E-ISSN: 2986-0105
P-ISSN: 2985-8402

VOKATEK Volume 01 Nomor 03 Oktober 2023

Blowfish Advanced CS Untuk Solusi Keamanan Sistem Komputer Sekolah

[1]Faisal Syafar[*], [2]Halimah Husain, [3]Sutarsih Suhaeb, [4]Putri Ida, [5]Supriadi

[1,3,4,5]Jurusan Pendidikan Teknik Elektronika Fakultas Teknik Universitas Negeri Makassar

[2]Jurusan Pendidikan Kimia Fakultas MIPA Universitas Negeri Makassar

*Corresponding author: faisal.syafar@unm.ac.id[1]

Received : 2 Okt 2023
Accepted: 28 Okt 2023
Published: 30 Okt 2023

ABSTRAK

Masalah keamanan dan kerahasiaan data merupakan hal yang sangat penting baik dalam suatu organisasi yang berupa komersial, perguruan tinggi, lembaga pemerintahan, maupun dalam hal individual (pribadi). Kegiatan PKM dilaksanakan di Laboratorium TKJ dimana siswa bebas mengakses komputer dalam lab tanpa dibatasi sistem keamanan pada setiap komputer yang bekerja. Dalam hal ini file yang dapat di enkripsi adalah file dokumen berupa teks, file citra berupa gambar, serta file audio dan file video dalam format digital. Luaran dan Target Program Kemitraan Masyarakat yang dilaksanakan pada kelompok mitra sebanyak 15 peserta dan menghasilkan luaran berupa; Buku Panduan bagaimana Langkah-langkah kriptografi keamanan sistem komputer menggunakan menggunakan *blowfish advanced cs* dan implementasi kriptografi keamanan sistem komputer menggunakan menggunakan *blowfish advanced cs.* Penelitian ini merupakan jenis penelitian yaitu jenis penelitian kualitatif. Dengan studi kasus yang bertujuan untuk mengetahui tata cara dalam mengimplementasi kriptografi pengamanan data pada pesan teks, file, dan dokumen menggunakan menggunakan aplikasi blowfish advanced cs. Hasil yang diharapkan dalam PKM ini adalah 1) Pada saat proses key set-up algoritma Blowfish, key ini digabungkannya sehingga menguatkan algoritmanya. 2) Pada saat proses simulasi file/folder data file enkripsi dalam program algoritma Blowfish ini menggunakan key dengan minimum bisa 4 karakter. 3) Kunci yang simetri pada algoritma Blowfish ini sehingga proses simulasi enkripsi dan dekripsi file/folder data selalu menggunakan key yang sama, begitu juga split file dan merger file menggunakan key yang sama.
Kata Kunci: Blowfish advanced CS, Keamanan Komputer, Komputer Sekolah

ABSTRACT

Data security and privacy are very important issues for businesses, colleges, the government, and even individuals. The TKJ Laboratory is where PKM events take place. Students are free to use the computers there as they please, as long as they don't break the security system on each one. The types of files that can be protected in this case are text-based document files, picture files, audio and video files that are stored digitally, and question files. In the Community Partnership Program, which had 15 participants, there were outcomes and goals. The program produced a guidebook on how to use Blowfish Advanced CS for computer system security cryptography and instructions on how to use Blowfish Advanced CS for computer system security cryptography. This study is a type of research called qualitative research. With a case study that aims to learn how to use the Blowfish Advanced CS tool to secure text messages, files, and documents with cryptographic data. The predicted outcomes of this PKM are 1) This key is combined to make the Blowfish algorithm stronger during the key setup process. 2) The Blowfish algorithm tool needs a key with at least 4 characters to encrypt the data file during the file/folder simulation. 3) The Blowfish method uses symmetric keys, which means that the simulation process always uses the same key to encrypt and decrypt data files and folders. The same key is also used to split and join files.
Keywords: Blowfish advanced CS, Computer Security, School Computers

E-ISSN: 2986-0105
P-ISSN: 2985-8402
VOKATEK Volume 01 Nomor 03 Oktober 2023

1. PENDAHULUAN

1) Dokumen Digital

Dokumen merupakan suatu sarana transformasi informasi dari satu orang ke orang lain atau dari suatu kelompok ke kelompok lain. Dokumen meliputi berbagai kegiatan yang diawali dengan bagaimana suatu dokumen dibuat, dikendalikan, diproduksi, disimpan, didistribusikan, dan digandakan. Dokumen digital merupakan setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara atau gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya .

2) Kompresi *File* (*File Compress*)

Kompresi *file* adalah suatu cara untuk mengkodekan informasi dengan menggunakan *bit* yang lebih rendah yang digunakan untuk memperkecil ukuran data agar dapat disimpan dengan ruang penyimpanan yang kecil dan juga dapat mempersingkat waktu dalam transfer data.

3) File

File adalah entitas dari data yang disimpan didalam sistem *file* yang dapat diakses dan diatur oleh pengguna. Sebuah *file* memiliki nama yang unik dalam direktori di mana ia berada. Alamat direktori dimana suatu berkas ditempatkan diistilahkan dengan *path.*

Sebuah *file* berisi aliran data (atau data stream) yang berisi sekumpulan data yang saling berkaitan serta atribut berkas yang disebut dengan properties yang berisi informasi mengenai *file* yang bersangkutan seperti informasi mengenai kapan sebuah berkas dibuat.

4) Kriptografi

Sejarah kriptografi sebagian besar merupakan sejarah kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau mungkin dengan bantuan alat mekanik sederhana. Secara umum algoritma kriptografi klasik dikelompokkan menjadi dua kategori, yaitu algoritma transposisi (*transposition cipher*) dan algoritma substitusi (*substitution cipher*). *Cipher* transposisi mengubah susunan huruf-huruf di dalam pesan, sedangkan *cipher* substitusi mengganti setiap huruf atau kelompok huruf dengan sebuah huruf atau kelompok huruf lain.

5) Tujuan kriptografi

Dari paparan awal dapat dirangkumkan bahwa kriptografi bertujuan untuk member layanan keamanan. Yang dinamakan aspek-aspek keamanan:

1. Kerahasiaan (*confidentiality*)

Adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.

2. Integritas data (*data integrity*)

Adalah layanan yang menjamin bahwa pesan masih asli atau belum pernah dimanipulasi selama pengiriman.

3. Otentikasi (*authentication*)

Adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak- pihak yang berkomunikasi (*user autehentication*).

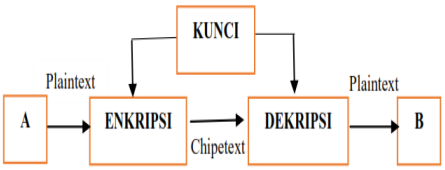
4. Non-repudiation

Adalah layanan untuk menjaga entitas yang berkomunikasi melakukan penyangkalan.

Algoritma kriptogarfi disebut juga *cipher*, yaitu aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa *cipher* memerlukan algoritma yang berbeda untuk enkripsi dan dekripsi. Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yang berisi elemen-elemen plainteks dan himpunan yang berisi cipherteks. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen Kriptografi mengatasi masalah keamanan data dengan menggunakan kunci, yang dalam hal ini algoritma tidak dirahasiakan lagi, tetapi kunci harus tetap dijaga

E-ISSN: 2986-0105
P-ISSN: 2985-8402
VOKATEK Volume 01 Nomor 03 Oktober 2023

kerahasiaannya. Kunci (*key*) adalah parameter yang digunakan untuk transformasi enkripsi dan dekripsi. Kunci biasanya berupa *string* atau deretan bilangan.



Gambar 1. Algoritma kunci simetri

Dari gambar diatas dapat kita lihat bahwa untuk mengirimkan pesan antara si pengirim dan si penerima menggunakan satu kunci atau kunci yang di gunkan sama. Maksudnya adalah kunci yang digunakan untuk mengenkripsi pesan dan kunci yang digunakan untuk mengdekripsikan pesan sama. Berarti mereka dalam melakukan komunikasi menggunkan satu kunci yang disebut kunci asimetri. Proses enkripsi dan dekripsi keduanya menggunakan kunci yang sama K1=K2.

Pertama kali sebelum pesan dikirim pesan tersebut masih dalam keadaan asli atau belum di enkripsi atau yang lebih dikenal dengan nama plaintext atau cleartext. Kemudian pada saat pesan tersebut dikirim pesan tersebut terlebih dahulu dilakukan proses encription (encipherment) yaitu proses menyandikan pesan plaintext kedalam chipertext yang apabila di buka akan berupa algoritma atau kata-kata yang sama sekali tidak dimengerti, sehingga orang lain tidak bisa membaca data yang telah di enkripsi tersebut. Kemudian setelah sampai di si penerima untuk mengubah chipertext tadi ke dalam plaintext disebut dengan decryption (dechiperment). Sedangkan Orang yang melakukan enkripsi terhadap suatu pesan atau praktisi kriptographi disebut *"Cryptographer"*. Pendistribusian Kunci pada Kriptografi Kunci Simetri tidak dapat dilakukan menggunakan saluran/ media yang akan digunakan untuk komunikasi, diperlukan media khusus untuk distribusi kunci, beberapa kunci mungkin membutuhkan beberapa media paralel untuk distribusinya.

6) Blowfish

Blowfish alias "*OpenPGP.Cipher.4*" merupakan enkripsi yang termasuk dalam golongan *Symmetric Cryptosystem* , metoda enkripsinya mirip dengan DES (DES-like Cipher) diciptakan oleh seorang *Cryptanalyst* bernama Bruce Schneier Presiden perusahaan Counterpane Internet Security, Inc (Perusahaan konsultan tentang kriptografi dan keamanan Komputer) dan dipublikasikan tahun 1994. Sejak saat itu telah dilakukan berbagai macam analisis, dan perlahan - lahan mulai mendapat penerimaan sebagai algoritma enkripsi yang kuat. Dibuat untuk digunakan pada komputer yang mempunyai microposesor besar (32-bit keatas dengan *cache* data yang besar). Sampai saat ini belum ada attack yang dapat memecahkan Blowfish.

Algoritma utama terbagi menjadi dua subalgoritma utama, yaitu bagian ekspansi kunci dan bagian enkripsi-dekripsi data. Pengekspansian kunci dilakukan pada saat awal dengan masukan sebuah kunci dengan panjang 32 bit hingga 448 bit, dan keluaran adalah sebuah array subkunci dengan total 4168 byte.

Bagian enkripsi-dekripsi data terjadi dengan memanfaatkan perulangan 16 kali terhadap jaringan feistel. Setiap perulangan terdiri dari permutasi dengan masukan adalah kunci, dan substitusi data. Semua operasi dilakukan dengan memanfaatkan operator Xor dan penambahan. Operator penambahan dilakukan terhadap empat array lookup yang dilakukan setiap putarannya.

Blowfish juga merupakan *cipher* blok, yang berarti selama proses enkripsi dan dekripsi, Blowfish akan membagi pesan menjadi blok-blok dengan ukuran yang sama panjang. Panjang blok untuk algoritma Blowfish adalah 64-bit. Pesan yang bukan merupakan kelipatan delapan *byte* akan ditambahkan bit-bit tambahan (*padding*) sehingga ukuran untuk tiap blok sama.

E-ISSN: 2986-0105
P-ISSN: 2985-8402
VOKATEK Volume 01 Nomor 03 Oktober 2023

2. METODE PELAKSANAAN

Dalam melakukan penelitian ini, jenis penelitian yang digunakan yaitu jenis penelitian kualitatif. Dengan studi kasus yang bertujuan untuk mengetahui tata cara dalam mengImplementasi kriptografi pengamanan data pada pesan teks, file, dan dokumen menggunakan menggunakan aplikasi *blowfish advanced cs.* Sebagian besar dari Blowfish yang menarik adalah f-fungsi yang tidak membalik. Fungsi ini menggunakan aritmatik modular untuk membangkitkan index-index ke dalam S-box. Tidak membalik (non-invertibility) ini dijelaskan sebagai berikut dengan contoh : Ambil fungsi $f(x) = x^2 \bmod 7$, lihat tabel 1 dibawah ini :

Tabel 1 Contoh fungsi $f(x) = x^2 \bmod 7$

X	X^2	X^2 Mod 7
1	1	1
2	4	4
3	9	2
4	16	2
5	25	4
6	36	1
7	49	0

Output yang dihasilkan tidak ada fungsi sehingga fungsi yang dihasilkanpun tidak ada fungsi khusus ke f(x). Sebagai contoh jika kita mengetahui bahwa fungsi kita mempunyai sebuah nilai 4 di beberapa nilai X, maka tidak ada cara untuk mengetahui jika nilai X tersebut adalah 2; 5; atau nilai X yang lain yang mempunyai fungsi f(x) = 4. Blowfish melakukan aritmatikanya sebesar mod 2^{32} (2^{32} sama dengan 4 milyar). Ini disebut aritmatik dalam bidang berhingga dan membuat banyak asumsi matematika yang sama yang tidak benar (1+1 tidak sama dengan 2 jika kita berada disebuah bidang ukuran 2 yang berhingga).

S-box adalah array yang besar dari data yang didefinisikan sebelumnya. Selama proses setup key, key tersebut menggabungkan dengan S-box. Detail key-setup ini relatif tidak menarik tetapi kenyataannya bahwa ia menggabungkan key tersebut dengan S-box yang menguatkan algoritma tersebut. Key-setup dalam Blowfish dirancang relatif lamban. Hal ini sangat bermanfaat karena seseorang akan melakukan suatu search-key brute-force yang akan menuju proses key-setup yang lamban untuk setiap key yang dicobanya. Meskipun seseorang melakukan enkripsi dan dekripsi harus hanya menuju proses key-setup satu kali, maka proses enkripsi dan dekripsi relatif cepat.

Elemen yang terpenting pada Blowfish yang lain adalah jaringan Feistel. Menggunakan jaringan Feistel yang menghasilkan cipher dengan dua sifat yang dapat diinginkan yaitu dekripsi menggunakan fungsi (f) yang sama dan kemampuan untuk mengiterasi fungsi tersebut beberapa kali ini disebut round (putaran). Semakin banyak round maka semakin banyak keamanan algoritma tersebut. Jumlah round yang direkomendasikan tergantung pada aloritma khusus; untuk Blowfish adalah 16 round.

3. HASIL DAN PEMBAHASAN

1) Hasil Yang Dicapai

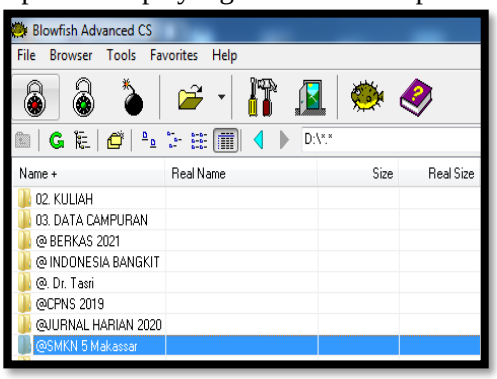
Kegiatan 1. Pendahuluan dan pembukaan kegiatan, pertemuan pertama di lakukan di dalam dengan pembukaan kegiatan, perkenalan antara pantia, pembantu lapangan dan mitra (peserta pelatihan) dan dilanjutkan dengan pemaparan materi pelatihan.

Kegiatan 2. Materi dasar dilakukan lab TKJ dengan memaparkan prinsip kerja utama materi PKM Peserta dijelaskan secara garis besar materi pelatihan.

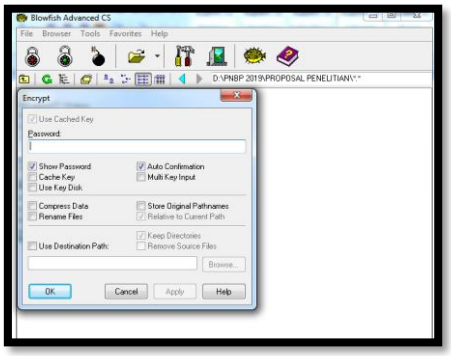
E-ISSN: 2986-0105
P-ISSN: 2985-8402
VOKATEK Volume 01 Nomor 03 Oktober 2023

Kegiatan 3. Selanjutnya peserta di berikan materi dengan cara menginstal aplikasi yang digunakan dalam PKM.

1 Kita terebih dahulu dapatkan toolsnya yang bisa di download secara gratis, saya mendapatkan toolsnya dengan lambang ikan kembung.
2 Lalu kita buka toolsnya dan pilih file apa yang akan kita enkripsikan

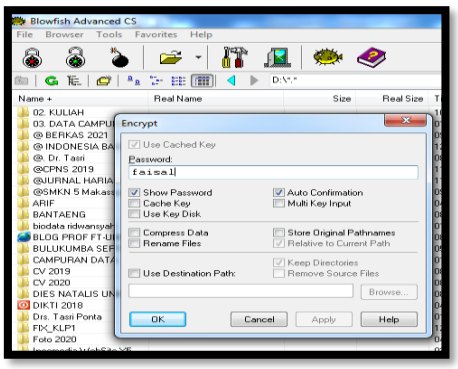


3 Dari gambar diatas saya memilih untuk meng-enkripsikan file ”Keamanan Password dan Enkripsi”
4 Lalu klik gambar kunci yang tertutup

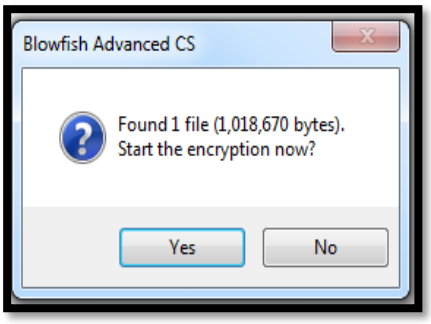


5 setelah di klik maka akan muncul seperti kotak di bawah ini :

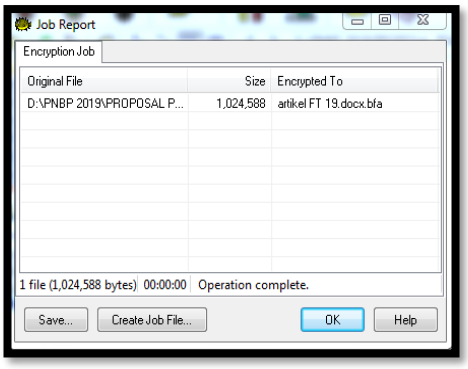
6 Lalu masukkan passwordnya kemudian klik OK



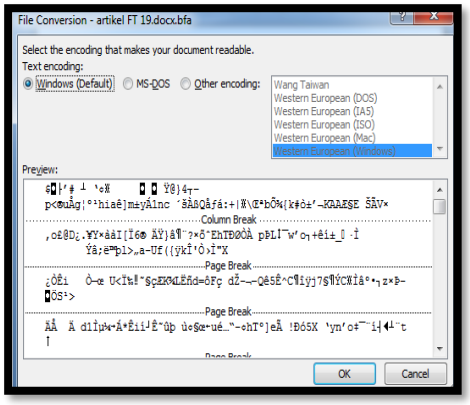
7 Lalu akan keluar tampilan seperti dibawah ini, lalu klik yes



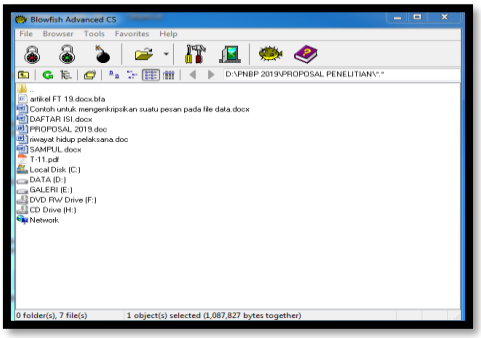
8 Setelah klik yes maka akan keluar tampilan kembali sepeti di bawah ini dan klik OK



9 Secara otomatis file yang kita enkripdi tadi akan tidak bisa di baca datanya oleh orang lain.
10 Untuk membuktikannya kita buka file tadi lalu lihat apakah yang terjadi pada file tersebut



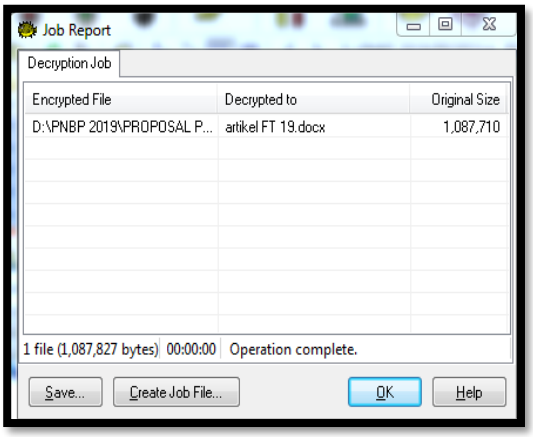
11. Dan ternyata file tersebut datanya telah aman, data yang ada pada file tersebut telah berubah menjadi sebuah bentuk tuisan aneh yang tdak dapt dimengerti.



11 Dengan itu kita dapat merasa aman dengan data yang kita rahasiakan tersebut.
12 Untuk membuka kembali datanya kita buka kembali toolsnya lalu kita klik tanda kunci yang terbuka.
13 masukkan kembali password kita yang tadi lalu kllik OK, dan pasword tadi jangan sampai lupa. Apabila hal tersebut terjadi maka file tersebut tidak akan pernah bisa dibaca kembali.

14 Setelah itu akan keluar kembali tampilan seperti di bawah ini dan klik yes

15 Maka akan tampil seperti tampilan di bawah ini, lalu klik OK :



16 Maka secara otomatis file yang telah di enkripsi tadi telah berubah menjadi seperti semula sebelum di enkripsi, atau kembali lagi menjadi plaintexs.

4. KESIMPULAN DAN SARAN

Dari analisa algoritma dan simulasi program Blowfish advance CS tersEbut dapat disimpulkan sebagai berikut: 1) Pada saat proses key set-up algoritma Blowfish, key ini digabungkannya sehingga menguatkan algoritmanya, 2) Pada saat proses simulasi file/folder data file enkripsi dalam program algoritma Blowfish ini menggunakan key dengan minimum bisa 4 karakter,3) Kunci yang simetri pada algoritma Blowfish ini sehingga proses simulasi enkripsi dan dekripsi file/folder data selalu menggunakan key yang sama, begitu juga split file dan merger file menggunakan key yang sama. Adapun saran untuk pengembangan selanjutnya adalah 1) Penulis mengharapkan dunia pendidikan mampu memanfaatkan kemajuan teknologi informasi dan komunikasi semaksimal mungkin untuk mengimplementasi kriptografi pengamanan data pada pesan teks, file, dan dokumen menggunakan menggunakan aplikasi *blowfish advanced cs, 2)* Dengan adanya aplikasi *blowfish advanced cs* maka penulis berharap adanya pengembangan lebih lanjut.

REFERENSI

Arikunto, Suharsimi. 2009. *Manajemen PKM*. Jakarta, PT. Rineka Cipta, 2010.

Ariyus, D. 2009. *Keamanan Multimedia.* Yogyakarta : Andi.

Bender. 1996. *Techniques For Data Hiding*. IBM Systems Journal.

Daemen, J; & Rijmen, V. 2001. *Advanced Encryption Standard*

(AES). Federal

Information Processing Standards Publication 197. Hariyanto, B. 2009. *Sistem Operasi*. Bandung : Informatika.

Noor, Juliansyah. 2011. *Metodologi PKM*. Jakarta: Kencana.

Lusiana, V. 2011. *Implementasi Kriptografi Pada File Dokumen Menggunakan Algoritma AES-128*. Jurnal Dinamika Informatika.

Moleong, Lexy J. Metodologi PKM Kualitatif, Bandung, PT. Remaja Rosdakarya, 2001.

Munir, R. 2006. *Kriptografi*. Bandung : Penerbit Informatika.Jurnal Ilmiah SAINTIKOM, 11-16.

Jurnal Sains, Teknologi dan Industri, Vol. 13, No. 2, Juni 2016, pp.218 – 228 ISSN 1693-2390 print/ISSN 2407-0939 online