

Meningkatkan Pemahaman Konsep Fungsi Mata Kuliah Matematika Ekonomi Melalui Permainan Kriptografi (*Cryptogame*)

Najib Mubarak

*Ekonomi Syariah STAINU Temanggung, Indonesia
najib.mubarak28@gmail.com*

Abstrak: Konsep fungsi merupakan salah satu materi abstrak matematika yang sangat penting dalam mata kuliah Matematika Ekonomi. Pembelajaran materi fungsi perlu disusun agar tidak deduktif, jauh dari unsur doktrinasi, serta bersifat konkret. Tulisan ini bertujuan untuk menyusun aktifitas pembelajaran materi fungsi melalui permainan pengiriman pesan rahasia menggunakan algoritma kriptografi sandi Caesar. Lebih lanjut, tulisan ini juga bertujuan untuk mengetahui pengaruh permainan kriptografi tersebut dalam meningkatkan pemahaman konseptual materi fungsi terhadap mahasiswa ES semester II STAINU Temanggung. Metode yang digunakan dalam penelitian ini adalah quasi eksperimen. Dari hasil uji perbandingan Mann Whitney-U, didapatkan nilai Asymp. Sig. (2 tailed) sebesar 0,039. Dengan demikian, terbukti bahwa permainan kriptografi memberikan dampak positif dalam memahami konsep fungsi.

Kata kunci: Pembelajaran Fungsi, Permainan Kriptografi, Sandi Caesar

Improving The Understanding of Function Concept in Matematika Ekonomi Course Through Game of Cryptography (Cryptogame)

Abstract: Concept of function is one of the most critical abstract mathematical material in the Economics Mathematics course. Learning processes of function concept need to be arranged to make it not deductive, far from the elements of doctrine, and are concrete. This paper aims to arrange learning activities of the function concept through secret message delivery games using Caesar cryptographic algorithms. Moreover, this paper also aims to determine the effect of the cryptographic game in increasing conceptual understanding of functional material for the second semester ES students of STAINU Temanggung. The method used in this research was quasi-experimental. From the results of the Mann Whitney-U comparison test, the value of Asymp. Sig (2 tailed) is 0.039. Thus, it is proved that cryptographic games have a positive impact on understanding the concept of function.

Keywords: Learning of Function, Cryptography Games, Caesar Cipher

PENDAHULUAN

Matematika merupakan alat untuk memahami ilmu pengetahuan (*science*). Dalam bidang ekonomi, matematika menjadi pondasi pokok dalam berbagai aspek. Dengan menerapkan teori-teori yang abstrak dalam matematika, permasalahan-permasalahan ekonomi dapat diformulasikan, dianalisa, dan disusun secara sistematis. Dalam kehidupan sehari-hari, setiap manusia membutuhkan matematika dalam memecahkan masalah. Dalam ilmu pengetahuan dan terapannya, matematika adalah ratu ilmu pengetahuan (*queen of science*) sebagai alat utama pemahaman dan analisa (Rizal M., Muh., Thamrin Tayeb, & Nurkholisah Latuconsina. 2016: 173).

Dalam praktiknya, pembelajaran materi-materi matematika abstrak mendapat tantangan besar. Salah satunya pembelajaran materi fungsi. Materi fungsi yang abstrak, teoritis, konseptual menjadikan materi ini terkesan sulit terutama bagi mahasiswa yang tidak menyukai matematika. Salah satu alat bantu yang dapat digunakan untuk menciptakan proses pembelajaran yang konkret dan dekat dengan peserta didik adalah permainan. Dengan permainan, proses pembelajaran yang monoton dan membosankan dapat diarahkan menjadi lebih santai dan menyenangkan. Melalui

permainan, peran serta peserta didik dalam pembelajaran dan interaksi peserta didik dengan pengajar dapat ditingkatkan (Hendrawati, Elly Dwiana. 2018:07).

Permainan kriptografi yang disusun dalam proses pembelajaran adalah konstruksi permainan kriptografi yang sesuai dengan capaian pembelajaran mata kuliah Matematika Ekonomi Prodi Ekonomi Syariah (ES) STAINU Temanggung. Adapun permainan kriptografi yang dimaksud adalah permainan pengiriman pesan rahasia. Algoritma kriptografi yang digunakan adalah sandi Caesar (*Caesar cipher*). Dengan permainan pengiriman pesan rahasia, diharapkan mahasiswa mampu memahami konsep abstrak fungsi sesuai tujuan proses pembelajaran yang diharapkan yaitu penemuan kembali, matematisasi, dan inovasi otentik oleh peserta didik.

Salah satu aplikasi kriptografi adalah dalam pengiriman pesan rahasia. Suatu pesan yang bersifat rahasia dan hanya orang-orang tertentu yang diperbolehkan membaca isi pesan membutuhkan kriptografi untuk menyandikan pesan tersebut. Hal ini dilakukan untuk menghindari pihak ketiga yang tidak berwenang mengetahui isi pesan tersebut. Penyandian pesan dilakukan dengan merubah pesan awal (plainteks) menjadi pesan tersandi (cipherteks). Proses ini disebut sebagai proses enkripsi (Dafid. 2006: 20-27).

Kriptografi merupakan aplikasi nyata matematika abstrak bidang aljabar yaitu konsep fungsi. Aplikasi konsep fungsi 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, Bruce. 1996: 14).

Dengan menggunakan konsep fungsi enkripsi dan dekripsi, serangkaian aktifitas pembelajaran konsep fungsi dapat disusun menggunakan simulasi pengiriman pesan rahasia dalam bungkus permainan kriptografi. Salah satu algoritma kriptografi yang sederhana adalah algoritma kriptografi sandi Caesar (*Caesar cipher*). Dengan menggunakan algoritma sandi Caesar, diharapkan mahasiswa dapat memahami materi fungsi dengan mudah dan terhindar dari kerumitan konsep-konsep penyandian pesan.

Sandi Caesar menggunakan aturan kunci simetris dalam penyandian pesan. Aturan kunci simetris disebut juga algoritma kunci rahasia. Dalam algoritma kunci rahasia, digunakan kunci yang sama dalam proses enkripsi maupun dekripsi (Ratih. 2010:01). Dengan konsep 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

$$d_k: C \rightarrow P$$

Dengan demikian, kunci rahasia k digunakan baik dalam proses enkripsi maupun dekripsi. Lebih lanjut, pengirim dan penerima pesan harus menyepakati dulu kunci rahasia k sebelum melakukan enkripsi dan dekripsi (Fajar, Eddo. 2013: 01). Adapun teknik penyandian yang digunakan dalam sandi Caesar adalah cipher substitusi. Cipher substitusi adalah algoritma kunci rahasia yang menggunakan aturan pergeseran karakter sebanyak n -kali untuk setiap blok plainteks. Aturan pergeseran ini disebut juga aturan *shift* yaitu menggeser pesan awal (plainteks) menjadi pesan tersandi (cipherteks) dengan mensubstitusi karakter alfabet menjadi karakter alfabet lain ke sebelah kanan atau kiri (Pradipta, Anjar. 2016: 3-6).

Untuk menggambarkan proses penyandian sandi Caesar, misalkan Alice dan Bob adalah dua pihak yang ingin berkomunikasi secara rahasia. Alice sebagai pengirim pesan dan Bob sebagai

penerima pesan. Agar isi pesan tidak diketahui pihak ketiga yang tidak berwenang, maka Alice dan Bob menggunakan sandi Caesar untuk menyandikan pesan. Pertama, Alice dan Bob harus menyepakati kunci rahasia yang digunakan. Misal kunci rahasia yang dipilih adalah $k = 7$. Kunci rahasia $k = 7$ harus disepakati oleh Alice dan Bob secara rahasia sehingga tidak ada pihak lain yang tidak berwenang yang mengetahui kunci tersebut.

Selanjutnya, Alice melakukan proses enkripsi dengan kunci k yang telah disepakati. Misalkan Alice ingin mengirimkan pesan "MAAF", maka dengan kunci rahasia $k = 7$ setiap karakter digeser ke kanan sebanyak 7. Secara matematis, enkripsi pesan tersebut adalah sebagai berikut:

$$\begin{aligned} e_k: P &\rightarrow C \\ e_7(M) &= T \\ e_7(A) &= H \\ e_7(A) &= H \\ e_7(F) &= M \end{aligned}$$

Dengan demikian, pesan "MAAF" dienkripsi menjadi "THHM". Selanjutnya pesan "THHM" dikirimkan kepada Bob.

Setelah Bob menerima pesan dari Alice, maka untuk membaca pesan Bob melakukan dekripsi pesan. Dengan menggunakan kunci yang sama yaitu $k = 7$, Bob melakukan dekripsi. Fungsi dekripsi merupakan invers dari fungsi enkripsi. Dengan kata lain, jika e_7 bermakna menggeser karakter plaintext sebanyak 7 ke sebelah kanan, maka fungsi dekripsi d_7 adalah menggeser setiap karakter ciphertext sebanyak 7 ke sebelah kiri. Secara matematis, Bob melakukan dekripsi ciphertext sebagai berikut:

$$\begin{aligned} d_k: C &\rightarrow P \\ d_7(T) &= M \\ d_7(H) &= A \\ d_7(H) &= A \\ d_7(M) &= F \end{aligned}$$

Dengan demikian, Bob mengetahui isi pesan yang dikirim oleh Alice yaitu "MAAF". Dari simulasi pengiriman pesan rahasia sandi Caesar tersebut, terlihat bahwa terdapat kejadian konkret yang melibatkan konsep fungsi yang abstrak. Dengan demikian, simulasi pengiriman pesan rahasia dapat dijadikan alat bantu proses pembelajaran untuk memahami konsep fungsi. Namun, modifikasi dan inovasi perlu dilakukan untuk menyesuaikan antara pengiriman pesan rahasia sandi Caesar dengan materi fungsi mata kuliah Matematika Ekonomi.

Dari permasalahan dan teori kriptografi yang telah dipaparkan, tulisan ini bertujuan untuk menyusun serangkaian aktifitas pembelajaran materi fungsi dengan algoritma Sandi Caesar (*Caesar Cipher*) dalam bentuk permainan kriptografi. Selain itu, tulisan ini juga bertujuan untuk mengetahui apakah ada perbedaan pemahaman antara mahasiswa yang diajar materi fungsi melalui permainan kriptografi dengan mahasiswa yang diajar dengan cara konvensional.

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah penelitian eksperimen. Adapun subjek penelitian adalah mahasiswa semester II Ekonomi Syariah (ES) STAINU Temanggung yang mendapat mata kuliah wajib Matematika Ekonomi di semester II. Penelitian eksperimen merupakan metode penelitian yang dapat digunakan untuk mengetahui eksistensi pengaruh suatu perlakuan dibandingkan yang lain dalam kondisi yang terkendalikannya (Sugiyono, 2015: 107).

Terdapat beberapa jenis desain penelitian eksperimen, diantaranya *pre-experimental design*, *true-experimental design*, *factorial design*, dan *quasi experimental design*. Dalam tulisan ini, desain penelitian

eksperimen yang dipilih adalah *quasi experimental design* (penelitian semu). Desain penelitian eksperimen semu memiliki kelompok kontrol. Namun, adanya kelompok kontrol tidak mampu mengontrol sepenuhnya variabel-variabel luar yang mempengaruhi pelaksanaan eksperimen. Hal ini dikarenakan dalam eksperimen semu, pembagian kelompok kontrol dan kelompok eksperimen tidak dilakukan secara random. Pembagian dilakukan berdasarkan kondisi awal subjek penelitian (Sheskin, David J. 2003: 496).

Eksperimen semu dipilih mengingat Prodi ES STAINU Temanggung memiliki dua kelas untuk ES Semester II yaitu ES A dan ES B. Penggunaan eksperimen semu memungkinkan penelitian dapat dilakukan tanpa mengganggu proses perkuliahan mata kuliah Matematika Ekonomi. Secara rinci, desain eksperimen semu yang digunakan dalam penelitian ini berbentuk *nonequivalent control group design*. Dalam desain ini, akan terdapat dua kelompok yang tidak dipilih secara random. Kelompok pertama adalah kelompok eksperimen yang diambil dari Prodi ES A berjumlah 10 mahasiswa. Kelompok kedua adalah kelompok kontrol yang diambil dari Prodi ES B berjumlah 8 mahasiswa. Kelompok eksperimen diberi perlakuan (*treatment*) khusus berupa aktifitas pembelajaran materi fungsi melalui permainan kriptografi, sedangkan kelompok kontrol mendapat materi fungsi melalui cara konvensional (ceramah dan diskusi). Tabel berikut ini menggambarkan desain penelitian eksperimen semu *nonequivalent control group design* (Sheskin, David J. 2003: 496).

Tabel 1: Nonequivalent Control Group Design

Grup	Tahap 1	Tahap 2	Tahap 3
Kelompok Eksperimen	<i>Pretreatment response measure</i>	<i>Treatment</i>	<i>Posttreatment response measure</i>
Kelompok Kontrol	<i>Pretreatment response measure</i>	-	<i>Posttreatment response measure</i>

Dari tabel di atas, *nonequivalent control group design* dilakukan dengan memberikan dua kali tes untuk masing-masing kelompok yaitu *pretest* dan *posttest*. Dari data *pretest* dan *posttest*, dilakukan dua kali uji komparasi antara kelompok eksperimen dan kelompok kontrol. Uji komparasi data *pretest* dilakukan untuk memastikan tidak terdapat perbedaan kemampuan yang signifikan antara kedua kelompok. Adapun hasil dari uji komparasi data *posttest* digunakan untuk mendapatkan kesimpulan perbedaan kemampuan pemahaman materi fungsi kelompok yang tidak diberi perlakuan permainan kriptografi dengan kelompok yang diajar dengan cara konvensional.

Lebih lanjut, sebelum uji komparasi dilakukan terlebih dahulu dilakukan uji prasyarat untuk melihat normalitas dan homogenitas data. Jika data berdistribusi normal dan homogen, maka uji komparasi yang digunakan adalah uji T sampel independen (*independent sample T test*). Jika data tidak berdistribusi normal atau tidak homogen, maka uji komparasi dilakukan dengan uji Mann Whitney-U.

Dalam penelitian ini, terdapat empat uji statistika yang digunakan untuk melakukan analisa data. Berdasarkan uji statistika yang dapat digunakan beserta kriteria penerimaannya adalah sebagai berikut: 1) Uji Kolmogorof Smirnov. Uji ini digunakan untuk menguji normalitas data. Dalam uji ini Hipotesa bahwa data berdistribusi normal diterima apabila nilai *Asymp. Sig. (2 tailed)* lebih besar dari taraf signifikansi α ; 2) Uji Levene's. Uji ini digunakan untuk menguji homogenitas dua data yang saling independen. Hipotesa bahwa data saling homogen (memiliki variansi yang sama) diterima apabila nilai signifikansi (Sig.) kedua kelompok lebih besar dari taraf signifikansi α ; 3) Uji T sampel independen. Uji ini merupakan uji perbandingan dua rata-rata untuk data-data yang berdistribusi normal dan homogen antara dua kelompok independen. Hipotesa bahwa terdapat perbedaan yang signifikan antara dua kelompok diterima apabila nilai $t_{hitung} > t_{tabel}$; dan 4) Uji Mann Whitney-U.

Uji ini merupakan uji komparasi dua kelompok independen yang tidak berdistribusi normal atau tidak homogen. Hipotesa bahwa terdapat perbedaan yang signifikan antara kedua kelompok diterima apabila nilai *Asymp. Sig. (2-tailed)* lebih kecil dari taraf signifikansi α (Setyawarno, Didik. 2016: 3). Adapun taraf signifikansi α yang digunakan adalah 5% (0,05).

HASIL DAN PEMBAHASAN

Hasil dan pembahasan akan dibagi dalam dua subbab. Subbab pertama menjelaskan bagaimana simulasi proses pembelajaran menggunakan permainan kriptografi sandi Caesar. Adapun subbab kedua menjelaskan bagaimana pengaruh proses pembelajaran menggunakan permainan kriptografi dalam meningkatkan pemahaman konsep fungsi mata kuliah Matematika Ekonomi mahasiswa ES STAINU Temanggung.

Simulasi Proses Pembelajaran Materi Fungsi Melalui Permainan Kriptografi Sandi Caesar

Telah dijelaskan sebelumnya bahwa sandi Caesar menggunakan aturan yang sangat sederhana yaitu menggeser karakter sejauh n -karakter. Secara matematis, untuk k adalah kunci rahasia yang disepakati pengirim dan penerima pesan, maka fungsi e_k memetakan plainteks x menjadi karakter y dengan y adalah karakter yang berada di sebelah kanan x sejauh k karakter.

Adapun konsep fungsi merupakan salah satu materi penting dalam matematika abstrak yang membahas tentang pemetaan dari himpunan domain menuju kodomain. Konsep kriptografi sandi Caesar dan materi fungsi jelas memiliki benang merah kesamaan substansi materi yaitu pemetaan suatu karakter menjadi karakter lain dengan aturan tertentu. Dengan sedikit penyesuaian, maka konsep kriptografi sandi Caesar dapat disesuaikan agar dapat digunakan sebagai alat bantu proses pembelajaran materi fungsi.

Selanjutnya, untuk menyesuaikan antara konsep sandi Caesar dengan capaian pembelajaran materi fungsi mata kuliah Matematika Ekonomi, maka perlu dilakukan modifikasi-modifikasi. Modifikasi yang pertama adalah berkenaan dengan domain fungsi. Dalam sandi Caesar, domain fungsi tidak lain adalah himpunan karakter-karakter dalam bentuk huruf alfabet. Untuk lebih mendekatkan konsep sandi Caesar dengan konsep matematis fungsi, maka domain perlu dikonversi menjadi bilangan asli. Hal ini dikarenakan materi fungsi yang diajarkan dalam mata kuliah Matematika Ekonomi menggunakan konsep bilangan termasuk bilangan asli. Konversi domain huruf alfabet menjadi bilangan asli permainan kriptografi sandi Caesar adalah sebagai berikut:

- (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

Dengan aturan konversi karakter-karakter domain fungsi di atas, aturan penyandian sandi Caesar dapat dirumuskan dalam formula fungsi linear sederhana. Untuk k adalah kunci rahasia, e_k fungsi enkripsi, d_k fungsi dekripsi, x karakter plainteks, dan y karakter cipherteks, maka e_k dan d_k adalah fungsi linear sebagai berikut:

$$y = e_k(x) = x + k \pmod{27}, \text{ dan}$$

$$x = d_k(y) = y - k \pmod{27}.$$

Secara substansi, konsep penyandian sandi Caesar tidak lain adalah penerapan konsep fungsi linear dalam bentuk $f(x)$. Dengan memperhatikan dokumen Rencana Pembelajaran Semester (RPS), materi fungsi mata kuliah Matematika Ekonomi memuat tiga macam jenis fungsi utama yaitu fungsi linear, fungsi kuadrat, dan fungsi pecahan. Adapun capaian pembelajarannya adalah tentang pemahaman konseptual fungsi, analisa fungsi, dan penerapan fungsi dalam aplikasi ekonomi salah satunya aplikasi dalam fungsi permintaan dan penawaran. Lebih lanjut, materi fungsi yang dibahas pada mata kuliah Matematika Ekonomi akan terus dipakai dalam memahami materi-materi selanjutnya selama satu semester yaitu materi limit fungsi, diferensial, dan integral. Dengan tujuan sebagai alat bantu proses pembelajaran materi fungsi dan meningkatkan pemahaman konseptual fungsi, perlu dilakukan modifikasi definisi fungsi enkripsi dan dekripsi. Untuk x karakter plainteks dan y karakter cipherteks, maka fungsi enkripsi e_k didefinisikan sebagai berikut:

$$y = e_k(x) = f(x) = ax + c, \text{ dengan } a \text{ suatu bilangan bulat yang bukan } 0.$$

$$y = e_k(x) = f(x) = \frac{ax+c}{bx+d}, \text{ dengan } -a, b, c, d \text{ bilangan asli dan untuk } b \neq 0 \text{ atau } d \neq 0.$$

$$y = e_k(x) = f(x) = ax^2 + c, \text{ untuk } a \text{ suatu bilangan bulat yang bukan } 0.$$

Dari definisi fungsi enkripsi yang telah dimodifikasi tersebut, fungsi dekripsi d_k yang merupakan invers dari fungsi e_k dapat didefinisikan. Untuk y adalah karakter cipherteks dan x karakter plainteks, fungsi dekripsi d_k dapat didefinisikan sebagai berikut:

$$x = d_k(y) = g(y) = \frac{y-c}{a}, \text{ dengan } a \text{ suatu bilangan bulat yang bukan } 0.$$

$$x = d_k(y) = g(y) = \frac{dy-c}{a-by}, \text{ dengan } -a, b, c, d \text{ bilangan asli dan untuk } b \neq 0 \text{ atau } d \neq 0.$$

$$x = d_k(y) = g(y) = \sqrt{\frac{y-c}{a}}, \text{ untuk } a \text{ suatu bilangan bulat yang bukan } 0.$$

Dengan menggunakan definisi fungsi enkripsi dan dekripsi di atas, simulasi permainan pengiriman pesan rahasia dengan menggunakan kriptografi sandi Caesar dapat disimulasikan untuk menstimulasi pemahaman materi fungsi mata kuliah Matematika Ekonomi. Permainan pengiriman pesan rahasia yang disusun sebagai alat bantu proses pembelajaran terdiri dari lima tahapan yaitu perjanjian kunci, enkripsi pesan, dekripsi pesan, balasan pesan, dan matematisasi.

Tahapan pertama adalah perjanjian kunci. Sebagaimana simulasi pengiriman pesan rahasia sandi Caesar yang telah dijelaskan, pengirim dan penerima pesan rahasia harus menyepakati kunci rahasia yang digunakan sebelum saling berkomunikasi. Sebelumnya, dosen perlu membagi mahasiswa di dalam kelas menjadi dua kelompok yaitu kelompok mahasiswa yang berperan sebagai pengirim pesan dan kelompok mahasiswa yang berperan sebagai penerima pesan.

Jika dalam kriptografi sandi Caesar perjanjian kunci adalah menyepakati nilai kunci rahasia k , maka dalam permainan kriptografi ini perjanjian kunci adalah perjanjian definisi fungsi yang digunakan. Misalkan Pengirim dan penerima pesan bersepakat bahwa fungsi enkripsi yang digunakan adalah fungsi jenis pertama yaitu:

$$e_k(x) = f(x) = ax + c.$$

Dengan memilih nilai $a = 3$ dan $c = 2$, maka fungsi enkripsi yang disepakati adalah sebagai berikut:

$$e_k(x) = f(x) = 3x + 2.$$

Untuk menghindarkan mahasiswa dari konsep fungsi yang abstrak di awal tahapan, dosen dapat memulai definisi fungsi dalam bentuk non simbolis. Bentuk fungsi dapat disusun dalam bentuk verbal. Untuk definisi fungsi enkripsi $f(x) = 3x + 2$, definisi dapat dirubah menjadi fungsi enkripsi dalam bentuk verbal "*cipherteks adalah tiga kali lipat plainteks yang kemudian ditambah 2*". Tujuan dari penggunaan fungsi dalam bentuk non simbolis adalah agar mahasiswa dapat memahami konsep fungsi melalui tahapan yang konkret. Setelah mahasiswa yang berperan sebagai pengirim dan penerima pesan menyepakati definisi fungsi enkripsi tersebut, maka tahapan permainan pengiriman pesan rahasia dapat dilanjutkan.

Tahapan kedua adalah enkripsi pesan oleh pengirim pesan. Misalkan pengirim pesan ingin mengirimkan pesan plainteks "SAYA TUNGGU DI KAMPUS". Enkripsi dilakukan dengan terlebih dahulu melakukan konversi masing-masing karakter menjadi angka dan selanjutnya dienkripsi dengan definisi fungsi yang telah disepakati. Tabel berikut ini berisi proses enkripsi yang dilakukan pengirim pesan.

Tabel 2: Proses Enkripsi Pesan

Karakter plainteks (huruf)	Karakter Plainteks (angka)	Analogi perhitungan enkripsi	Karakter Cipherteks
S	19	$3(19)+2$	59
A	1	$3(1)+2$	5
Y	25	$3(25)+2$	77
A	1	$3(1)+2$	5
(spasi)	0	$3(0)+2$	2
T	20	$3(20)+2$	62
U	21	$3(21)+2$	65
N	14	$3(14)+2$	44
G	7	$3(7)+2$	23
G	7	$3(7)+2$	23
U	21	$3(21)+2$	65
(spasi)	0	$3(0)+2$	2
D	4	$3(4)+2$	14
I	9	$3(9)+2$	29
(spasi)	0	$3(0)+2$	2
K	11	$3(11)+2$	35
A	1	$3(1)+2$	5
M	13	$3(13)+2$	41
P	16	$3(16)+2$	50
U	21	$3(21)+2$	65
S	19	$3(19)+2$	59

Dari tabel proses enkripsi di atas, mahasiswa dituntut untuk memahami makna substansi fungsi dan melakukan perhitungan pemetaan fungsi melalui permainan enkripsi pesan. Setelah pengirim pesan melakukan enkripsi pesan dan memperoleh cipherteks "59 5 77 5 2 62 65 44 23 23 65 2 14 29 2 35 5 41 50 65 59", pengirim pesan menuliskan cipherteks tersebut pada selembar kertas. Selanjutnya, kertas tersebut diberikan kepada penerima pesan.

Tahapan selanjutnya adalah dekripsi pesan oleh penerima pesan. Setelah mahasiswa yang berperan sebagai penerima pesan menerima selembar kertas berisi cipherteks dari pengirim pesan, pesan cipherteks perlu didekripsi agar penerima pesan dapat membaca isi pesan. Dari definisi fungsi yang telah disepakati, penerima pesan diarahkan untuk menemukan sendiri fungsi dekripsi dari fungsi enkripsi verbal. Fungsi enkripsi verbal adalah "*cipherteks adalah tiga kali lipat plainteks yang kemudian ditambah dua*". Mahasiswa diarahkan untuk menemukan fungsi dekripsi verbal yaitu "*plainteks adalah*

cipherteks dikurangi dua kemudian dibagi tiga". Dosen dapat mengarahkan mahasiswa dengan memberi petunjuk bahwa definisi fungsi dekripsi adalah kebalikan dari definisi fungsi enkripsi. Dengan menggunakan definisi fungsi dekripsi tersebut, penerima pesan melakukan dekripsi sebagaimana digambarkan tabel di bawah ini.

Tabel 3: Proses Dekripsi Pesan

Karakter Cipherteks	Analogi Perhitungan Dekripsi	Karakter Plainteks (angka)	Karakter Plainteks (huruf)
59	$(59-2)/3$	19	S
5	$(5-2)/3$	1	A
77	$(77-2)/3$	25	Y
5	$(5-2)/3$	1	A
2	$(2-2)/3$	0	(spasi)
62	$(62-2)/3$	20	T
65	$(65-2)/3$	21	U
44	$(44-2)/3$	14	N
23	$(23-2)/3$	7	G
23	$(23-2)/3$	7	G
65	$(65-2)/3$	21	U
2	$(2-2)/3$	0	(spasi)
14	$(14-2)/3$	4	D
29	$(29-2)/3$	9	I
2	$(2-2)/3$	0	(spasi)
35	$(35-2)/3$	11	K
5	$(5-2)/3$	1	A
41	$(41-2)/3$	13	M
50	$(50-2)/3$	16	P
65	$(65-2)/3$	21	U
59	$(59-2)/3$	19	S

Dari tabel tersebut, mahasiswa yang berperan sebagai penerima pesan dituntut untuk memahami makna substansi konsep pemetaan fungsi melalui proses dekripsi. Dari tahapan dekripsi, penerima pesan mengetahui bahwa pengirim pesan mengirimkan pesan yang berisi "SAYA TUNGGU DI KAMPUS".

Tahapan keempat adalah balasan pesan. Dalam tahapan ini, pengirim dan penerima pesan saling bertukar peran. Setelah penerima pesan melakukan dekripsi dan berhasil membaca isi pesan, maka selanjutnya penerima pesan bertindak sebagai pengirim pesan untuk membalas pesan yang diterima. Misalkan balasan pesan yang akan dikirim adalah "BAIK KITA BERTEMU JAM ENAM PAGI", maka selanjutnya dilakukan proses enkripsi dan dekripsi sebagaimana tahapan kedua dan ketiga. Hanya saja, mahasiswa yang berperan sebagai pengirim dan penerima pesan saling bertukar peran. Tahapan balasan bertujuan agar masing-masing kelompok mahasiswa mengalami seluruh tahapan proses enkripsi dan dekripsi.

Tahapan terakhir adalah tahapan matematisasi. Dengan bimbingan dosen, mahasiswa diminta melakukan tahapan simbolisasi dari simulasi permainan yang telah dilakukan. Matematisasi yang dilakukan meliputi berbagai hal. Dalam tahapan perjanjian kunci, mahasiswa dibimbing untuk menemukan sendiri bentuk simbolis fungsi $f(x) = 3x + 2$ dari bentuk verbalnya "*cipherteks adalah dua kali lipat dari plainteks kemudian ditambah dua*". Dari tahapan enkripsi pesan, mahasiswa dibimbing untuk menemukan sendiri konsep simbolis pemetaan fungsi. Misalkan untuk karakter "S" yang dienkripsi menjadi angka 59, mahasiswa diarahkan untuk memahami substitusi angka 19 pada fungsi $f(x) = 3x + 2$ sebagai berikut:

$$\begin{aligned} \Leftrightarrow f(x) &= 3x + 2 \\ \Leftrightarrow f(19) &= 3(19) + 2 \\ \Leftrightarrow f(19) &= 57 + 2 \\ \Leftrightarrow f(19) &= 59 \end{aligned}$$

Dari tahapan dekripsi, mahasiswa diarahkan untuk melakukan simbolisasi fungsi dekripsi. Dari fungsi dekripsi verbal "*plaintexts adalah cipherteks yang dikurangi dua kemudian dibagi tiga*", mahasiswa diarahkan untuk menemukan sendiri fungsi $g(y) = \frac{x-2}{3}$. Lebih lanjut, dosen dapat memberikan tambahan pengetahuan bahwa fungsi $g(y)$ adalah invers dari fungsi $f(x)$ untuk mengarahkan pemahaman substantif makna fungsi invers. Kemudian, mahasiswa diarahkan untuk memahami konsep substitusi pada fungsi dekripsi $g(x)$. Misalkan untuk cipherteks angka 59, mahasiswa diarahkan untuk menemukan karakter plaintexts "S" dengan substitusi sebagai berikut:

$$\begin{aligned} \Leftrightarrow g(y) &= \frac{x-2}{3} \\ \Leftrightarrow g(59) &= \frac{59-2}{3} \\ \Leftrightarrow g(59) &= \frac{57}{3} \\ \Leftrightarrow g(59) &= 19 \text{ (yang kemudian dikonversi menjadi huruf "S").} \end{aligned}$$

Dari lima tahapan yang telah dipaparkan, terlihat bahwa tahapan-tahapan tersebut menuntut mahasiswa untuk memahami konsep abstrak fungsi melalui media yang konkret dan menyenangkan. Lebih lanjut, untuk mengarahkan mahasiswa memahami seluruh konsep jenis fungsi yang lain seperti fungsi kuadrat dan fungsi pecahan, maka cukup merubah jenis fungsi yang digunakan mulai dari tahapan pertama sampai terakhir. Dengan lima tahapan simulasi tersebut, diharapkan proses pembelajaran materi fungsi yang abstrak dapat dilakukan dengan cara yang konkret melalui permainan pengiriman pesan rahasia kriptografi sandi Caesar.

Analisa Statistika Pengaruh Permainan Kriptografi Sandi Caesar Dalam Meningkatkan Pemahaman Konseptual Fungsi Mata Kuliah Matematika Ekonomi

Selanjutnya akan dibahas bagaimana penerapan strategi permainan kriptografi dapat meningkatkan pemahaman konsep mahasiswa tentang materi fungsi.

Pertama adalah analisa komparasi data nilai *pretest*. Data *pretest* diambil dari kelas eksperimen dan kelas kontrol untuk mengukur kemampuan pemahaman awal sebelum diberi perlakuan. Soal terdiri dari lima butir soal untuk mengukur daya ingat dan pemahaman mahasiswa materi fungsi yang pernah diajarkan di sekolah menengah. Lima butir soal yang diberikan berisi dua soal mudah, dua soal sedang, dan satu soal sulit. Sebelum digunakan sebagai soal *pretest*, terlebih dahulu soal divalidasi oleh dosen mata kuliah Matematika Ekonomi dan diujicobakan kepada mahasiswa ES semester IV sebagai mahasiswa yang pernah mendapat materi fungsi di semester II. Adapun untuk *posttest*, jenis soal yang sama tetap digunakan dengan merubah angka tanpa mengurangi substansi dan tingkat kesulitan soal.

Data hasil *pretest* dan *posttest* kelas ES IIA (kelas eksperimen) dan ES IIB (kelas kontrol) adalah sebagai berikut:

Tabel 4: Data Nilai Pretest dan Posttest Kelas Eksperimen dan Kelas Kontrol

Kelas Eksperimen (ES IIA)			Kelas Kontrol (ES IIB)		
Nama	Nilai pretest	Nilai posttest	Nama	Nilai pretest	Nilai posttest
APS	20	60	AN	20	20
Am	25	65	Af	25	45
Ai	20	70	At	30	40
AMM	40	70	BA	50	75
DUK	45	80	FLM	50	75
FCA	50	80	MJR	55	55
IAA	30	55	MAM	25	25
JWF	20	65	RM	20	55
KT	35	75			
SN	30	55			

Adapun deskripsi data dari data nilai pretest adalah sebagai berikut:

Tabel 5: Deskripsi Data Nilai Pretest

Grup	Mean	Std. Deviasi	Max	Min
Kelas Eksperimen (ES IIA)	31,500	10,814	50	20
Kelas Kontrol (ES IIB)	34,375	14,745	55	20

Dari deskripsi data nilai pretest, rata-rata nilai kelompok kontrol lebih baik dari kelompok eksperimen. Tujuan dari analisa data pretest adalah untuk menjamin kedua kelompok memiliki kondisi kemampuan yang sama sebelum diberi perlakuan. Kondisi kemampuan yang sama sebelum perlakuan menunjukkan signifikansi dampak perbedaan yang timbul pada kedua kelas adalah akibat perlakuan yang diberikan (Gravetter, Frederick J. and Lori-Ann B. Forzano. 2018).

Dengan demikian, perlu dibuktikan bahwa perbedaan rata-rata yang ada tidak bermakna. Sebelumnya, dilakukan uji normalitas dan homogenitas dari kedua kelompok. Dengan SPSS, hasil output uji Kolmogorov Smirnov (K-S) didapatkan nilai *Asymp. Sig. (2 tailed)* untuk kelas eksperimen dan kontrol berturut-turut 0,968 dan 0,738. Karena nilai *Asymp. Sig. (2 tailed)* lebih besar dari nilai $\alpha = 0,05$, maka kedua kelas berdistribusi normal. Lebih lanjut, hasil uji Levene's kedua kelompok menghasilkan nilai signifikansi (Sig.) kedua kelompok adalah 0,119 yang lebih besar dari $\alpha = 0,05$. Berdasarkan kriteria penerimaan hipotesa, maka kedua kelas memiliki varian yang sama (homogen).

Untuk menguji perbedaan mean kedua kelompok, dilakukan uji statistika parametris uji T sampel independen karena data sampel berdistribusi normal dan homogen. Dari uji T, didapatkan nilai $t_{hitung} = 0,478$ yang lebih kecil dari $t_{tabel} = 1,746$. Dengan demikian hipotesa nihil diterima yaitu tidak terdapat perbedaan yang bermakna antara kelas eksperimen dan kelas kontrol berkenaan nilai pretest.

Selanjutnya adalah analisa data nilai posttest. Deskripsi data nilai posttest kedua kelompok adalah sebagai berikut:

Tabel 6: Deskripsi Data Nilai Posttest

Grup	Mean	Std. Deviasi	Max	Min
Kelas Eksperimen (ES IIA)	67,500	9,205	80	55
Kelas Kontrol (ES IIB)	48,750	20,485	75	20

Dari deskripsi data di atas, terlihat rata-rata kelas eksperimen lebih besar dari rata-rata kelas kontrol. Namun, analisa komparasi perlu dilakukan untuk membuktikan perbedaan tersebut

bermakna. Jika terdapat perbedaan yang bermakna, maka dapat disimpulkan nilai *posttest* kelas eksperimen lebih baik dari kelas kontrol secara signifikan.

Dengan langkah yang analog dengan sebelumnya, hasil uji Kolmogorov-Smirnov menunjukkan nilai *Asymp. Sig. (2-tailed)* kelas eksperimen dan kelas kontrol berturut-turut 1,000 dan 0,994. Nilai tersebut lebih besar dari $\alpha = 0,05$, sehingga data nilai *posttest* kedua kelompok berdistribusi normal. Selanjutnya, hasil uji Levene's menunjukkan nilai signifikansi (*Sig.*) kedua kelompok adalah 0,035. Dengan demikian data nilai *posttest* kedua kelompok memiliki varian yang berbeda (tidak homogen). Oleh karena itu, dilakukan uji statistika nonparametris untuk mengetahui perbedaan rata-rata kedua kelompok.

Uji statistika nonparametris yang dipilih adalah uji Mann Whitney-U. Dari hasil uji Mann Whitney-U, didapatkan nilai *Asymp. Sig. (2 tailed)* adalah 0,039. Berdasarkan kriteria penerimaan hipotesa uji Mann Whitney-U, nilai *Asymp. Sig. (2 tailed)* lebih kecil dari $\alpha = 0,05$. Dengan demikian, hipotesa aksi diterima yaitu terdapat perbedaan yang bermakna antara kelas eksperimen dan kelas kontrol. Berdasarkan nilai rata-rata kedua kelompok, Mean kelompok eksperimen sebesar 67,500 lebih besar dari mean kelompok kontrol sebesar 48,750. Dengan demikian, disimpulkan bahwa nilai *posttest* kelas eksperimen lebih baik dari kelas kontrol secara signifikan (bermakna). Dengan kata lain, permainan kriptografi terbukti dapat meningkatkan pemahaman materi fungsi mata kuliah Matematika Ekonomi.

SIMPULAN

Algoritma kriptografi sandi Caesar dapat digunakan sebagai alat bantu proses pembelajaran materi fungsi mata kuliah Matematika Ekonomi. Proses pembelajaran materi fungsi menggunakan algoritma kriptografi sandi Caesar dikemas dalam permainan kriptografi pengiriman pesan rahasia. Dalam tulisan ini, permainan kriptografi terbagi dalam lima tahapan yaitu perjanjian kunci, enkripsi pesan, dekripsi pesan, balasan pesan, dan matematisasi. Dalam permainan kriptografi sandi Caesar, Mahasiswa diarahkan untuk mengalami makna substantif konsep fungsi yang abstrak melalui media yang konkret dan menyenangkan.

Hasil uji komparasi data *posttest* menggunakan uji Mann Whitney-U menghasilkan nilai *Asymp. Sig. (2 tailed)* sebesar 0,039 sehingga hipotesa aksi diterima yaitu terdapat perbedaan yang bermakna antara kelas yang diberi perlakuan permainan kriptografi sandi Caesar dengan yang diajar menggunakan metode konvensional. Hasil uji statistika yang telah dilakukan menunjukkan bahwa perlakuan (*treatment*) permainan kriptografi sandi Caesar dalam proses pembelajaran mampu meningkatkan kemampuan pemahaman konsep fungsi mata kuliah Matematika Ekonomi.

DAFTAR PUSTAKA

- Dafid. (2006). Kriptografi Kunci Simetris Dengan Menggunakan Algoritma Crypton. *Alogaritma*, 2(3), 20–27.
- Fajar, Eddo. (2013). Studi Enkripsi Dan Kriptanalisis Terhadap ENigma. *STEI ITB*, 2(1), 1–7.
- Gravetter, Frederick J. & Lori-Ann B. Forzano. (2018). *Research Methods for the Behavioral Sciences*. Cengage Learning. Belmont: Wadsworth.
- Hendrawati, Elly Dwiana. (2018). Penggunaan Media Permainan Dalam Pembelajaran Matematika Untuk Pengembangan Karakter Siswa Di SMP Negeri 24 Surakarta. *Naskah Publikasi Sekolah Pascasarjana Universitas Muhammadiyah Surakarta*.
- Pradipta, Anjar. (2016). Implementasi Metode Caesar Chiper Alphabet Majemuk Dalam Kriptografi Untuk Pengamanan Informasi. *Indonesian Journal of Networking and Security*, 5(3), 3–6.
- Ratih. (2013). Studi Dan Perbandingan Penggunaan Kriptografi Kunci Simetri Dan Asimetri Pada Telepon Selular. *STEI ITB*, 1, 1–8.

- Schneier, Bruce. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Canada: John Wiley & Sons, Inc.
- Setyawarno, Didik. (2016). *Panduan Statistik Terapan Untuk Penelitian Pendidikan*. Yogyakarta: FMIPA UNY Yogyakarta.
- Sheskin, David J. (2003). *Handbook of Parametric and Nonparametric Statistical Procedures*. Florida: Chapman & Hall.
- Sugiyono. (2015). *Statistik Untuk Penelitian*. Surakarta: ALFABETA.
- Rizal M., Muh., Thamrin Tayeb, & Nurkholisah Latuconsina. 2016. Efektifitas Penerapan Metode Ekspositori Berbasis Kuis Terhadap Hasil Belajar Matematika Siswa Kelas VIII MTsN Ma'rang Kabupaten Pangkep. *MaPan: Jurnal Matematika Dan Pembelajaran*, 4(2), 172–185.