APLIKASI KRIPTOGRAFI KOMPOSISI *ONE TIME PAD CIPHER* DAN *AFFINE CIPHER*

Ivan Luckiyana Firdaus[1)], Rini Marwati[2)], Ririn Sispiyati[3)]

[1), 2), 3)] Departemen Pendidikan Matematika FPMIPA UPI

*Surel: ivan.luckiyana@student.upi.edu

ABSTRAK. Kriptografi *one time pad cipher* memiliki kelemahan pada kurangnya keefisienan dalam pembentukan dan pengiriman kuncinya jika menggunakan cara manual untuk menentukan kuncinya. Salah satu cara agar pembentukkan kuncinya lebih mudah dengan menggunakan aturan barisan Fibonacci terhadap teks asli(*plaintext*) sehingga menghasilkan kunci untuk *one time pad cipher*. Untuk lebih mempersulit pemecahan, *one time pad cipher* dikomposisikan dengan *affine cipher* yang merupakan dasar dari algoritma kriptografi klasik yang menggunakan metode subtitusi. Skripsi ini membahas bagaimana pengkonstruksian kunci untuk *one time pad cipher* dan pembuatan program aplikasi komposisi *one time pad cipher* dan *affine cipher*. Hasil dalam penulisan skripsi ini berupa program aplikasi untuk mempermudah enkripsi dan dekripsi komposisi *one time pad cipher* dan *affine cipher* yang dibuat menggunakan bahasa pemrograman Delphi 7.0.

Kata kunci: program aplikasi, *one time pad cipher*, *affine cipher.*

ABSTRACT. One time pad cipher has a weakness on generating it's key. There are many ways to cover it's weakness,such as using Fibonacci series formula on the plaintext to generate one time pad cipher's key. One time pad cipher is an encryption technique that difficult to be cracked. One way for a cipher to become more difficult to resolve is by composing two encryption technique. One time pad cipher which is difficult to be cracked will be composed by affine cipher which is the base of classic cryptography whose using substitution methode. This paper aimed to discuss how to generate one time pad cipher's key with Fibonacci series formula and how to make application program crptography composition of one time pad cipher and affine cipher. And the result of this paper is a program application cryptography composition of one time pad cipher and affine cipher using Borland Delphi 7.0, which made encrypting and decrypting became easier.

Keywords: application program, one time pad cipher, affine cipher.

1. PENDAHULUAN

Teknologi merupakan sesuatu yang tidak bisa kita pungkiri pengaruhnya terhadap perubahan zaman. Sudah banyak kegiatan kita sehari-hari yang membutuhkan bantuan teknologi. Salah satu teknologi yang dibutuhkan dewasa ini adalah internet, karena penggunaanya yang praktis dan luas dapat digunakan di mana saja dan kapan saja, tentu dengan bantuan teknologi elektronik yang memadai. Internet menjadi sebuah kebutuhan sekarang ini, banyaknya penggunaan internet seperti media sosial, media komunikasi, media pemasaran dan masih banyak lagi menunjukkan bahwa internet merupakan teknologi yang perkembangannya sangatlah pesat. Internet yang bisa digunakan dalam bertukar informasi dengan mudah dan cepat keamanan menjadi aspek yang penting dalam menjaga informasi yang dikirim atau diterima. Jaringan komputer menggunakan konsep sistem terbuka, maka orang lain dapat masuk ke jaringan tersebut, sehingga pengiriman informasi menjadi tidak aman dan dapat dimanfaatkan oleh orang lain untuk mengubah atau mengambil informasi tersebut di tengah jalan. Agar tidak terjadi kebocoran maka diperlukan sandi agar informasi tersebut bersifat rahasia.

Ilmu yang mempelajari kode atau sandi yaitu Kriptografi. Kriptografi berasal dari bahasa Yunani: *cryptos* dan *graphein*. *Cryptos* artinya rahasia, sedangkan *graphein* artinya tulisan. Jadi, kriptografi berarti tulisan rahasia. Sedangkan definisi kriptografi adalah suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, integritas suatu data, serta otentifikasi data (Menezes, 1996 : 4). Menurut Kromodimoeljo (2009 : 5) kriptografi adalah ilmu mengenai teknik enkripsi di mana data diacak menggunakan suatu kunci enkripsi menjadi data yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Proses enkripsi dilakukan menggunakan suatu algoritma dengan beberapa parameter. Secara garis besar, proses enkripsi adalah proses pengacakan pesan yang dapat dibaca "teks asli" (*plaintext*) menjadi pesan yang sulit dibaca "teks sandi" (*ciphertext*). Tentunya *ciphertext* harus dapat didekripsi oleh seseorang yang mempunyai kunci dekripsi untuk mendapatkan kembali *plaintext*. Orang yang tidak memiliki kunci dekripsi akan sulit mendapatkan kembali *plaintext* yang telah diubah menjadi *ciphertext*.

Menurut Sadikin (2012) algoritma kriptografi dapat diklasifikasikan menjadi menjadi dua jenis berdasarkan perkembangannya, yaitu algoritma kriptografi klasik dan algoritma kriptografi modern. Algoritma kriptografi klasik umumnya merupakan teknik penyandian dengan kunci simetrik, sedangkan algoritma kriptografi modern menggunakan kunci asimetris di mana kunci dekripsi berbeda dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibandingkan

enkripsi simetris, karena enkripsi asimetris menggunakan bilangan-bilangan yang sangat besar. Metode yang digunakan dalam algoritma kriptografi klasik merupakan metode subtitusi (perpindahan / pergantian huruf) atau metode transposisi (pertukaran posisi huruf). *One time pad cipher* merupakan salah satu jenis algoritma klasik yang menggunakan metode subtitusi.

Algoritma kriptografi klasik yang hanya memiliki satu kunci untuk memecah dekripsi dan enkripsi memiliki tingkat keamanan yang lebih lemah dibandingkan dengan algoritma kriptografi modern yang memiliki kunci berbeda untuk mengenkripsi dan mendekripsi. Sehingga algoritma kriptografi klasik mudah dipecahkan oleh pihak ketiga yang ingin mengetahui informasi yang dikirimkan. Namun demikian bukan berarti algoritma kriptografi klasik kurang bagus untuk digunakan dalam sistem keamanan, banyak cara agar algoritma kriptografi klasik dapat menjadi lebih aman. Salah satu cara agar algoritma kriptografi klasik menjadi lebih aman adalah dengan mengkomposisikan dua jenis algoritma kriptografi klasik, sehingga pengekripsian menjadi lebih rumit untuk didekripsi. Dengan mengkomposisikan dua algoritma kriptografi klasik artinya dua kali mengenkripsi pesan atau informasi, $f(g(x))$ atau $g(f(x))$. Misalnya pertama mengenkripsikan pesan dengan *affine cipher* sehingga menghasilkan *cipher text*, lalu *cipher text* kembali dienkripsi dengan *one time pad cipher* atau sebaliknya sehingga pesan akan semakin sulit untuk dipecahkan bagi orang yang tidak memiliki kunci untuk mendekripsinya.

2. KAJIAN LITERATUR

2.1. *One Time Pad Cipher*

One time pad cipher merupakan salah satu algoritma kriptografi klasik yang kerahasiaannya mencapai sempurna karena menggunakan kunci yang tidak membentuk barisan yang berulang dan panjang kunci sama dengan panjang teks yang akan dirahasiakan. Dikarenakan menggunakan teknik tersebut *one time pad cipher* menjadi tidak efisien, karena membutuhkan waktu yang lama untuk menentukan kunci yang sama panjang dengan panjang teks yang akan dirahasiakan. Berikut ini adalah proses pengenkripsian dari *one time pad cipher*

$$c_i \equiv p_i + k_i \ (mod\ n) \quad , \qquad i = 1,2,3, \dots, r$$

p_i merupakan nilai *plaintext* ke-i

k_i merupakan nilai kunci ke-i

c_i merupakan nilai *ciphertext* ke-i

nilai n dapat ditentukan berdasarkan berapa banyak jenis karakter huruf yang digunakan dalam pengenkripsian. Dan berikut ini adalah proses pendekripsian *one time pad cipher*

$$p_i \equiv c_i - k_i \ (mod\ n) \quad , \qquad i = 1,2,3, \dots, r$$

2.2. *Affine Cipher*

Affine cipher merupakan sandi monoalfabetik yang menggunakan teknik subtitusi yang menggunakan fungsi linier $ap + b$ untuk enkripsi teks asli p dan $a^{-1}(c - b)$ untuk dekripsi teks sandi c. a dan b merupakan kunci dari *affine cipher* untuk setiap p huruf dalam pesan dan c merupakan huruf sandi yang dihasilkan (Sadikin, 2012).

Agar a memiliki nilai invers (a^{-1}) pada modulo n, $\gcd(a, n)$ harus bernilai 1. Dengan fungsi liner yang diberikan berikut ini rumus transformasi enkripsi dan dekripsi dari *affine cipher* :

Enkripsi : $c_i = ap_i + b \ (mod\ n)$

Dekripsi : $p_i = a^{-1}(c_i - b)(mod\ n)$

2.3. Barisan Fibonacci

Definisi 2.3.1 (Bartle & Sherbert, 2000)

Sebuah barisan dari bilangan real (atau barisan di $\mathbb{R}$) adalah sebuah fungsi yang didefinisikan pada himpunan bilangan asli $\mathbb{N}$ ={1,2,…} di mana *range*nya dimuat di himpunan bilangan real $\mathbb{R}$.

Barisan Fibonacci memiliki pola dalam barisan yang menggunakan rumus

$$x_i = x_{i-2} + x_{i-1}\ , untuk\ i \geq 3$$

Dimana $x_{n-2} = x_{n-1} = 1$.

2.4. Komposisi Fungsi

Definisi 2.4.2 Komposisi Fungsi (Bartle & Sherbert, 2000)

Jika $f: A \to B$ dan $g: B \to C$, dan jika $R(f) \subseteq D(g) = B$, maka fungsi komposisi f dan g ditulis $g \circ f$ adalah fungsi dari A ke C yang didefinisikan sebagai $(g \circ f)(x) = g(f(x))$ untuk setiap $x \in A$.

3. HASIL DAN PEMBAHASAN

3.1. Mengkonstruksi Kunci *One Time Pad Cipher* Dengan Aturan Barisan Fibonacci

Untuk mempermudah mendapatkan kunci untuk *one time pad cipher* bisa menggunakan banyak cara, salah satunya menggunakan aturan dari sebuah

barisan. Dalam artikel ini akan digunakan aturan barisan Fibonacci untuk mengkonstruksi kunci *one time pad cipher*. Dengan menggunakan aturan Fibonacci

$$x_i = x_{i-2} + x_{i-1}\,, untuk\ i \geq 3$$

x_{n-2} dan x_{n-1} merupakan kunci dari kunci *one time pad cipher*. Di mana x_{n-2} dan x_{n-1} huruf pertama dan kedua dari *plaintext* secara berturut-turut.

Contoh: *Plaintext* "TEKS RAHASIA" terdiri dari 12 karakter diubah menjadi kode ASCII 95 karakter maka menjadi (52, 37, 43, 51, 0, 50, 33, 40, 33, 51, 41, 33). Dengan menggunakan aturan Fobonacci "TE" dua huruf pertama dalam *plaintext* akan menjadi kunci yang membentuk kunci dari *one time pad cipher*. Dengan "TE" atau (52, 37) sebagai kunci untuk k_i di mana $i \geq 3$

$$k_3 \equiv 52 + 37\ mod\ 95 \qquad k_8 \equiv 50 + 33\ mod\ 95$$
$$k_3 = 89 \qquad k_8 = 83$$
$$k_4 \equiv 37 + 43\ mod\ 95 \qquad k_9 \equiv 33 + 40\ mod\ 95$$
$$k_4 = 80 \qquad k_9 = 73$$
$$k_5 \equiv 43 + 51\ mod\ 95 \qquad k_{10} \equiv 40 + 33\ mod\ 95$$
$$k_5 = 94 \qquad k_{10} = 73$$
$$k_6 \equiv 51 + 0\ mod\ 95 \qquad k_{11} \equiv 33 + 51\ mod\ 95$$
$$k_6 = 51 \qquad k_{11} = 84$$
$$k_7 \equiv 0 + 50\ mod\ 95 \qquad k_{12} \equiv 51 + 41\ mod\ 95$$
$$k_7 = 50 \qquad k_{12} = 92$$

Diperoleh kunci (89, 80, 94, 51, 50, 83, 73, 73, 84, 92). Dengan $k_1 = 0$ dan $k_2 = 0$, kunci K *one time pad cipher* yang akan digunakan untuk *plaintext* "TEKS RAHASIA" adalah K = (0, 0, 89, 80, 94, 51, 50, 83, 73, 73, 84, 92).

Dengan menggunakan metode ini, untuk menentukan kunci *one time pad cipher* akan lebih mudah dan lebih efisien untuk *plaintext* yang mencapai ratusan huruf atau lebih.

3.2. Komposisi Kriptografi *One Time Pad Cipher dan Affine Cipher*

a. *One Time Pad Cipher* Komposisi *Affine Cipher*

Proses enkripsi *one time pad cipher* komposisi *affine cipher* merupakan proses dua kali pengenkripsian, yang pertama pengenkripsian dengan *affine cipher* lalu *ciphertext* yang diperoleh dari pengenkripsian *affine cipher* dienkipsi kembali dengan menggunakan *one time pad cipher*. Berikut ini adalah proses pengenkripsian *one time pad cipher* komposisi *affine cipher*:

$$C = E_{otp}(E_{aff}(P))$$
$$= E_{otp}(aP + b)$$
$$= (aP + b) + K$$

E_{aff} = proses enkripsi *affine cipher*
E_{otp} = proses enkripsi *one time pad cipher*
P = *plaintext*
C = *ciphertext*
a,b = kunci untuk *affine cipher*
K = kunci untuk *one time pad cipher*

Dan berikut ini adalah proses pendekripsian *one time pad cipher* komposisi *affine cipher :*

$$P = D_{aff}(D_{otp}(C))$$
$$= D_{aff}(C - K)$$
$$= a^{-1}((C - K) - b)$$

D_{otp} = proses dekripsi *one time pad cipher*
D_{aff} = proses dekripsi *affine cipher*

Contoh : *Plaintext* "TEKS RAHASIA" diubah ke dalam kode ASCII 95 karakter menjadi (52, 37, 43, 51, 0, 50, 33, 40, 33, 51, 41, 33), dengan kunci *affine cipher* $a = 2$ dan $b = 4$. Sebelum mengenkripsi akan ditunjukkan $\gcd(2,95) = 1$ dengan menggunakan algoritma Euclid

$$95 = 2 \times 47 + 1$$
$$\therefore \gcd(2,95) = 1$$

Berikut adalah proses enkripsi dan dekripsi kriptografi *one time pad cipher* komposisi *affine cipher* :

$$c_1 \equiv 2 \times 52 + 4 \; mod \; 95$$
$$c_1 = 13$$
$$c_2 \equiv 2 \times 37 + 4 \; mod \; 95$$
$$c_2 = 78$$
$$c_3 \equiv 2 \times 43 + 4 \; mod \; 95$$
$$c_3 = 90$$
$$c_4 \equiv 2 \times 51 + 4 \; mod \; 95$$
$$c_4 = 11$$
$$c_5 \equiv 2 \times 0 + 4 \; mod \; 95$$
$$c_5 = 4$$
$$c_6 \equiv 2 \times 50 + 4 \; mod \; 95$$
$$c_6 = 9$$
$$c_7 \equiv 2 \times 33 + 4 \; mod \; 95$$
$$c_7 = 70$$
$$c_8 \equiv 2 \times 40 + 4 \; mod \; 95$$
$$c_8 = 84$$
$$c_9 \equiv 2 \times 33 + 4 \; mod \; 95$$
$$c_9 = 70$$
$$c_{10} \equiv 2 \times 51 + 4 \; mod \; 95$$
$$c_{10} = 11$$
$$c_{11} \equiv 2 \times 41 + 4 \; mod \; 95$$
$$c_{11} = 86$$
$$c_{12} \equiv 2 \times 33 + 4 \; mod \; 95$$
$$c_{12} = 70$$

Diperoleh C = (13, 78, 90, 11, 4, 9, 70, 84, 70, 11, 86, 70) hasil dari enkripsi *affine cipher*. Akan dicari kunci untuk *one time pad cipher* dari C dengan aturan Fibonacci

$$k_3 \equiv 13 + 78 \; mod \; 95$$
$$k_3 = 91$$
$$k_4 \equiv 78 + 90 \; mod \; 95$$
$$k_4 = 73$$
$$k_5 \equiv 90 + 11 \; mod \; 95$$
$$k_5 = 6$$
$$k_6 \equiv 11 + 4 \; mod \; 95$$
$$k_6 = 15$$
$$k_7 \equiv 4 + 9 \; mod \; 95$$
$$k_7 = 13$$
$$k_8 \equiv 9 + 70 \; mod \; 95$$
$$k_8 = 79$$
$$k_9 \equiv 70 + 84 \; mod \; 95$$
$$k_9 = 59$$
$$k_{10} \equiv 84 + 70 \; mod \; 95$$
$$k_{10} = 59$$
$$k_{11} \equiv 70 + 11 \; mod \; 95$$
$$k_{11} = 81$$
$$k_{12} \equiv 11 + 86 \; mod \; 95$$
$$k_{12} = 2$$

Dengan $k_1 = 0$ dan $k_2 = 0$ diperoleh K=(0, 0, 91, 73, 6, 15, 13, 79, 59, 59, 81, 2). Dan terkahir mengenkripsi C menggunakan *one time pad cipher* dengan kunci K

$$c'_1 \equiv 13 + 0 \; mod \; 95$$
$$c'_1 = 13$$
$$c'_2 \equiv 78 + 0 \; mod \; 95$$
$$c'_2 = 78$$
$$c'_3 \equiv 90 + 91 \; mod \; 95$$
$$c'_3 = 86$$
$$c'_4 \equiv 11 + 73 \; mod \; 95$$
$$c'_4 = 84$$
$$c'_5 \equiv 4 + 6 \; mod \; 95$$
$$c'_5 = 10$$
$$c'_6 \equiv 9 + 15 \; mod \; 95$$
$$c'_6 = 24$$
$$c'_7 \equiv 70 + 13 \; mod \; 95$$
$$c'_7 = 83$$
$$c'_8 \equiv 84 + 79 \; mod \; 95$$
$$c'_8 = 68$$
$$c'_9 \equiv 70 + 59 \; mod \; 95$$
$$c'_9 = 34$$
$$c'_{10} \equiv 11 + 59 \; mod \; 95$$
$$c'_{10} = 70$$
$$c'_{11} \equiv 86 + 81 \; mod \; 95$$
$$c'_{11} = 72$$
$$c'_{12} \equiv 70 + 2 \; mod \; 95$$
$$c'_{12} = 72$$

Diperoleh C' = (13, 78, 86, 84, 10, 24, 83, 68, 34, 70, 72, 72). Jadi *plaintext* "TEKS RAHASIA" dienkripsi dengan kriptografi *one time pad cipher* komposisi *affine cipher* menjadi "-nvt*8sdBfhh". Untuk pendekripsian akan ditentukan nilai a^{-1} dengan algoritma Euclid yang diperluas

$$1 = 95 - (2 \times 47)$$

Diperoleh $a^{-1} = -47$

$$-47 \; mod \; 95 = 48$$
$$\therefore a^{-1} = 48$$

Dengan a^{-1} dan rumus dekripsi *one time pad cipher* komposisi *affine cipher*, *ciphertext* "-nvt*8sdBfhh" dapat didekripsi menjadi *plaintext* "TEKS RAHASIA".

b. *Affine Cipher* Komposisi *One Time Pad Cipher*

Dengan formula enkripsi dan dekripsi *affine cipher* dan *one time pad cipher* yang sudah diberikan, berikut adalah proses enkripsi dari kriptografi *affine cipher* komposisi *one time pad cipher* :

$$\begin{aligned} C &= E_{aff}(E_{otp}(P)) \\ &= E_{aff}(P + K) \\ &= a(P + K) + b \end{aligned}$$

Dan untuk proses dekripsinya

$$\begin{aligned} P &= D_{otp}(D_{aff}(C)) \\ &= D_{otp}\left(a^{-1}(C \quad - b)\right) \\ &= a^{-1}\left(C \quad - b\right) - K \end{aligned}$$

Contoh : *Plaintext* "TEKS RAHASIA" diubah ke dalam kode ASCII 95 karakter menjadi P = (52, 37, 43, 51, 0, 50, 33, 40, 33, 51, 41, 33), dengan kunci *affine cipher* $a = 2$ dan $b = 4$. Berikut adalah proses enkripsi kriptografi *affine cipher* komposisi *one time pad cipher* :

Berdasarkan contoh sebelumnya kunci *one time pad cipher* untuk *plaintext* "TEKS RAHASIA" adalah K = (0, 0, 89, 80, 94, 51, 50, 83, 73, 73, 84, 92).

$$c_1 \equiv 52 + 0 \; mod \; 95$$
$$c_1 = 52$$
$$c_2 \equiv 37 + 0 \; mod \; 95$$
$$c_2 = 37$$
$$c_3 \equiv 43 + 89 \; mod \; 95$$
$$c_3 = 37$$
$$c_4 \equiv 51 + 80 \; mod \; 95$$
$$c_4 = 36$$
$$c_5 \equiv 0 + 94 \; mod \; 95$$
$$c_5 = 94$$
$$c_6 \equiv 50 + 51 \; mod \; 95$$
$$c_6 = 6$$
$$c_7 \equiv 33 + 50 \; mod \; 95$$
$$c_7 = 83$$
$$c_8 \equiv 40 + 83 \; mod \; 95$$
$$c_8 = 28$$
$$c_9 \equiv 33 + 73 \; mod \; 95$$
$$c_9 = 11$$
$$c_{10} \equiv 51 + 73 \; mod \; 95$$
$$c_{10} = 29$$
$$c_{11} \equiv 41 + 84 \; mod \; 95$$
$$c_{11} = 30$$
$$c_{12} \equiv 33 + 92 \; mod \; 95$$
$$c_{12} = 30$$

Diperoleh C = (52, 37, 37, 36, 94, 6, 83, 28, 11, 29, 30, 30) hasil dari enkripsi *one time pad cipher*. dengan kunci $a = 2$ dan $b = 4$, C akan dienkripsi menggunakan *affine cipher*

$$c'_1 \equiv 2 \times 52 + 4 \; mod \; 95 \qquad c'_7 \equiv 2 \times 83 + 4 \; mod \; 95$$
$$c'_1 = 13 \qquad c'_7 = 75$$
$$c'_2 \equiv 2 \times 37 + 4 \; mod \; 95 \qquad c'_8 \equiv 2 \times 28 + 4 \; mod \; 95$$
$$c'_2 = 78 \qquad c'_8 = 60$$
$$c'_3 \equiv 2 \times 37 + 4 \; mod \; 95 \qquad c'_9 \equiv 2 \times 11 + 4 \; mod \; 95$$
$$c'_3 = 78 \qquad c'_9 = 26$$
$$c'_4 \equiv 2 \times 36 + 4 \; mod \; 95 \qquad c'_{10} \equiv 2 \times 29 + 4 \; mod \; 95$$
$$c'_4 = 76 \qquad c'_{10} = 62$$
$$c'_5 \equiv 2 \times 94 + 4 \; mod \; 95 \qquad c'_{11} \equiv 2 \times 30 + 4 \; mod \; 95$$
$$c'_5 = 2 \qquad c'_{11} = 64$$
$$c'_6 \equiv 2 \times 6 + 4 \; mod \; 95 \qquad c'_{12} \equiv 2 \times 30 + 4 \; mod \; 95$$
$$c'_6 = 16 \qquad c'_{12} = 64$$

Diperoleh C' = (13, 78, 78, 76, 2, 16, 75, 60, 26, 62, 64, 64). Jadi *plaintext* "TEKS RAHASIA" dienkripsi dengan kriptografi *affine cipher* komposisi *one time pad cipher* menjadi "-nnl"0k\:^``". Dengan $a^{-1}$ sama seperti di contoh sebelumnya dan rumus pendekripsian *affine cipher* komposisi *one time pad cipher*, *ciphertext* "-nnl"0k\:^``" bisa kembali didekripsi menjadi *plaintext* "TEKS RAHASIA".

4. KESIMPULAN

Berdasarkan rumusan masalah dan tujuan penelitian serta isi yang telah diuraikan, maka dapat disimpulkan beberapa hal, antara lain:

1. Kunci dari *one time pad cipher* dapat dibangun dari suatu formula. Pada kasus penulisan ini, penulis menggunakan formula barisan Fibonacci agar kunci yang diperoleh tidak membentuk suatu barisan yang berulang ikut sertakan *plaintext* untuk membangun kunci dari *one time pad*.
2. Pengenkripsian dan pendekripsian dari algoritma kriptografi komposisi *one time pad cipher* dan *affine cipher* menggunakan konsep-konsep matematika yaitu, komposisi fungsi, kongruensi, faktor persekutuan terbesar dan grup.

5. DAFTAR PUSTAKA

[1] Bartle, R. G., & Sherbert, D. R. (2000). *Introduction to Real Analysis, Fourth Edition.*

[2] Burton, D. M. (2007). *Elementaru Number Theory (sixht edition).* New York: McGraw-Hill.

[3] Kromodimoeljo, S. (2009). *Teori & Aplikasi Kriptografi*. SPK IT Consulting.

[4] Malik, D. S., Moderson, J. M., & Sen, M. K. (1997). *Fundamentas of Abstract Algebra.* Singapore: McGraw-Hill.
[5] Menezes, A., Oorschot. P., & Vanstone, A. (1996). *Hand book of Applied Cryptography*. USA: CRC Press.
[6] Munir, R. (2004b). *Bahan Kuliah ke-1: Pengantar Kriptografi.* Bandung:Departemen Teknik Informatika ITB.
[7] Munir, R. (2004c). *Bahan Kuliah ke-3: Teori Bilangan (Number Theory).* Bandung: Departemen Teknik Informatika ITB.
[8] Raji, W. (2013). *An Introduction Course in Elementary Number Theory*. The Saylor Foundation.
[9] Sadikin, R. (2012). *Kriptografi Untuk Keamanan Jaringan.* Yogyakarta: Andi.
[10] The Ascii Code. (2016). *ASCII Table* [Online]. Tersedia di: http://www.theasciicode.com.ar/ Diakses 7April 2016.
[11] Varberg, D., Purcell, E.J., & Rigdon, S.E. (2003). *Kalkulus Edisi 8.* Jakarta: Erlangga.