**Bab I**

* 1. **Latar Belakang**

Menjaga keamanan data merupakan hal yang sangat penting, terutama bagi pengguna yang sering berbagi informasi rahasia. Oleh karena itu, perlu dilakukan proses penyandian data agar tidak dapat diakses oleh pihak yang tidak berwenang. Salah satu cara untuk meningkatkan keamanan data adalah dengan menggunakan kriptografi, yaitu ilmu yang mempelajari cara menjaga keamanan pesan atau data saat dikirimkan dari pengirim ke penerima tanpa gangguan dari pihak ketiga. Salah satu teknik kriptografi yang digunakan adalah mengenkripsi pesan menjadi karakter acak yang tidak dimengerti oleh pihak yang tidak berwenang, dan untuk mendapatkan pesan asli, dilakukan proses mendeskripsi dengan kunci yang tepat.

Puslitbang Polri adalah singkatan dari Pusat Penelitian dan Pengembangan Polri yang berada di Lembaga pemerintah yaitu Polisi Republik Indonesia (POLRI). Pusat Penelitian dan Pengembangan (Puslitbang) adalah elemen penting dalam penelitian, evaluasi, dan pengembangan di tingkat Mabes Polri yang dikelola oleh Kapolri. Tugas utama Puslitbang adalah merencanakan dan menyusun program penelitian, evaluasi, dan pengembangan, baik dalam pembinaan maupun operasional kepolisian melalui kegiatan inovatif dan rekayasa, serta melakukan pengawasan dan uji coba terhadap materiil, fasilitas, dan layanan yang digunakan oleh satuan kerja kepolisian lainnya dalam organisasi.

Puslitbang Polri Sebagai kantor Lembaga pemerintah yang memiliki banyak data penting, salah satunya data anggota. Data penelitian tersebut hanya di simpan di komputer atau di file biasa tidak ada kemanan yang lebih untuk mengamankan data tersebut, sehingga rentannya kehilangan data tersebut. Data tersebut harus memiliki sistem keamanan yang baik, karena data tersebut sangatlah penting dan tidak boleh sampai hilang. Puslitbang Polri tidak memiliki sistem keamanan data yang baik sekarang, sehingga bisa terjadi kebocoran data yang dilakukan oleh pihak yang tidak bertanggung jawab dan mudah di akses oleh orang lain.

Agar Puslitbang Polri tidak mengalami dampak yang merugikan, perlindungan perlindungan data penting harus dilakukan dengan cermat. Agar tidak ada kehilangan data atau penyalahgunaan data tersebut, sehingga dibutuhkan sistem keamanan file pada Puslitbang Polri. Dengan menerapkan kriptografi AES-128 Berbasis web dapat memastikan bahwa data tersebut terlindungi dan aman.

PT. Capella Medan adalah sebuah perusahaan swasta yang bergerak di bidang otomotif di wilayah Sumatera Utara. Di perusahaan ini, upah yang diterima karyawan sesuai dengan UMR setiap bulannya, dan pemberian insentif dilakukan setiap tahunnya sesuai dengan kedisiplinan dan semangat kerja karyawan, staf, dan teknisi. Data upah karyawan merupakan salah satu informasi rahasia yang hanya dapat diakses oleh bendahara atau kepala kantor. Oleh karena itu, perusahaan berusaha untuk mengamankan data tersebut agar terhindar dari penyalahgunaan atau manipulasi data oleh pihak yang tidak berhak yang dapat menyebabkan kerugian pada perusahaan. (Prayudha, 2019)

Implementasi kriptografi algoritma IDEA pada kemanan data teks berbasis android(Informasi & Logika, 2021). Impementasi Kriptografi pada pengamanan data pembayaran piutang pelanggan menggunakan Vigenere Cipher(Risna et al., 2022). Penerapan Kriptografi untuk pengamanan data penjualan sepatu dengan metode AES(Advanced Encryption Standard)(Putra et al., 2023). Sebelumnya, telah dilakukan studi mengenai kasus yang sama dan beberapa penelitian tersebut dijadikan sebagai rujukan untuk penelitian ini. Beberapa jurnal yang digunakan sebagai acuan telah disebutkan di atas. Namun, penelitian ini menggunakan metode yang berbeda dari penelitian sebelumnya. Metode yang digunakan dalam penelitian ini adalah AES-128. Kelebihan menggunakan AES-128 sendiri yaitu dari segi jenis kunci yang simetris maka kecepatan operasi lebih baik jika dibandingkan dengan asimetrik dan mempunyai panjang kunci paling sedikit yaitu 128 bit, maka AES memiliki ketahanan yang kuat terhadap serangan exhaustive key search atau teknik dasar dari mencoba setiap kemungkinan kunci secara berturut-turut hingga kunci yang benar ditemukan.

* 1. **Rumusan Masalah**

Berdasarkan paparan latar belakang sebelumnya, maka rumusan masalah yang dapat disusun adalah:

1. **B**agaimana meningkatkan keamanan data di Puslitbang Polri untuk meminimalisir terjadinya kebocoran data ?
2. Bagaimana menerapkan modifikasi algoritma kriptografi Advanced Encryption Standard (AES-128) dan menggunakan Base 64 untuk enkripsi pada Puslitbang Polri ?
3. Metode apakah yang dapat digunakan untuk mengamankan atau melindungi dari kehilangan data atau pencurian data ?
   1. **Batasan Masalah**

Adapun batasan masalah pada penelitian adalah sebagai berikut:

1. Algoritma yang digunakan adalah modifikasi penggabungan algoritma Advanced Encryption Standard (AES 128) dan Base 64
2. Bahasa pemograman yang digunakan dalam aplikasi yaitu PHP
3. Dokumen yang digunakan dalam aplikasi ini yaitu : .docx, .pdf, .pptx, .xlsx, .txt
4. Dalam melakukan proses enkripsi dan dekripsi, ukuran file hanya di batasi tidak lebih dari 3mb
   1. **Tujuan Penelitian**

Dengan mengetahui pokok dari permasalahan diatas, maka dikembangkanlah suatu aplikasi keamanan data dengan pengimplementasian AES128, dengan tujuan:

1. Mengamankan data ….
2. Dengan adanya cara pengamanan ini, pengembang aplikasi yang menggunakan bahasa pemograman PHP dapat menyembunyikan skrip PHP agar tidak mudah disalin, diubah oleh orang yang tidak berhak.
3. Dengan menggunakan kriptografi AES-128 berbasis web data penelitian pada Puslitbang Polri akan aman dan terlindungi.
   1. **Manfaat**

Adapun beberapa manfaat dari penelitian ini adalah sebagai berikut:

1. Manfaat untuk instansi, hasil dari penelitian dapat memberikan keamanan pada file-file penting yang tersimpan dengan baik, Serta menambah wawasan dan edukasi baru mengenai algoritme kriptografi ini.
2. Manfaat untuk bidang ilmu, dapat menjadi referensi bagi penelitian-penelitian selanjutnya dalam bidang keamanan suatu file dengan menggunakan algoritme kriptografi.
3. Manfaat untuk masyarakat, dengan dilakukannya pengujian pada sistem keamanan file pada bidang ini, penggunaan algoritme AES-128 dapat digunakan dalam berbagai bidang lain dengan baik dan bijak.
   1. **Sistematika Penulisan**

Sistematika penulisan bertujuan untuk memberikan penjelasan guna mempermudah pembaca dalam memahami isi secara garis besar. Sistematika yang digunakan dalam penulisan laporan Tugas Akhir ini adalah sebagai berikut:

**BAB I PENDAHULUAN**

Meguraikan bagaimana pendahuluan yang berisikan tentang gambaran umum yang meliputi latar belakang masalah, tujuan penulisan, ruang lingkup/batasan masalah, metode penelitian dan sistematika penulisan.

**BAB II LANDASAN TEORI**

Bab ini berisikan pembahasan tentang landasan teori yang berhubungan dengan Tugas Akhir mulai dari topik yang bersifat khusus, sampai dengan yang mendukung perancangan dan sistematika penulisan, buku-buku, internet atau referensi lainnya dipergunakan sebagai acuan atas sistem yang dibuat.

**BAB III METODOLOGI PENELITIAN**

Bab ini berisi tahapan dari metodologi yang diterapkan terkait permasalahan dan solusi yang dibahas dalam penelitian ini. Hal yang dibahas berupa data Penelitian, Penerapan Metode, Rancangan Pengujian, Rancangan Basis Data, Rancangan Menu, Rancangan Layar.

**Bab IV HASIL DAN PEMBAHASAN**

Bab ini beriskan penjelasan mengenai implementasi dan uji coba solusi, Seperti lingkungan percobaan, data masukan, langkah pengujian, dan evaluasi solusi mengenai kelebihan dan kekurangan program.

**BAB V PENUTUP**

Bab ini merupakan kesimpulan yang diambil dari pembahasan topik Tugas Akhir, serta saran yang bertujuan untuk peningkatan topik Tugas Akhir yang bisa dibahas di masa mendatang.

**BAB II**

**LANDASAN TEORI**

1. **Kriptografi**
2. **Sejarah Kriptografi**

Sejarah kriptografi adalah sejarah kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau menggunakan bantuan alat mekanik yang sangat sederhana. Secara umum algoritma kriptografi klasik dikelompokkan menjadi dua kategori, yaitu :

1. Algoritma Cipher Transposisi, dilakukan dengan cara mengubah susunan huruf-huruf yang ada didalam suatu pesan.
2. Algoritma Cipher Substitusi, dilakukan dengan cara mengganti setiap huruf atau kelompok huruf yang ada didalam suatu pesan dengan sebuah huruf atau kelompok huruf berbeda.

Kedua pengelompokan algoritma kriptografi ini karena sejarah kriptografi klasik mencatat penggunaan algoritma cipher transposisi oleh tentara Sparta di Yunani pada awal tahun 400 SM saat menggunakan suatu alat yang disebut scytale. Alat ini terdiri dari sebuah kertas panjang seperti pita dari daun papyrus yang dililitkan pada sebuah tabung selinder yang diameter tertentu. Diameter tabung selinder ini yang menyatakan kunc penyandian pesan. Pesan yang dikirimkan ditulis secara horizontal, baris per baris. Bila pita kertas ini dilepas dari tabung selinder, maka huruf-huruf dalam pita kertas telah tersusun acak membentuk pesan rahasia. Untuk membaca pesan, si penerima harus melilitkan kembali pita kertas tersebut pada tabung selinder yang berdiameter sama dengan diameter tabung selinder si pengirim.(*51-172-1-PB*, n.d.)

1. **Definisi Kriptografi**

Kata kriptografi berasal dari bahasa Yunani “kryptos” yang berarti menyembunyikan, dan graphein yang berarti menulis. Kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. (Munir, n.d.)

1. **Tujuan Kriptografi**

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu:

1. Kerahasiaan adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
2. Integritas data adalah berrhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
3. Autentifikasi adalah berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, dan waktu pengiriman.
4. Nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman atau terciptanya suatu informasi oleh yang orang mengirimkan atau membuat.(Dwi Nurcahya, 2022)
5. **Base64**
6. **Sejarah Base64**

Base64 sejatinya bukan enkripsi, namun hanyalah sebuah standar penyandian (encoding). Sejarah Base64 berawal dari surat elektronik (email). Pada waktu itu, email dikirim dengan protokol SMTP (simple mail transfer protocol) ke mail server kita, lalu dikirim ke mailbox orang yang dituju di mail server tujuan. "Protokol" adalah tata cara mesin (komputer) saling berkomunikasi via jaringan. Supaya email bisa sampai ke orang yang dituju, ia harus mengunduhnya terlebih dahulu. Proses download email menggunakan protokol POP (post office protocol). Saat ini POP sudah mencapai versi 3 sehingga disebut POP3. Alternatif yang lebih baik dari POP adalah IMAP (internet mail access protocol). IMAP sudah mencapai versi 4. Baik POP maupun SMTP adalah protokol berbasis teks. Encoding yang digunakan adalah ASCII. Tidak masalah bila kita hanya ingin mengirim email teks saja. Masalah muncul ketika email berkembang, menjadi punya kemampuan untuk mengirim lampiran (attachment). Apa yang dilampirkan adalah file, dan file ini bisa file apa saja — termasuk file biner. Kebetulan POP dan SMTP sama dalam hal terminasi pesan. Mereka menggunakan deretan karakter CR LF . CR LF (carriage return – line feed – tanda titik – carriage return – line feed) sebagai akhir dari pesan. Apa yang terjadi bila file biner kita di tengah-tengah terdapat byte-byte berikut: 0D 0A 2E 0D 0A? Nilai rangkaian byte tadi adalah kode ASCII dari CR LF . CR LF sehingga server akan menganggap pesan yang dikirim berhenti sampai di sana. File yang kita lampirkan kita akan putus di tengah.

Untuk mengatasi masalah ini, dibuatlah penyandian Base64. Cara kerja Base64 adalah sebagai berikut:

* Kelompokkan pesan setiap 3 karakter (3 byte = 24 bit). Bila terdapat sisa di akhir, tambahkan (padding) bit 0 sehingga panjangnya genap 24 bit.
* Pecah 24 bit tadi menjadi 4 kelompok yang masingmasing beranggotakan 6 bit.
* Setiap kelompok sekarang punya 26 kemungkinan susunan bit, berarti ada 26 = 64 karakter tersedia untuk merepresentasikan 6 bit ini. Petakan setiap kelompok dengan karakter yang terdapat dalam tabel. Karakter yang dipakai adalah huruf latin A-Z, huruf kecil a-z, dan angka 0-9. Semua berjumlah 62. Dua sisanya memakai simbol + dan / sehingga totalnya 64.(Adriansyah, n.d.)

1. **Definisi Base64**

Algoritma Base64 merupakan salah satu algoritma untuk Enkripsi dan Dekripsi suatu data ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metode yang digunakan untuk melakukan enkripsi terhadap data binary. Karakter yang dihasilkan pada transformasi Base64 ini terdiri dari A..Z, a..z dan 0..9, serta ditambah dengan dua karakter terakhir yang bersimbol yaitu + dan / serta satu buah karakter sama dengan (=) yang digunakan untuk penyesuaian dan menggenapkan data binary atau istilahnya disebut sebagai pengisi pad. Karakter simbol yang akan dihasilkan akan tergantung dari proses algoritma yang berjalan.(Haris, 2020)

1. **Tujuan Base64**

Tujuan base64 adalah untuk memudahkan melakukan enkripsi dan dekripsi data dalam encoding kriptografi yang didasarkan pada bilangan dasar 64. Dan file atau data bisa di pastikan aman dikarenakan file di enkrip dan dekripsi.

1. **Algoritma kriptografi**

Algoritma kriptografi simetris menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Skema enkripsi akan disebut symmetric-key apabila pasangan kunci untuk proses enkripsi dan dekripsinya sama. Algoritma kriptografi simetris dibagi menjadi dua kategori yaitu algoritma aliran (stream cipher) dan algoritma blok (block cipher). (Kurniadi & Ariyus, n.d.)

1. **Algoritma Simetris**

Algoritma simetris memiliki kelebihan mengonsumsi daya komputasi komputer yang kecil dan bekerja secara cepat pada pengenkripsian data. Kriptografi kunci simetris memiliki dua mode sebagai block cipher atau sebagai stream cipher. Dalam block cipher semua data dibagi menjadi beberapa blok dan kunci akan diberikan tergantung dari panjang blok, sedangkan dalam stream cipher data dibagi menjadi -bits kecil yang diacak lalu dienkripsi.(Suhandinata et al., 2019)

1. **Algoritma Asimetris**

Algoritma asimetris penting karena dapat digunakan untuk membagikan kunci enkripsi atau data lainnya secara aman meskipun kedua belah pihak tidak memiliki kesempatan untuk menyetujui kunci privat. Kunci yang digunakan pada algoritma asimetris umumnya panjang dimana meningkatkan keamanan data yang dikirim, setidaknya berukuran 3000-bit atau lebih untuk mencapai tingkat keamanan algoritma simetris 128-bit.(Suhandinata et al., 2019)

1. **Algoritma Advanced Encryption Standard (AES)**

Urutan data yang diolah oleh algoritma AES terdiri dari 128 bit. Urutan data tersebut dapat disebut sebagai blok data atau plaintext yang akan diubah menjadi ciphertext. Cipher key yang digunakan pada algoritma AES terdiri dari key dengan ukuran 128 bit, 192 bit, atau 256 bit. Perbedaan ukuran kunci akan mempengaruhi jumlah round yang akan digunakan pada algoritma AES. Di bawah ini tertera pada gambar 2.4 yang menunjukkan jumlah putaran (Nr) yang perlu diterapkan pada setiap ukuran kunci.(Eka Putri et al., 2021)

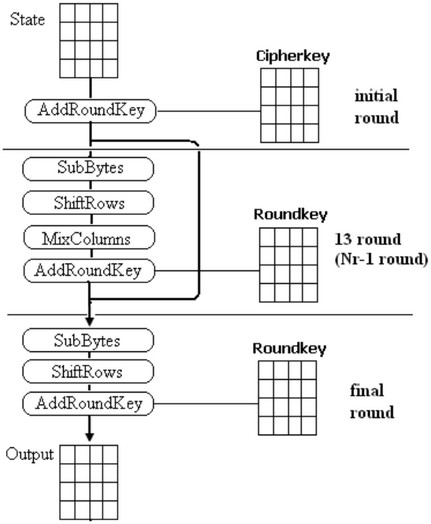


**Gambar 2.1 Jumlah Putaran AES** (Eka Putri et al., 2021)

1. **Enkripsi Algoritma Advanced Encryption Standard (AES)**

Prosedur penyandian AES terdiri dari empat jenis perubahan byte, yakni SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey. Di awal proses penyandian, input yang telah disalin ke dalam keadaan akan melalami perubahan byte AddRoundKey. Kemudian, keadaan akan mengalami perubahan SubBytes, ShiftRows, MixColumns, dan AddRoundKey berulang kali sebanyak Nr. Prosedur ini dalam algoritma AES disebut sebagai fungsi putaran. Putaran terakhir sedikit berbeda dari putaran sebelumnya di mana pada putaran terakhir, keadaan tidak mengalami perubahan MixColumns.(Eka Putri et al., 2021)

Proses Enkripsi AES dapat dilihat pada gambar 2.5 berikut ini.



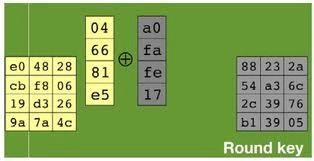
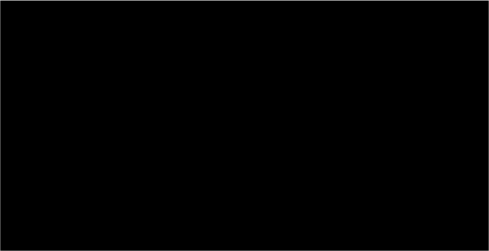
**Gambar 2.2 Proses Enkripsi AES-128** (Eka Putri et al., 2021)

Secara umum, langkah-langkah enkripsi AES-128 dengan kunci 128 bit adalah sebagai berikut.(Eka Putri et al., 2021)

1. AddRoundKey

Pada akhirnya setiap elemen state mengalami perubahan nilai sesuai dengan round key yang ditambahkan. Pada tahap enkripsi dan dekripsi AES, langkah AddRoundKey dilakukan dengan cara yang sama. Round key akan di-XOR-kan dengan state yang sedang diproses. Setiap round key terdiri dari sejumlah Nb kata, dan setiap kata akan dijumlahkan dengan kata atau kolom yang sesuai dalam state sehingga :

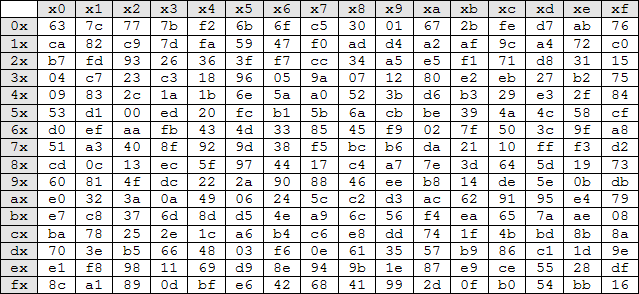
[s’o,c , s’1,c , s’2,c , s’3,c ] [so,c , s1,c , s2,c , s3,c] [wround\*Nb+c ] untuk 0≤c≤Nb [ wi merupakan kata dari kunci yang sesuai untuk i = round\*Nb+c. Transformasi AddRoundKey dilakukan pada proses enkripsi saat round pertama yaitu round = 0. Untuk round selanjutnya, round akan bertambah satu. Sedangkan pada proses dekripsi, AddRoundKey dilakukan saat round terakhir yaitu round = 14. Untuk round selanjutnya, round akan berkurang satu. Untuk memudahkan pemahaman, dapat dilihat pada gambar 2.6 dimana ciphertext terletak di sebelah kiri dan roundkey terletak di sebelah kanan. XOR dilakukan pada setiap kolom, dimulai dari kolom-1 ciphertext yang di-XOR dengan kolom-1 roundkey, dan seterusnya.



**Gambar 2.3 Add Round Key** (Eka Putri et al., 2021)

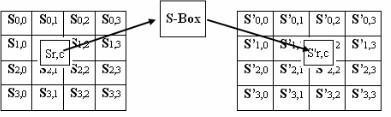
1. SubBytes

SubBytes adalah transformasi byte dimana setiap elemen pada state akan dihubungkan dengan menggunakan sebuah tabel subtitusi (S-Box). Pada gambar 2.7 tabel subtitusi S-Box akan dipaparkan.



**Gambar 2.4 Tabel S-BOX** (Eka Putri et al., 2021)

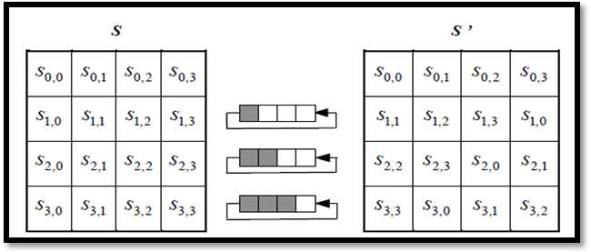
Bagi setiap byte dalam array state, jika Տ[r,c]=xy, di mana xy adalah digit heksadesimal dari nilai Տ[r,c], nilai substitusinya, yang dinyatakan sebagai Տ[r,c], adalah elemen dalam tabel substitusi yang mempengaruhi pemetaan byte pada setiap byte dan state. Seperti pada gambar 2.8 yang akan menunjukan pengaruh pemetaan byte dalam state.



**Gambar 2.5 Pengaruh Pemetaan pada setiap byte dalam state** (Eka Putri et al., 2021)

1. ShiftRows

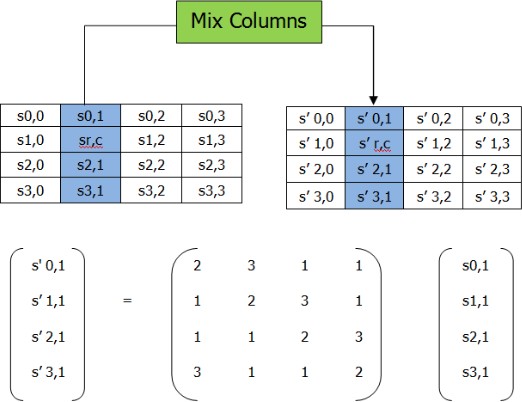
Pada intinya, Shiftrows Transformation ialah proses menggeser bit di mana bit paling kiri akan dipindahkan ke posisi paling kanan (rotasi bit). Proses pergeseran ShiftRows ditunjukan dalam gambar 2.9 berikut :



**Gambar 2.6 Transformasi ShiftRows** (Eka Putri et al., 2021)

1. MixColumns

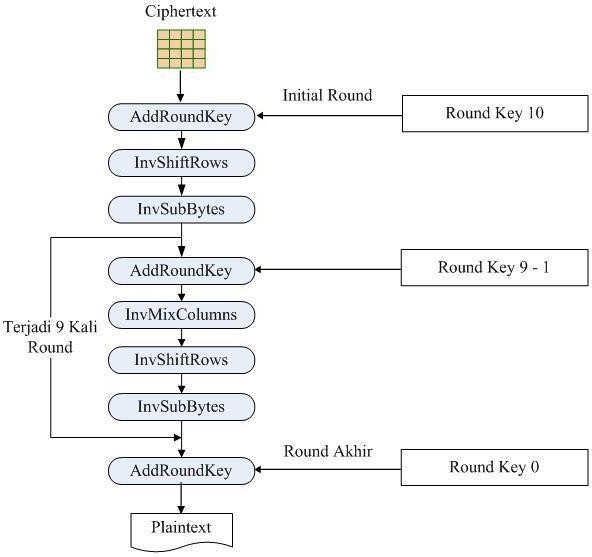
Pada langkah MixColumn mengalikan tiap elemen blok sandi dengan matriks. Tabel telah didefinisikan dan siap digunakan. Perkalian dijalankan seperti perkalian matriks biasa, yakni dengan perkalian skalar lalu hasil perkalian dua dimasukkan ke dalam blok sandi baru. Ilustrasi pada gambar 2.10 menjelaskan bagaimana perkalian ini dijalankan. Setelah semua tahapan dalam AES diuraikan, langkah berikutnya adalah menjelaskan pemanfaatan tiap proses.



**Gambar 2.7 Perkalian matriks** (Eka Putri et al., 2021)

1. Putaran Akhir: Langkah terakhir yang harus dilakukan antara lain :
2. SubBytes
3. ShiftRows
4. AddRoundKey
5. Pada tahap akhir, akan tercipta karakter atau teks dalam bentuk chipertext.
6. **Dekripsi algoritma Advanced Encryption Standard (AES)**

Untuk melakukan Dekripsi pada AES-128, diperlukan transformasi sandi yang dibalik sehingga menghasilkan sandi terbalik dengan langkah-langkah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey. Algoritma Dekripsi tertera pada gambar 2.11 di bawah ini:(Andriyanto et al., 2020)

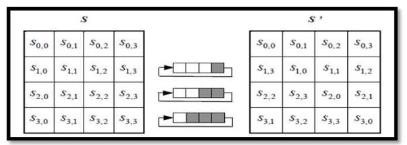


**Gambar 2.8 Proses Dekripsi AES-128** (Andriyanto et al., 2020)

Secara umum, langkah-langkah dekripsi AES-128 dengan menggunakan kunci 128 bit dapat dijelaskan sebagai berikut.(Eka Putri et al., 2021)

1. InvShiftRows

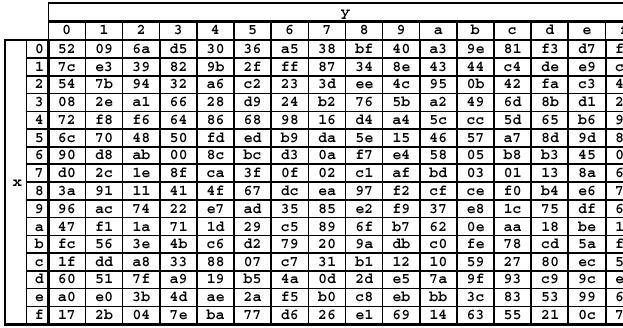
Transformasi InvShiftRows merupakan kebalikan dari transformasi ShiftRows di mana terjadi pergeseran bit ke kiri pada ShiftRows dan pergeseran bit ke kanan pada InvShiftRows. Gambar 2.12 menunjukkan ilustrasi dari transformasi InvShiftRows.(Eka Putri et al., 2021)



**Gambar 2.9 Transformasi Invshiftrows** (Eka Putri et al., 2021)

1. InvSubBytes

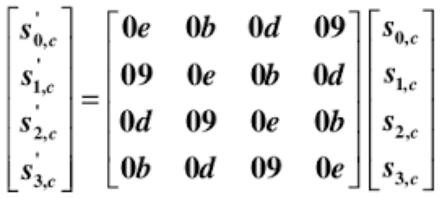
InvSubBytes merupakan perubahan bytes yang berlawanan dengan perubahan SubBytes. Dalam InvSubBytes, setiap unsur pada keadaan dipetakan dengan menggunakan tabel Inverse S-Box. Gambar 2.13 menunjukkan Inverse S-Box.(Eka Putri et al., 2021)



**Gambar 2.10 Invers S-Box** (Eka Putri et al., 2021)

1. InvMixColumns

Tiap kolom dalam state dikalikan dengan operasi matrik perkalian dalam AES. Perkalian dalam matrik dapat dituliskan pada Gambar 2.14.(Eka Putri et al., 2021)



**Gambar 2.11 Perkalian matrix Invmixcolumns**(Eka Putri et al., 2021)

Transformasi dilaksanakan dengan mengalikan setiap kolom dari susunan state dengan polinom a(x) mod (x 8 + x 4 + x 3 + x + 1). Setiap kolom dianggap sebagai polinom 4-suku pada Galois Field (GF)28. Polinom a(x) yang dipakai adalah: a(x) = {03}x3 + {01}x2 + {01}x + {02} Transformasi ini dijelaskan sebagai perkalian matriks: s(x) = a(x) s(x) dapat dilihat pada gambar 2.15.



**Gambar 2.12 Hasil Perkalian Matrix** (Eka Putri et al., 2021)

Perkalian array dengan polinom a(x) mod (x 8 +x 4 +x 3 +x+1) pada Galois Field(28 ). Mencari H0,1 H0,1 = ({02} d4) ({03} bf) 5d 30. Cara ini dapat diekuivalenkan juga dengan menggunakan gabungan operasi left shift dan operator XOR.

1. Pada tahap terakhir, akan dihasilkan karakter atau teks yang sama dengan aslinya (plaintext).