



PEMODELAN ENCODING DAN DECODING BASE64 DALAM MENYEDERHANAKAN DAN MENGAMANKAN PENGIRIMAN DATA

Andysah Putera Utama Siahaan^{1*}, Supiyandi²

¹Magister Teknologi Informasi, Universitas Pembangunan Panca Budi, Medan, Indonesia

²Teknologi Informasi, Universitas Pembangunan Panca Budi, Medan, Indonesia

e-mail: ¹andiesiahaan@gmail.com, ²supiyandi@dosen.pancabudi.ac.id

*Corresponding Author

Abstrak

Keamanan data sangat penting untuk menjaga kerahasiaan dan integritas informasi. Dalam konteks ini, Base64 merupakan salah satu metode enkripsi yang sering digunakan dalam pengiriman data melalui jaringan. Base64 mengubah data biner menjadi teks ASCII agar dapat dengan mudah ditransmisikan melalui media yang tidak mendukung transmisi data biner, seperti email. Algoritma Base64 adalah salah satu proses enkripsi yang ideal digunakan dalam transmisi data. Fungsi utama Base64 adalah mengonversi data biner menjadi karakter ASCII yang lebih sederhana. Dalam proses ini, setiap tiga byte data biner diubah menjadi empat karakter ASCII. Hal ini menyebabkan peningkatan ukuran data sekitar 33%, namun memungkinkan data untuk dikirim melalui berbagai media dengan aman dan efisien. Selain itu, Base64 juga berguna dalam menyembunyikan informasi sensitif, seperti kata sandi, karena teks hasil enkripsi tidak dapat dengan mudah dibaca oleh manusia tanpa proses dekripsi yang sesuai. Sandi teks yang diperoleh adalah serangkaian karakter yang telah dipetakan dalam tabel karakter. Tabel-tabel ini telah dirancang untuk memudahkan pengiriman data selama transmisi. Dengan menerapkan algoritma ini, kesalahan dapat dihindari, dan keamanan juga dapat terjamin.

Kata kunci—Base64, pengiriman, pengamanan, data

Abstract

Data security is crucial for maintaining the confidentiality and integrity of information. In this context, Base64 is one of the encryption methods commonly used for data transmission over networks. Base64 converts binary data into ASCII text so that it can be easily transmitted through media that do not support binary data transmission, such as email. The Base64 algorithm is one encryption process that is ideal for use in data transmission. The main function of Base64 is to convert binary data into simpler ASCII characters. In this process, every three bytes of binary data are converted into four ASCII characters. This results in a 33% increase in data size, but enables data to be securely and efficiently transmitted through various media. Additionally, Base64 is useful for hiding sensitive information, such as passwords, because the encrypted text cannot be easily read by humans without appropriate decryption. The obtained ciphertext is a series of characters that have been mapped in character tables. These tables are designed to facilitate data transmission during transmission. By implementing this algorithm, errors can be avoided, and security can be ensured.

Keywords— Base64, transmission, security, data

I. PENDAHULUAN

Transmisi data melalui jaringan memegang peran penting dalam sistem komunikasi modern (Salim, 2020). Memastikan keamanan dan integritas data

yang ditransmisikan sangatlah penting, terutama ketika melibatkan informasi sensitif. Salah satu tantangan mendasar dalam transmisi data adalah kebutuhan untuk mengonversi data biner ke dalam format yang dapat dengan mudah



ditransmisikan melalui protokol berbasis teks, seperti email atau HTTP (Lubis, 2018). Pengekodaan Base64 menyediakan solusi untuk tantangan ini dengan mengubah data biner menjadi format teks yang kompak dan aman untuk ditransmisikan (Supiyandi et al., 2020).

Pengekodaan Base64 bekerja dengan mewakili data biner sebagai rangkaian karakter ASCII (Rahim et al., 2018). Skema pengkodean ini menggunakan seperangkat 64 karakter cetak untuk mewakili 256 nilai yang mungkin dari grup data biner enam bit. Proses ini meningkatkan ukuran data sekitar 33% namun memungkinkannya untuk ditransmisikan dengan aman melalui protokol berbasis teks tanpa risiko korupsi data.

Penggunaan pengkodean Base64 umum dalam berbagai aplikasi, termasuk lampiran email, transmisi data melalui HTTP, dan sistem kriptografi. Ini memungkinkan transmisi data yang aman melalui jaringan publik, memastikan bahwa informasi sensitif tetap rahasia dan utuh selama transmisi.

Memahami secara lengkap prinsip-prinsip pengkodean Base64 dan aplikasinya sangat penting bagi pengembang, administrator jaringan, dan profesional keamanan cyber yang terlibat dalam transmisi dan keamanan data.

II. TEORI PENDUKUNG

A. Base64

Base64 adalah sebuah skema pengkodean yang digunakan untuk mengubah data biner menjadi representasi teks ASCII. Skema ini menggunakan 64 karakter yang terdiri dari huruf besar A-Z, huruf kecil a-z, angka 0-9, serta simbol '+' dan '/'. Penggunaan karakter '=' juga kadang-kadang digunakan sebagai padding untuk memastikan panjang data yang dapat dibagi dengan tiga.

Proses pengkodean Base64 bekerja dengan membagi data biner menjadi blok-blok 24-bit, yang kemudian dipecah menjadi empat blok 6-bit. Setiap blok 6-bit kemudian diubah menjadi karakter ASCII sesuai dengan tabel konversi Base64. Misalnya, nilai 0 hingga 25 akan diwakili oleh huruf besar A-Z, nilai 26 hingga 51 akan diwakili oleh huruf kecil a-z, nilai 52 hingga 61 akan diwakili oleh angka 0-9, dan nilai 62 dan 63 akan diwakili oleh simbol '+' dan '/' secara berurutan.

Tabel 1. Karakter Base64

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Tabel 1 merupakan tabel yang digunakan untuk mengonversi blok 6-bit menjadi karakter Base64 yang sesuai. Misalnya, jika kita memiliki blok 6-bit dengan nilai 27, maka nilai tersebut akan dikonversi menjadi karakter 'b' berdasarkan tabel di atas.

Penggunaan tabel ini sangat penting dalam proses pengkodean dan decode Base64, karena tabel ini menentukan bagaimana data biner akan diubah menjadi



teks ASCII dan sebaliknya (Sumartono et al., 2016).

Penyederhanaan dari 8 bit ke 6 bit pada karakter ASCII adalah proses mengubah representasi biner dari sebuah karakter ASCII, yang biasanya direpresentasikan dalam format 8-bit (1 byte), menjadi format 6-bit. Hal ini terkait dengan penggunaan Base64, di mana setiap karakter ASCII diubah menjadi format 6-bit untuk menghasilkan representasi yang lebih ringkas dan mudah ditransmisikan (Nugroho, 2015).

Dalam konteks Base64, penyederhanaan dari 8 bit ke 6 bit dilakukan dengan membagi 8-bit binary dari karakter ASCII menjadi dua bagian, masing-masing berukuran 6 bit. Proses ini memungkinkan setiap karakter ASCII (yang memiliki 256 kemungkinan nilai dengan 8 bit) direpresentasikan dalam format yang lebih efisien (hanya 64 kemungkinan nilai dengan 6 bit) untuk tujuan enkripsi dan transmisi data. Dengan demikian, penyederhanaan ini membantu dalam mengurangi ukuran data yang dikirim dan memperbaiki efisiensi komunikasi.

Proses decode Base64 adalah kebalikan dari proses pengkodean. Karakter ASCII dari data Base64 diubah kembali menjadi blok-blok 6-bit, yang kemudian digabungkan menjadi blok-blok 8-bit dan dikonversi kembali menjadi data biner asli.

Base64 sering digunakan dalam berbagai aplikasi, seperti pengiriman data melalui email, penyimpanan data gambar dalam format HTML, serta dalam pengkodean data biner dalam URL. Meskipun Base64 meningkatkan ukuran data sebesar 33% dibandingkan dengan data asli, ia sangat berguna dalam mengatasi batasan protokol yang hanya mendukung transmisi teks ASCII (Muła & Lemire, 2018).

B. Encoding

Encoding adalah proses mengonversi data dari satu bentuk ke bentuk lain yang dapat lebih cocok untuk keperluan tertentu, seperti penyimpanan atau transmisi data. Dalam konteks komputasi, encoding sering digunakan untuk mengonversi data menjadi format yang lebih efisien atau sesuai dengan standar tertentu. Salah satu contoh encoding yang umum adalah Base64, di mana data biner dikonversi menjadi teks ASCII agar dapat dengan mudah ditransmisikan melalui protokol yang hanya mendukung teks (Sumartono et al., 2016).

Encoding juga digunakan dalam berbagai konteks lain, seperti encoding karakter dalam teks (seperti ASCII atau Unicode), encoding gambar (seperti JPEG atau PNG), dan encoding audio dan video (seperti MP3 atau MPEG). Tujuan dari encoding adalah untuk mengubah data menjadi bentuk yang lebih mudah dikelola, disimpan, atau ditransmisikan, sering kali dengan mempertahankan sebanyak mungkin informasi asli.

C. Decoding

Decoding adalah proses kebalikan dari encoding, yaitu mengonversi data dari format yang telah diencode menjadi format aslinya. Decoding sering digunakan untuk mengembalikan data ke format aslinya setelah telah diencode untuk tujuan penyimpanan atau transmisi. Misalnya, dalam konteks Base64, decoding digunakan untuk mengonversi teks Base64 kembali ke data biner asli (Sumartono et al., 2016).

Decoding juga digunakan dalam berbagai konteks lain, seperti decoding karakter dalam teks (misalnya, dari Unicode ke ASCII), decoding gambar (misalnya, dari format JPEG ke data gambar asli), dan decoding audio dan video (misalnya, dari format MP3 ke data audio asli). Tujuan utama dari decoding adalah untuk mengembalikan data ke format



aslinya sehingga dapat digunakan atau diproses sesuai dengan kebutuhan aplikasi.

III. METODOLOGI PENELITIAN

Metodologi dalam pembahasan Base64 dapat mencakup beberapa langkah utama, seperti berikut:

1. **Pengertian Base64:** menjelaskan konsep dasar dari Base64, termasuk tujuan penggunaannya, bagaimana cara kerjanya, dan mengapa Base64 penting dalam transmisi data.
2. **Proses Pengkodean:** menjelaskan langkah-langkah yang terlibat dalam proses pengkodean data menjadi format Base64, termasuk pembagian data biner ke dalam blok 6-bit, konversi blok tersebut menjadi karakter Base64 menggunakan tabel konversi, dan penanganan padding jika diperlukan.
3. **Proses Dekode:** menjelaskan langkah-langkah yang terlibat dalam proses dekode data Base64 kembali menjadi data biner asli, termasuk konversi karakter Base64 kembali ke nilai 6-bit, penggabungan blok-blok 6-bit menjadi data biner, dan penanganan padding.
4. **Kelebihan dan Kekurangan:** menguraikan kelebihan dan kekurangan dari penggunaan Base64, termasuk efisiensi penyimpanan data, overhead yang dihasilkan, dan keamanan data.
5. **Perhitungan:** memberikan contoh perhitungan Base64 dalam mengirimkan data.
6. **Kesimpulan:** meringkaskan dengan menyimpulkan pentingnya Base64 dalam transmisi data dan pentingnya pemahaman tentang cara kerjanya.

Transformasi Base64 adalah salah satu algoritma untuk mengkodekan dan mendekodekan data ke dalam format ASCII,

yang didasarkan pada angka 64. Karakter yang dihasilkan dari Base64 terdiri dari "A..Z", "a..z", dan "0..9", serta dua karakter terakhir adalah "/" dan "+".

Teknik pengkodean Base64 sederhana. Ada beberapa langkah yang harus dilakukan untuk menyelesaikan algoritma Base64:

1. Cari kode ASCII dari setiap teks.
2. Cari bilangan biner 8 bit dari kode ASCII tersebut.
3. Gabungkan 8 bit terakhir menjadi 24 bit.
4. Kemudian, pecahkan 24 bit tersebut menjadi 6 bit. Ini akan menghasilkan empat pecahan.
5. Setiap pecahan dikonversi menjadi nilai desimal.
6. Terakhir, ubah nilai desimal tersebut ke indeks untuk memilih karakter konstituen dari base64 dan maksimal adalah 63 atau 64 untuk indeks.

IV. HASIL DAN PEMBAHASAN

A. *Encoding*

Bagian ini akan menganalisis algoritma Base64. Teks biasa akan dienkripsi menjadi teks sandi, kemudian didekripsi kembali menjadi teks biasa. Anggap teks biasa adalah "Putera". Teks ini terdiri dari enam karakter. Ilustrasi dalam Tabel 2 menunjukkan penjelasan contoh Base64.

Tabel 2. Hasil konversi ASCII

Index	1	2	3	4	5	6
Char	P	u	t	e	r	a
Decimal	80	117	116	101	114	97

Perhitungan:

Index 1 : P
 ASCII : 80
 Binary : 01010000



Index 2 : u
ASCII : 117
Binary : 01110101

Index 3 : t
ASCII : 116
Binary : 01110100

Index 4 : e
ASCII : 101
Binary : 01100101

Index 5 : r
ASCII : 114
Binary : 01110010

Index 6 : a
ASCII : 97
Binary : 01100001

Setelah data biner telah diperoleh untuk seluruh karakter, nilai biner dari semua karakter akan digabungkan sehingga menghasilkan:

010100000111010101110100011001
010111001001100001

Tabel 3. Hasil konversi Base64

Index	Binary 6-bit	Char
1	010100	20
2	000111	7
3	010101	21
4	110100	52
5	011001	25
6	010111	23
7	001001	9
8	100001	33

Dari tabel 2, dapat dilihat bahwa setiap karakter dalam teks "Putera" diubah menjadi representasi Base64. Proses ini mengubah teks menjadi format yang dapat dengan mudah ditransmisikan melalui

berbagai protokol yang mendukung hanya karakter ASCII.

Tabel 2 menunjukkan bit biner akhir dari contoh sebelumnya. Jumlah teks biasa adalah enam karakter. Total bit adalah 6×8 bit = 48 bit. Ke-48 bit tersebut dibagi menjadi delapan bagian karakter 6 bit. Akan ada delapan karakter dalam format Base64. Sandi teksnya adalah UHV0ZXJh berdasarkan tabel karakter Base64 pada Tabel 1.

B. Decoding

Dalam proses konversi dari format Base64 ke ASCII, langkah pertama adalah menggabungkan semua bit dari karakter-karakter Base64 menjadi satu rangkaian bit tunggal. Misalnya, jika kita memiliki data Base64 "UHV0ZXJh", kita mengonversi setiap karakter Base64 menjadi representasi biner 6-bit dan menggabungkannya menjadi satu rangkaian bit tunggal:

U = 010100, H = 000111, V = 010101, 0 = 110100, E = 011001, R = 010111, a = 001001, h = 100001

Gabungan dari representasi biner setiap karakter di atas adalah:

010100000111010101110100011001
01010111001000001

Selanjutnya, rangkaian bit tunggal ini akan dibagi menjadi blok-blok 8-bit, karena setiap karakter ASCII direpresentasikan oleh 8-bit. Oleh karena itu, kita dapat membagi rangkaian bit di atas menjadi blok 8-bit sebagai berikut:

01010000 01110101 01110100 01100101
01110010 01100001

Setiap blok 8-bit ini akan diubah menjadi karakter ASCII sesuai dengan nilai biner yang mereka wakili. Misalnya, blok



pertama 01010000 akan menjadi karakter ASCII 'P', blok kedua 01110101 akan menjadi karakter 'u', dan seterusnya. Setelah mengonversi setiap blok, kita akan mendapatkan teks ASCII yang sesuai dengan data Base64 yang awalnya telah dikodekan.

Berikut ini adalah beberapa kelebihan dari Base64:

1. Kompatibilitas:

Base64 memungkinkan data biner dikodekan ke dalam format teks ASCII, yang dapat dengan mudah ditransmisikan melalui protokol yang hanya mendukung teks.

2. Keamanan:

Base64 dapat digunakan untuk menyembunyikan informasi sensitif, karena teks hasil enkripsi tidak dapat dengan mudah dibaca tanpa proses dekripsi yang sesuai.

3. Penggunaan yang luas:

Base64 digunakan dalam berbagai aplikasi, termasuk pengiriman email, penyimpanan data gambar dalam format HTML, dan enkripsi data dalam protokol HTTPS.

Berikut ini adalah beberapa kekurangan dari Base64:

1. Peningkatan ukuran data:

Pengkodean Base64 meningkatkan ukuran data sekitar 33% dibandingkan dengan data asli, karena setiap 3 byte data diubah menjadi 4 karakter Base64.

2. Overhead:

Pengkodean dan dekode Base64 memerlukan proses tambahan yang dapat meningkatkan beban pemrosesan pada sistem.

3. Tidak cocok untuk data biner besar:

4. Base64 tidak efisien untuk data biner besar, karena dapat menghasilkan

data yang sangat besar setelah dienkrpsi.

Meskipun Base64 memiliki kelemahan, kegunaannya dalam menyembunyikan informasi sensitif dan memungkinkan transmisi data melalui protokol teks membuatnya tetap menjadi metode yang berguna dalam pengembangan aplikasi dan komunikasi digital.

V. KESIMPULAN

Base64 adalah metode pengkodean yang penting dalam transmisi data melalui jaringan, terutama ketika data biner perlu dikirim melalui protokol yang hanya mendukung teks ASCII. Metode ini mengubah data biner menjadi teks ASCII yang aman untuk ditransmisikan, meskipun dengan sedikit penambahan ukuran data.

Kelebihan dari Base64 termasuk kemampuannya untuk menyembunyikan informasi sensitif, seperti kata sandi, dan memungkinkan transmisi data melalui protokol teks. Namun, penggunaan Base64 juga memiliki beberapa kelemahan, seperti peningkatan ukuran data yang diperlukan dan potensi overhead yang dihasilkan.

Pemahaman tentang Base64 penting bagi para profesional IT, terutama dalam pengembangan aplikasi web, pengiriman email, dan pengolahan data dalam format teks. Dengan memahami prinsip dasar Base64, para profesional dapat memastikan keamanan dan integritas data yang ditransmisikan melalui jaringan.

VI. SARAN

Sebagai saran pengembangan, dapat dipertimbangkan untuk menggabungkan Base64 dengan metode enkripsi yang lebih kuat, seperti AES (Advanced Encryption Standard), untuk meningkatkan keamanan data. Dengan menggabungkan kedua metode ini, data akan dienkrpsi menggunakan AES terlebih dahulu,



kemudian hasil enkripsi AES akan diubah menjadi format Base64 sebelum ditransmisikan. Hal ini akan meningkatkan tingkat keamanan data karena data tidak hanya dienkripsi, tetapi juga diubah ke dalam format yang lebih sulit dibaca oleh manusia tanpa proses dekripsi yang benar.

Selain itu, pengembangan algoritma kompresi khusus untuk data Base64 juga bisa menjadi langkah yang menarik. Karena Base64 meningkatkan ukuran data sebesar 33%, pengembangan algoritma kompresi yang dioptimalkan untuk data Base64 dapat membantu mengurangi ukuran data yang dikirim, sehingga mengurangi beban pada jaringan dan meningkatkan efisiensi transmisi data.

Terakhir, untuk pengembangan lebih lanjut, bisa dipertimbangkan untuk mengembangkan metode enkripsi yang lebih ringan namun aman untuk menggantikan Base64 dalam kasus-kasus di mana keamanan data tidak menjadi prioritas utama, tetapi efisiensi transmisi data tetap penting. Dengan terus mengembangkan dan mengoptimalkan penggunaan Base64, dapat membawa manfaat yang lebih besar dalam transmisi dan keamanan data di lingkungan digital.

VII. DAFTAR PUSTAKA

- Lubis, J. H. (2018). Implementasi Keamanan Data Dengan Metode Kriptografi XOR. *Jurnal Sistem Informasi Kaputama*, 2(2), 2–4.
- Mula, W., & Lemire, D. (2018). Faster Base64 Encoding and Decoding Using AVX2 Instructions. *ACM Transactions on the Web*, 12(3), 1–26. <https://doi.org/10.1145/3132709>
- Nugroho, A. Y. (2015). Pembuatan Aplikasi Kriptografi Algoritma Base64 Menggunakan PHP Untuk Mengamankan Data Text. *Seminar Nasional Informatika*, 1(1).
- Rahim, R., Nurdyanto, H., Hidayat, R., Saleh Ahmar, A., Siregar, D., Utama Siahaan, A. P., Faisal, I., Rahman, S., Suita, D., Zamsuri, A., Abdullah, D., Napitupulu, D., Setiawan, M. I., Sriadhi, S., Ahmar, A. S., Siregar, D., Siahaan, A. P. U., Faisal, I., Rahman, S., ... Zamsuri, A. (2018). Combination Base64 Algorithm and EOF Technique for Steganography. *Journal of Physics: Conference Series*, 1007(1), 1–5. <https://doi.org/10.1088/1742-6596/1007/1/012003>
- Salim, Y. (2020). Implementasi Algoritma Vertical Bit Rotation (VBR) Pada File Teks. *Jurnal Sains Komputer Dan Teknologi Informasi*, 3(1), 41–51. <https://doi.org/10.33084/jsakti.v3i1.1742>
- Sumartono, I., Siahaan, A. P. U., & Arpan. (2016). Base64 Character Encoding and Decoding Modeling. *International Journal of Recent Trends in Engineering & Research*, 2(12), 63–68.
- Supiyandi, S., Hermansyah, H., & Sembiring, K. A. P. (2020). Implementasi dan Penggunaan Algoritma Base64 dalam Pengamanan File Video. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, 4(2), 340. <https://doi.org/10.30865/mib.v4i2.2042>