DOI: 10.47002/seminastika.v3i1.250

APLIKASI MOBILE MESSENGER DENGAN KEAMANAN DATA MENGGUNAKAN METODE *SHIFT CHIPPER (CAESAR)* KRIPTOGRAFI

MOBILE MESSENGER APPLICATION WITH DATA SECURITY USING SHIFT CHIPPER (CAESAR) CRYPTOGRAPHY METHOD

Djumhadi [1*], Arby Hamka[2]
[1,2]Universitas Mulia, Balikpapan, Kalimantan Timur

[*]*Email: djumhadi@universitasmulia.ac.id*

ABSTRAK

Proses pengiriman dan penerimaan pesan melalui perangkat mobile dijaman sekarang merupakan suatu hal yang biasa tetapi seberapa jauh tingkat keamanan dalam proses pengiriman dan penerimaan pesan itu yang belum dipikirkan atau belum menjadi perhatian khusus para penggunanyaPerkembangan teknologi dan kebutuhan manusia yang semakin meningkat merupakan dua hal yang saling mempengaruhi satu sama lain. Kebutuhan manusia yang meningkat akan memicu perkembangan teknologi, sedangkan perkembangan teknologi juga akan memacu kebutuhan lain untuk menangani dampak negatif dari adanya teknologi baru. Sudah banyak hal yang dilakukan untuk mencegah terjadinya dampak negatif pengriman dan penerimaan berupa penyadapan data, khususnya saat terjadi komunikasi yang bersifat rahasia dan penting. Kriptografi merupakan bidang pengetahuan yang menggunkan persamaan matematis untuk melakukan proses enkripsi maupun deskripsi. Teknik ini digunakan untuk mengkonversi data kedalam bentuk kode-kode tertentu, agar informasi yang terkirim dan diterima tidak dapat terbaca oleh orang-orang yang tidak berhak.Dalam penelitian ini penulis mencoba membuat sebuah aplikasi masengger baru berbasis mobile yang telah memiliki fitur kriptografi metode Shift Chiper di dalamnya, yang bertujuan agar user dapat mengirim pesan dengan aman dan rahasia karena harus mencantumkan kunci (key) yang diketahui oleh orang orang yang berhak.

Kata Kunci: *Kriptografi, Mesangging, Shift Chiper, Mobile*

ABSTRACT

The process of sending and receiving messages through now mobile devices is a common thing, but how far the level of security in the process of sending and receiving messages is that has not been considered or has not been a special concern of its users. The development of technology and increasing human needs are two things that influence each other. Increased human needs will trigger technological developments, while technological developments will also spur other needs to deal with the negative impacts of new technologies. Many things have been done to prevent the negative impact of sending and receiving data in the form of wiretapping, especially when there are confidential and important communications. Cryptography is a field of knowledge that uses mathematical equations to perform the encryption and description processes. This technique is used to convert data into certain codes, so that the information sent and received cannot be read by unauthorized persons. In this study, the author tries to create a new mobile-based masengger application that has a cryptographic feature of the Shift Ciper method in it, which aims to enable users to send messages safely and confidentially because they must include a key that is known by authorized people.

Keywords: *Kriptografi, Mesangging, Shift Chiper, Mobile*

DOI: 10.47002/seminastika.v3i1.250

PENDAHULUAN

Dewasa ini penggunaan telepon seluler begitu pesatnya berbagi platform sistem operasi menawarkan berbagai kemudahan layanan seperti layanan *mobile messenger*, masalah keamanan dan kerahasiaan data merupakan suatu hal yang sangat penting untuk menjadi pertimbangan. Seringkali kita mendengar bahwa pesan yang dikirimkan menggunakan salah satu aplikasi tersebut masih saja mengalami kebocoran oleh pihak yang tidak bertanggung jawab untuk kepentingan tertentu, ini sangat merugikan pihak pengirim jika informasi yang dikirimkan tersebut sangat sensitif dan sifatnya rahasia. Tanpa mengesampingkan pengguna terbesar *mobile messenger* yaitu kalangan pribadi atau individual, faktor kemananan merupakan masalah terbesar bagi pengguna *mobile messenger* lingkup perusahaan atau pada dunia bisnis.

Smartphone sebagai penunjang segala aktivitas dan kegiatan manusia sehari-hari sangat berperan dalam kegiatan komunikasi dan penyampaian informasi karena ada 3 faktor yang menentukan kualitas informasi yang baik, yaitu informasi yang akurat, tepat waktu saat diperlukan dan relevan atau sesuai dengan yang di inginkan. Tidak salah kalau dalam kegiatannya manusia menggunakan *smartphone* sebagai saran mengirim dan menerima iinformasi karena sangat efisien dan efektif. Dengan melihat hal tersebut maka diperlukannya aplikasi *mobile messenger* yang sistem enkripsinya sulit untuk dipecahkan oleh pihka yang tidak berhak menerima pesan dengan kemudahan ukuran kunci yang dapat disesuaikan dan tidak terlalu panjang. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat yang lain. Seperti contoh algoritma kriptografi yaitu :algoritma *caesar cipher* adalah teknik kriptografi yang dilakukan dengan mensubtitusi setiap abjad dari pesan yang akan dienkripsi melalui pergeseran susunan sebagai kunciny,Sebagai metode enkripsi pesannya memenuhi persyaratan tersebut. Algoritma *caesar cipher* termasuk kedalam sistem kriptografi kunci publik yang mendasarkan keamanannya, Pada penelitian ini Algoritma *caesar cipher* dalam enkripsi dan dekripsi pada pengiriman dan penerimaan pesan dapat meningkatkan keamanan karena pesan dikirimkan berupa ciphertext dan hanya bisa dirubah ke plaintext dengan cara melakukan penukaran karakter pada plainteks menjadi tepat satu karakter pada chiperteks.

METODOLOGI

A. Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan aspek keamanan informasi, seperti kerahasian data, keabsahan data, integritas data, serta *autentikasi* data. Secara umum kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan berita. Selain defenisi tersebut ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi [2]. Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

1. Kerahasiaan, adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihakpihak yang tidak berhak
2. Integritas data, adalah layanan yang menjamin pesan masih asli / utuh atau belum pernah dimanipulasi selama pengiriman.berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerimaan pesan menyangkal telah menerimanya [2].
3. Otentikasi, adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-phak yang berkomunikasi (*user authentication* atau *entry authentication*) maupun mengidentifikasi kebenaran sumber pesan (*origin authentication*).
4. Nirpenyangkalan (*non-repudiation*), adalah layanan untuk mencegah entitas yang

Kriptografi memiliki beberapa hal yang harus diketahui antara lain [4]:

1. Pengirim dan Penerima
   Pengirim (*sender*) merupakan kesatuan yang mengirimkan *message* kepada penerima (*reciever*) dengan aman tanpa ada gangguan dari penyadap (*eavesdropper*). Penerima merupakan entitas yang memperoleh pesan oleh pengirim.

DOI: 10.47002/seminastika.v3i1.250

2. *Plaintext* dan *Ciphertext*
   Pesan murni pada kriptografi disebut dengan *plaintext*, sedangkan pesan murni yang telah disamarkan disebut *ciphertext*.

3. Enkripsi dan Dekripsi
   Pada prosedurnya, pergantian plaintext jadi ciphertext disebut enkripsi (*encryption*) dan pergantian ciphertext jadi plaintext disebut dekripsi (*decryption*) .

4. Kriptografer, Kriptanalis, dan Kriptologis
   Seseorang yang mempelajari dan menggunakan metode kriptografi untuk mengamankan pesan dinamakan kriptografer. Sebaliknya, metode yang menggunakan teknik komputasi matematika untuk menyerang metode kriptografi dinamakan kriptanalisis dinamakan kriptanalis. Kata kriptologi merupakan cabang ilmu yang mempelajar kriptografi sekaligus dengan kriptanalisis. Orang yan mempelajari kriptologi tersebut dinamakan kriptologis.

5. Cipher
   Algoritma kriptografi (cipher) merupakan fungsi matematika dalam penggunaan enkripsi dan dekripsi. Dalam menyelesaikan persoalaan *cipher*, dibutuhkan sebuah entitas yang disebut dengan kunci (dilambangkan K). Kunci mempunyai nilai bilangan yang sangat besar. Besar kecilnya nilai ini dinamakan keyspace. Beberapa algoritma kriptografi menggunakan cipher dengan beda kunci antara kunci bagi enkripsi dan dekripsi.

6. Penyadap (*Eavesdropper*)
   Penyadap (*eavesdropper*) adalah orang yang ingin mendapatkan informasi sebanyakbanyaknya dari pesan yang telah dikirim dan memecahkan *ciphertext* dari system kriptografi. Penyadap mempunyai akses komunikasi antara pengirim dan penerima.

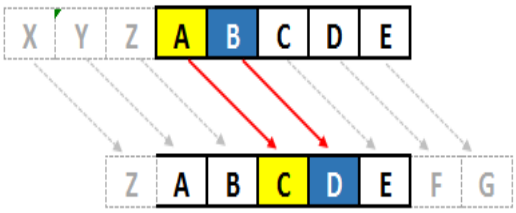
B. Algoritma Caesar Cipher

Pada kriptografi, sandi Caesar, atau sandi pindah, kode Caesar yaitu metode enkripsi sangat sederhana dan sangat populer. Kode ini terdiri dari semua huruf pada teks asli (*plaintext*) disubstitusi dengan kode kemudian berubah menjadi huruf lain yang mempunyai selisih posisi tertentu dalam alfabet. Dalam Caesar cipher, huruf-huruf diubah dengan huruf selanjutnya dari posisi alphabet yang sama.[6]

Caesar cipher merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan cara melakukan penukaran karakter pada plainteks menjadi tepat satu karakter pada chiperteks. Teknik seperti ini disebut juga sebagai chiper abjad tunggal.Algoritma kriptografi *Caesar Cipher* sangat mudah untuk digunakan. Inti dari algoritma kriptografi ini adalah melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama. Adapun langkahlangkah yang dilakukan untuk membentuk chiperteks dengan *Caesar Cipher* adalah menentukan besarnya pergeseran karakter yang digunakan dalam membentuk cipherteks ke plainteks, penukarkan karakter pada plainteks menjadi cipherteks dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya. Algoritma dari *Caesar Cipher* adalah C = E (P) = (P + K) mod 26 untuk fungsi enkripsi. Sedangkan untuk fungsi depenelitian adalah P = D (C) = (C - 7) mod 26 .

Proses Caesar Cipher adalah :[5]

1. Tentukan berapa besar pemindahan karakter yang dipakai untuk membuat cipherteks ke plainteks.
2. Tukar posisi karakter plainteks menjadi cipherteks berdasarkan pemindahan ang telah ditentukan sebelumnya. Contoh, pemindahan = 2. Jadi huruf A digeser menjadi huruf C, huruf B menjadi huruf D, dan berikutnya.



Gambar 1 Proses Chiper Caesar

Berikut satuan dari abjad atau alphabet ada Caesar Cipher sebagai berikut [7]:

DOI: 10.47002/seminastika.v3i1.250

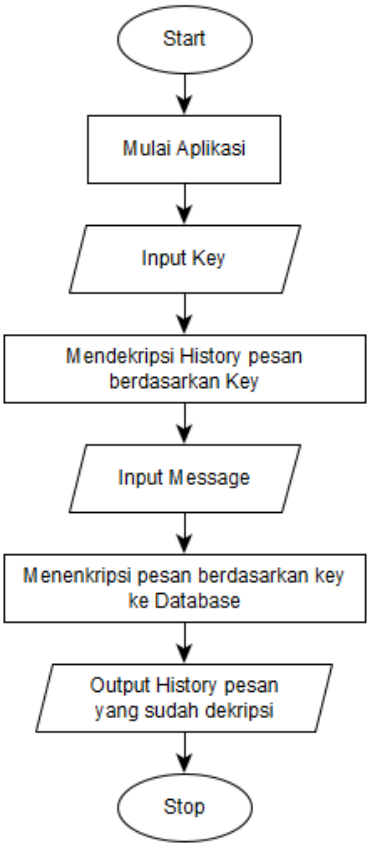
 ISSN: 2655-0881

Tabel 1. Satuan Alphabet

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

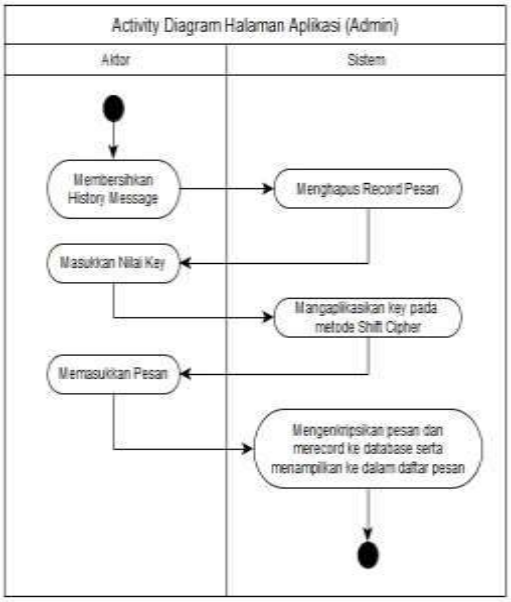
HASIL DAN PEMBAHASAN

Proses alur sistem aplikasi dapat dilihat pada gambar di bawah ini,



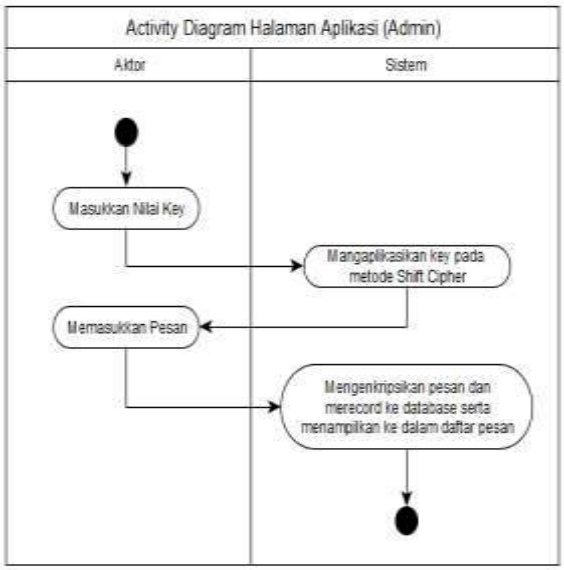
Gambar 2 *Flowchart* Kripto Chart

Dalam gambar activity diagram dibawah dapat dijelaskan bahwa sebagai admin dari aplikasi sebelum memulai komunikasi harus mengirimkan kunci dulu ke penerima pesan



Gambar 3. Activity Diagram Admin Aplikasi

Selanjutnya user penerima pesan untuk dapat mengirim pesan harus memasukan kunci yang telah di kirimkan oleh admin sebelumnya, pada contoh dibawah ini teradi komunikasi antara admin dan user melalui aplikasi chating “Kripto Chat”

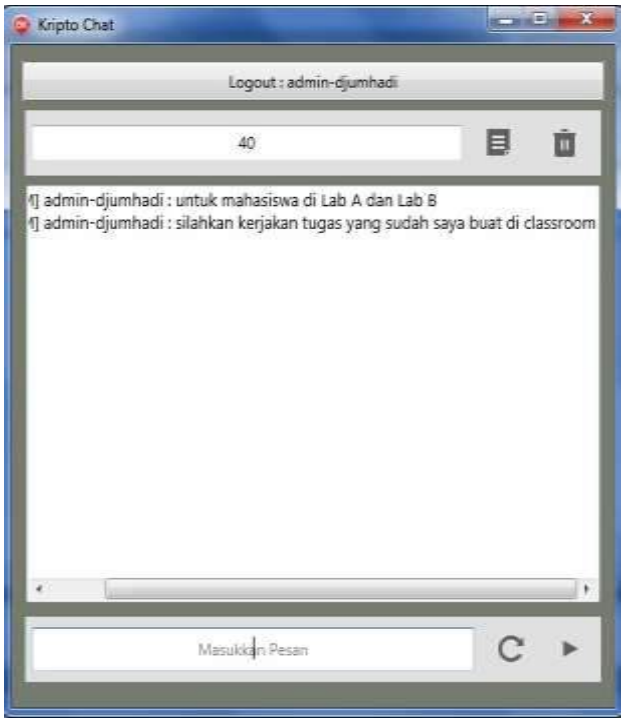


Gambar 3 Proses pengiriman pesan

DOI: 10.47002/seminastika.v3i1.250

 ISSN: 2655-0881

Untuk proses pengiriman pesan, pertama yang dilakukan adalah admin mengirimkan kunci ke penerima pesan, agar komunikasi hanya terjadi 2 arah dan terenkripsi. Pada gambar 4, menjelaskan proses pemasukan kunci oleh admin untuk memulai awal komunikasi

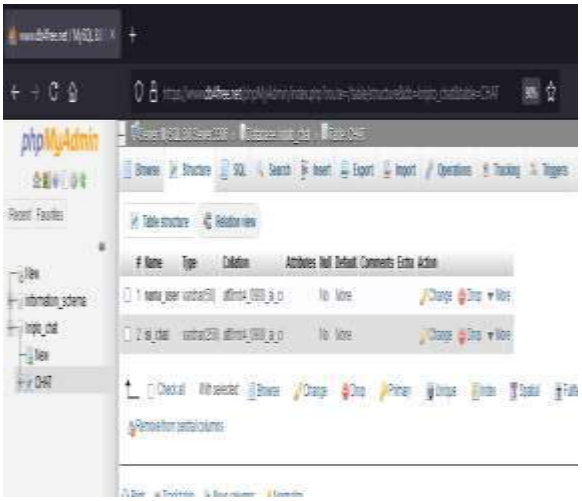


Gambar 4 Admin mengirim pesan

Pada gambar 5, dibawah ini user menerima pesan dari admin berupa pesan dan kunci yang harus dipakai untuk membalas pesan dari si pengirim pesan, dengan masukan kunci yang dikirimkan maka pesan yg sebelumnya terenkripsi bisa terbuka dan bisa dibaca oleh user penerima pesan.

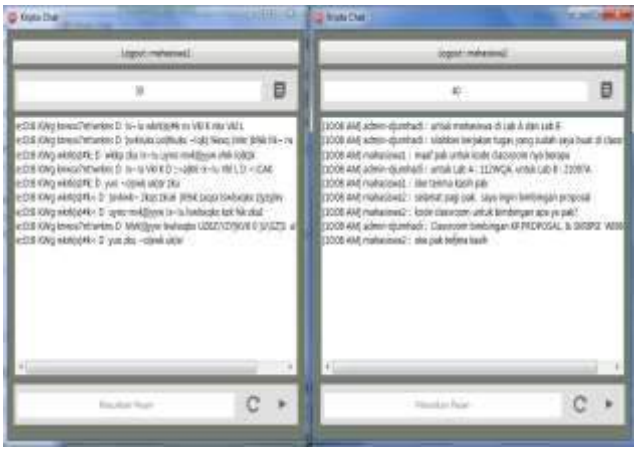
Gambar 5 User mengirim pesan

Dalam aplikasi ini nama user dan isi history chat disimpan kedalam sebuah database SQL online melalui www.db4free.net sehingga data tetap tersimpan walaupun sudah keluar masuk aplikasi, dan juga dapat di update dan di perbaharui dan di bersihkan history chat. Berikut adalah bentuk dari database yang digunakan pada aplikasi kripto chat ini, terlihat pada Gambar 6



Gambar 6 Database aplikasi Kripto Chat

DOI: 10.47002/seminastika.v3i1.250



Gambar 7 Contoh pesan jika kunci salah

Pada gambar 7, terlihat jika ada user lain yang coba melihat pesan dengan memasukan kunci yang salah maka pesan yang diterima berupa kode-kode hasil enkripsi dari pesan asli. Penanganan kesalahan ini bertujuan untuk memberikan informasi tentang kesalahan yang terjadi pada saat proses pengujian sistem aplikasi dan untuk melihat apakah program aplikasi sudah menghasilkan output yang diinginkan atau belum.

KESIMPULAN

Dalam proses membangun aplikasi kriptografi chat berbasis android terdapat beberapa hal yang dapat disimpulkan oleh penulis, yaitu :

1. Aplikasi kriptografi messenger ini telah berhasil di implementasikan.
2. Berdasarkan hasil dari pengujian sistem hasil yang didapatkan berhasil dijalankan.
3. Kriptografi messenger akan mempermudah dalam pengamankan pesan yang bersifat messenger.
4. Hasil pengujian mengunakan metode *Shift Cipher (caesar)* telah berhasil di jalankan dan di implementasikan..
5. Hasil pengujian dukungan ASCII menggunakan format teks abjad kecil ataupun besar serta angka dan simbol berhasil di implementasikan..

SARAN

Dalam proses Penulis menyadari bahwa aplikasi ini memiliki banyak kekurangan, saran untuk pengembangan aplikasi pada waktu mendatang adalah :

1. Diharapkan pengembangan kedepan pada aplikasi ini adalah dapat mendukung metode lain selain *Shift Cipher (Caesar).*
2. Dapat mendukung fungsi chatting messager dari user ke user lain nya.

DAFTAR PUSTAKA

[1] J.H. An, B.H. Kim, J.H. Jeong, D.M. Kim, Y.S. Jeon, K.O. Jeon and K.S. Hwang. “Preparation of vanadium-doped TiO_2 thin films on glass substrates”, *Ceramic Processing Research*, 6.2 (2005): 163-166

[2] Rinaldi Munir, “Kriptografi”, Penerbit Informatika, Bandung, 2006.

[3] Gurning, R.R.A. 2014. Perancangan Aplikasi Pengamanan Pesan Dengan Algoritma *Caesar Cipher*. Pelita Informatika Budi Darma, Volume: VI, Nomor: 3, April 2014: 106-110

[4] Rachmawati, D., Candra, A. 2015. Implementasi Kombinasi *Caesar* dan *Affine Cipher* untuk Keamanan Data Teks. Jurnal Edukasi dan Penelitian Informatika (JEPIN). Volume 1, No. 2 : 60-63.

[5] Basuki, Armaja.2016. Aplikasi Kriptografi Berlapis Menggunakan Algoritma Tansposisi, *Vigenere* dan Blok Cipher Berbasis *Mobile*. Seminar Nasional Teknologi Informasi dan Multimedia 20116, Februari 2016 : 31-35

[6] Seftyanto, Donny. 2012. Peran Algoritma *Caesar Cipher* Dalam Membangun Karakter Akan Kesadaran Keamanan Informasi. Seminar Nasional Matematikan dan Pendidikan Matematikan FMIPA UNY. November 2012 : MP 883-890

[7] Rahima. 2014. Implementasi Penyembunyian dan Penyandian Pesan Pada Citra Menggunakan Algoritma *Affine Cipher* dan Metode *Least Significant Bit*. Pelita Informatika Budi Darma, Volume: VI, Nomor: 1, Maret 2014: 144-148.

[8] Prayitno, A., Nurdin, N., 2017, *Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia Menggunakan Algoritma Cipher Transposition*, Jurnal Elektronik Sistem Informasi Dan Komputer, Volume 3 No.1 Juni 2017.

[9] Sandika, 2017, *Penggunaan Model Problem Based Learning Untuk Meningkatkan Sikap Percaya Diri Dan Hasil Belajar Siswa Pada Subtema Sumber Energi (Penelitian Tindakan Kelas Di*

DOI: 10.47002/seminastika.v3i1.250

Kelas IV 086 Cimincrang Kecamatan Gedebage Kota Bandung), Online Pada http://repository.unpas.ac.id/30787/, diakses tanggal 14 Mei 2020.