SISTEM KEAMANAN ATTACHMENT EMAIL PADA MOBILE PHONE ANDROID MENGGUNAKAN ALGORITMA HILL CIPHER

Isbat Uzzin Nadhori[1], Tita Karlita[2], Mohammad Azis Khoirul Fata[3]
Jurusan Teknik Informatika
Politeknik Elektronika Negeri Surabaya[1,2,3]
isbat@pens.ac.id[1], tita@pens.ac.id[2], azisfata@gmail.com[3]

ABSTRAK

Nowadays, email has become an alternative to formal communication through the Internet. One important feature on the email system is a file attachment. Email attachments are often used to send important documents. Whereas an e-mail protocol is less secure protocol. To enhance the security of e-mail attachment, developed a security system on an email attachment to an Android phone using Hill Cipher Algorithm. The system is trying to build a special attachment to the document file. From the experimental results it can be concluded that the hill cipher, documents encrypted attachment has the same size as the original attchment so as not to overload the system and secure in its distribution..
***Keywords**:Hill Chiper,email, android*

ABSTRAK

Saat ini, email telah menjadi alternatif untuk komunikasi formal melalui Internet. Salah satu fitur penting pada sistem email adalah file attachment/Lampiran. Lampiran email sering digunakan untuk mengirim dokumen penting. Pada prinsipnya protokol email kurang aman. Untuk meningkatkan keamanan lampiran e-mail, dikembangkan sistem keamanan pada lampiran email pada ponsel Android menggunakan Algoritma Hill Cipher. Sistem ini mencoba untuk membangun sebuah lampiran khusus untuk file dokumen. Dari hasil percobaan dapat disimpulkan bahwa lampiran dokumen hasil enkripsi memiliki ukuran yang sama dengan lampiran asli sehingga tidak membebani sistem dan aman dalam distribusi.
Keywords: Hill Chiper, email, android

PENDAHULUAN

Saat ini, email telah menjadi alternatif komunikasi format melalui internet. Salah satu fitur penting email adalah attachment file. Attachment email sering dipakai oleh pengirim email untuk mengirimkan dokumen penting. Sedangkan protokol email merupakan protokol kurang aman. Perlu ada penambahan keamanan pada email tapi tanpa efisien sehingga tidak membebani sistem. Penelitian ini mengajukan suatu pendekatan baru untuk membangun piranti keamanan attachment pada e-mail dengan algoritma hill cipher pada android. Piranti tersebut bekerja dengan cara melakukan proses persandian pesan menggunakan algorima hill chiper yang dikirim melalui perangkat android pengirim dan hanya bisa dibuka oleh piranti yang sama pada perangkat android penerima.Dari hasil percobaan didapatkan kesimpulan bahwa dengan hill chiper, attachment dokumen yang disandikan akan memiliki ukuran yang sama seperti attchment aslinya sehingga tidak membebani sistem dan aman dalam pendistribusiannya.

Sebelumnya telah ada penelitian mengenai Kriptografi Hill Cipher. Pada penelitian ini menjelaskan mengenai proses enkripsi dan dekripsi untuk 26 karakter dengan menggunakan matriks 2x2 oleh Todd Douglas dan Dustin Helliwell (1997)[8]. Penelitian Maya Basoeki (2008)[6] mengenai kompresi menggunakan algoritma Aritmetic Coding pada Mobile Phone berbasis Java. Aplikasi ini hanya menggunakan proses kompresi yang terdiri dari beberapa karakter.

Pada kesempatan kali ini, penulis menerapkan algoritma kriptography hill chiper untuk pengiriman attachment dokumen email. Proses enkripsi dilakukan dengan algoritma Hill Cipher menggunakan dua tipe metriks, yakni 2x2 dan 3x3 dan menggunakan 95 karakter yang umum digunakan untuk pengiriman attachment email.

DASAR TEORI

Algoritma Hill Cipher

Hill Cipher merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi. Hill Cipher diciptakan oleh Lester S. Hill pada tahun 1929. Hill Cipher tidak mengganti tiap abjad yang sama pada plaintext dengan abjad lainnya yang sama pada ciphertext karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya. Plaintext yang akan diproses pada Hill Cipher akan dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter plaintext pada satu blok akan mempengaruhi karakter lainnya dalam proses enkripsi maupun dekripsi, sehingga karakter plaintext yang sama belum tentu menjadi karakter ciphertext yang sama pula.

Dasar teknik Hill Cipher adalah modulo terhadap matriks. Dalam penerapannya, Hill Cipher menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci Hill Cipher adalah matriks n x n dengan n merupakan ukuran blok. Jika n=2 , maka enkripsi dilakukan setiap 2 karakter. Matriks K yang menjadi kunci ini harus merupakan matriks yang invertible, yaitu memiliki invers K-1, sehingga:

$$K.K^{-1} = I \quad (1)$$

Kunci harus memiliki invers karena matriks K-1 adalah kunci yang digunakan untuk melakukan dekripsi.

Algoritma Enkripsi Hill Cipher
Secara umum, tahapan-tahapan enkripsi Hill Cipher adalah sebagai berikut:

1. Buat matrik K yang dipakai sebagai kunci berukuran nxn.

$$K_{nxn} = \begin{pmatrix} k_{11} & k_{12} & .... & k_{1n} \\ k_{21} & k_{22} & .... & k_{2n} \\ .... & .... & .... & .... \\ k_{n1} & k_{n2} & .... & k_{nn} \end{pmatrix} \quad (2)$$

2. Korespondenkan abjad dengan numeric

   A → 1 , B → 2, C → 3, ……., Z → 0

3. Kelompokkan barisan angka yang didapat kedalam beberapa blok vector P yang panjangnya sama dengan ukuran matriks “K”.
4. Hitung Ciphertext (modulo 26) untuk tiap vector P

   $C = K . P(\text{mod } 26)$ (3)

   denganC = Ciphertext, K = Matriks kunci, dan P = Plaintext
5. Kembalikan tiap angka dalam vektor sandi C ke huruf yang sesuai untuk mendapatkan ciphertext sandi.

Algoritma Dekripsi Hill Cipher
Secara umum, tahapan dekripsi Hill Cipher adalah sebagai berikut:

1. Korespondenkan abjad hasil enkripsi dengan numeric

   A → 1 , B → 2, C → 3, ……., Z → 0

2. Kunci yang digunakan untuk mendekrip ciphertext ke plaintext adalah invers dari matriks K_{nxn}
3. Hitung K^{-1} (invers) dengan cara:

$$K\text{-}1 = \frac{1}{\text{Det } K} adj(K) \quad (4)$$

   dengan nilai 1/Det K dalam mod 26

4. Hitung plaintext dengan cara:

   $P = K^{-1} . C$ (5)

5. Kembalikan tiap angka dalam vector P ke huruf yang sesuai untuk mendapatkan plaintext kembali

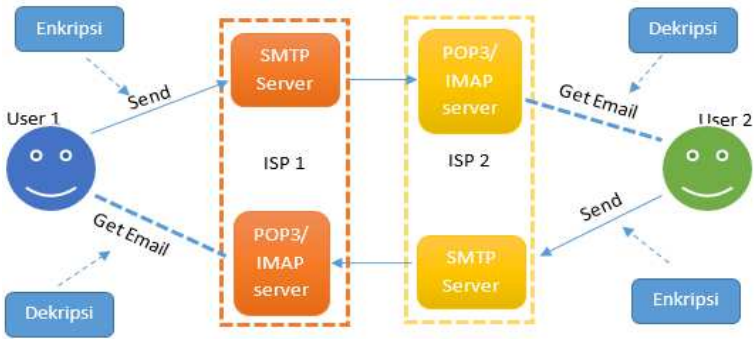
ISSN 2541-5662 (Cetak)
ISSN 2541-5670 (Online)

METODE PENELITIAN

Dalam penelitian ini dibangun sistem enkripsi dan kompresi pada pesan singkat yang dapat memudahkan pengguna dalam menggunakan layanan SMS yang mengamankan isi pesan. Untuk proses enkripsi digunakan algoritma Hill Cipher, untuk kompresi digunakan algoritma Arithmetic Coding.

Blok Diagram

Blok diagram sistem secara keseluruhan dapat dilihat pada Gambar 1.Terbangun aplikasi yang bisa dimanfaatkan oleh pengirim dan penerima email pada smartphone android. Pengirim dapat melakukan pengiriman attachment terenkripsi dan di sisi penerima terdapat fitur dekripsi attachment email.

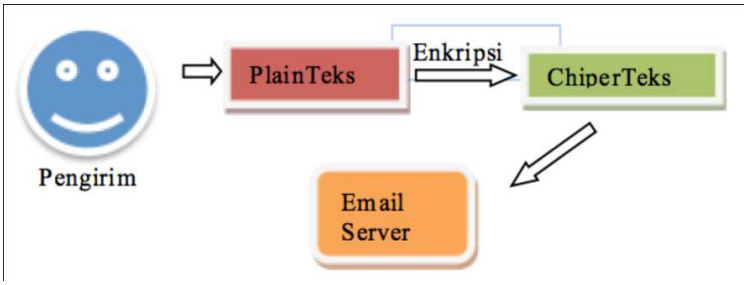


Gambar 1. Blok Diagram Sistem Pengamanan Email

Aplikasi ini bisa digunakan untuk mengirim email melalui port dan protokol SMTP ke Mail Server. Dengan enkripsi pesan tersimpan dalam bentuk chiperteks, sehingga tidak akan bisa dibaca oleh pihak lain. Kemudian mail server mengirim pesan chiperteks ke Mail Server Email tujuan. Dengan protokol IMAP Penerima dapat memperoleh email tersebut dilakukan proses dekripsi untuk membuka email. Selain itu ditambahkan fitur enkripsi attachment.

Proses Enkripsi

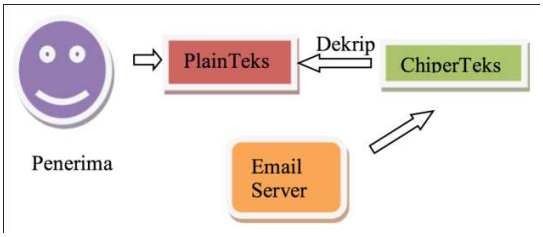
Alur proses enkripsi bisa dilihat pada gambar 2, dimulai dengan user memasukkan pesan (plainteks) yang selanjutnya akan disandikan oleh sistem dengan menggunakan algoritma Hill Cipher. Setelah cipherteks terbentuk selanjutnya pesan yg telah disandikan tersebut akan di kirim ke email server menuju alamat yang dituju.



Gambar 2. Alur Proses Enkripsi

Proses Dekripsi

Alur proses dekripsi bisa dilihat pada gambar 3, pesan email yang telah terkirim dan disandikan tersimpan di server, maka selanjutnya system aplikasi akan mengambil pesan email tersebut dari server, kemudian dilakukan dekripsi pada pesan dan menghasilkan pesan plainteks yang dapat dibaca dengan normal.



Gambar 3 Alur Proses Dekripsi

Proses Enkripsi dan Dekripsi

Proses enkripsi dilakukan dengan metode *Hill Cipher*. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi. Kunci matriks yang digunakan pada aplikasi ini adalah matriks nxn.Karena operasi matrik merupakan operasi aritmatika yang menggunakan nilai angka dalam operasinya maka pesan yang secara default memiliki tipe String perlu dikonversikan ke angka. Konversi angka bisa dilihat pada tabel 1.

Tabel 1. Konversi String ke Angka

0	1	2	3	4	5	6	7	8	9	A	B	C	D
0	1	2	3	4	5	6	7	8	9	10	11	12	13
E	F	G	H	I	J	K	L	M	N	O	P	Q	R
14	15	16	17	18	19	20	21	22	23	24	25	26	27
S	T	U	V	W	X	Y	Z	a	b	c	d	e	f
28	29	30	31	32	33	34	35	36	37	38	39	40	41
g	h	i	j	k	l	m	n	o	p	q	r	s	t
42	43	44	45	46	47	48	49	50	51	52	53	54	55
u	v	w	x	y	z		!	@	#	$	%	^	&
56	57	58	59	60	61	62	63	64	65	66	67	68	69
*	(	)	_	+	-	=	[	]	{	}	\	|	:
70	71	72	73	74	75	76	77	78	79	80	81	82	83
;	'	"	<	>	,	.	~	`	?	/	\t	\n	
84	85	86	87	88	89	90	91	92	93	94	95	96	

Kunci matriks yang digunakan pada aplikasi ini adalah matriks nxn, n merupakan ukuran blok. Jumlah karakter kunci yang dimasukkan user harus sejumlah hasil bilangan kuadrat, misal 4, 9, 16 dan seterusnya. Untuk menangani kekakuan dalam kunci, program telah diatur agar memenuhi bagian kunci yang kurang jika user tidak memasukkan kunci dengan jumlah hasil bilangan kuadrat. Contohya jika user memasang kunci dengan kata LAPAR dengan jumlah 5 karakter, kata tersebut tidak memenuhi syarat kunci yang seharusnya berjumlah 4, 9 atau 16. Maka program secara otomatis menambahkan indek string sejumlah kekurangannya, yaitu tiga karakter. Penambahan karakter dimulai dari indek 0 dari daftar string dan seterusnya, sehingga hasi kunci yang telah di generate menjadi LAPAR123.

Misal terdapat plainteks MENCOBA ENKRIPSI dan nilai n adalah 3, maka plainteks dikelompoknya tiga-tiga menjadi :

MEN|COB|A E|NKR|IPS|I

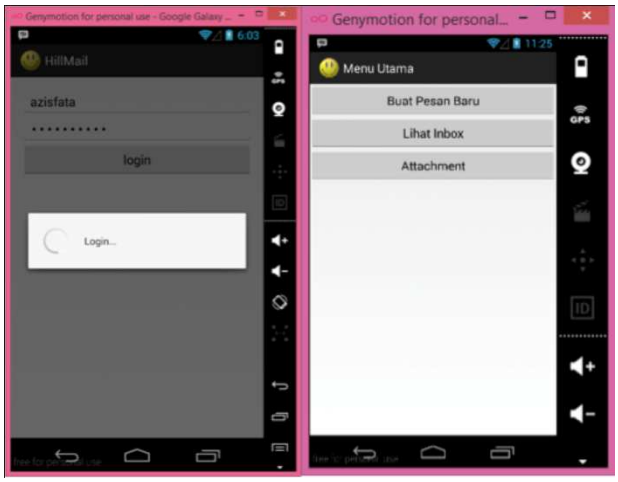
Jika pada karakter terakhir kurang dari 3 maka akan dibangkitkan karakter random untuk memenuhi matrik pesan n x m. Lalu tiap tiga string dikalikan matrik kunci 3x3. Dan hasil perkalian matrik tersebut di modulus dengan jumlah indek String. Hasil dari modulus akan dikonversi kembali ke tipe String, dan chiperteks dapat terbentuk. Pesan telah berhasil disandikan dengan algoritma Hill Chiper.

Proses dekripsi untuk mengembalikan chiperteks ke plainteks dengan cara matrik plainteks dikalikan dengan invers dari matrik kunci.
untuk menghasilkan invers matrik, dapat mengikuti langkah-langkah berikut :

1. Menghitung matrik minor.
2. Lalu rubah menjadi cofaktor matrik.
3. Lakukan adjoint matrik
4. Bagi dengan determinan

HASIL DAN PEMBAHASAN

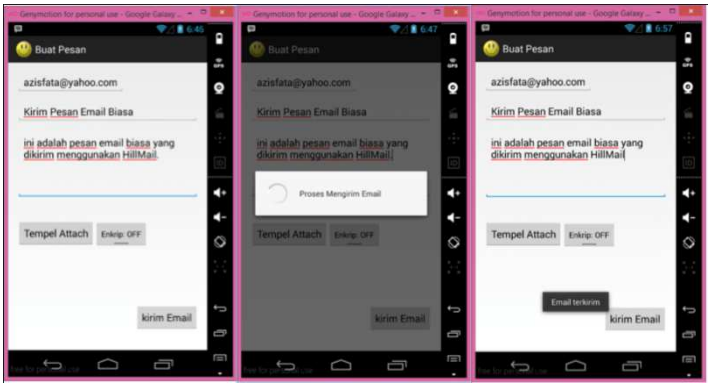
Tujuan dari pengujian aplikasi ini adalah untuk mengetahui tingkat keberhasilan dan resposibilitas aplikasi. Pengujian dilakukan dengan menggunakan Android Mobile Phone untuk menguji hasil pengiriman dan penerimaan attachment email terenskripsi.
Aplikasi diawali dengan proses login untuk masuk ke aplikasi, selanjutnya terdapat menu membuat pesan baru, lihat pesan di inbox dan kirim attachment email.



Gambar 4. Menu Aplikasi

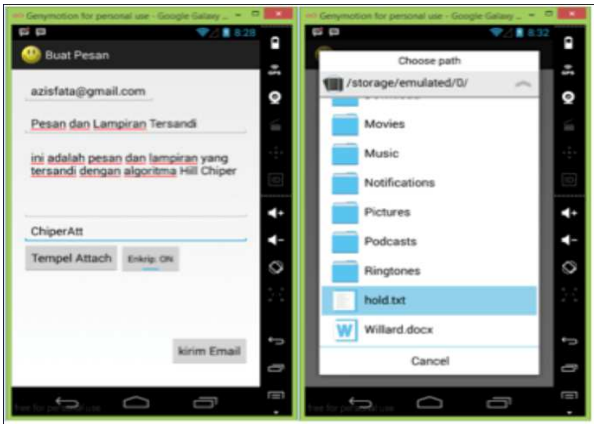
ISSN 2541-5662 (Cetak)
ISSN 2541-5670 (Online)

Proses kirim email bisa dilihat pada gambar 5, dimana didalamnya terdapat penambahan attachment dokumen di dalamnya.



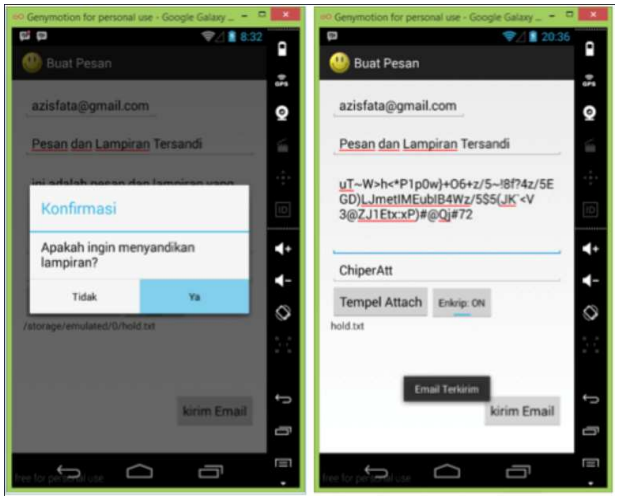
Gambar 5. Pengiriman Email

Pengiriman pesan dengan enkripsi dilakukan dengan menekan tombol enkrip:OFF sehingga menjadi enkrip:ON. Untuk pengiriman attachment bisa dilakukan dengan menekan tombol TempelAttach. Proses pengiriman email dengan atatchment bisa dilihat pada gambar 6.



Gambar 6. Hasil Enkripsi Email

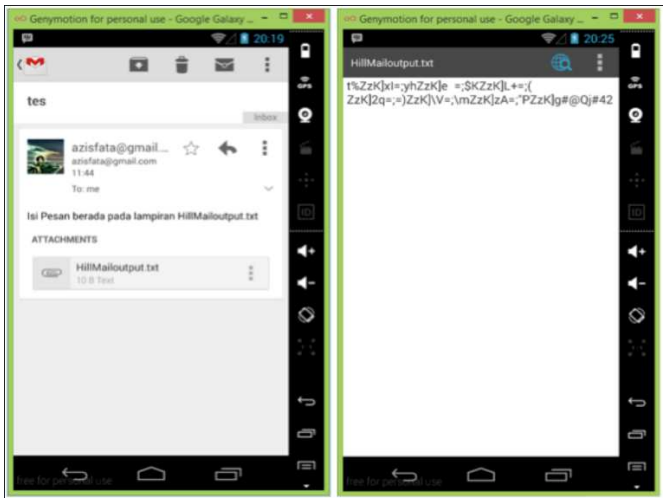
Sedangkan contoh proses penyandian atatchment bisa dilihat pada gambar 7.



Gambar 7. Hasil Enkripsi Email

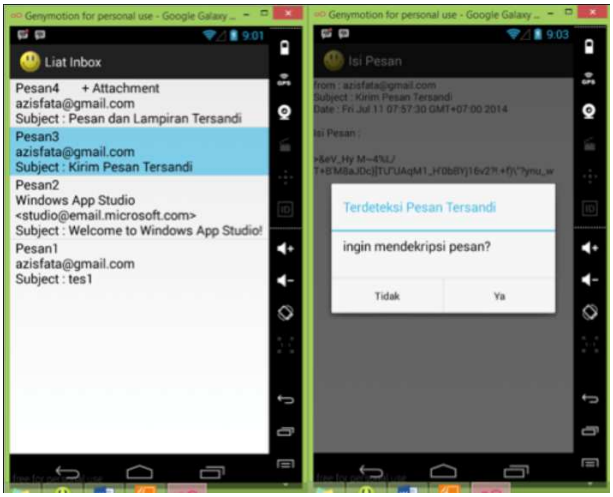
ISSN 2541-5662 (Cetak)
ISSN 2541-5670 (Online)

Contoh hasil pengiriman email dan attachment yang terenkripsi bisa dilihat pada gambar 8.



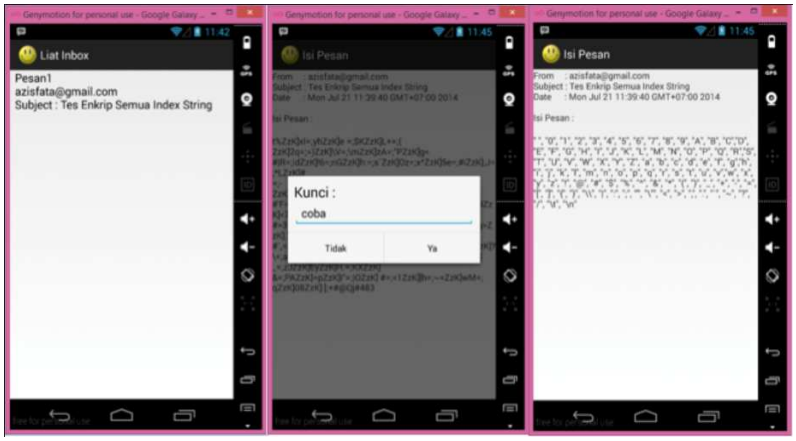
Gambar 8. Hasil Enkripsi Email

Proses dekripsi dilakukan dengan cara pembacaan teks pada file lampiran yang berisi isi pesan terenkrip, kemudian teks didekripsi dengan cara memasukkan kunci pesan, jika kunci benar maka pesan asli akan terlihat. Tetapi jika kunci tidak benar, maka pesan akan tetap dengan karakter-karakter yang random. Contoh proses dekripsi bisa dilihat pada gambar 9.



Gambar 9. Proses dekripsi

Contoh hasil dekripsi bisa dilihat pada gambar 10.



Gambar 10. Hasil Proses dekripsi

KESIMPULAN

Berdasarkan hasil uji coba dan analisa berikut kesimpulan yang bisa ditarik dari aplikasi yang dibuat :

1. Hasil enkripsi dan dekripsi memiliki akurasi prosentase 100%.
2. Aplikasi ini dapat bekerja dengan baik pada mobile phone Android dan memiliki respon yang baik.
3. Penerapan Algoritma Kriptografi Hill Chiper pada sistem yang dibuat menghasilkan panjang string hasil chiperteks yang sama panjang string plainteks, membuat ukuran file plain dan chiper sama sehingga tidak membebani sistem daripada pada saat tidak dilakukan proses kriptografi.
4. Proses enkripsi dan dekripsi attachment file yang berisi teks dapat diaplikasikan pada sistem ini yang menghasilkan akurasi dengan prosentase100%
5. Input karakter hanya bisa diterima hanya dengan karakter-karakter tersebut terdefinisi dalam 97 karakter yang sudah didefinisikan, jika terdapat karakter yang tidak dikenali, maka otomatis karakter dirubah menjadi karakter spasi.

DAFTAR PUSTAKA

[1.] Eric Neidhard, ”Asymmetric Cryptography for Mobile Devices”, *Service-centric Networking Telekom Innovation Laboratories and TU Berlin*, Germany.

[2.] Peter Robinson, ”Applying Cryptography as a Service to Mobile Applications”, *RSA Conference*, Senior Engineering Manager RSA, The Security Division of EMC February 24-28, Session ID: CSV-F02, Moscone Center, San CCFrancisco, 2014.

[3.] Prof.Sana F Amin, Prof. Nilofar S Hunnergi, ”Hill Cipher algorithm with Self Repetitive Matrix for Secured Data Communication”, *International Journal of Engineering Research & Technology (IJERT)*, ISSN: 2278-0181, Vol. 2 Issue 9, September – 2013.

[4.] Hüseyin Bodur and Resul Kara, ”Secure SMS Encryption Using RSA Encryption Algorithm on Android”, Message Application, *International*

Symposium On Innovative Technologies In Engineering And Science (ISITES2015), Valencia-Spain, 2015.

[5.] Isbat Uzzin Nadhori, Tita Karlita, Rani Ismawati Dewi, "Sistem Pengamanan Pesan Singkat Untuk Mobile Phone Berbasis Android Menggunakan Algoritma Hill Cipher", *The 7th Conference on Information Technology and Electrical Engineering (CITEE 2015),* Teknik Elektronika-UGM, 15 September 2015.

[6.] Tita Karlita, Isbat Uzzin Nadhori, Rani Ismawati Dewi, "Short Message Security System for Android-Based Mobile Phone Using Hill Cipher and Arithmetic Coding Algorithm", *International Conference on Electrical Engineering, Informatics, and Its Education 2015 (CEIE 2015),* Universitas Malang, 3 Oktober 2015.

[7.] Chumaidi Rahman, "Studi dan implementasi Algoritma Blowfish untuk Enkripsi Email", *Diploma Final Project PENS*, 2009.