Nama: Irham Hamed Ayani

NIM: 200411100114

Kelas: Kriptografi 6B

## Identitas Jurnal

Judul: PENYANDIAN DATA TEKS MENGGUNAKAN ALGORITMA CIPHER FEEDBACK DAN CHAOTIC SKEW TENT MAP

Jurnal: J-Icon : Jurnal Komputer dan Informatika

Nomor jurnal: J-ICON, Vol. 5 No. 2, Oktober 2017, pp. 12~20

Penulis: Anita M. Sonbay , Adriana Fanggidae , Kornelis Letelay

# Latar belakang

Keamanan dokumen pada perusahaan instansi sangat penting. Maka dibutuhkan sebuah metode kriptografi mengamankan/mengenkripsi dan dapat dibaca kembali oleh yang berhak (mendekripsi). Salat satu metode adalah Chiper Feed Back (CFB), namun terdapat kelemahan yaitu dimana setiap blok memiliki kuncinya yang sama, sehingga diperlukan metode pembangkit bilangan acak (chaotic) untuk menghasilkan kunci yang berbeda pada setiap blok nya.

# Materi dan Metode Penelitian

## Data penelitian

Data penelitian berupa file teks dengan 18 file doc dan docx serta 8 file txt dengan ukuran bervariasi mulai dari 24 kb sampai 305 kb.

## Algoritma CFB (Modifikasi)

Pada mode CFB yang asli, kunci yang digunakan pada setiap blok sama. Oleh karena itu, diusulkan mode CFB dengan menggunakan kunci yang berbeda pada setiap blok yang dibangkitkan dengan oleh fungsi chaotic skew tent map (CSTM).

1. Session keys

Algoritma yang diusulkan

Mengubah kunci ke numerik untuk CTSM dengan panjang kunci 16 karakter desimal atau sebesar 128-bit

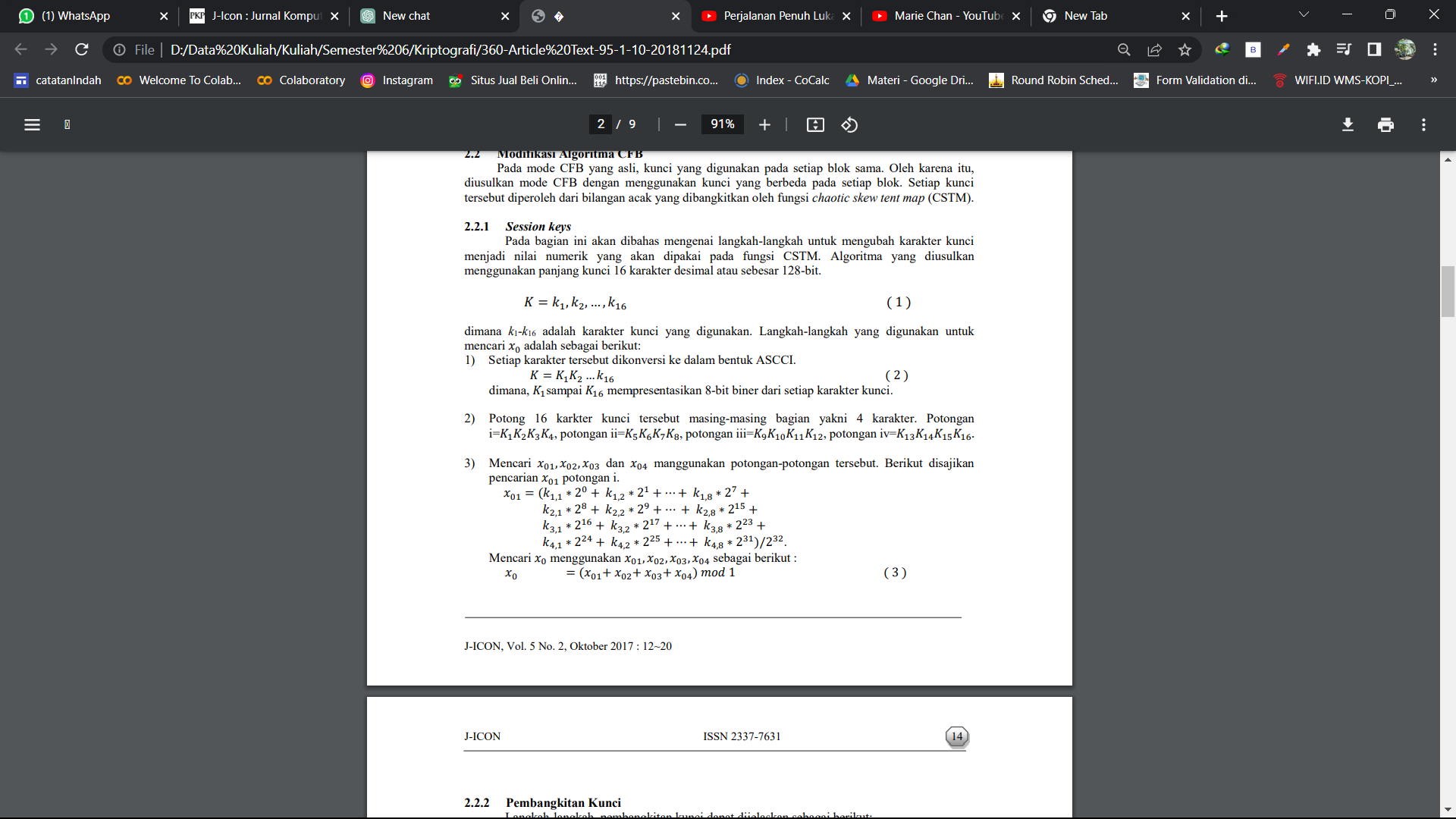
K = k\_1, k\_2, …, k\_16

Langkah:

1. Setiap karakter tersebut dikonversi ke dalam bentuk ASCCI.

dimana, k\_1 sampai k\_16 mempresentasikan 8-bit biner dari setiap karakter kunci.

1. Bagi atau potong 16 karkter kunci tersebut masing-masing bagian yakni 4 karakter.
2. Mencari 𝑥\_01, 𝑥\_02, 𝑥\_03 dan 𝑥\_04 manggunakan potongan-potongan tersebut. Berikut disajikan pencarian 𝑥\_01 potongan i.



1. Pembangkitan kunci

Langkah:

1. Penentuan iterasi awal menggunakan fungsi pemotongan
2. Membangkitkan bilangan acak kunci menggunakan fungsi CSTM:
3. Membangkitkan bilangan acak total pergeseran bit karakter teks
4. bilangan acak pertama, nilai x0 yang telah diperoleh dimasukkan ke fungsi pemotongan. nilai CSTM1 melalui iterasi awal yang diperoleh dari langkah 1, kemudian nilai CSTM1 tersebut dipotong dengan persamaan (3)
5. Enkripsi Dekripsi
6. Enkripsi
   1. Masukan plaintext, kunci dan ukuran blok.
   2. Bagi blok plaintext sesuai dengan ukuran blok dan jumlah karakter plaintext.
   3. Lakukan fungsi CSTM dan fungsi pemotongan untuk membangkitkan deretan bilangan acak kunci dan total pergeseran.
   4. Lakukan operasi CFB dan pergeseran karakter ke kanan sebesar total pergeseran.
   5. Hasil enkripsi (ciphertext).
7. Dekripsi
   1. Masukan ciphertext, kunci dan ukuran blok.
   2. Bagi blok plaintext sesuai dengan ukuran blok dan jumlah karakter plaintext.
   3. Lakukan operasi CFB dan pergeseran karakter ke kiri sebesar total pergeseran.
   4. Lakukan fungsi CSTM dan fungsi pemotongan untuk membangkitkan deretan bilangan acak kunci dan total pergeseran.
   5. Hasil dekripsi (plaintext)

# Hasil dan Pembahasan

Pengujian 18 file doc, docx dan 8 file txt, dengan 4 macam pengujian.

(i) pengujian 1 (ukuran file ≤ 35kb dan ukuran file mod blok = 0), (ii) pengujian 2 (ukuran file 36kb – 60kb dan ukuran file mod blok = 0), (iii) pengujian 3 (ukuran file 61kb – 80kb dan ukuran file mod blok ≠ 0) dan (iv) pengujian 4 (ukuran file > 80kb dengan ukuran file mod blok ≠ 0).

## Enkripsi Dekripsi.

Key: “ANITAMARIANYSONB”

Ukuran blok = 100

## Analisis

1. Korelasi (hubungan antar data)

Hasil enkripsi dari pengujian menunjukkan korelasi 0,163326411. Hal itu menunjukkan tidak ada korelasi antara data input dan output (0=tidak ada korelasi, 1=korelasi)

1. Analisis Standar Deviasi dan Variansi (sebaran data)

Rata-rata standar deviasi dan variansi dari

plaintext dan ciphertext yang memiliki perbedaan cukup besar yaitu nilai standar deviasi dari plaintext =371,18 dan ciphertext = 1111,9175 sedangkan nilai variansi plaintext = 98491.04 dan ciphertext = 10.256.837,77.

Hal tersebut menunjukkan bahwa hasil enkripsi memiliki sebaran karakter lebih banyak.

1. Analisis histogram

Histogram menunjukkan frekuensi distribusi yang lebih banyak dan berbeda.