, sehingga siswa berupaya mengurangi bilangan tersebut dengan 12. Jika hasil yang diperoleh adalah bilangan negatif, maka bilangan tersebut ditambahkan dengan bilangan 26 atau kelipatannya. Secara matematis, proses deskripsi pada *Caesar Cipher* adalah sebagai berikut:

   $P = (K - C)\ mod\ 26$

   C = Cipherteks | K = Kunci | P = Plainteks

   Kunci: 12

   $P_1 = (C_1 - K) mod\ 26 = (22 - 10) mod\ 26 = 10\ mod\ 26 = 10 = M$

   $P_2 = (10 - 10) mod\ 26 = 0\ mod\ 26 = 0 = A$

   $P_3 = (3 - 10) mod\ 26 = -7\ mod\ 26 = 19 = T$

   $P_4 = (14 - 10) mod\ 26 = 4\ mod\ 26 = 4 = E$

   $P_5 = (22 - 10) mod\ 26 = 10\ mod\ 26 = 10 = M$

   $P_6 = (10 - 10) mod\ 26 = 0\ mod\ 26 = 0 = A$

   $P_7 = (3 - 10) mod\ 26 = -7\ mod\ 26 = 19 = T$

   $P_8 = (18 - 10) mod\ 26 = 8\ mod\ 26 = 8 = I$

   $P_9 = (20 - 10) mod\ 26 = 10\ mod\ 26 = 10 = K$

   $P_{10} = (10 - 10) mod\ 26 = 0\ mod\ 26 = 0 = A$

   $P_{11} = (1 - 10) mod\ 26 = -9\ mod\ 26 = 17 = R$

$P_{12} = (14 - 10) mod\ 26 = 4\ mod\ 26 = 4 = E$

$P_{13} = (10 - 10) mod\ 26 = 0\ mod\ 26 = 0 = A$

$P_{14} = (21 - 10) mod\ 26 = 11\ mod\ 26 = 11 = L$

$P_{15} = (18 - 10) mod\ 26 = 8\ mod\ 26 = 8 = I$

$P_{16} = (2 - 10) mod\ 26 = -8\ mod\ 26 = 18 = S$

$P_{17} = (3 - 10) mod\ 26 = -7\ mod\ 26 = 19 = T$

$P_{18} = (18 - 10) mod\ 26 = 8\ mod\ 26 = 8 = I$

$P_{19} = (20 - 10) mod\ 26 = 10\ mod\ 26 = 10 = K$

c. Dari hasil deskripsi di atas hasilnya kembali semula, yaitu: **MATEMATIKA REALISTIK.** Dari hasil yang diperoleh guru menjelaskan kepada siswa kalau apa yang telah mereka lakukan adalah menggunakan konsep modulo kemudian modulo 26, kemudian guru membimbing siswa untuk menemukan definisi dari modulo tersebut.

2. *Hill Cipher*

Pada bagian 1) telah dijelaskan mengenai media pembelajaran realistik mengenai modulo menggunakan kriptografi Caesar chipper. Selain menggunakan kriptografi Caesar Chiper, kriptografi Hill Chiper juga diyakini bisa digunakan sebagai media pembelajaran matematika realistik. Adapun Langkah-langkah yang dapat dilakukan adalah sebagai berikut:

Proses enskripsi

Pada bagian ini guru memberikan pesan rahasia pada kelompok A, misal isi pesan tersebut adalah PERGI LUSA. Guru meminta kelompok tersebut untuk mengubah pesan menjadi suatu sandi dengan cara sebagai berikut.

a. Membuat enkripsinya dengan mengkodekan atau mengubah setiap huruf abjad integer sebagai berikut.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
S	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**										

18	**19**	**20**	**21**	**22**	**23**	**24**	**25**

Maka pesan **PERGI LUSA** akan dikodekan/diintegerkan menjadi:

$$P = \mathbf{15\ 4\ 17\ 6\ 8\ 11\ 20\ 18\ 0}$$

Bilangan P dijadikan entri dari matriks berukuran 3x3, yaitu $P = \begin{bmatrix} 15 & 4 & 17 \\ 6 & 8 & 11 \\ 20 & 18 & 0 \end{bmatrix}$

b. Guru memberikan kunci, misal kunci yang diberikan adalah $K = \begin{bmatrix} 1 & 1 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 2 \end{bmatrix}$.

c. Proses penghitungan enskripsi guru meminta siswa mengalikan matriks P dengan K. Jika hasil yang diperoleh lebih dari 25, maka bilangan tersebut dikurangi dengan 26 atau kelipatannya. Secara matematis proses enkripsi Hill Chiper yang dilakukan adalah:

C = P . K mod 26

C = Cipherteks | K = Kunci | P = Plainteks

Diperoleh matriks $C = \begin{bmatrix} 15 & 4 & 17 \\ 6 & 8 & 11 \\ 20 & 18 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 15 & 19 & 76 \\ 6 & 14 & 58 \\ 20 & 38 & 94 \end{bmatrix} = \begin{bmatrix} 15 & 19 & 24 \\ 6 & 14 & 6 \\ 20 & 12 & 16 \end{bmatrix} = \begin{bmatrix} P & T & Y \\ G & O & G \\ U & M & Q \end{bmatrix}$

d. Pesan $P = PERGILUSA$ disandikan menjadi $C = PTYGOGUMQ$

Proses deskripsi:

Guru meminta kelompok B menerjemahkan sandi dari kelompok A yaitu $C = PTYGOGUMQ$. Langkah-langkah yang dilakukan adalah sebagai berikut:

a. Ubah sandi C menjadi matriks sandi berukuran 3x3 yaitu $C = \begin{bmatrix} P & T & Y \\ G & O & G \\ U & M & Q \end{bmatrix}$

b. Entri matriks C diganti dari huruf menjadi bilangan yang bersesuaian, yaitu $C = \begin{bmatrix} 15 & 19 & 24 \\ 6 & 14 & 6 \\ 20 & 12 & 16 \end{bmatrix}$

c. Guru memberitahu cara mendapatkan matriks C adalah dengan mengalikan matriks Pdan K, kemudian dikurangi kelipatan 26 jika hasilnya lebih dari 25 atau C = P . K. Siswa dibimbing untuk menemukan rumus matriks P yaitu $P = CK^{-1}$.

d. Siswa diminta menentukan matriks K^{-1}, yaitu $K^{-1} = \begin{bmatrix} 1 & -1 & \frac{1}{2} \\ 0 & 1 & -\frac{3}{2} \\ 0 & 0 & \frac{1}{2} \end{bmatrix}$

e. Siswa diminta menentukan nilai matriks P, yaitu $P = CK^{-1} = \begin{bmatrix} 15 & 19 & 24 \\ 6 & 14 & 6 \\ 20 & 12 & 16 \end{bmatrix} = \begin{bmatrix} 1 & -1 & \frac{1}{2} \\ 0 & 1 & -\frac{3}{2} \\ 0 & 0 & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 15 & 4 & -9 \\ 6 & 8 & -15 \\ 20 & 18 & 0 \end{bmatrix}$. Karena huruf A sampai Z berada pada rentangan 0-25, maka ketika bilangan P bernilai negative, maka bilangan tersebut ditambah dengan kelipatan 26. Begitupun sebaliknya jika bilangan pada P bernilai lebih dari 25 maka bilangan tersebut dikurangi dengan 26. Dengan demikin diperoleh nilai P adalah $P = \begin{bmatrix} 15 & 4 & 17 \\ 6 & 8 & 11 \\ 20 & 18 & 0 \end{bmatrix}$. Setelah dikonversi ke bentuk huruf menjadi $P = \begin{bmatrix} P & E & R \\ G & I & L \\ U & S & A \end{bmatrix}$

f. Pesan sandi $C = PTYGOGUMQ$ diterjemahkan Kembali ke pesan asli yaitu $P = PERGILUSA$.

g. Guru menginformasikan bahwa aktivitas pembelajaran yang mereka lakukan tadi adalah menggunakan konsep modulo, khususnya modulo 26. Dari sini guru Bersama siswa menemukan definisi formal dari modulo.

E. KESIMPULAN

Algoritma kriptografi *Caesar Cipher* dan *Hill Cipher* dapat diterapkan pada pelajaran modulo dan matriks sebagai pengiriman pesan rahasia antar siswa di kelas. Pengiriman pesan ini dikemas dalam bentuk permainan *role play*, dimana kegiatan ini merupakan salah satu dari media pembelajaran yang menjadikan matematika terasa hidup. Sederhananya konkret, yang dinamakan matematika realistik.

Dalam penerapannya di pembelajaran, media kriptografi tidak hanya bisa digunakan untuk mata pelajaran modulo dan matriks. Terdapat materi-materi lain yang dapat menggunakan kriptografi, salah satunya adalah materi komposisi fungsi dan komposisi invers yang diteliti oleh Najib Mubarak (2019) yang menggunakan kriptografi enigma termodifikasi yang djadikan sebagai media pembelajaran berbasis matematika realistic.

REFERENCES

UNDANG-UNDANG TENTANG SISTEM PENDIDIKAN NASIONAL. (2003).

Yanti, Ili. 2022. *Analisis Kemampuan Literasi Matematika Siswa dalam Menyelesaikan Soal Higher Order Thingking Skill (HOTS) pada Materi Matriks di Sekolah Menengah Atas Al-Azhar Jambi.* Skripsi UIN Sulthan Thaha Saifuddin Jambi. Dipublikasikan.

Widaya, Wayan. 2018. *Modul Penyusunan Soal Keterampilan Berpikir Tingkat Tinggi (Higher Order Thingking Skills) Matematika.* Jakarta: Direktorat Pembinaan Sekolah Menengah Atas.

Ibrahim. (2012). *Pembelajaran Matematika dengan ICT Sebagai Sarana Pengembangan Kecerdasan Emosional Siswa Menuju Pembangunan Karakter Bangsa*. Jurnal Fourier, *1*(2), 47–51.

Siregar, Nurul Hudaini Halim. 2018. *Implementasi Algoritma Kriptografi Hill Cipher Dalam Penyandian Data Gambar.* Tugas Akhir Universitas Sumatera Utara: Medan.

Arrijal, I. M. A., Efendi, R., & Susilo, B. (2016). Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks. Jurnal Pseudocode, 3(1), 69-82.).

Puspita, K., &Wayahdi, M. R. (2015, February). Analisis Kombinasi Metode Caesar Cipher, Vernam Cipher, Dan Hill Cipher Dalam Proses Kriptografi. In Jurnal Seminar Nasional Teknologi Informasidan Multimedia).

Arrijal, I. M. A., Efendi, R., & Susilo, B. (2016). Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks. Jurnal Pseudocode, 3(1), 69-82. Sasongko "Kriptografi Hill Chiper",2005

F. Aryani and Yulianis, "Trace Matriks Berbentuk Khusus 2 x 2 Berpangkat Bilangan Bulat Negatif," *J. Sains Mat. dan Stat.*, vol. 4, no. 2, pp. 105–113, 2018

Puspita, K., &Wayahdi, M. R. (2015, February). Analisis Kombinasi Metode Caesar,
Vernam Cipher, Dan Hill Cipher Dalam Proses Kriptografi. In Jurnal Seminar Nasional Teknologi Informasidan Multimedia.

Endaryono; Dwitiyanti, Nurfidah; Setiawan, Heri Satria. 2021. *Aplikasi Operasi Matriks pada Perancangan Simulasi Metode Hill Cipher Menggunakan Microsft Excel.* STRING, Vol.6 No.1 Agustus 2021.

Ginting, Dahlia Br. 2010. *Peranan Aritmetika Modulo dan Bilangan Prima pada Algoritma Kriptografi RSA.* Media Informatika Vol.9 No.2 (2010).

T, A. M., Konseling, B., Pendidikan, F. I., & Surabaya, U. N. (2018). Studi Kepustakaan Mengenai Landasan Teori Dan Praktik Konseling Expressive Writing. *Jurnal BK UNESA, 8*, 1–8.

Lismareni, N., Somakim., Kesumawati, N. (2014). Pengembangan Bahan Ajar Materi Aritmetika Sosial Menggunakan Konteks Bahan Bakar Minyak Dengan Pendekatan Pendidikan Matematika Realistik Indonesia Di SMP. *Jurnal Pendidikan Matematika UNSRI*, *1*, 1–12.

Schneier B, 1996. *Applied Cryptography: Protocols, Algorithms and Source Code in C 2nd Ed*. John Wiley & Sons, Inc. New Jersey.

Ariyus D, 2006. *Kriptografi: Keamanan Data dan Komunikasi*. Graha Ilmu. Yogyakarta.

A. Prayitno and N. Nurdin, "Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia," *J. Elektron. Sist. Inf. dan Komput.*, vol. 3, no. 1, pp. 1–11, 2017, [Online]. Available: nnurdin69@gmail.com

B. Solihin Hasugian, "Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2019, doi: https://doi.org/10.46576/wdw.v0i53.269.

Musrikah. 2016. *Model Pembelajaran Matematika Realistik Sebagai Optimalisasi Kecerdasan Logika Matematika pada Siswa SD/MI.* TA'ALLUM, Vol.04., No.01, Juni 2016.

Khabibah, "Suatu Alternatif Pembelajaran Matematika SD" *Makalah* disampaikan dalam seminar Nasional PMRI Tanggal 21 November 2001.

Yuwono I., "Pengembangan Model Pembelajaran Matematika secara Membumi", Disertasi, UNESA, 2006, tidak dipublikasikan.

Fatonah, Siti; Yulandari, Ania; Ariyus, Dony. (tanpa tahun). *Analisis Penerapan Modifikasi Algoritma Vigenere Cipher, Caesar Cipher, Vernam Cipher dan Hill Cipher untuk Penyisipan Pesan Dalam Gambar.*