Implementasi Algoritma Kriptografi Enigma Termodifikasi Sebagai Media Pembelajaran Matematika Berbasis Pmri Untuk Materi Komposisi Fungsi Dan Fungsi Invers

Najib Mubarok
Ekonomi Syariah, STAINU Temanggung
Jl. Suwandi-Suwardi No.2 Temanggung
Email: najib.mubarok28@gmail.com

ABSTRAK

Kriptografi merupakan salah satu cabang ilmu bidang matematika terapan yang menggunakan konsep aljabar abstrak dalam penerapannya. Dalam penerapannya untuk pengiriman pesan rahasia, kriptografi mendasarkan keamanannya pada aljabar yang termasuk di dalamnya konsep komposisi fungsi dan fungsi invers. Di sisi lain, Pendidikan Matematika Realistik Indonesia (PMRI) menghadapi tantangan dalam penyiapan bahan ajar dalam desain media pembelajaran yang konkret terutama untuk materi-materi matematika abstrak seperti komposisi fungsi dan fungsi invers. Dengan melakukan modifikasi algoritma kriptografi Enigma, tulisan ini bertujuan untuk mengimplementasikan kriptografi sebagai media pembelajaran berbasis PMRI untuk materi komposisi fungsi dan fungsi invers.
Kata Kunci: PMRI, Kriptografi Enigma, Komposisi fungsi, fungsi invers

ABSTRACT

Cryptography is one of applied mathematic studies that uses abstract algebra in its application. In securing secret message, cryptography uses algebra including composition and invers fungtion as its foundation. In other side, Indonesian Realistic Mathematic Education (PMRI) faces obstacle in preparing realistic media for some abstract mathematic subjects such as composition and invers function. The aim of this paper is to provide an exaple of concrete media using modified Enigma algorithm in learning composition and invers function based on PMRI.
Keywords: PMRI, Enigma cryptography, Composition of function, Invers of a function

PENDAHULUAN

Matematika memiliki peran penting dalam kemajuan peradaban umat manusia. Hal ini dapat dipahami 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). Namun, pentingnya pembelajaran matematika menghadapi tantangan-tantangan besar. Salah satunya adalah tentang bagaimana merubah paradigma lama pendekatan pengajaran matematika dari yang semula deduktif dan bersifat doktrinasi menuju paradigma baru yang menggiring peserta didik untuk menemukan sendiri konsep-konsep matematika melalui media realistik. Dengan kata lain, matematika di sekolah

seharusnya bukan lagi tentang bagaimana menghafalkan rumus matematika yang tidak diketahui asal usulnya. Lebih dari itu, matematika di sekolah hendaknya diarahkan menjadi suatu pendekatan pembelajaran konsep matematisasi permasalahan nyata (Soviawati, 2011).

Pendekatan pembelajaran yang menekankan pada matematisasi permasalahan nyata inilah yang saat ini disebut sebagai Pendidikan Matematika Realistik Indonesia (PMRI). Setidaknya terdapat tiga karakteristik utama PMRI. Pertama adalah menemukan kembali secara terbimbing melalui fenomena didaktik yang memungkinkan peserta didik menemukan titik tolak proses matematisasi dengan bimbingan pengajar. Kedua adalah matematisasi progresif yaitu melibatkan siswa secara langsung untuk menalami sendiri penemuan konsep matematika tahap demi tahap. Ketiga adalah mengembangkan model sendiri yaitu memberi kesemp-atan peserta didik untuk berinovasi terhadap konsep yang ditemukan. Dengan demikian, peserta didik memiliki ruang untuk mengembangkan konsep otentik dari proses matematisasi masing-masing (Zulkardi, Putri, & Ilma, 2010).

Dilihat dari tahapnya, PMRI diawali dengan konteks matematika informal yang realistik menuju konsep matematika formal yang abstrak. Dengan kata lain, pembelajaran dimulai dari konteks permasalahan yang konkret, semi konkret, lalu diakhiri dengan penyimpulan secara abstrak (Tampubolon & Asran, 2017). Dalam penerapannya di lapangan, PMRI menghadapi beberapa tantangan mulai dari merubah paradigma mengajar dari menggurui menjadi memfasilitasi sampai pada penyiapan bahan ajar yang diakui memiliki kompleksitas penyesuaian antara konsep teori dan aplikasi. Bahan ajar yang sesuai dengan PMRI merupakan bahan ajar yang dekat dengan kehidupan peserta didik dalam realita sekaligus bersesuaian dengan konsep matematika yang diajarkan (Sembiring, 2010).

Berbicara tentang bahan ajar yang memiliki kesesuaian antara konsep dan realita, materi-materi dasar matematika seperti operasi hitung aritmatika, pecahan, geometri dan statistika adalah beberapa contoh materi yang sangat dekat dengan kehidupan peserta didik karena sifatnya yang cenderung mudah diaplikasikan. Namun, hal sebaliknya terjadi pada beberapa materi matematika lanjut yang memiliki sifat abstrak dan jauh dari penerapan di dunia nyata seperti aljabar, analisis dan kalkulus. Pada sisi ini, PMRI menghadapi tantangan tentang bagaimana menyiapkan bahan ajar yang realistik dan dekat dengan peserta didik sekaligus mampu mengakomodir konsep matematika yang abstrak dalam kurikulum pendidikan (Soviawati, 2011).

Salah satu pokok bahasan matematika yang bersifat abstrak yang merupakan materi pokok mata pelajaran matematika wajib kelas XI adalah materi tentang komposisi fungsi

dan fungsi invers. Materi tentang komposisi fungsi dan fungsi invers dapat diklasifikasikan dalam lingkup materi aljabar. Mempertimbangkan sifat materi ini yang merupakan salah satu cabang matematika yang abstrak yaitu aljabar, menemukan media konkret sebagai media pembelajaran berbasis PMRI untuk materi pokok komposisi fungsi dan fungsi invers adalah tantangan bagi para peneliti dan pengajar.

Untuk menghadapi tantangan tersebut, perlu dikaji beberapa materi yang masuk dalam cakupan matematika terapan *(applied mathematic)*. Pengkajian ini dimaksudkan untuk menemukan media konkret aplikasi matematika abstrak dengan harapan dapat digunakan sebagai media konkret untuk dijadikan media pembelajaran matematika berbasis PMRI. Dari kajian yang dilakukan, terdapat salah satu materi dalam matematika terapan yang memuat berbagai teori matematika lanjut yaitu kriptografi. Secara sederhana, kriptografi dapat diartikan sebagai ilmu dan seni yang digunakan untuk merahasiakan pesan atau data. Dalam aplikasi nyata, kriptografi sangat dekat dengan kehidupan manusia misalnya dalam penggunaan password, pengamanan data perbankan, maupun pengamanan data keamanan negara. Dalam penerapannya, kriptografi menggunakan konsep matematika lanjut yang sangat abstrak dalam bidang aljabar dan kalkulus. Dalam kriptografi, konsep abstrak matematika lanjut aljabar dan kalkulus dijadikan pondasi landasan tingkat keamanan kerahasiaan data (Twindania Namiesyva, 2014).

Dengan demikian, kriptografi memenuhi salah satu syarat perlu media pembelajaran berbasis PMRI yaitu kesesuaian antara konsep matematika dengan media yang konkret dan dekat dengan kehidupan. Namun, hal tersebut tidaklah cukup ketika digunakan sebagai media pembelajaran di tingkat sekolah menengah. Konsep matematika dalam kriptografi yang sangat lanjut menjadikan kriptografi tidak sesuai dengan kurikulum pendidikan menengah. Lebih lanjut, kriptografi memerlukan perangkat komputer spesifikasi tinggi dan perangkat mesin canggih kriptografi yang sangat sulit dihadirkan dalam proses pembelajaran.

Dari permasalahan tersebut, penulis bermaksud untuk melakukan modifikasi dan inovasi pada algoritma kriptografi. Adapun algoritma kriptografi yang dipilih adalah algoritma kriptografi mesin Enigma. Modifikasi algoritma kriptografi Enigma dimaksudkan untuk menjawab tantangan permasalahan yang dihadapi dalam menemukan media pembelajaran berbasis PMRI untuk materi pokok komposisi fungsi dan fungsi invers melalui kriptografi.

METODE PENELITIAN

Jenis peneletian 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 buku tentang kriptografi dan beberapa jurnal tentang kriptografi dan pendidikan matematika. Buku berjudul *Understanding Cryptography* karya Paar dan Pelzl digunakan sebagai referensi utama dalam mempelajari materi-materi kriptografi. Adapun jurnal yang menjadi rujukan utama dalam penelitian ini adalah jurnal berjudul *Studi Enkripsi dan Kriptanalisis terhadap Enigma* karya Eddo Fajar N yang digunakan sebagai rujukan utama dalam mempelajari Enigma. Adapun jurnal berjudul *Pemahaman Konsep Siswa Pada Materi Volume Prisma Dengan Pendekatan Pendidikan Matematika Realistik Indonesia (Pmri)* karya Nur Fadlilah yang digunakan sebagai rujukan dalam memahami PMRI. Selain itu, digunakan buku-buku dan jurnal-jurnal lain untuk melengkapi data-data yang dibutuhkan.

HASIL DAN PEMBAHASAN

Banyak sekali penelitian yang sudah membuktikan efektifitas pembelajaran matematika berbasis PMRI. Dalam (Lismareni, N., Somakim., Kesumawati, 2014), disimpulkan bahwa pendekatan PMRI untuk materi aritmatika sosial telah mampu meningkatkan pemahaman peserta didik kelas VII. Dalam (Fadlilah, 2013), pendekatan PMRI dalam pembelajaran matematika untuk materi volume prisma mampu meningkatkan hasil belajar peserta didik secara signifikan. Bahkan, Dalam (Tahun & Taman, 2015), pendekatan PMRI dalam materi perkalian tidak hanya meningkatkan hasil belajar akan tetapi juga karakter peserta didik yaitu demokratis, mandiri, dan kreatif.

Hasil penelitian tersebut menunjukkan efek potensial pendekatan PMRI dalam meningkatkan hasil belajar matematika sekaligus mengembalikan inti pendidikan yaitu pembentukan karakter peserta didik. Adapun tulisan ini akan fokus membahas bagaimana modifikasi algoritma kriptografi dapat diimplementasikan sebagai media pembelajaran berbasis PMRI untuk materi pokok komposisi fungsi dan fungsi invers.

Pembahasan akan dibagi menjadi tiga sub pembahasan yaitu: dasar kriptografi, algoritma kriptografi Enigma termodifikasi, dan implementasinya sebagai media pembelajaran berbasis PMRI untuk materi pokok komposisi fungsi dan fungsi invers.

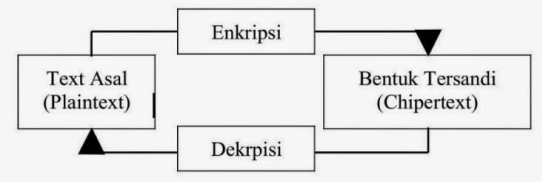
Dasar Kriptografi

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).

Salah satu aplikasi nyata kriptografi adalah pada pengiriman pesan rahasia. Dua pihak yang saling berkomunikasi rahasia atau mengirimkan pesan dengan isi pesan yang bersifat rahasia memerlukan kriptografi untuk menjaga kerahasiaan pesan. Hal ini dilakukan untuk menghindari pihak ketiga yang tidak berwenang *(unauthorized)* mengetahui makna pesan rahasia tersebut. Dalam pengiriman pesan rahasia, kriptografi mengambil peran dalam penyandian pesan awal yang dapat dibaca maknanya (plainteks) menjadi pesan tersandi yang tidak dapat dibaca (cipherteks) serta mengubah kembali cipherteks menjadi plainteks (Dafid, 2006).

Kriptografi merupakan aplikasi nyata matematika abstrak bidang aljabar. Aplikasi matematika abstrak pada kriptografi dapat dilihat pada algoritma pengiriman pesan rahasia yang terdiri dari fungsi matematis yaitu fungsi enkripsi dan dekripsi. Enkripsi adalah fungsi matematika yang memetakan plainteks menjadi cipherteks. Sedangkan dekripsi adalah fungsi invers dari enkripsi yang memetakan kembali cipherteks menjadi plainteks (Schneier, 1996).

Fungsi enkripsi dan dekripsi inilah yang akan digunakan sebagai ide dasar media pembelajaran materi komposisi fungsi dan fungsi invers berbasis PMRI.



Gambar 1: Skema Fungsi Enkripsi dan Dekripsi

Dalam melakukan enkripsi dan dekripsi, perlu ditentukan terlebih dahulu kunci yang digunakan. Berdasarkan kunci yang digunakan, algoritma pengiriman pesan rahasia dibagi menjadi dua yaitu algoritma kunci simetris yang disebut juga algoritma kunci rahasia dan algoritma kunci asimetris yang disebut juga algoritma kunci publik. Algoritma kunci rahasia menggunakan kunci yang sama dalam proses enkripsi dan dekripsi. Sedangkan algoritma

kunci publik menggunakan kunci yang berbeda pada proses enkripsi dan dekripsinya (Ratih, 2013).

Gambar berik-ut ini menunjukkan bagaimana proses pengiriman pesan rahasia menggunakan algoritma kunci simetris.

Gambar 2: Pengiriman Pesan Rahasia Algoritma Kunci Simetris

Secara matematis, untuk k adalah kunci rahasia yang disepakati untuk enkripsi dan dekripsi, P himpunan karakter-karakter plainteks, C himpunan karakter-karakter cipherteks, e fungsi enkripsi, dan d fungsi dekripsi, maka fungsi e dan d didefinisikan sebagai berikut:

$$e_k: P \rightarrow C$$

dan

$$d_k: C \rightarrow P$$

Salah satu manifestasi algoritma kunci rahasia yang sangat terkenal adalah mesin Enigma. Mesin Enigma adalah mesin untuk melakukan enkripsi dan dekripsi pesan rahasia militer Jerman pada Perang Dunia II.

Gambar 3: Mesin Kriptografi Enigma

Enigma dibuat oleh Arthur Schebius di Berlin pada 1918. Enigma sempat dipercaya sebagai mesin kriptografi yang mustahil dipecahkan *(unbreakable)* pada Perang Dunia II. Namun, asumsi tersebut patah saat sekelompok ahli matematika Polandia berhasil memecahkan Enigma dan mempercepat kemenangan sekutu atas Jerman untuk mengakhiri Perang Dunia II (Fajar, 2013).

Enigma menggunakan algoritma kunci rahasia yaitu algoritma cipher substitusi dalam melakukan enkripsi dan dekripsi. Cipher substitusi adalah dasar penyandian Enigma. Cipher substitusi adalah salah satu algoritma kunci rahasia (simetris) dengan konsep merubah karakter pesan awal (plainteks) menjadi karakter yang lain dengan aturan tertentu. Cipher substitusi yang paling sederhana adalah Sandi Caesar.

Untuk menggambarkan proses enkripsi Sandi Caesar, misalkan plainteks yang akan dikirimkan adalah "PESAN". Kunci rahasia yang disepakati pengirim dan penerima pesan adalah 9 yaitu menggeser setiap huruf pada kata "PESAN" menjadi sembilan karakter setelahnya. Semua pergeseran huruf dihitung dalam modulo 26 karena jumlah huruf abjad yang dipakai berjumlah 26. Plainteks dan cipherteks yang didapat adalah sebagai berikut:

- `Plainteks :PESAN`
- `Cipherteks :YNBJW`

Secara matematis, untuk $k = 9$ (kunci rahasia yang disepakati), P himpunan plainteks, C himpunan cipherteks, e fungsi enkripsi, dan d fungsi dekripsi, proses enkripsi dilakukan sebagai berikut:

$$e_9 : P \rightarrow C$$

$$e_9 : \mathrm{P} \rightarrow \mathrm{Y}$$

$$e_9 : \mathrm{E} \rightarrow \mathrm{N}$$

$$e_9 : \mathrm{S} \rightarrow \mathrm{B}$$

$$e_9 : \mathrm{A} \rightarrow \mathrm{J}$$

$$e_9 : \mathrm{N} \rightarrow \mathrm{W}$$

Dari simulasi enkripsi tersebut, cipherteks “YNBJW” dapat didekripsi oleh penerima pesan dengan menghitung hasil fungsi invers dari e_9 yaitu fungsi d_9 dengan menghitung 9 karakter sebelumnya dari cipherteks YNBJW.

Dengan demikian, Sandi Caesar tersebut hanya memiliki 26 kemungkinan kunci. Pihak ketiga yang ingin menyadap pesan akan cukup mudah memecahkan sandi tersebut walaupun tidak mengetahui nilai kunci rahasia k. Pada mesin Enigma, proses enkripsi dilakukan dengan ide penyandian yang lebih rumit sesuai tuntutan militer pada Perang Dunia II. Ide awal dari penyandian Enigma adalah dengan menukar karakter huruf menjadi huruf lainnya dengan urutan acak yang dilakukan melalui rotor penggerak yang terhubung dengan sistem elektronik. Lebih lanjut, proses enkripsi tidak hanya dilakukan sekali saja namun berkali-kali untuk melipatgandakan keamanan pesan dalam transmisi pesan militer (Fajar, 2013).

Dalam (Fajar, 2013), disebutkan bahwa banyaknya kemungkinan kunci rahasia yang mungkin adalah kurang lebih 15.000.000.000.000.000.000 kemungkinan kunci. Dengan tingkat keamanan tersebut dan belum ditemukannya komputer spesifikasi tinggi, sangat beralasan saat dikatakan Enigma tidak dapat dipecahkan waktu itu.

Dilihat dari prinsip enkripsi Enigma, proses enkripsi adalah fungsi matematis yang memetakan setiap huruf menjadi huruf lainnya dengan aturan tertentu. Lebih lanjut, dalam enkripsi Enigma, pemetaan haruslah bersifat bijektif untuk menjamin tingkat keamanan pesan dan menjamin proses dekripsi dapat dilakukan. Adapun enkripsi ganda mesin Enigma menggunakan konsep pemetaan fungsi berganda yang tidak lain adalah komposisi fungsi.

Dengan demikian, algoritma kriptografi Enigma dalam pengamanan pesan rahasia dapat dijadikan media konkret dalam pembelajaran materi pokok komposisi fungsi dan fungsi invers. Akan tetapi, jika melihat kompetensi dasar dan cakupan materi jenis-jenis fungsi yang harus diajarkan, maka perlu dilakukan modifikasi pada algoritma kriptografi Enigma.

Algoritma Kriptografi Enigma Termodifikasi

Modifikasi algoritma kriptografi Enigma meliputi modifikasi jenis fungsi enkripsi yang digunakan dan penyederhanaan alat peraga yang digunakan. Modifikasi jelas akan mengurangi tingkat keamanan penyandian. Namun, proses pembelajaran tidak memerlukan tingkat keamanan tinggi karena hanya sebagai simulasi proses pengiriman pesan rahasia. Adapun penyederhanaan alat peraga yang digunakan adalah dengan mengganti mesin Enigma asli dengan media yang mudah didapatkan di lingkungan sekolah.

Modifikasi awal yang dilakukan adalah pada sistem konversi karakter huruf menjadi angka. Pada konversi yang paling sederhana, konversi dilakukan dengan aturan sebagai berikut:

- Karakter A dikonversi menjadi angka 1
- Karakter B dikonversi menjadi angka 2
- Karakter C dikonversi menjadi angka 3

  ...
- Karakter Z dikonversi menjadi angka 26

Namun, untuk membuat algoritma kriptografi Enigma dapat digunakan lebih luas dalam cakupan materi pokok komposisi fungsi dan fungsi invers, maka aturan konversi adalah sebagai berikut:

- Karakter A dikonversi menjadi angka 1
- Karakter B dikonversi menjadi angka 2
- Karakter C dikonversi menjadi angka 3

...

- Karakter Z dikonversi menjadi angka 26
- (spasi) dikonversi menjadi angka 0
- Karakter a dikonversi menjadi angka -1
- Karakter b dikonversi menjadi angka -2
- Karakter c dikonversi menjadi angka -3

...

- Karakter z dikonversi menjadi angka -26

Tujuan penggunaan aturan konversi tersebut adalah agar domain fungsi enkripsi lebih variatif yang akan sangat berperan dalam memahami fungsi kuadrat dan fungsi akar kuadrat saat domain terdiri dari bilangan positif dan negatif.

Modifikasi selanjutnya adalah pada definisi fungsi enkripsi yang digunakan. Jika dalam fungsi enkripsi mesin Enigma menggunakan fungsi sesuai aturan sandi substitusi, maka modifikasi yang dilakukan pada fungsi enkripsi Enigma menggunakan fungsi-fungsi sesuai tuntutan kompetensi dasar kurikulum 2013 kelas XI.

Definisi fungsi enkripsi Enigma termodifikasi adalah fungsi-fungsi sebagai berikut:

1. $f(x) = 2x + 1$
2. $f(x) = \frac{x+2}{x-2}$
3. $f(x) = \sqrt[2]{x-9}$
4. $f(x) = x^2 + 2$
5. $f(x) = x + 2$ lalu $g(x) = 2x$

Alasan penggunaan fungsi-fungsi tersebut adalah untuk menstimulasi pemahaman peserta didik pada masing-masing sub materi pokok yang menjadi pembahasan materi pokok komposisi fungsi dan fungsi invers.

Implementasi pada Materi Pokok Komposisi Fungsi dan Fungsi Invers

Sebelum dijelaskan implementasi algoritma Enigma termodifikasi, terlebih dahulu diberikan penjelasan mengenai sub-sub materi pokok komposisi fungsi dan fungsi invers kelas XI kurikulum 2013. Adapun penggunaan kurikulum 2013 sebagai acuan adalah karena semangat kurikulum 2013 yang sejalan dengan semangat PMRI (Soviawati, 2011).

Berdasarkan kajian yang dilakukan penulis terhadap dokumen kurikulum dan buku ajar matematika kelas XI, setidaknya terdapat 7 (tujuh) sub materi pokok untuk materi pokok komposisi fungsi dan fungsi invers yaitu (1) relasi dan fungsi, (2) fungsi khusus, (3) fungsi surjektif, injektif, dan bijektif, (4) aljabar fungsi, (5) fungsi komposisi, (6) sifat-sifat

komposisi fungsi, dan (7) fungsi invers. Adapun implementasi algoritma termodifikasi yang dibahas pada tulisan ini diupayakan untuk dapat sesuai dengan sub-sub materi tersebut, sejalan dengan kompetensi dasar yang diharapkan, dan sejalan dengan semangat PMRI.

Sejalan dengan semangat PMRI, Bruner dalam (Rahmawati, 2011) memberikan tiga tahapan utama dalam pelaksanaan pembelajaran berbasis PMRI. Tiga tahapan tersebut adalah enaktif (aktifitas peserta didik melalui observasi nyata media konkret), ikonik (merepresentasikan kembali dalam visualisasi, gambar, atau diagram), dan simbolik (melakukan abstraksi perumusan tahap-tahap sebelumnya ke dalam simbol matematis). Tiga tahap inilah yang akan digunakan untuk mendesain proses pembelajaran dengan menjadikan algoritma kriptografi Enigma termodifikasi sebagai media pembelajarannya.

Simulasi proses pembelajaran materi pokok komposisi fungsi dan fungsi invers menggunakan algoritma kriptografi Enigma termodifikasi 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. Untuk menambah minat dan perhatian peserta didik, terlebih dahulu pengajar dapat menceritakan narasi cerita Perang Dunia II atau memutarkan video dokumenter Perang Dunia II antara pihak militer Jerman dan sekutu.

Setidaknya terdapat lima tahapan dalam permainan pengiriman pesan rahasia. Pertama, pihak pengirim dan penerima pesan melakukan perjanjian kunci yang memuat definisi fungsi enkripsi yang ingin disepakati kedua belah pihak. Sebagaimana telah dijelaskan pada sub pembahasan sebelumnya, definisi fungsi enkripsi merupakan fungsi dalam lima variasi bentuk. Misalkan pada simulasi ini, dilakukan perjanjian kunci dengan definisi fungsi enkripsi sebagai berikut:

$$f(x) = 2x + 1$$

Untuk menghindarkan peserta didik dari unsur-unsur simbolik di awal tahapan, maka bentuk fungsi linear tersebut dapat dirubah menjadi definisi fungsi verbal *"cipherteks adalah dua kali lipat plainteks yang kemudian ditambah satu"*.

Dari proses perjanjian kunci, pihak pengirim dan penerima pesan sudah memiliki aturan yang disepakati dalam melakukan enkripsi dan dekripsi pesan rahasia. Penggunaan definisi fungsi linear menjadi bentuk verbal akan menstimulasi pemahaman substantif makna fungsi linear. Lebih lanjut, penggunaan dalam bentuk verbal mengarahkan peserta didik untuk

memulai tahap pembelajaran dari tahap enaktif yang konkrit dan non simbolis sesuai dengan semangat PMRI.

Tahapan kedua adalah proses enkripsi atau penyandian pesan awal (plainteks) menjadi pesan tersandi (cipherteks) oleh pengirim pesan. Misalkan pesan yang ingin dikirim pengirim pesan adalah "Temui Aku Jam Enam Pagi", maka pengirim pesan melakukan enkripsi pesan dengan terlebih dahulu melakukan konversi karakter-karakter pesan menjadi angka sebagaimana aturan konversi yang telah disepakati. Dengan kunci *"cipherteks adalah dua kali lipat plainteks yang kemudian ditambah satu"*, maka pesan tersandi (cipherteks) yang diperoleh adalah sebagai berikut:

Tabel 1: Proses Enkripsi Pesan Rahasia

karakter plainteks (huruf)	Karakter Plainteks (angka)	analogi perhitungan enkripsi	karakter cipherteks
T	20	2(20)+1	41
e	-5	2(-5)+1	-9
m	-13	2(-13)+1	-25
u	-21	2(-21)+1	-41
i	-9	2(-9)+1	-17
(spasi)	0	2(0)+1	1
A	1	2(1)+1	3
k	-11	2(-11)+1	-21
u	-21	2(-21)+1	-41
(spasi)	0	2(0)+1	1
J	10	2(10)+1	21
a	-1	2(-1)+1	-1
m	-13	2(-13)+1	-25
(spasi)	0	2(0)+1	1
E	5	2(5)+1	11
n	-14	2(-14)+1	-27
a	-1	2(-1)+1	-1
m	-13	2(-13)+1	-25
(spasi)	0	2(0)+1	1
P	16	2(16)+1	33
a	-1	2(-1)+1	-1
g	-7	2(-7)+1	-13
i	-9	2(-9)+1	-17

Dari proses enkripsi di atas, karakter "a" dan "A" dienkripsi menjadi cipherteks yang berbeda. Hal ini bertujuan untuk menstimulasi pemahaman peserta didik tentang domain fungsi bilangan bulat positif dan negatif. Dari proses enkripsi ini pula, peserta didik

mengalami tahapan ikonik dengan merealisasikan pesan yang hendak dikirim dalam bentuk visualisasi mereka sendiri dalam tabel diagram penyandian pesan.

setelah pesan dienkripsi, pengirim pesan menuliskan cipherteks tersebut dalam selembar kertas untuk dimasukkan ke dalam amplop yang telah disediakan pengajar sebelumnya. Amplop berisi cipherteks tersebut kemudian dikirimkan kepada peserta didik lain yang bermain sebagai penerima pesan.

Tahapan ketiga adalah dekripsi pesan oleh penerima pesan. Cipherteks yang telah diterima dari pengirim pesan harus didekripsi agar pesan awal dapat dibaca. Dengan kunci yang telah disepakati yaitu *"cipherteks adalah dua kali lipat plainteks yang kemudian ditambah satu"*, pihak penerima pesan harus menemukan aturan dekripsi dari kunci tersebut. Dengan bimbingan pengajar, peserta didik yang bermain sebagai penerima pesan diarahkan untuk menemukan sendiri kunci untuk mengembalikan pesan cipherteks menjadi pesan awal.

Dari kunci *"cipherteks adalah dua kali lipat plainteks yang kemudian ditambah satu"*, , kunci untuk melakukan dekripsi adalah *"plainteks adalah cipherteks dikurangi satu kemudian hasilnya dibagi dua"*. Dengan kunci dekripsi tersebut, penerima pesan melakukan dekripsi sebagai berikut:

Tabel 2: Proses Dekripsi Pesan Rahasia

Karakter cipherteks	Analogi Perhitungan dekripsi	Karakter Plainteks (angka)	Karakter Plainteks (huruf)
41	(41-1)/2	20	T
-9	(-9-1)/2	-5	e
-25	(-25-1)/2	-13	m
-41	(-41-1)/2	-21	u
-17	(-17-1)/2	-9	i
1	(1-1)/2	0	(spasi)
3	(3-1)/2	1	A
-21	(-21-1)/2	-11	k
-41	(-41-1)/2	-21	u
1	(1-1)/2	0	(spasi)
21	(21-1)/2	10	J
-1	(-1-1)/2	-1	a
-25	(-25-1)/2	-13	m
1	(1-1)/2	0	(spasi)
11	(11-1)/2	5	E
-27	(-27-1)/2	-14	n
-1	(-1-1)/2	-1	a
-25	(-25-1)/2	-13	m

Karakter cipherteks	Analogi Perhitungan dekripsi	Karakter Plainteks (angka)	Karakter Plainteks (huruf)
1	(1-1)/2	0	(spasi)
33	(33-1)/2	16	P
-1	(-1-1)/2	-1	a
-13	(-13-1)/2	-7	g
-17	(-17-1)/2	-9	i

Dengan demikian penerima pesan mengetahui isi pesan yang dikirimkan pengirim pesan yaitu "Temui Aku Jam Enam Pagi". Dengan mengalami tahapan dekripsi, peserta didik akan dapat terstimulasi untuk memahami makna substantif dari konsep fungsi invers karena fungsi dekripsi tidak lain adalah fungsi invers dari fungsi enkripsi.

Tahapan keempat adalah balasan pesan. Pada tahap ini, peserta didik yang bermain sebagai pengirim dan penerima pesan bertukar peran. Penerima pesan sekarang bermain sebagai pengirim pesan untuk menkonfirmasi atau membalas pesan sebelumnya. Misal balasan pesan tersebut berisi "Aku Tunggu di Sekolah", maka selanjutnya dilakukan proses enkripsi dan dekripsi sebagaimana tahapan kedua dan ketiga. Dari tahapan ini, peserta didik yang terbagi menjadi dua pihak akan dapat mengalami keseluruhan proses dalam permainan.

Tahapan kelima adalah tahapan matematisasi yaitu memberi kebebasan peserta didik untuk menemukan sendiri formula dan pola matematis dari tahapan pertama sampai keempat. Pada tahapan pertama sampai keempat, peserta didik sudah mengalami bagaimana mengaplikasikan fungsi dalam permainan pengiriman pesan rahasia. Pada tahap terakhir ini, pengajar melakukan arahan dan bimbingan agar peserta didik dapat melakukan matematisasi permainan kriptografi menjadi simbol matematis konsep fungsi dan fungsi invers. Namun, tahapan kelima ini harus dilakukan dengan memberi ruang kebebasan peserta didik menemukan sendiri temuan otentik masing-masing.

Telah dijelaskan sebelumnya bahwa definisi fungsi yang digunakan memiliki setidaknya 5 (lima) variasi definisi fungsi enkripsi untuk memenuhi target kurikulum. Pada tahapan pertama sampai kelima yang telah dicontohkan, telah dilakukan simulasi permainan kriptografi dengan menggunakan definisi fungsi linear yaitu$f(x) = 2x + 1$. Untuk empat bentuk fungsi yang lain, maka simulasi permainan kriptografi dilakukan dengan cara yang analog dengan simulasi sebelumnya mulai dari tahapan pertama sampai kelima.

Adapun masing-masing variasi definisi fungsi yang telah ditentukan memiliki tujuan yang berbeda-beda sesuai dengan sub materi pokok yang ditargetkan kurikulum. Berikut ini

diberikan penjelasan penentuan definisi variasi-variasi tersebut dalam menstimulasi pemahaman materi pokok komposisi fungsi dan fungsi invers.

Tabel 3: Jenis Fungsi dan Stimulasi Pemahaman yang Diharapkan

Fungsi	Stimulasi pemahaman konsep yang diharapkan
$f(x) = 2x + 1$	- Pemahaman tentang konsep fungsi dan bagaimana fungsi diaplikasikan. Penggunaan fungsi linear di simulasi awal dimaksudkan agar peserta didik memahami konsep melalui permainan kriptografi yang paling sederhana - Pemahaman cara menentukan fungsi invers dari fungsi linear
$f(x) = \frac{x+2}{x-2}$	- Pemahaman definisi fungsi melalui domain fungsi. Dengan menggunakan definisi fungsi pecahan tersebut, peserta didik akan mengalami kegagalan dalam melakukan enkripsi salah satu karakter pesan yaitu karakter "B" yang dikonversi menjadi angka 2. Kegagalan dalam melakukan enkripsi karena terjadi pembagian oleh angka 0 diharapkan akan menstimulasi pemahaman peserta didik tentang domain fungsi dan definisi fungsi yang harus terdefinisi untuk setiap anggota domain fungsi. - Pemahaman cara menentukan fungsi invers dari fungsi pecahan
$f(x) = \sqrt[2]{x-9}$	- Pemahaman definisi fungsi melauli domain fungsi. Sejalan dengan fungsi pecahan, definisi fungsi akar tersebut diharapkan dapat menstimulasi pemahaman domain fungsi karena kegagalan proses enkripsi yang diakibatkan penarikan akar kuadrat dari bilangan negatif. - Pemahaman cara menentukan fungsi invers dari fungsi akar
$f(x) = x^2 + 2$	- Pemahaman tentang sifat-sifat fungsi yaitu surjektif, injektif, dan bijektif. Dalam aturan konversi, Huruf "A" dan "a" dikonversi menjadi 1 dan -1. Hal ini bertujuan untuk menstimulasi pemahaman konsep injektifitas fungsi. Ketika fungsi enkripsi didefinisikan dalam$x^2 + 2$, maka plainteks yang berbeda yaitu karakter "A" dan "a" akan dienkripsi menjadi cipherteks yang sama. Dengan demikian, akan terjadi kegagalan proses dekripsi. Hal ini disebabkan dua karakter plainteks "A" dan "a" dienkripsi menjadi 3 dan didekripsi kembali menjadi "A" dan "A" (bukan "A" dan "a"). - Pemahaman cara menentukan fungsi invers dari fungsi kuadrat
$f(x) = x + 2$ Lalu $g(x) = 2x$	- Pemahaman konsep komposisi fungsi dan sifatnya. Dengan menggunakan definisi fungsi enkripsi ganda, diharapkan peserta didik akan memahami konsep komposisi fungsi yaitu $(g \circ f)(x) = g(f(x))$ yang tidak lain adalah fungsi f yang dilanjutkan fungsi g. Lebih lanjut, pemahaman sebelumnya tentang domain dan range serta sifat-sifat fungsi (injektif, surjektif, dan bijektif) dapat dikombinasikan dalam

Fungsi	Stimulasi pemahaman konsep yang diharapkan
	pembahasan seusai permainan kriptografi untuk memahami sifat-sifat komposisi fungsi. Pemberian narasi cerita bagaimana kriptografi Enigma menggunakan enkripsi ganda untuk menambah keamanan pesan dapat ditambahkan oleh pengajar sebelum memulai permainan pada definisi fungsi enkripsi ganda ini. - Pemahaman cara menentukan fungsi invers dari fungsi komposisi

KESIMPULAN

Algoritma kriptografi Enigma dalam penerapannya untuk pengiriman pesan rahasia menggunakan konsep komposisi fungsi dan fungsi invers. Lebih lanjut, kriptografi Enigma dapat dikemas menjadi permainan pengiriman pesan rahasia yang menjadikan kriptografi Enigma dekat dan konkret sebagai media pembelajaran materi pokok komposisi fungsi dan fungsi invers.

Dengan modifikasi, definisi fungsi enkripsi algoritma kriptografi Enigma dapat dirubah untuk menyesuaikan antara media kriptografi Enigma dan tuntutan kurikulum materi pokok komposisi fungsi dan fungsi invers. Definisi fungsi enkripsi meliputi lima fungsi utama yaitu: fungsi linear, fungsi pecahan, fungsi akar, fungsi kuadrat, dan komposisi dua fungsi. Dengan modifikasi tersebut, kriptografi dapat diimplementasikan menjadi media pembelajaran materi komposisi fungsi dan fungsi invers dengan tanpa menghilangkan inti utama kriptografi Enigma dalam pengamanan pesan rahasia.

Implementasi kriptografi Enigma termodifikasi sebagai media pembelajaran komposisi fungsi dan fungsi invers dikemas dalam permainan kriptografi yang merupakan permainan *role play* pengiriman pesan rahasia. Simulasi permainan kriptografi Enigma termodifikasi terbagi dalam lima tahapan yaitu: perjanjian kunci, enkripsi, dekripsi, balasan pesan, dan matematisasi. Lima tahapan tersebut didesain untuk menstimulasi pemahaman peserta didik terhadap materi komposisi fungsi dan fungsi invers sesuai kompetensi dasar yang diharapkan kurikulum dan karakteristik PMRI.

UCAPAN TERIMAKASIH

Ucapan terimakasih penulis haturkan kepada teman-teman dosen STAINU Temanggung yang sangat membantu dalam penyusunan dan saran dalam penulisan. Tidak lupa ucapan terimakasih penulis haturkan kepada teman-teman komunitas Studi Sandi Yogyakarta yang sangat membantu dalam menyusun gagasan bidang kriptografi

DAFTAR PUSTAKA

Dafid. (2006). Kriptografi Kunci Simetris Dengan Menggunakan Algoritma Crypton. *STMIK MDP Palembang*, *2*(3), 20–27.

Fadlilah, N. (2013). Pemahaman Konsep Siswa Pada Materi Volume Prisma Dengan Pendekatan Pendidikan Matematika Realistik Indonesia (Pmri). *Jurnal Pendidikan Matematika UNSRI*, *8*, 1–10.

Fajar, E. (2013). Studi Enkripsi dan Kriptanalisis terhadap ENigma. *STEI ITB2*, *1*, 1–7.

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

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.

Paar, C., & Pelzl, J. (2009). *Cryptography*, *Understanding* (Second Edi). Germany: Springer. https://doi.org/10.1007/978-3-642-04101-3

Rahmawati. (2011). Desain pembelajaran penjumlahan dan pengurangan pecahan dengan menggunakan timbangan siswa kelas iv. *Jurnal Pendidikan Matematika*, *1*, 1–12.

Ratih. (2013). Studi dan Perbandingan Penggunaan Kriptografi Kunci Simetri dan Asimetri pada Telepon Selular Ratih – NIM: 13503016. *STEI ITB*, *1*, 1–8.

Schneier, B. (1996). Applied cryptography-protocols, algorithms, and source code in C. USA: Wiley New York.

Sembiring, R. K. (2010). Pendidikan Matematika Realistik Indonesia (PMRI): Perkembangan dan Tantangannya. *Journal on Mathematics Education (JME)*, *1*(1), 11–16. https://doi.org/10.22342/jme.1.1.791.11-16

Soviawati, E. (2011). Pendekatan Matematika Realistik (PMR) untuk Meningkatkan Kemampuan Berpikir Siswa di Tingkat Sekolah Dasar. *Jurnal UPI*, (2), 79–85.

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.

Tahun, U., & Taman, D. I. (2015). Upaya Guru Mengembangkan Kemandirian Anak. *Jurnal Pendidikan Dan Pembelajaran*, *4*, 1–13.

Tampubolon, B., & Asran, M. (2017). Pengaruh Media Konkret pada Pembelajaran Matematika Terhadap Hasil Belajar Siswa SDN 15 Sempalai Tebas. *Jurnal Pendidikan Dan Pembelajaran*, *6*(7).

Twindania Namiesyva. (2014). Kriptografi Sebagai Media Pembelajaran Dalam Studi Matematika Tingkat Sekolah. *ITB*, *1*, 1–12.

Zulkardi, Z., Putri, I., & Ilma, R. (2010). Pengembangan blog support untuk membantu siswa dan guru matematika Indonesia belajar pendidikan matematika realistic Indonesia (PMRI). *Jurnal Inovasi Perekayasa Pendidikan (JIPP)*, *2*(1), 1–24.