

## ANALISIS MENGATASI SNIFFING DAN SPOOFING MENGGUNAKAN METODE ENKRIPSI DAN DEKRIPSI ALGORITMA HILL CHIPER

Anjar Wanto<sup>1</sup>

Mahasiswa S2 Fakultas Ilmu Komputer Dan Teknologi Informasi, Universitas Sumatera Utara

anjarwanto@gmail.com

### Abstrak

Usaha Mikro, Kecil dan Menengah (UMKM) adalah salah satu motor penggerak perekonomian di negara Indonesia, bahkan Usaha Mikro, Kecil, Dan Menengah (UMKM) merupakan salah satu tulang punggung perekonomian. Usaha Mikro Kecil menengah (UMKM) menyumbang sekitar 60% dari PDB (*Product Domestic Bruto*). UMKM juga menciptakan peluang kerja yang cukup besar bagi tenaga kerja dalam negeri, sehingga sangat membantu upaya mengurangi pengangguran. Jadi, bisnis Usaha Mikro, Kecil dan Menengah (UMKM) di Indonesia akan terus berkembang dan memberikan peluang usaha bagi mereka yang menyukai dunia wirausaha. UMKM dengan menggunakan *E-Commerce* sangat penting untuk meningkatkan kemajuan usaha dari UMKM itu sendiri, karena dengan fasilitas *E-Commerce* transaksi bisnis dan *work flow* akan menjadi lebih efektif dan efisien. Walaupun demikian, usaha & bisnis dengan *E-Commerce* juga rentan dari pencurian (*Sniffing*) dan manipulasi (*Spoofing*) dari orang-orang yang tidak bertanggung jawab, seperti pencurian data rahasia sampai pembobolan situs web dari UMKM tersebut, sehingga diperlukan adanya keamanan yang baik dari situs web UMKM untuk melindungi data-data dan informasi penting, baik data pelanggan maupun data pemilik UMKM itu sendiri. Oleh karena itu untuk mengatasi hal ini penulis menggunakan Algoritma *Hill Chipper* untuk melakukan enkripsi dan dekripsi nya. Algoritma *Hill Chipper* merupakan algoritma kriptografi algoritma simetris (*symmetric algorithms*).

**Kata kunci:** *Sniffing, Spoofing, E-Commerce, Hill Chipper*

### PENDAHULUAN

Keamanan dan kerahasiaan dalam berbisnis dan bertransaksi merupakan aspek yang sangat vital dalam dunia teknologi dewasa ini. *E-Commerce* atau yang biasa disebut juga dengan perdagangan elektronik merupakan aktifitas yang berkaitan dengan pembelian, penjualan, pemasaran barang ataupun jasa dengan memanfaatkan sistem internet ataupun jaringan yang sekarang ini sering digunakan oleh para usahawan UMKM untuk meningkatkan dan mengembangkan usahanya menjadi lebih besar dan maju serta semakin memperluas akses pasar. *E-Commerce* juga melibatkan aktifitas yang berhubungan dengan proses transaksi elektronik, seperti transfer dana elektronik, pertukaran data elektronik, sistem pengolahan data inventori yang dilakukan dengan sistem komputer ataupun jaringan komunikasi. Jadi secara garis besar tujuan pembuatan paper ini adalah :

1. Meningkatkan UMKM lebih maju dan berkembang didalam *E-Commerce*.
2. Menciptakan komunikasi berbasis Web yang mumpuni pada UMKM sehingga masalah dalam pemasaran dalam *E-Commerce* dapat teratasi.

Pesatnya perkembangan ilmu pengetahuan dan teknologi zaman ini memungkinkan munculnya teknik-teknik baru yang kadang kala disalahgunakan oleh pihak-pihak tertentu yang mengancam keamanan dan stabilitas dari sistem yang telah

ada. Jatuhnya Informasi ketangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi. Karena itu muncul suatu gagasan untuk membuat suatu sistem keamanan yang dapat melindungi data yang dianggap penting dengan penyandian data serta membuat kunci rahasia untuk dapat membuka data tersebut yang sulit untuk di deteksi oleh pihak yang tidak berhak.

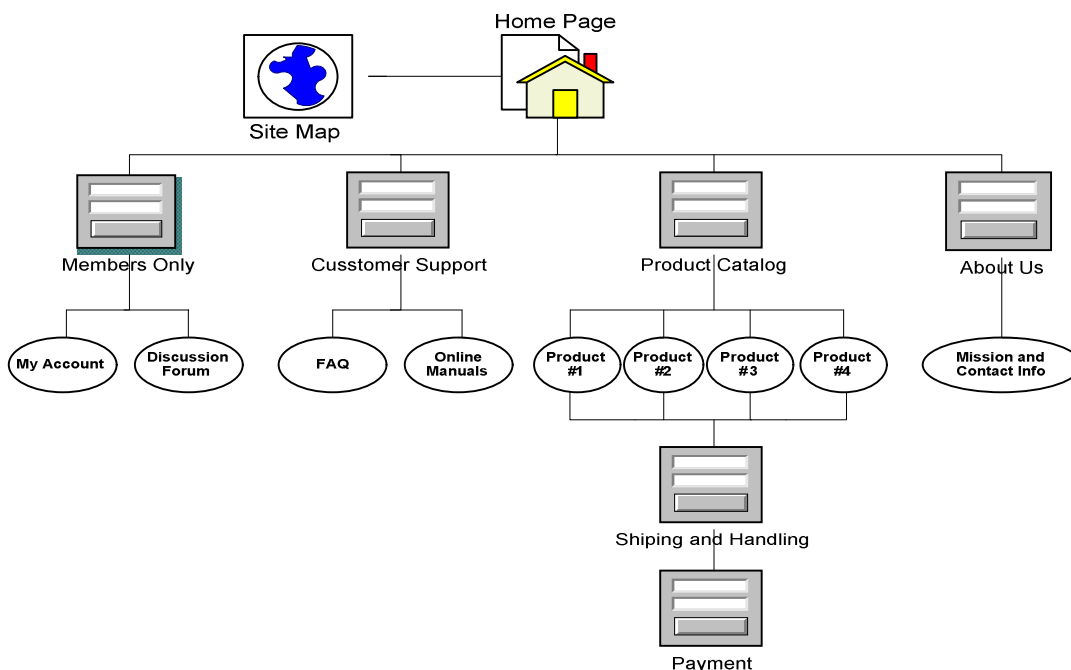
*Hill Cipher* yang merupakan *poly alphabetic cipher* dapat dikategorikan sebagai *block cipher*, karena teks yang akan diproses akan dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama pula.

## METODE PENELITIAN

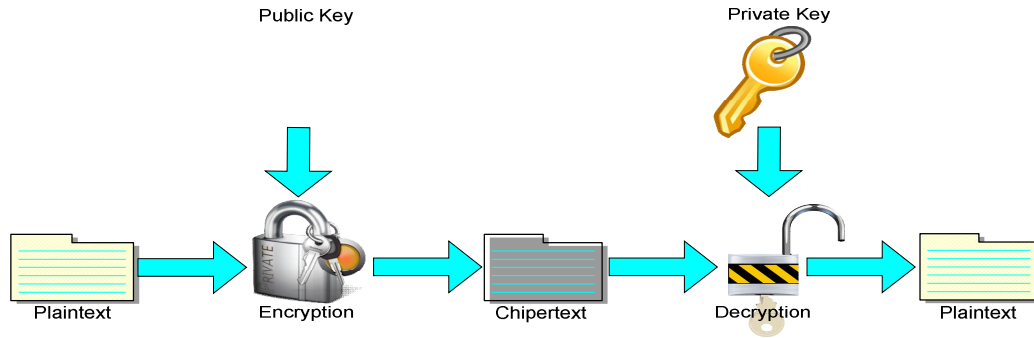
Metode penelitian adalah rangkaian dari cara/kegiatan pelaksanaan penelitian dan didasari oleh pandangan filosofis, asumsi dasar dan ideologis serta pertanyaan dan isu yang dihadapi.

- **Rancangan Penelitian**

Rancangan penelitian adalah suatu kesatuan, rencana terinci dan spesifik mengenai cara memperoleh, menganalisis, dan menginterpretasi data. Berikut ini adalah gambar struktur sederhana Situs Web *E-Commerce* :



**Gambar 3.1.** gambar struktur sederhana Situs Web *E-Commerce*



**Gambar 3.2.** Enkripsi dan Dekripsi

- **Ruang Lingkup Penelitian**

Ruang lingkup penelitian ini adalah bagaimana perilaku konsumen, khususnya pada web *E-Commerce* di Indonesia. Lingkup bahasan yang diteliti adalah dimensi kepercayaan konsumen dan pengaruhnya terhadap partisipasi dalam transaksi melalui *E-Commerce*. Subyek penelitian ini adalah pengguna internet di Indonesia yang telah melakukan transaksi pembelian barang/jasa melalui media *E-Commerce* atau internet. Barang/jasa yang dibeli harus berasal dari vendor/penjual yang ada di Indonesia, dengan tanpa membatasi jenis barang/jasa yang dibeli.

- **Teknik Pengumpulan Data**

Teknik pengumpulan data yang penulis gunakan adalah dengan menggunakan Metode Kualitatif dengan melihat pada kondisi objek yang alamiah. Dalam penelitian kualitatif ini penulis mengumpulkan data dengan cara triangulasi (gabungan), analisis data bersifat induktif. Hasil penelitian kualitatif ini lebih menekankan makna dari pada generalisasi. Metode ini juga ditunjang dengan metode library search yang mana metode dalam penelitian ini nantinya menggunakan teori-teori yang diambil dari buku literatur yang mendukung dan relevan serta berasal dari sumber data sekunder (teori, data dan informasi) seperti dokumen-dokumen, penelusuran internet maupun media cetak.

- **Objek Penelitian**

Objek penelitian adalah para pengguna internet di Indonesia yang telah melakukan transaksi pembelian barang/jasa melalui web *E-Commerce* UMKM.

- **Variabel Penelitian**

Variabel yang digunakan meliputi variabel *eksogen*, indikator (variabel terukur/measured variable/observed variable), dan *endogen*.

1. Variabel *eksogen* merupakan source variable atau independent variable yang tidak diprediksi oleh variabel yang lain dalam *Model*.
2. Variabel *endogen* merupakan outcome variable atau dependent variable dari paling sedikit satu hubungan kausalitas dalam *Model*.

3. Indikator merupakan variabel terukur yang digunakan untuk mengukur konsep (variabel *eksogen* dan *endogen*) yang tidak dapat diukur secara langsung. Dalam penelitian ini, variabel *eksogen* nya adalah ability, benevolence dan integrity. Sedangkan variabel *endogennya* adalah trust dan participation

Definisi operasional variabel *diatas* dapat dilihat pada tabel berikut ini :

KONSTRUK	INDIKATOR	KODE
Ability	Kompetensi	X1
	Pengalaman	X2
	Pengetahuan Luas	X3
	Pengesahan Institusional	X4
Benevolence	Perhatian	X5
	Kemauan Berbagi	X6
	Dapat Diharapkan	X7
Integrity	Pemenuhan	X8
	Keterusterangan	X9
	Kehandalan	X10
Trust	Kenyamanan	Y1
	Kepuasan	Y2
	Tanggung Jawab	Y3
Participation	Keberlanjutan	Y4
	Frekwensi	Y5
	Rekomendasi	Y6

**Tabel 3.1.** operasional variabel eksogen, variabel endogen

#### 1. Variabel *Eksogen Ability*.

Ability didefinisikan sebagai persepsi pelanggan tentang kemampuan penjual melalui media *E-Commerce* dalam menyediakan barang, memberikan rasa aman dan nyaman dalam transaksi. Indikator yang digunakan untuk mengukur variabel ini adalah :

- Kompetensi (X1): *E-Commerce* mempunyai kemampuan dalam menyediakan barang yang berkualitas bagi pelanggan.
- Pengalaman (X2): *E-Commerce* mempunyai pengalaman sehingga mampu mengirim barang tepat pada waktunya.
- Pengetahuan Luas (X3): *E-Commerce* memiliki pengetahuan yang baik dalam mengamankan transaksi.
- Pengesahan Institusional (X4): *E-Commerce* telah diakui keberadaannya oleh pihak-pihak lain, seperti supplier, distributor, jasa pengiriman, dan sebagainya.

#### 2. Variabel *Eksogen Benevolence*

Benevolence didefinisikan sebagai persepsi pelanggan terhadap keinginan baik penjual melalui media *E-Commerce* dalam memberikan kepuasan transaksi. Indikator yang digunakan untuk mengukur variabel ini adalah:

- Perhatian (X5): *E-Commerce* memiliki perhatian untuk memberikan pelayanan terbaik bagi pelanggannya.
- Kemauan Berbagai (X6): *E-Commerce* memiliki kemauan untuk memberikan keuntungan bagi pelanggannya.
- Dapat Diharapkan (X7): *E-Commerce* memiliki itikad baik untuk memberikan kepuasan kepada pelanggannya.

3. Variabel *Eksogen Integrity*

Integrity adalah komitmen penjual melalui media *E-Commerce* dalam menjaga nilai-nilai untuk memberikan pelayanan terbaik kepada pelanggan. Indikator yang digunakan untuk mengukur variabel ini adalah:

- Pemenuhan (X8): *E-Commerce* akan memenuhi apa yang diharapkan pelanggannya.
- Keterusterangan (X9): *E-Commerce* tidak akan menyembunyikan informasi yang penting bagi pelanggannya.
- Keandalan (X10): *E-Commerce* selalu menjaga reputasinya.

4. Variabel *Endogen Trust*

Trust didefinisikan sebagai kepercayaan dan kepuasan pelanggan pada transaksi melalui media *E-Commerce*. Indikator yang digunakan untuk mengukur variabel ini adalah:

- Kenyamanan (Y1): *E-Commerce* memberikan kenyamanan dalam bertransaksi.
- Kepuasan (Y2): *E-Commerce* memberikan kepuasan dalam bertransaksi.
- Tanggung Jawab (Y3): *E-Commerce* memenuhi tanggung jawabnya terhadap pelanggan

5. Variabel *Endogen Participation*

Participation didefinisikan sebagai intensitas pelanggan dalam melakukan transaksi melalui media *E-Commerce*. Indikator nya adalah:

- Keberlanjutan (Y4): Pelanggan akan terus bertransaksi (intention to purchase) melalui media *E-Commerce*.
- Frekuensi (Y5): pelanggan akan meningkatkan frekuensi bertransaksi melalui media *E-Commerce*.
- Rekomendasi (Y6): Pelanggan akan merekomendasikan kepada pihak lain agar bertransaksi melalui media *E-Commerce*.

## HASIL DAN PEMBAHASAN

- Enkripsi Hill Chiper

Langkah-langkah untuk proses enkripsi plaintext dengan *Hill Cipher* adalah sebagai berikut:

1. Pilih suatu matriks kunci K yang berupa matriks bujur sangkar yang dipakai sebagai kunci.
2. Transformasikan tiap huruf dalam teks ke bilangan bulat yang sesuai (A = 0; B = 1; ... Z = 25)
3. Kelompokkan barisan angka yang didapat ke dalam beberapa blok vektor P yang panjangnya sama dengan ukuran matriks K.
4. Hitung  $C = K \cdot P \pmod{26}$  untuk tiap vektor P. Kembalikan tiap angka dalam vektor sandi C ke huruf yang sesuai untuk mendapatkan teks sandi.



**Gambar 4.1.** Proses Enkripsi Hill Chiper

Gambar diatas menjelaskan enkripsi dengan *Hill Cipher* dengan memberikan contoh. *Hill Cipher* menggunakan matriks untuk mentransformasikan string plaintext menjadi ciphertext.

Untuk mentransformasikan plaintext maka pertama sekali semua huruf alphabet dinyatakan dalam nilai seperti pada tabel 4.1 berikut ini :

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

**Tabel 4.1.** Nilai Transformasi Plaintext

Penjelasan :

Misalkan terdapat pesan berikut yang akan dienkrpsi dengan Hill Cipher: “ **ANJAR**

**WANTO** “ dengan matriks Kunci :  $K = \begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix}$

maka menjadi :

<b>AN</b>	0	<b>JA</b>	9	<b>RW</b>	17	<b>AN</b>	0	<b>TO</b>	19
	13		0		22		13		14

**Tabel 4.2.** Konversi ke bentuk nilai berdasarkan ekivalen dari huruf

Memulai proses enkripsi (**Matriks kunci \* blok matriks(Plain text)**)

**C(AN) :**

$$\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} 0 \\ 13 \end{bmatrix} = \begin{bmatrix} 4.0 & + & 3.13 \\ 3.0 & + & 3.13 \end{bmatrix} = \begin{bmatrix} 39 \\ 39 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 13 \\ 13 \end{bmatrix}$$

**C(JA) :**

$$\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} 9 \\ 0 \end{bmatrix} = \begin{bmatrix} 4.9 & + & 3.0 \\ 3.9 & + & 3.0 \end{bmatrix} = \begin{bmatrix} 36 \\ 27 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 10 \\ 1 \end{bmatrix}$$

**C(RW) :**

$$\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} 17 \\ 22 \end{bmatrix} = \begin{bmatrix} 4.17 & + & 3.22 \\ 3.17 & + & 3.22 \end{bmatrix} = \begin{bmatrix} 134 \\ 117 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 4 \\ 13 \end{bmatrix}$$

**C(AN) :**

$$\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} 0 \\ 13 \end{bmatrix} = \begin{bmatrix} 4.0 & + & 3.13 \\ 3.0 & + & 3.13 \end{bmatrix} = \begin{bmatrix} 39 \\ 39 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 13 \\ 13 \end{bmatrix}$$

**C(TO) :**

$$\begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} 19 \\ 14 \end{bmatrix} = \begin{bmatrix} 4.19 & + & 3.14 \\ 3.19 & + & 3.14 \end{bmatrix} = \begin{bmatrix} 118 \\ 99 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 14 \\ 21 \end{bmatrix}$$

Maka Hasil cipher text = 13,13,10,1,4,13,13,13,14,21 = NNKBENNNNOV

#### • Dekripsi Hill Chiper

Memulai proses dekripsi (**invers matriks kunci \*blok matriks (cipher text)**).

Langkah pertama adalah mencari invers matriks kunci menggunakan invers *Modulo* determinan matriks kunci :

$$K = \begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix} \longrightarrow \det K = (4 \cdot 3) - (3 \cdot 3) = 3$$

Invers *Modulo*

$$3^{-1} \text{Mod } 26 \longrightarrow 3x=1 \text{Mod } 26 \longrightarrow 3x=1 + 26k \longrightarrow x= (1+26k)/3$$

cari k=n sehingga hasil x adalah bilangan bulat

$$k=0 \longrightarrow x=(1+26 \cdot 0)/3= 1/3 \text{ (bukan bilangan bulat)}$$

$$k=1 \longrightarrow x=(1+26 \cdot 1)/3= 9 \text{ (bilangan bulat)}$$

sehingga invers dari 3 *Mod* 26 ekuivalen dengan 9 *Mod* 26

yaitu **9**

invers *Modulo* determinan digunakan untuk mencari invers matriks

$$\text{Misal } K = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ maka } K^{-1} = \frac{1}{\text{Determinan}} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$\text{Sehingga } K^{-1} = 9 \begin{bmatrix} 3 & -3 \\ -3 & 4 \end{bmatrix} = \begin{bmatrix} 27 & -27 \\ -27 & 36 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 1 & 25 \\ 25 & 10 \end{bmatrix}$$

Untuk *Modulo* bilangan negatif dapat dikerjakan sebagai berikut:

$$\text{-27 Mod 26 = -n Mod x}$$

$$\text{maka : -n Mod x = x-(n Mod x) } \longrightarrow 26-(27 \text{ Mod } 26) \longrightarrow 26-1=25.$$

**Dekripsi = invers K \* cipher text**

$$\begin{aligned} \begin{bmatrix} 1 & 25 \\ 25 & 10 \end{bmatrix} \begin{bmatrix} 13 \\ 13 \end{bmatrix} &= \begin{bmatrix} 1.13 & + & 25.13 \\ 25.13 & + & 10.13 \end{bmatrix} = \begin{bmatrix} 338 \\ 455 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 0 \\ 13 \end{bmatrix} \quad \begin{matrix} A \\ N \end{matrix} \\ \begin{bmatrix} 1 & 25 \\ 25 & 10 \end{bmatrix} \begin{bmatrix} 10 \\ 1 \end{bmatrix} &= \begin{bmatrix} 1.10 & + & 25.1 \\ 25.10 & + & 10.1 \end{bmatrix} = \begin{bmatrix} 35 \\ 260 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 9 \\ 0 \end{bmatrix} \quad \begin{matrix} J \\ A \end{matrix} \\ \begin{bmatrix} 1 & 25 \\ 25 & 10 \end{bmatrix} \begin{bmatrix} 4 \\ 13 \end{bmatrix} &= \begin{bmatrix} 1.4 & + & 25.13 \\ 25.4 & + & 10.13 \end{bmatrix} = \begin{bmatrix} 329 \\ 230 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 17 \\ 22 \end{bmatrix} \quad \begin{matrix} R \\ W \end{matrix} \\ \begin{bmatrix} 1 & 25 \\ 25 & 10 \end{bmatrix} \begin{bmatrix} 13 \\ 13 \end{bmatrix} &= \begin{bmatrix} 1.13 & + & 25.13 \\ 25.13 & + & 10.13 \end{bmatrix} = \begin{bmatrix} 338 \\ 455 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 0 \\ 13 \end{bmatrix} \quad \begin{matrix} A \\ N \end{matrix} \\ \begin{bmatrix} 1 & 25 \\ 25 & 10 \end{bmatrix} \begin{bmatrix} 14 \\ 21 \end{bmatrix} &= \begin{bmatrix} 1.14 & + & 25.21 \\ 25.14 & + & 10.21 \end{bmatrix} = \begin{bmatrix} 539 \\ 560 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 19 \\ 14 \end{bmatrix} \quad \begin{matrix} T \\ O \end{matrix} \end{aligned}$$

Dapat dilihat diatas bahwa hasil dekripsi **cipher text** menghasilkan **plain text** yang menandakan bahwa pengerjaan di atas Valid / sudah benar.

## KESIMPULAN

Kesimpulan yang dapat diambil dari penulisan ini antara lain :

1. Algoritma Chipper ini dapat digunakan sebagai penyandian data yang berupa karakter yang berbentuk huruf dengan cara membagi perblok setiap karakter yang dienkripsi. Diantara nya saat memasukkan data Username dan Password pada saat Login ke situs Web UMKM.
2. Keamanan dan kenyamanan konsumen dalam transaksi *E-Commerce* mempunyai pengaruh positif yang sangat signifikan terhadap kemajuan dan perkembangan sebuah UMKM.
3. Keamanan dari sebuah web *E-Commerce* UMKM mutlak sangat diperlukan untuk menangkal dan mencegah kejahatan dunia maya dari pihak-pihak yang tidak bertanggungjawab.

## DAFTAR PUSTAKA

- [1] Hasibuan, Zainal. A. 2007. Metode Penelitian Pada Bidang Ilmu Komputer Dan Teknologi Informasi : Konsep, Teknik dan Aplikasi. Jakarta.
- [2] Suryani. E dan S. M. Titin. 2008. Kombinasi Kriptografi Dengan *Hill Cipher* Dan Steganografi Dengan LSB Untuk Keamanan Data Teks.
- [3] Munawar. 2012. Perancangan Algoritma Sistem Keamanan Data Menggunakan Metode Kriptografi Asimetris. Vol.1.
- [4] R. Sadikin. 2012. Kriptografi untuk Keamanan Jaringan. Andi. Yogyakarta.
- [5] Hill, Lester, S., 1929, Cryptography in an Algebraic Alphabet: The American Mathematical Monthly, 36 (6), pp.306-312.
- [6] Ainur. R. 2007. Pengaruh Dimensi Kepercayaan (Trust) Terhadap Partisipasi Pelanggan *E-Commerce*. Tesis. Universitas Brawijaya, Malang.
- [7] Pramudiya (2015). Pengimplementasian CRM Pada Pembangunan E-Commerce untuk Usaha Mikro Kecil Menengah. Jurnal Buana Informatika. Vol. 6, 257-268.



- [8] Tomy Satria Alasi. 2015. Penerapan Hill Chiper Pada Kemanan Pesan Teks <http://ilmukomputer.org/2015/04/06/pene-rapan-hill-chiper-pada-kemanan-pesan-teks/>. 29 September 2015.