

LEMBAR
HASIL PENILAIAN SEJAWAT SEBIDANG ATAU *PEER REVIEW*
KARYA ILMIAH : PROSIDING NASIONAL

Judul Jurnal Ilmiah (Artikel) : Kriptografi Kurva Eliptik atas Lapangan Galois Prima GF (p) dengan Basis 95

Nama/ Jumlah Penulis : Nikken Prima Puspita/3

Status Pengusul : penulis ke-3

Identitas Jurnal Ilmiah : a. Nama Prosiding : Prosiding, SENATIK, Universitas PGRI Semarang 2016

b. Nomor ISSN : ISSN: - / e-ISSN: -

c. Vol, No., Bln Thn : Vol. -, No.-, November 2016

d. Penerbit : Universitas PGRI Semarang

e. DOI artikel (jika ada) : -

f. Alamat web jurnal : <http://prosiding.upgris.ac.id/index.php/index/index/index/index>

Alamat Artikel : <http://prosiding.upgris.ac.id/index.php/SENATIK2016/senatik/paper/viewFile/1061/1011>

g. Terindex : -

Kategori Publikasi Prosiding : ☐ Prosiding Internasional terindek pada scimagojr dan scopus
(beri ✓ pada kategori yang tepat) ☐ Prosiding Internasional terindek scopus, IEEE Eexplore
☒ Prosiding Nasional

Hasil Penilaian *Peer Review* :

Komponen Yang Dinilai	Nilai Reviewer		Nilai Rata-rata
	Reviewer 1	Reviewer 2	
a. Kelengkapan unsur isi Prosiding (10%)	1	0,9	0,95
b. Ruang lingkup dan kedalaman pembahasan (30%)	3	2,8	2,9
c. Kecukupan dan kemutahiran data/informasi dan metodologi (30%)	2	2,8	2,4
d. Kelengkapan unsur dan kualitas terbitan/ Prosiding (30%)	3	2,7	2,85
Total = (100%)	9	9,2	9,1
Nilai Pengusul = 40% x 9,1/2 = 1,82			

Reviewer 1

Nama : Prof. Dr. Sunarsih, M.Si
NIP. : 195809011986032002
Unit Kerja : FSM Undip
Bidang Ilmu: Matematika

Semarang,

Reviewer 2

Nama : Bayu Surarso, Ph.D
NIP. : 196311051988031001
Unit Kerja : FSM Undip
Bidang Ilmu: Matematika

LEMBAR
HASIL PENILAIAN SEJAWAT SEBIDANG ATAU *PEER REVIEW*
KARYA ILMIAH : PROSIDING NASIONAL

Judul Jurnal Ilmiah (Artikel) : Kriptografi Kurva Eliptik atas Lapangan Galois Prima GF (p) dengan Basis 95
Nama/ Jumlah Penulis : Nikken Prima Puspita/3
Status Pengusul : penulis ke-3
Identitas Jurnal Ilmiah : a. Nama Prosiding : Prosiding, SENATIK, Universitas PGRI Semarang 2016
b. Nomor ISSN : ISSN: - / e-ISSN: -
c. Vol, No., Bln Thn : Vol. -, No.-, November 2016
d. Penerbit : Universitas PGRI Semarang
e. DOI artikel (jika ada) : -
f. Alamat web jurnal : <http://prosiding.upgris.ac.id/index.php/index/index/index/index>
Alamat Artikel : <http://prosiding.upgris.ac.id/index.php/SENATIK2016/senatik/paper/viewFile/1061/1011>
g. Terindex : -

Kategori Publikasi Prosiding : ☐ Prosiding Internasional terindek pada scimagojr dan scopus
(beri ✓ pada kategori yang tepat) ☐ Prosiding Internasional terindek scopus, IEEE Eexplore
☒ Prosiding Nasional

Hasil Penilaian *Peer Review* :

Komponen Yang Dinilai	Nilai Maksimal Prosiding			Nilai Akhir Yang Diperoleh
	Internasional terindek cimagojr & scopus 	Internasion al scopus IEEE 	Nasional 10	
a. Kelengkapan unsur isi Prosiding (10%)			1	1
b. Ruang lingkup dan kedalaman pembahasan (30%)			3	3
c. Kecukupan dan kemutahiran data/informasi dan metodologi (30%)			3	2
d. Kelengkapan unsur dan kualitas terbitan/ Prosiding (30%)			3	3
Total = (100%)			10	9
Nilai Pengusul = 40%/2 x 9 = 5,4				
Catatan Penilaian artikel oleh Reviewer :				
1. Kesesuaian dan kelengkapan unsur isi prosiding: Kelengkapan unsur isi prosiding dan kesesuaian paper telah ditulis dengan baik mulai dari abstrak, pendahuluan, metode riset, Hasil dan Pembahasan berupa beberapa algoritm kriptosistem yang mendukung, penutup berupa kesimpulan dan open problem sertadaftar pustaka yang lengkap 2. Ruang lingkup dan kedalaman pembahasan: Paper ini berisi kriptosistem yang berupa kriptografi kurva eliptik kunci publik. Kriptosistem ini didefinisikan pada lapangan berhingga yang disebut lapangan Galois. Lapangan Galois yang elemennya direpresentasikan dalam modulo prima disebut lapangan Galois prima $GF(p)$. Himpunan titik-titik yang terbentuk dari kurva eliptik membentuk suatu grup berhingga. Penelitian ini merupakan hasil dari aplikasi Teori Grup pada Aljabar. 3. Kecukupan dan kemutakhiran data/informasi dan metodologi: Kecukupan dan kemutakhiran data berasal dari berbagai sumber dari referensi sebanyak 9 referensi dan dengan metodologi yang baik. 4. Kelengkapan unsur dan kualitas terbitan: Kelengkapan unsur dan kualitas terbitan adalah baik dengan simililarity artikel sebesar 17%.				

Semarang, 14 Maret 2023
Reviewer 1

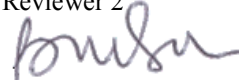
Nama : Prof. Dr. Sunarsih, M.Si
NIP. : 195809011986032002
Unit Kerja : FSM Undip
Bidang Ilmu: Matematika

LEMBAR
HASIL PENILAIAN SEJAWAT SEBIDANG ATAU *PEER REVIEW*
KARYA ILMIAH : PROSIDING NASIONAL

Judul Jurnal Ilmiah (Artikel) : Kriptografi Kurva Eliptik atas Lapangan Galois Prima GF (p) dengan Basis 95
Nama/ Jumlah Penulis : Nikken Prima Puspita/3
Status Pengusul : penulis ke-3
Identitas Jurnal Ilmiah : a. Nama Prosiding : Prosiding, SENATIK, Universitas PGRI Semarang 2016
b. Nomor ISSN : ISSN: - / e-ISSN: -
c. Vol, No., Bln Thn : Vol. -, No.-, November 2016
d. Penerbit : Universitas PGRI Semarang
e. DOI artikel (jika ada) : -
f. Alamat web jurnal : <http://prosiding.upgris.ac.id/index.php/index/index/index/index>
Alamat Artikel : <http://prosiding.upgris.ac.id/index.php/SENATIK2016/senatik/paper/viewFile/1061/1011>
g. Terindex : -
Kategori Publikasi Prosiding : ☐ Prosiding Internasional terindek pada scimagojr dan scopus
(beri ✓ pada kategori yang tepat) ☐ Prosiding Internasional terindek scopus, IEEE Eexplore
☒ Prosiding Nasional

Hasil Penilaian *Peer Review* :

Komponen Yang Dinilai	Nilai Maksimal Prosiding			Nilai Akhir Yang Diperoleh
	Internasional terindek Scimagojr &scopus	Internasional scopus IEEE	Nasional	
			10	
e. Kelengkapan unsur isi Prosiding (10%)			1	0,9
f. Ruang lingkup dan kedalaman pembahasan (30%)			3	2,8
g. Kecukupan dan kemutahiran data/informasi dan metodologi (30%)			3	2,8
h. Kelengkapan unsur dan kualitas terbitan/ Prosiding (30%)			3	2,7
Total = (100%)				9,2
Nilai Pengusul = (40/2)% x 9,2 = 1,84				
Catatan Penilaian artikel oleh Reviewer :				
5. Kesesuaian dan kelengkapan unsur isi prosiding: Artikel berisi pembahasan bidang kriptosistem khususnya kriptografi kurva eliptik kunci publik abstrak. Kelengkapan artikel cukup baik, mulai dari abstrak, pendahuluan, pembahasan, kesimpulan dan daftar pustaka, namun metodologi tidak disampaikan secara eksipisit.				
6. Ruang lingkup dan kedalaman pembahasan: Artikel ini membahas Kriptosistem sebagai aplikasi Teori Grup pada Aljabar. Kriptosistem didefinisikan pada lapangan berhingga yang disebut lapangan Galois. Lapangan Galois yang elemennya direpresentasikan dalam modulo prima merupakan lapangan Galois prima $GF(p)$. Dibuktikan himpunan titik-titik yang terbentuk dari kurva eliptik membentuk suatu grup berhingga.				
7. Kecukupan dan kemutakhiran data/informasi dan metodologi: Kecukupan dan kemutakhiran data dan metodologi cukup baik, artikel didukung referensi sebanyak 8 referensi, 2 diantaranya cukup up to date..				
8. Kelengkapan unsur dan kualitas terbitan: Artikel diterbitkan pada prosiding tanpa issn/isbn Semnatik, IKIP PGRI, dengan similarity artikel 9%.				

Semarang, Maret 2023
Reviewer 2

Nama : Bayu Surarso, Ph.D
NIP. : 196311051988031001
Unit Kerja : FSM Undip
Bidang Ilmu: Matematika