BAB I

PENDAHULUAN

1.1 Latar Belakang

Tiket merupakan sesuatu yang di anggap sebagai alat pembayaran yang digunakan oleh alat transportasi, selain itu tiket dapat digunakan dalam berbagai bidang event atau acara. Dimana tiket merupakan bagian yang penting dalam pelaksanaan sebuah acara berbayar, tiket digunakan sebagai alat bukti untuk mendapatkan hak penonton sebagai penerima layanan[1].

Berdasarkan wawancara dengan salah satu komunitas dimana didalamnya terdiri dari beberapa pelaku usaha yang sering mengadakan *event* atau acara dalam bidang *fashion* dikuningan adalah Ciremai Clothing Club yang mencakup brand-brand lokal di kuningan. Seri pertama diselenggarakan pada tanggal 25-27 maret 2022 dengan tema "*Getting Started"* yang dimana dalam seri ini CCC mengratiskan pengunjung. Kemudian sesi kedua diselenggaran pada tanggal 17-19 maret 2023 dengan tema "*Moving Forward",* pada sesi kedua ini berhasil menjual tiket sebanyak 3000 tiket lebih yang terjual. Akan tetapi sistem pengelolaan tiket yang di pakai oleh CCC ini masih menggunakan pencatatan sederhana dengan media cetak dan media stample. Dalam proses pemesanan tiket pengunjung harus datang langsung ke lokasi tempat tiket dibuka. Sehingga pencatatan tidak efisien dari segi waktu karena antrian yang panjang, pencatatan masih menggunakan buku besar, sehingga seringkali terjadi kesalahan pencatatan oleh admin

pengelola data tiket. Pada saat acara berlangsung, pengecekan tiket masih dilakukan secara manual dimana petugas mengecek satu persatu tiket pengunjung. Dikarnakan banyak nya pengunjung seringkali menyulitkan petugas dalam pengecekan sehingga terkadang terjadi ketidak telitian dalam proses pengecekan. Dikarnakan tiket hanya berisi *expired date* berupa stample sehingga sering terjadi pengulangan pemakaian tiket, hal ini dapat merugikan tim penyelenggara dikarnakan tiket seharusnya di pakai satu kali dalam satu hari.

Seiring berkembang nya ilmu pengetahuan dan teknologi, dalam hal ini teknologi menjadi sebuah kebutuhan tersendiri baik bagi individual ataupun kelompok, dengan kemudahan nya dalam menggunakan sebuah teknologi saat ini, tak lupa begitu banyak juga peluang dalam kerentanan sistem keamanan. Hal ini perlu diperhatikan, karena jika sebuah sistem informasi bisa di akses oleh orang yang tidak berhak atau tidak bertanggungjawab, maka keakuratan informasi tersebut akan diragukan, bahkan akan menjadi sebuah informasi yang menyesatkan. tantangan tersendiri dalam menentukan inovasi yang tepat[2].

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi[3]. Dalam ilmu kriftografi terdapat istilah enkripsi dan deskripsi. Enkripsi adalah proses mengubah *plaintext* (pesan asli) menjadi *ciphertext* (pesan tersandi). Sedangkan deskripsi adalah mengembalikan *ciphertext* (pesan tersandi)

menjadi *plaintext* (pesan asli) sesuai dengan text asli. Salah satu algoritma kriptografi yaitu SPECK.

Algoritma SPECK adalah algoritma terbaru yang dibuat oleh Nasional Security Agency(NSA) pada tahun 2013, SPECK block cipher memiliki 10 macam versi dimana block atau key nya terdiri dari 32bit yang paling terkecil hingga 128bit block yang terbesar. Keunggulan algoritma speck ini yaitu dalam kecepatan proses enkripsi dan deskripsi, dalam penelitian sebelum nya pada dengan judul "Analisis perbandingan Block Cipher Simon-Speck, Simeck, dan Skinny pada komunikasi berbasis Lora" pada tahun 2022[4].

Berdasarkan uraian diatas maka dilakukan penelitian dengan judul **"RANCANG BANGUN APLIKASI *E-TICKETING* MENGGUNAKAN ALGORITMA SPECK UNTUK MENINGKATKAN KEAMANAN DATA TIKET ELEKTRONIK".**

1.2 Identifikasi Masalah

Berdasarkan latar belakang masalah diatas, maka peneliti dapat mengindetifikasi permasalahan yang ada yaitu :

1. Adanya pengulangan pemakaian *expired data* tiket, hal ini dapat merugikan tim penyelenggara *event*.
2. Pemesanan tiket pengunjung yang tidak efisien dari segi waktu karena antrian yang panjang.

Dalam pencatatan masih menggunakan buku besar. Sehingga seringkali terjadi kesalahan pencatatan oleh admin pengelola data tiket

1.3 Rumusan Masalah

Berdasarkan masalah yang telah diuraika dari latar belakang diatas, maka didapat rumusan masalah yaitu sebagai berikut :

1. Bagaimana merancangbangun aplikasi *E-Ticketing* di komunitas Ciremai Clothing Club ?
2. Bagaimana mengimplementasikan algoritma *SPECK* dalam aplikasi *E-Ticketing* untuk proses enkripsi dan deskripsi dalam bentuk *QR-Code*?

1.4 Batasan Masalah

Agar penelitian yang dilakukan terarah maka diperlukan batasan mengenai permasalahan yang akan diselesaikan. Adapun batasan masalah dalam penelitian ini, yaitu sebagai berikut :

1. Aplikasi yang dibangun :
    a. Aplikasi digunakan oleh 3 *user*, yaitu admin, petugas dan pengguna. Admin digunakan oleh panitia penyelenggara acara atau *event* Ciremai Clothing Club dalam mengelola acara Ciremai Clothing Club. Petugas dapat mengecek data tiket pelanggan, dan Pengguna digunakan oleh pelanggan. Masing-masing memiliki hak akses sebagai berikut :
        - Panitia (admin) dapat mengelola data *event* dan mengkonfirmasi pembayaran tiket online dan melihat data pemesanan tiket.

- Petugas tiket dapat mengecek *expired date* tiket pengunjung pada saat *event* diselenggarakan.
- Pengguna dapat membeli tiket secara online, akses yang didapat oleh pelanggan yaitu : melakukan regristrasi, mengetahui informasi *event*, pembelian tiket, dan download tiket.

b. Algoritma yang digunakan adalah algoritma *SPECK 32* bit untuk enkripsi kode transaksi dengan contoh : "CCC Tahun Kode Event, Nomor Tiket/Nomor Antrian" kedalam bentuk *QR-Code* menggunakan Javascript.

c. Hasil deskripsi berupa : event , tgl event, tgl pemesanan tiket (Contoh : Day 1), status tiket (Aktif dan Nonaktif), status penggunaan tiket (Digunakan dan Belum digunakan). tgl pengecekan.

2. Aplikasi pengecekan tiket pengguna digunakan oleh petugas pengecekan tiket dengan berbasis Android dan dibuat menggunakan React Native yang nantinya berfungsi untuk petugas pengecekan tiket *event* atau acara. Untuk versi android yang digunakan yaitu versi Marsmallow.

3. Aplikasi android digunakan oleh petugas pengecekan dan pengguna. Petugas pengecekan memiliki akses untuk mengecek tiket pengunjung, sedangkan pelanggan memiliki akses untuk melakukan regristrasi, mengetahui informasi *event*, pembelian tiket, dan download tiket.

4. Aplikasi website, digunakan oleh admin dalam mengelola event atau acara yang diselenggarakan oleh panitia.

1.5 Tujuan Masalah

Berdasarkan perumusan masalah yang telah diuraikan diatas maka didapat tujuan sebagai berikut:

1. Merancang bangun aplikasi untuk mempermudah dalam pengecekan tiket *event* dan meminimalisir terjadinya penggunaan ulang tiket *event* Ciremai Clothing Club oleh pengunjung
2. Dapat mempermudah dalam mengelola data tiket yang terjual.
3. Mengimplementasikan teknik enkripsi dan deskripsi dengan menggunakan algoritma *SPECK* pada media tiket dengan *QR-Code.*

1.6 Manfaat Penelitian

Dalam hal ini manfaat yang ingin dicapai dan diambil dalam penelitian ini yaitu :

1. Manfaat bagi penulis
    a. Dapat menambah pengetahuan dalam merancang bangun infrastruktur aplikasi.
    b. Dapat mengetahui dalam mengimplementasikan enkripsi dan deskripsi dengan algoritma kriptografi *SPECK.*

2. Manfaat bagi Pelanggan

    Dalam pembelian tiket pelanggan dapat membeli dengan mudah secara online.

3. Manfaat bagi Penyelenggara
    a. Dapat meminimalisir terjadinya penggunaan ulang tiket event oleh pengunjung.
    b. Dalam segi pelayanan, penyelenggara event dapat memberikan pelayanan lebih cepat dalam pengecekan tiket customer.

1.7 Pertanyaan Penelitian

Dari identifikasi masalah yang telah diuraikan sebelumnya maka terdapat pertanyaan penelitian, yaitu :

1. Apakah dengan adanya aplikasi e-ticketing berbasis QR-Code dapat mengatasi terjadinya pemakaian ulang data *expired date* tiket?
2. Apakah aplikasi yang dibuat dapat memberi kemudahan kepada pelanggan dalam pembelian tiket?
3. Apakah Algoritma SPECK dapat diimplementasikan untuk keamanan pada tiket Ciremai Clothing Club?

1.8 Hipotesis Peneliti

Aplikasi dapat mengelola E-Ticketing dan menerapkan algoritma untuk meningkatkan keamanan data tiket elektronik

1.9 Metodologi Penelitian

1.9.1 Metode Pengumpulan Data

1. Observasi

   Observasi dilakukan secara langsung terhadap komunitas Ciremai Clothing Club yang beralamat di Jl. Ir. Juanda No.201, Purwawinangun, Kec.Kuningan, Kabupaten Kuningan, Jawa Barat 45512, Indonesia. Pada tanggal 29 Maret 2023. Kedatangan ke lokasi tersebut untuk mengetahui lokasi komunitas, berkenalan dengan penyelenggara dari Acara Ciremai Clothing Club, melakukan pengamatan pada acara *event* CCC berlangsung dan mencatat hal-hal yang dibutuhkan.

2. Wawancara

   Setelah dilakukan observasi terhadap komunitas Ciremai Clothing Club, Saya melakukan wawancara dan meminta ijin untuk melakukan penelitian kepada penyelenggara sekaligus sekertaris dari Ciremai Clothing Club yaitu Bapak Azhar Natsir, M.Ds yang bertempat di Jl. Ir. Juanda No.201, Purwawinangun, Kec.Kuningan, Kabupaten Kuningan, Jawa Barat 45512, Indonesia

3. Studi Pustaka

   Studi pustaka dilakukan dengan menggunakan sumber-sumber seperti jurnal untuk mendapatkan sumber informasi yang bersifat ilmiah

mengenai keamanan data produk, algoritma *SPECK*, *QR-Code* dan lainnya yang berkaitan dengan penelitian.

1.9.2 Metode Pengembangan Sistem

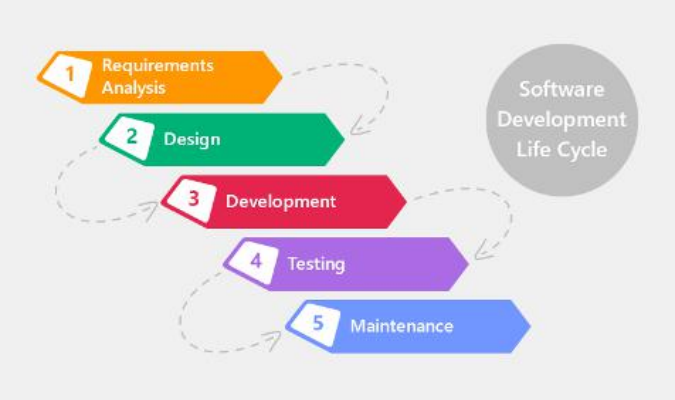
Menurut Sholikhah, Sairan, dan Syamsiah [5], menjelaskan bahwa, "Waterfall merupakan model klasik yang memiliki sifat berurut dalam merancang software".

Metode Waterfall adalah metode dengan pendekatan secara sistematis dan juga berurutan (*step-by-step*) pada sebuah pengembangan perangkat lunak. Tahapan dengan spesifikasi kebutuhan pengguna lalu berlanjut melalui tahapan-tahapan perencanaan yaitu planning, permodelan, konstruksi, sebuah system dan penyerahan sistem kepara pengguna, dukungan pada perangkat lunak lengkap yang dihasilkan (Novitasari 2018). Kelebihan menggunakan metode Waterfall diantaranya yaitu :

1. Sistem yang dihasilkan memiliki kualitas yang tebih baik, karena mengikuti proses bertahap.
2. Dalam dokumen pengembangan sistem dapat terorganisir dengan baik, karena setiap fase harus diselesaikan secara korehan dan lengkap sebelum melanjutkan ke fase selanjutnya.

3. Metode ini merupakan salah satu metode yang sangat baik digunakan.Dikarenakan dalam prosesnya semakin rinci dan di tinjau kembali setiaptahapannya saat pengujian system.[7]

Gambar 1.1 merupakan metode Waterfall, metode pengembangan sistem yang akan digunakan dalam perancangan aplikasi yang akan dibangun:



Gambar 1.1 Waterfall (bodoystudio)

Sumber : Waterfall [7]

Waterfall memiliki beberapa tahapan yaitu :

1. Requirement, pada tahap ini pengembahan harus mengetahui seluruh informasi mengenai kebutuhan software atau system seperti kegunaan software yang diinginkan oleh pengguna dan batasan software. Dimana teknik dalam requirement ini dengan cara observasi dan juga wawancara.

2. Design, pada tahap ini dilakukan sebelum proses coding atau pembuatan sistem. Tahap ini bertujuan untuk memberikan gambaran lengkap tentang apa yang harus dikerjakan dan

bagaimana tampilan dari sistem yang diinginkan. Sehingga dapat membantu memspesifikasikan kebutuhan hardware dan sistem, dan mendefinisikan arsitektur sistem yang akan dibuat secara keseluruhan. Dalam tahap design ini menggunakan sebuah tehnik UML (Unified Modeling Language) dengan pemodelan secara visual yang digunakan serana perancangan *system* berorientasi objek.

3. Development, tahap penulisan code dimana pembuatan software akan dipecah kedalam modul-modul kecil yang nantinya akan digabungkan dalam tahap selanjutnya. Dalam tahap ini juga akan dilakukan pemeriksaan mendalam terhadap modul yang sudah dibuat, apakah sudah memenuhi fungsi yang diinginkan atau belum. Dalam tahap development ini menggunakan sebuah freamwork dari javascript yaitu React Native untuk membangun aplikasi Mobile, sedangkan untuk Web admin dengan Freamwork PHP yaitu Codeigniter 4.

4. Testing, tahap testing dilakukan untuk menggabungkan semua modul-modul yang sudah dibuat sebelumnya. Setelah itu akan dilakukan pengujian yang bertujuan untuk mengetahui apakah software sudah sesuai dengan desain yang diinginkan dan apakah masih ada kesalahan atau tidak. Dalam tahap testing ini penulis menggunakan sebuah teknik White Box dan Black Box Testing

5. Maintenance, tahap ini merupakan tahap terakhir dalam pengembangan waterfall. Software yang sudah jadi akan dijalankan atau diperasikan oleh penggunanya. Pengguna dapat mengetahui aplikasi tersebut melalui akun sosial media Ciremai Clothing Club ini. Disamping itu dilakukan pula pemeliharaan yang termasuk : perbaikan permasalan, perbaikan implementasi unit sistem, peningkatan jasa sistem sesuai kebutuhan baru

1.9.3 Metode Penyelesaian Masalah

Berdasarkan tujuan dari penelitian skripsi ini adalah membuat sebuah aplikasi E-Ticketing yang dapat mengecek keterangan data *expired date* tiket acara berdasarkan data dari penyelenggara disertai dengan penerapan keamanan dengan algoritma *SPECK* yang diterapkan dalam aplikasi baik dalam proses enkripsi dan deskripsi nya. Algoritma *SPECK* merupakan algoritma yang dapat melakukan enkripsi dan deskripsi berdasarkan kunci asimetris yang dimana *key public* dan *key private* itu berbeda, sehingga untuk melakukan sebuah enkripsi dan deskripsi juga dilakukan dengan rumus yang berbeda. Dalam algoritma *SPECK* mempunyai tiga tahapan proses, proses pertama yaitu pembangkitan kunci (*key schedule*), proses kedua yaitu proses enkripsi, dan proses terakhir yaitu proses deskripsi. Berdasarkan salah satu jurnal mengenai implementasi algoritma *SPECK* mengatakan bahwa langkah pertama dalam proses algoritma *SPECK* dimulai dari mengimputkan

sebuah *plaintext* dan *ciphertext* kemudian input *key,* dimana *key* tesebut akan digunakan dalam proses enkripsi dan deskripsi. Dalam proses perhitungan *key schedule*, akan menghasilkan sebuah *key* sebanyak *round* yang telah ditentukan berdasarkan jenis *SPECK* yang akan digunakan pada proses enkripsi dan deskripsi. Kemudian terdapat juga subproses enkripsi dan deskripsi data dengan menggunakan algoritma *SPECK*. *S*elanjutnya proses terakhir adalah mengeluarkan hasil *ciphertext* atau *plaintext* untuk masing-masih proses enkripsi dan deskripsi.

Algoritma *SPECK* memiliki 10 variasi berdasarkan block *size* dan *key size.* Block *size* terdiri dari 32-bit, 48-bit, 64-bit, 96-bit, dan terakhir 128-bit. Sedangkan untuk *key size* terdiri dari 64-bit, 72-bit, 96-bit, 128-bit, 144-bit, 192-bit, dan 256-bit. Dalam masing-masing block *size* memiliki pasangan *key size* nya sendiri. Berikut adalah notasi atau operasi perhitungan dan tabel variasi algoritma *SPECK* dan parameter yang akan digunakan :

$\oplus$	:	Operator *bitwise* atau XOR
n	:	Ukuran panjang *word* pada algoritma *SPECK* (n = 16, 24, 32, 48, dan 64).
$+$	:	Operator penjumlahan atau *addition modulo* 2^n
$-$	:	Operator pengurangan atau *substaction modulo* 2^n
S^-	:	Rotasi ke kanan sebanyak S bit
S	:	Rotasi ke kiri sebanyak S bit

r : Jumlah round

Tabel 1.1 Tabel Varian algoritma SPECK dan parameter yang digunakan

Block *Size* 2n	Key *Size* *mn*	Word Size *n*	Key Word *m*	Rot α	Rot β	Rounds r
32	64	16	4	7	2	22
48	72	24	3	8	3	22
48	96	24	4	8	3	23
64	96	32	3	8	3	26
64	128	32	4	8	3	27
96	96	48	2	8	3	28
96	144	48	3	8	3	29
128	128	64	2	8	3	32
128	192	64	3	8	3	33
128	256	64	4	8	3	34

Keterangan :

Block Size 2n : Ukuran Block

Key Size : Ukuran Kunci

Word Size : Ukuran Kata

Key Word : Jumlah Kata Kunci

Rot α : Rotasi ke kiri

Rot β : Rotasu ke kanan

Rounds : Jumlah Ronde

Penjabaran dalam proses utama pada algortima *SPECK* :

1. Proses Pembangkitan kunci (*key schedule*)

Proses pembangkitan atau *key schedule* pada algoritma *SPECK* digunakan untuk membuat kunci pada setiap rounde. Kunci yang telah dibuat akan digunakan pada setiap funsi rounde, dalam proses ini terdapat 2 variable yang akan proses, yaitu ki dan li. Proses li dilakukan dengan rumus :

$$li + m\text{-}1 = (ki + S^{-a}) \oplus i$$

Pada rumus diatas, nilai m adalah nilai word pada *key*. Nilai i adalah rounde yang digunakan sesuai dengan jenis *SPECK* yang digunakan. Pada nilai i akan terus bertambah dari 0 sampai jumlah rounde jenis *SPECK* yang digunakan. Proses nilai li + m-1 didapatkan dengan cara melakukan *modulo addition* 2^n antara ki dengan li yang telah dilakukan rotasi ke kanan sejumlah round jenis *SPECK* yang diambil (α bit). Selanjutnya hasil dari *modulo addition* 2^n akan di XOR kan dengan jumlah rounde (i). Untuk mendapatkan nilai ki, dilakukan dengan rumus sebagai berikut :

$$ki+1 = S\,\beta\, ki \oplus li + m\text{-}1$$

Pada rumus diatas, nilai ki+1 didapatkan dengan cara melakukan operasi *bitwise* atau XOR antara ki yang telah dilakukan rotasi ke kiri sebanyak β bit dengan nilai li + m-1 yang di dapat dari rumus sebelumnya. Kedua rumus tersebut akan dilakukan perulangan sebanyak jumlah rounde jenis *SPECK* yang digunakan. Berikut proses pembangkitan kunci sebagai berikut :

Input : $k_{(mn)}$

Output : $k_{0,.....,kT-1}$

Proses :

- $k_{0(n)} \mid l_{0(n)} \mid ... \mid l_{m-2(n)} \longleftarrow k_{(mn)}$
- Untuk i = 1 sampai dengan T-1

  $tmp \longleftarrow (k_1 + (S^{-a}\ l_0)) \oplus$ i

  $k_{i+1} \longleftarrow (S^{\beta}\ k_1) \oplus tmp$

- Output : $k_{0(n)} \mid k_{1(n)} \mid ... \mid k_{T-1(n)}$

Sumber : Sulistyowati, K.D, et al (2019) [6]

2. Proses Enkripsi

Proses enkripsi berfungsi untuk mengubah sebuah *plaintext* menjadi sebuah *ciphertext* dengan memanfaatkan kunci yang telah dibuat pada proses *key schedule.* Pada proses enkripsi ini sama hal nya dengan proses *key schedule* dengan membuat rumus proses enkripsi yang ditunjukkan pada persamaan dibawah ini :

R_k (x,y)= $(S^{-a}$x + y)) $\oplus$ k,

S^{β}y$\oplus$ $(S^{-a}$x + y) $\oplus$ k

Pada proses enkripsi ini, dimulai dari membuat sebuah putaran sebanyak T-1, dilanjut dengan mengolah sebuah nilai x dengan melakukan sebuah pergeseran ke kanan pada nilai x sebanyak alfa (α) kali. Dalam mengelola nilai y, lakukan pergeseran ke kiri

pada nilai y sebanyak beta (β) kal. Berikut proses enkripsi dapat dilihat dibawah ini :

Input : $X_{(2n)}; k_0 \ldots, k_{T-1}$

Output : $Y_{(2n)}$

Proses :

- $X_{0(n)} \mid X_{1(n)} \longleftarrow X_{(2n)}$
- Untuk i = 1 sampai dengan T-1

  $X_0 \longleftarrow ((S^{-a} X_0) + X_1) \oplus k_i$

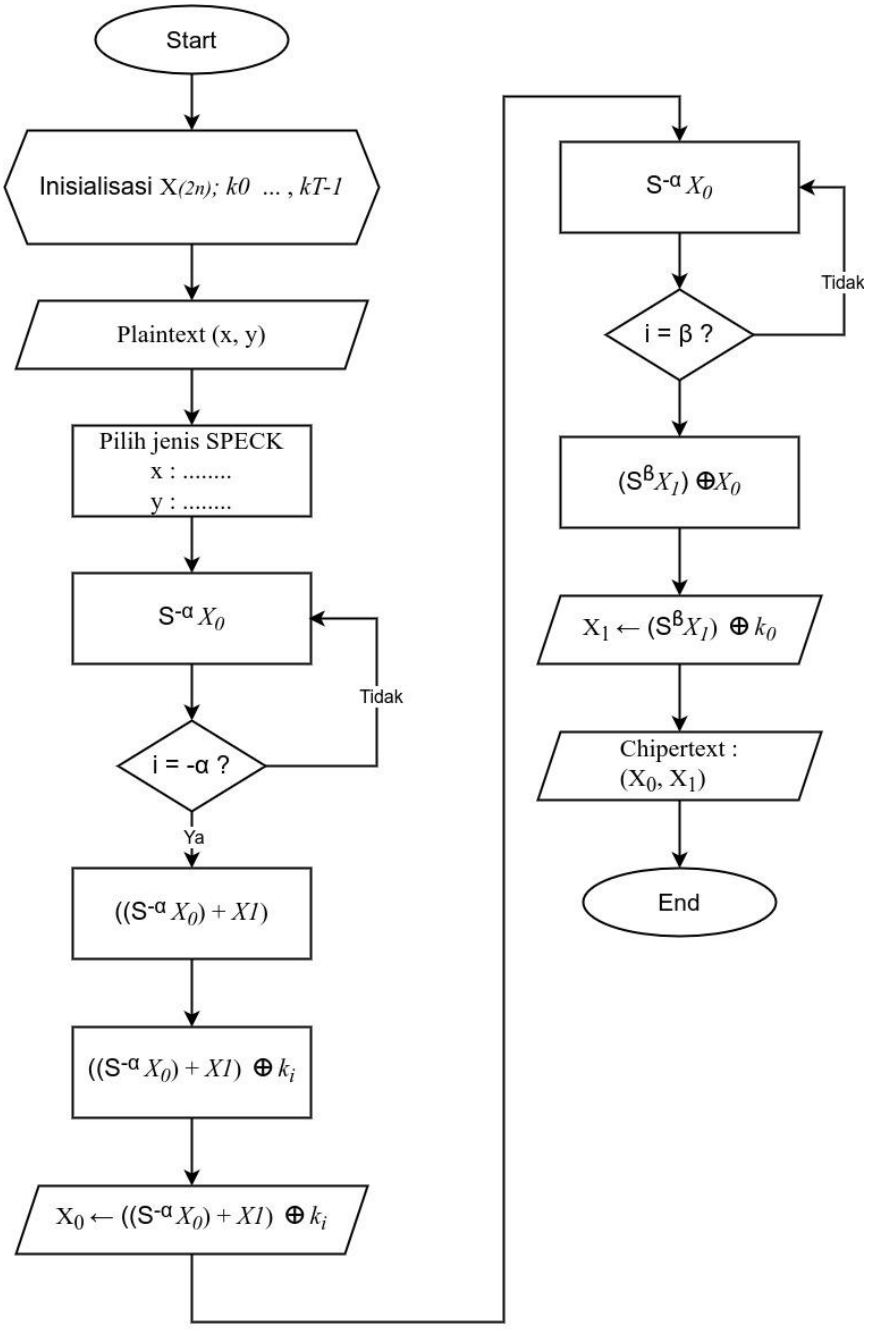
  $X_1 \longleftarrow (S^{\beta} X_1) \oplus X_0$
- Output : $Y_{(2n)} \longleftarrow X_{0(n)} \mid X_{1(n)}$

Sumber : Diadaptasi dari Sulistyowati, K.D, et al (2019) [6]

Penjelasan proses enkripsi adalah sebagai berikut :

1. Pada X_0 mengalami *circular shift* bit ke kanan sebanya S^- kali tergantung jenis *SPECK* yang diambil.
2. Hasil pergeseran di *modulo addition* dengan X_1.
3. Hasil *modulo addition*, di XOR kan dengan k_i dan akan menghasilkan nilai X_0.
4. Pada X_1 mengalami circular shift sebanya S kali ke kiri tergantung jenis SPECK yang diambil.
5. Hasil pergeseran di XOR kan dengan X_0.
6. Dilakukan dengan dengan jumlah *round* yang telah ditetapkan dalam tabel algoritma *SPECK*.

Untuk flowchart proses enkripsi algoritma SPECK dapat dilihat pada Gambar 1.2



Gambar 1.2 Flowchart Enkripsi pada algoritma SPECK

Sumber : Pseudocode Sulistyowati, K.D, et al (2019) [6]

3. Proses Deskripsi

Proses deskripsi berfungsi untuk mengubah hasil dari *chipertext* menjadi *plaintext*. Perbedaan dari proses enkripsi dengan deskripsi yaitu pada proses deskripsi, *key scheduling* dilakukan secara dibalik mulai dari round paling akhir ke round paling awal dengan memanfaatkan *modulo substraction.* Dalam proses deskripsi ini mempunyai rumus sebagai berikut :

$$R_k^{-1}(x,y) = S^a((x \oplus k)) - S^{-\beta}(x \oplus y)),$$

$$S^{-\beta}(x \oplus y)$$

Berikut adalah proses deskripsi dapat dilihat dibawah ini :

Input : $Y_{(2n)}; k_0 \ldots, k_{T-1}$

Output : $X_{(2n)}$

Proses :

- $Y_{0(n)} \mid Y_{1(n)} \longleftarrow Y_{(2n)}$
- Untuk i = 1 sampai dengan T-1

  $Y_0 \longleftarrow S^a((Y_0 \oplus k_{T-1})) - Y_1))$

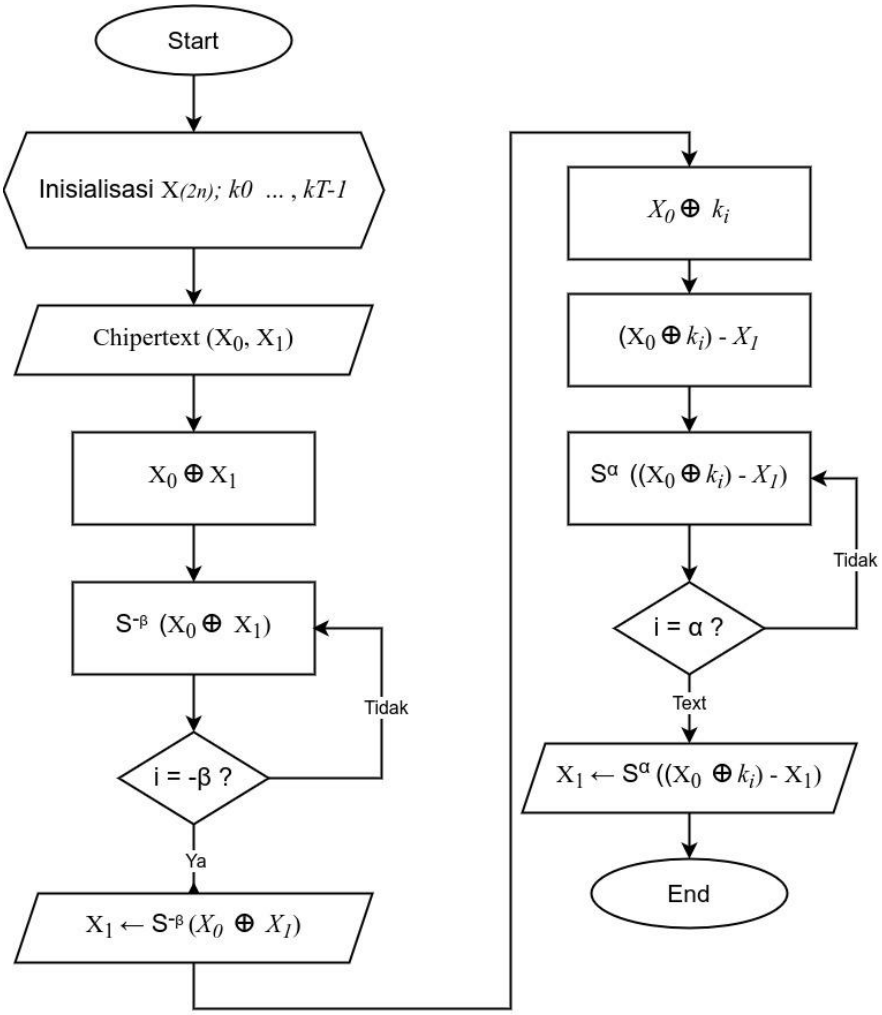
  $Y_1 \longleftarrow S^\beta (Y_0 \oplus Y_1)$
- Output : $X_{(2n)} \longleftarrow Y_{0(n)} \mid Y_{1(n)}$

Sumber : Diadaptasi dari Sulistyowati, K.D, et al (2019) [6]

Penjelasan proses enkripsi adalah sebagai berikut :

1. Pada Y_0 akan di XOR kan dengan K_{T-1}.
2. Hasil XOR dari Y_0 akan dilakukan *circular shift* ke kiri sebanyak S kali tergantung dengan jenis yang algoritma *SPECK*.
3. Hasil pergeseran akan di *modulo substruction* dengan Y_1 dan akan menghasilkan Y_0.
4. Hasil Y_0 yang di *modulo substruction* akan di XOR kan dengan Y_1.
5. Hasil XOR akan dilakukan *circular shift* ke kanan sebanyak S^- kali tergantung dengan jenis algoritma *SPECK*.
6. Dilakukan dengan dengan jumlah *round* yang telah ditetapkan dalam tabel algoritma *SPECK*.

Untuk flowchart proses enkripsi algoritma SPECK dapat dilihat pada Gambar 1.3



Gambar 1.3 Flowchart Deskripsi pada algoritma SPECK

Sumber : Pseudocode Sulistyowati, K.D, et al (2019) [6]

1.10 Jadwal Penelitian

Jadwal pelaksanaan penelitian dibuat dengan tahapan yang jelas dalam bentuk bar chart

Tabel 1.2 Tabel Varian algoritma SPECK dan parameter yang digunakan

Kegiatan	Bulan 2023															
	September				Oktober				November				Desember			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Penyusunan Proposal																
Pembuatan Data dan Studi Pustaka																
Seminar Proposal																
Analisis Data																
Design System																
Pembuatan Program																
Testing Program																
Pelatihan User																
Implementasi Program																
Dokumentasi																

1.11 Sistematika Penelitian

BAB I : PENDAHULUAN

Pada bab ini berisi tentang latar belakang masalah, identifikasi masalah, rumusan masalah, batasan masalah, tujuan penetlitian, manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II : LANDASAN TEORITIS

Pada bab ini berisi tentang penjelasan teori-teori yang relevan dan melandasi penulisan skripsi ini.

BAB III : ANALISA DAN PERANCANGAN

Pada bab ini berisi tentang deskripsi sistem, analisis kebutuhan dalam pembangunan sistem serta perancangan sistem yang dikembangkan.

BAB IV : IMPLEMENTASI DAN PENGUJIAN

Pada bab ini berisi tentang merancangbangun sitem dari hasil analisi dan perancangan yang sudah dibuat, serta menguji sistem untuk menemukan kelebihan dan kekurangan pada sistem yang dibuat.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini berisi tentang kesimpulan yang diperoleh dari hasil pengujian sistem, serta saran yang diharapkan dapat bermanfaat dalam pengembangan sistem selanjutnya.