BAB II

TINJAUAN PUSTAKA

A. Penelitian Terdahulu

Penelitian terdahulu ialah suatu berkas penelitian yang telah ada dengan tema atau jenis yang nyaris serupa dengan program yang hendak terbuat. Ada pula penelitian terdahulu yang nyaris serupa dengan Penelitian yang dilaksanakan ini tertera dalam tabel 2. 1.

Tabel 2.1 Tabel Penelitian Terdahulu

No	Judul	Latar Belakang	Metode Penelitian	Hasil Penelitian	Penulis
1.	Penelitian *Algoritma Encoding Base64* dan Implementasi PHP	Dengan perkembangan informasi perusahaan yang semakin meningkat, keamanan dan kerahasiaan data memiliki persyaratan yang lebih tinggi. Cara memastikan keamanan informasi data menjadi masalah yang perlu dipecahkan untuk setiap perusahaan aplikasi komputer, kunci untuk memastikan keamanan data adalah enkripsi data. Teknologi enkripsi data komputer mengacu pada enkripsi data dari informasi input plaintext, pengodean ulang melalui kunci, konten nyata implisit, metode pemrosesan teknis yang membuat pengguna ilegal tidak dapat memperoleh informasi data yang efektif. Dengan mengenkripsi data sistem, keamanan transmisi data dapat ditingkatkan, dan efek keamanan dan	Metode Enkripsi dan Dekripsi *algoritma Base64*	Dalam aplikasi sederhana pemrosesan keamanan data dalam pengembangan perangkat lunak perusahaan, menggunakan fitur pengkodean *base64* untuk membuat aplikasi enkripsi dan dekripsi data sederhana. Karakteristiknya adalah operasinya relatif sederhana, operasinya lebih sedikit, efisiensinya tinggi. Analisis dari definisi yang ketat, *base64* bukanlah arti enkripsi data yang lengkap, karena proses konversi tidak menghasilkan kunci, hanya dapat konversi dan rekombinasi kode. *Standar encoding base64* adalah A –	1. Somchai Wen Dong. 2. Wen Dong (GIS *Technology Engineering Research Centre for West- China Resources and Environment of Educational Ministry Yunnan Normal* University Kunming, China, 2018)

No	Judul	Latar Belakang	Metode Penelitian	Hasil Penelitian	Penulis
		kerahasiaan dapat dicapai.		Z, a – z, 0 – 9, +, dan /, selama program secara dinamis mengubah urutannya. Karakter yang sama akan dikodekan secara berbeda tergantung pada posisinya, kemungkinan diretas akan sangat dikurangi untuk meningkatkan keamanan data.	
2.	Kombinasi *Base64* dan Panjang Variabel *Hashing* untuk Mengamankan Data	Menjaga data tetap utuh tanpa berubah menjadi faktor penting dalam suatu komunikasi, data itu sendiri memiliki banyak bentuk seperti data teks, data audio, data gambar dan untuk mengamankan setiap data	kombinasi dengan algoritma *Hashing Variable Length* (HAVAL) dengan *Algoritma Base64*	*algoritma HAVAL* memiliki cara kerja mengamankan dan mengompresi plaintext, sehingga hasil *encoding* dari *Base64* diamankan kembali dan dikompresi menggunakan *algoritma HAVAL* dengan panjang *hashing* 32 *bit* atau 4 *byte* sehingga pada saat proses transmisi data tidak akan memakan banyak byte data dibandingkan dengan *algoritma Base64*	1. M Mesran 2. Dahlan Abdullah 3. Dedy Hartama 4. R Roslina 5. A Asri 6. Robbi Rahim* 7. Ansari Saleh Ahmar (*Department of Informatics Engineering*, STMIK Budi Darma, Medan, Indonesia. *Department of Informatics*, Universitas Malikussaleh, Aceh, Indonesia. *Department of Information System*, STIKOM Tunas Bangsa, Pematang Siantar, Indonesia. *Department of Informatics and Computer Engineering*, Politeknik Negeri Medan, Medan, Indonesia. *Department of Electrical*, Universitas

No	Judul	Latar Belakang	Metode Penelitian	Hasil Penelitian	Penulis
					Malikussaleh, Aceh, Indonesia. *School of Computer and Communication Engineering*, Universiti Malaysia Perlis, Kubang Gajah, Malaysia. *Department of Statistics*, Universitas Negeri Makassar, Makassar, Indonesia.2018)
3.	Algoritma Enkripsi *Vigenere* yang Dimodifikasi dan Implementasi Hibridanya dengan *Base64* dan *AES*	Keamanan adalah mekanisme di mana informasi dilindungi dari akses, perubahan, atau penghancuran yang tidak diinginkan atau tidak sah. Untuk mengamankan informasi tersebut digunakan proses enkripsi. Enkripsi adalah tindakan mengubah data sensitif melalui algoritma untuk membuat data tidak dapat dibaca sedemikian rupa sehingga hanya orang (atau komputer) yang memiliki kunci yang dapat mengaksesnya.	pendekatan hybrid digunakan untuk menerapkan algoritma enkripsi.	Keamanan sistem sangat ditingkatkan, melalui penelitian beberapa algoritma enkripsi data terkenal, meningkatkan beberapa algoritma enkripsi data dan mengaturnya dalam urutan yang sesuai. *Avalanche Effect* dipilih sebagai metrik untuk mengukur kinerja algoritma yang diusulkan dan implementasinya. Algoritma yang diusulkan menunjukkan Efek *Avalanche* tinggi yang signifikan, dibandingkan dengan Algoritma Enkripsi *Vigenere*.	1. Gurpreet Singh, 2. Supriya, (*Computer Science and Engineering Department*, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, INDIA. 2013)
4.	Kerangka Kerja Aman untuk Enkripsi File Menggunakan Pengkodean *Base64*	Keamanan file adalah praktik untuk mencegah akses, penggunaan, pengungkapan, gangguan, modifikasi, inspeksi, atau penghancuran file yang disimpan di database oleh pihak yang tidak berwenang. Saat ini keamanan menjadi isu yang sangat menantang, seiring dengan meningkatnya jumlah serangan terhadap	metode aman untuk memberikan keamanan ke semua jenis format file menggunakan pengkodean *AES (Rijndael)* dan *Base64*	Model terdiri dari tiga lapisan. Lapisan pertama melakukan encoding dan enkripsi. Aspek penting dari penggunaan *Base64* adalah untuk mengkodekan data biner ke dalam teks ASCII yang dapat dienkripsi, disimpan, dan ditransmisikan.	1. Ajeet Ram Pathak 2. Sarita Deshpande 3. Mudra Panchal (*Department of Information Technology, PES's Modern College of Engineering*, Pune, India. 2019)

No	Judul	Latar Belakang	Metode Penelitian	Hasil Penelitian	Penulis
		keamanan siber yang berdampak pada kerahasiaan, otentikasi, integritas, dan ketersediaan file.		Selanjutnya, data yang dikodekan dienkripsi dengan algoritma *AES (Rijndael*). Kedua, file terenkripsi disimpan ke dalam Server MySQL, dan akhirnya pada pemrosesan langkah ketiga dilakukan melalui cloud, yang melindungi informasi penting dari pencurian, kebocoran data, dan penghapusan, sehingga memberikan total tiga lapisan keamanan.	
5.	Penerapan Kombinasi Algoritma *BASE64* dan *ROT47* Untuk Enkripsi Database Pasien Rumah Sakit Jiwa Prof. DR. Muhammad Ildrem	Pada sesuatu industri, informasi ialah perihal yang amat berarti buat dilindungi alhasil permasalahan keamanan informasi ialah perihal yang amat di cermati. Perihal yang bisa dicoba buat mencegah informasi supaya tidak bisa disalah maanfaatkan oleh orang lain yakni dengan memakai metode kriptografi.	Metode enkripsi memakai algoritma *ROT47* yang dipakai buat mengenkripsi informasi data	Enkripsi menggunakan algoritma *Base64* yang merupakan skema pengkodean data biner menjadi rangkaian kode ASCII sesuai index pada Base64. Dengan demikian menggunakan kedua metode perlindungan tersebut secara bersama-sama akan meningkatkan keamanan untuk melindungi data.	1. Rachmat Aulia 2. Ahmad Zakir 3. Dian Agung Purwanto (Prodi Teknik Informatika, Fakultas Teknik dan Ilmu Komputer Universitas Harapan Medan, indonesia, 2018)

B. Keamanan Sistem Informasi

Permasalahan keamanan ialah salah satu pandangan berarti dari suatu sistem data informasi, hendak namun permasalahan keamanan ini kerapkali kurang memperoleh *atensi* dari *owner* serta pengolah sistem data informasi. Tumbangnya data informasi ke pihak lain, misalnya pihak saingan bidang usaha yang bisa memunculkan kehilangan untuk *owner* data informasi. Untuk itu keamanan dari sistem data yang dipakai wajib aman dalam batasan yang diperoleh (Siswanto, Anif, and Gata 2018). *Web server* serta *database server*

bagaikan jantung serta otak dari badan internet. 2 bagian ini jadi bagian utama dari suatu aplikasi internet yang kuat serta tepatlah keduanya jadi sasaran hacker. Dalam sebagian permasalahan kita bisa memastikan titik- titik lemas dalam aplikasi yang dapat jadi target penyerbu.

Dalam penafsiran ataupun definisinya (Indra Gunawan 2021), keamanan sistem data ialah upaya yang dicoba buat mencegah dan menjamin 3 aspek terutama dalam dunia siber antara lain

1. Kerahasiaan Data.
2. Keutuhan Data.
3. Ketersediaan Data.

Kerahasiaan Data Menjamin pemakai siber aman privasinya bagus itu *privacy* yang terletak pada komputer individu, peranti genggam ataupun aman informasi privasinya kala melaksanakan bermacam kegiatan jelajah internet. Keutuhan data menjamin konsumen siber memperoleh informasi utuh serta betul tanpa dimodifikasi serta dirubah pihak lain ditengah- tengah jalur. Ketersediaan data menjamin konsumen siber memperoleh informasi pada dikala yang diinginkannya tanpa ditutupi serta tanpa dilindungi oleh pihak lain.

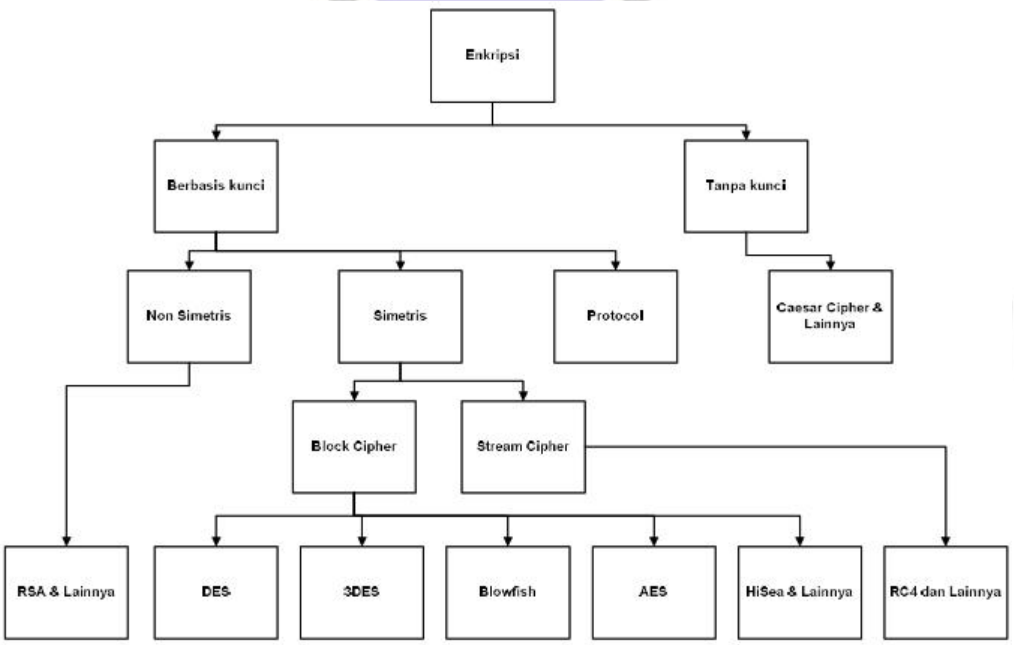
Kemajuan keamanan informasi diawali semenjak terdapatnya kesalahan pc. Kesalahan pc yang sangat *Early Republic* masa modern terdaftar diawali dari tahun 70- an akhir oleh hacker populer sejauh era ialah kevin Mitnick. Mangulas keamanan informasi pasti tidak dapat bebas dari permasalahan *cryptography*(ilmu penyandian). *Cryptography* ialah penopang penting sekalian ialah tata cara teraman serta sangat efisien dalam bumi keamanan informasi, berikutnya kemajuan keamanan informasi dikala ini biasanya banyak bersaingan buat menghasilkan tata cara *encryption*(penyandian) yang terkuat (de Rosal Ignatius Moses Setiadi et al. 2019).

C. Kriptografi

Kriptografi(*Cryptography*) merupakan ilmu yang mangulas mengenai ilmu penyandian, encryption merupakan tata cara dalam *cryptography* dimana informasi yang beragam panjangnya atau ukurannya diganti atau diacak jadi informasi yang panjangnya tetap(Murdowo 2017).

Enkripsi ialah tata cara sangat penting, efisien serta berdaya guna dalam metode keamanan informasi. Enkripsi membenarkan cara komunikasi informasi dimana satu pihak mengirim informasi pada pihak lain bisa dicoba dengan cara nyaman, cermat serta berdaya guna (Leman and Rahman 2020).

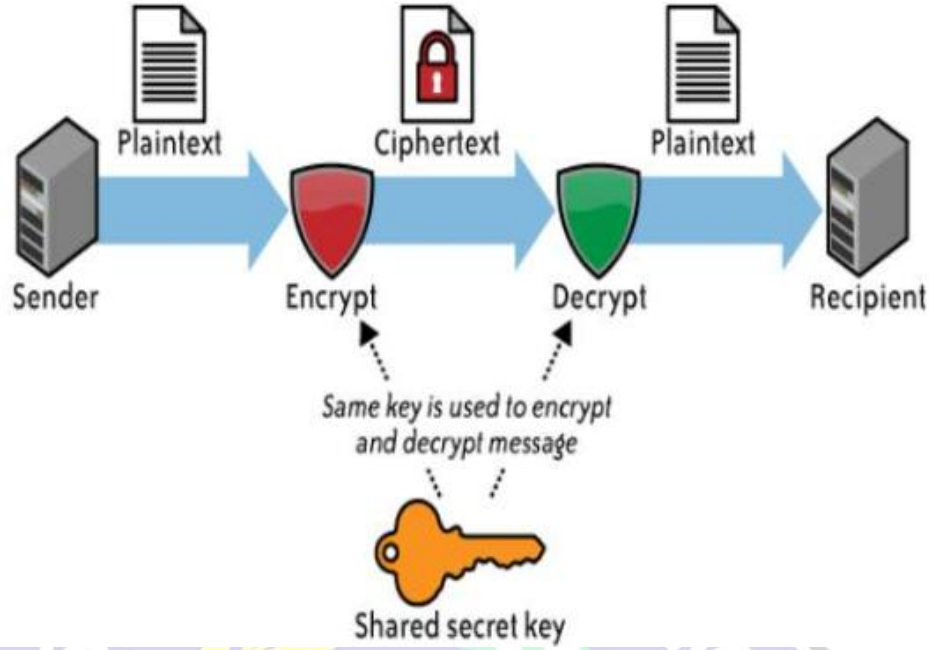
Tata cara kriptografi terdiri dari 2 ialah berplatform kunci serta tanpa kunci, setelah itu dari penjatahan ini diturunkan jadi banyak tata cara yang ditemui oleh sebagian industri serta periset keamanan. Sebagian tata cara kriptografi popular itu bisa diamati pada gambar 2.1.



Gambar 2.1 Algoritma kriptografi enkripsi popular (Faheem et al., 2017).

1. Kriptografi Simetris

   Kriptografi simetris memakai kunci yang serupa buat cara enkripsi serta dekripsi. Tata cara ini diucap pula *secret key cryptography* (Indra Gunawan 2021). Desain metode kegiatan kriptografi harmonis bisa diamati pada lukisan 2. 2 dibawah ini.

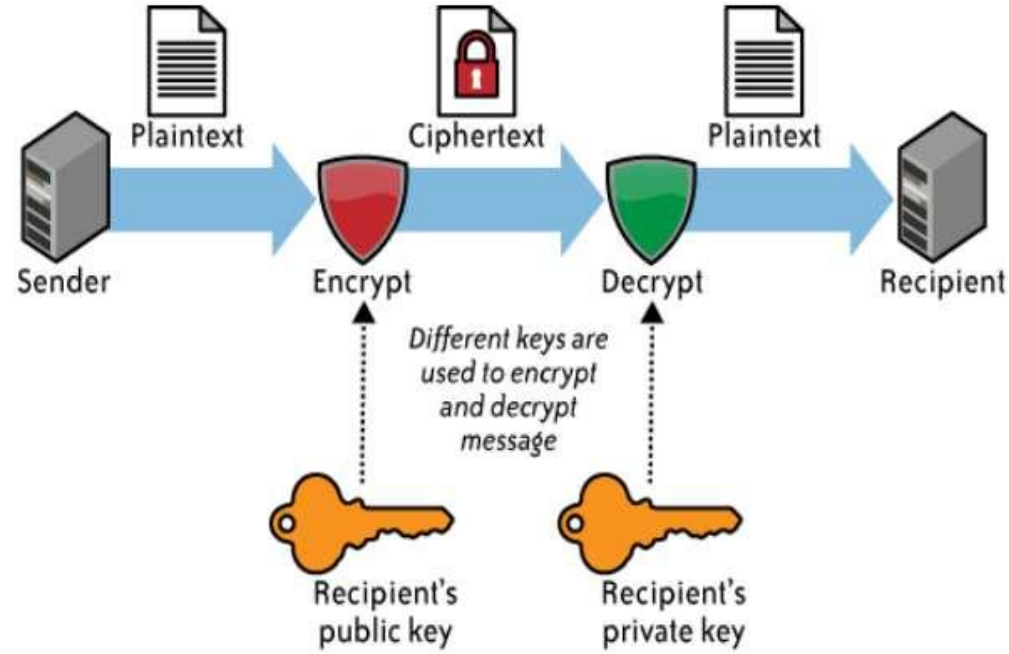


Gambar 2.2 Skema Kriptografi Simetris (Amalraj, 2016).

Metode fungsi kriptografi simetris diawali kala pihak *sender* mengirim informasi dengan bentuk *plaintext*(file normal) setelah itu dicoba cara enkripsi dengan sesuatu kunci. File yang sudah dienkripsi itu berganti jadi file *ciphertext*(file yang diacak). Sehabis *ciphertext* hingga di pihak *recipient*, *recipient* mendekripsi file *ciphertext* itu memakai kunci yang serupa yang dipakai oleh pihak *sender* jadi plaintext.

2. *Kriptografi Non Simetris*

Enkripsi *non* simetris memakai 2 kunci yang berlainan buat cara enkripsi serta dekripsi. Cara enkripsi memakai *public key*, cara dekripsi memakai *private key*. Desain metode kegiatan enkripsi non simetris bisa diamati pada gambar 2.3.



Gambar 2.3 Skema kriptografi non simetris (Amalraj, 2016).

Metode kegiatan kriptografi non simetris diawali pada saat pihak s*ender* mengirim informasi dengan bentuk *plaintext*(file wajar) setelah itu dicoba cara enkripsi dengan sesuatu kunci A(*recipient public key*). File yang sudah dienkripsi itu berganti jadi file *ciphertext*(file yang diacak). Sehabis *ciphertext* hingga di pihak *recipient*, *recipient* mendekripsi file *ciphertext* itu memakai kunci B(*recipient private key*) jadi *plaintext*. Kunci B terbuat memakai algoritma khusus yang dibangkitkan bersumber pada kunci A.

OWASP(*Open Website Application Security Project*) selaku badan keamanan bumi sudah merumuskan prinsip dalam memakai kriptografi alhasil diperoleh hasil pemakaian kriptografi dalam penjagaan informasi dengan cara maksimum. Rambu- rambu itu merupakan selaku selanjutnya:

1. Kunci kriptografi wajib diamankan dengan cara maksimum memakai hak akses pada tingkat sistem pembedahan. Hak

akses biasanya merupakan read only serta berikutnya cuma dapat dibuka oleh pihak yang mempunyai hak kepada file itu.

2. *Private key* wajib ditentukan serta diisyarati buat tidak bisa di *export* kala melaksanakan pembuatan akta kunci.
3. Sehabis melaksanakan pembuatan *private key*, lekas hancurkan serta lenyap *private key* pada sistem serta amankan ketempat lain.
4. Bila dipakai *host based intrusion detection system*(pendeteksi serbuan *berplatform host*), hingga system itu wajib bisa mengetahui pergantian file kunci.
5. Aplikasi pula wajib bisa mengetahui pergantian file kunci
6. Password buat membuka *private key* wajib diamankan ditempat raga terpisah yang memiliki sistem keamanan raga standar.
7. Janganlah meletakkan kunci pada *source code* ataupun aplikasi.
8. Bila dipakai sistem berplatform *website*, yakinkan *webserver* tidak bisa mengakses file kunci alhasil bisa meminimalkan efek kala *webserver* terserang serbuan.
9. Bila dipakai sistem berp*latform* interaktif, yakinkan dipakai aplikasi penjagaan bonus buat mencegah file kunci pada seluruh situasi apalagi pada dikala booting.

D. Algoritma

Algoritma merupakan antrean langkah- langkah penanganan permasalahan dengan cara analitis serta masuk akal, langkah- langkah penanganan permasalahan buat permasalahan yang bisa diproses dengan cara terkomputerisasi. Algoritma dipakai buat kalkulasi, pemrosesan informasi, serta penalaran otomatis. Algoritma amat berfungsi dalam pembangunan sesuatu aplikasi. Dalam bumi tiap hari bisa jadi tanpa kita sadari algoritma sudah masuk dalam kehidupan kita(Sukmana, Agustini, and Siregar 2017)

Secara lazim deskripsi Algoritma merupakan antrean langkah- langkah masuk akal penanganan permasalahan yang disusun dengan cara analitis serta masuk akal. Tutur masuk akal ialah tutur kunci dalam algoritma. Langkah-

langkah dalam algoritma wajib masuk akal serta wajib bisa didetetapkan berharga salah ataupun betul. Dalam sebagian kondisi, algoritma merupakan detail antrean tahap buat melaksanakan profesi tertentu

Kewajiban sederhana bisa dituntaskan dengan algoritma yang diperoleh dengan sebagian menit, tingkatan kerumitan melaksanakan tantangan yang jauh, tetapi hingga pada permasalahan yang amat kompleks alhasil mereka sudah membatasi matematikawan yang tidak terbatas jumlahnya sepanjang bertahun- tahun apalagi berabab- abab. Pc modem mengalami permasalahan pada tingkatan keamanan bumi maya dan penindakan informasi besar, penyaringan set informasi yang berdaya guna serta global sedemikian besar sehinggah pc standar tidak bisa memprosesnya dengan cara pas durasi.

Kala konsep algoritma terkini diimplementasikan dalam sebutan prektis, patuh terpaut diketahui selaku rekayasa algoritma. Walaupun badan yang lebih besar semacam amazon serta google memperkerjakan pendesain serta insinyur spesial, mengenang tingkatan keinginan mereka hendak algoritma terkini serta spesial. Semacam cara konsep, rekayasa algoritma kerap kali mengaitkan pengakuan ilmu pc, dengan kerangka belakag yang kokoh dalam matematika dimana mereka terdapat selaku pekerjaan yang terpisah serta terspesialisasi, insinyur algoritma mengutip gagasan abstrak dari pendesain serta cara inovatif dari mereka yang hendak dimengerti oleh pc. Dengan perkembangan teknologi digital yang semakin hari semakin pesat, para insinyur yang berdedikasi hendak lalu jadi terus menjadi biasa.

E. Algoritma Base64

Algoritma Base64 ialah salah satu algoritma buat *Encoding* serta *Decoding* sesuatu informasi ke dalam bentuk ASCII, yang didasarkan pada angka dasar 64 ataupun dapat dibilang selaku salah satu tata cara yang dipakai buat melaksanakan *encoding*(penyandian) kepada informasi binary (Hayaty and Putra 2018).

Algoritma ini banyak dipakai di dunia Internet selaku alat data format buat mengirimkan data, pemakaian itu disebabkan hasil serta *encode base64* berbentuk *plaintext*, hingga informasi ini hendak jauh lebih gampang dikirim,

dibanding dengan bentuk informasi yang berbentuk binary. Desain *Base64* umumnya dipakai kala terdapat keinginan buat menyandikan informasi biner yang butuh ditaruh serta ditransfer lewat alat yang didesain buat menanggulangi informasi tekstual.

Algoritma Base64 memakai isyarat ASCII serta isyarat *index base64* dalam melaksanakan cara enkripsi atau dekripsinya. Dalam melaksanakan enkripsi pada URL web, isyarat *index base64* butuh dimodifikasi. Ikon(+) dimodifikasi jadi(-) serta ikon ikon(atau) jadi(_). Algoritma kriptografi *Base64* ini sesungguhnya memakai algoritma kunci simetris ataupun dituturkan pula algoritma kriptografi konvensional, yakni algoritma yang memakai kunci untuk prosedur enkripsi serupa dengan kunci untuk prosedur dekripsi.

Ada pula tahapan- tahapan enkripsi memakai *Algoritma Base64* ialah antara lain:

1. Mengkonversi kepribadian ke biner.
2. Cermati serta yakinkan kalau terdapat 24 bit.
3. Mengkonversi 24 bit dari 3 golongan 8 bit ke 4 golongan 6 bit.
4. *Convert* tiap- tiap 4 golongan 6 bit ke desimal.
5. Maanfaatkan tiap- tiap desimal buat mencari sandi karakter pada *index Base64*.

Ada pula tahapan- tahapan dekripsi memanfaatkan *Algoritma Base64* ialah antara lain:

1. Mengkonversi karakter *Base64* ke biner dengan memakai 6 bit.
2. Alterasi 24 bit dari 4 golongan 6 bit ke 3 golongan 8 bit.
3. Alterasi tiap- tiap 3 golongan 8 bit ke desimal.
4. Maanfaatkan tiap- tiap 3 desimal buat mencari karakter ASCII buat angka yang ada.

Selanjutnya table pencodean radix 64 bisa diamati pada table 2. 1

Tabel 2.1 Pengkodean *Radix Base64*

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

Cara pengcodean *BASE64* ialah seperti dibawah ini:

1. Input informasi diganti kedalam Angka ASCII serta didapat angka binernya.
2. Angka biner seluruh angka ASCII digabungkan serta dikelompokkan kedalam 1 golongan memiliki 6 bit.

3. Tiap golongan yang bermuatan 6 bit dipetakan ke 1 kepribadian yang bisa dicetak serta didasarkan pada angka 6- bit memakai denah set kepribadian *Base64.*
4. Kepribadian *padding*"=" pula dipakai pada akhir bacaan yang dikodekan bila jumlah bit(ataupun jumlah kepribadian pada *plaintext*) tidak banyak dari 3. Bila jumlah bit dalam bacaan merupakan 3n+ 1, hingga encoder menaruh satu"=" pada akhir bacaan yang dikodekan, serta bila jumlah bit dalam bacaan merupakan 3n+ 2, hingga hendak menaruh 2"=" pada akhir keluaran.

Text	A	B	C
ASCII value	65	66	67
Bit pattern	0 1 0 0 0 0 0 1	0 1 0 0 0 0 1 0	0 1 0 0 0 0 1 1
Index	16	20	9	3
Encoded Text	Q	U	J	D

Gambar 2.4 Proses sandi *base64*

F. Konsep Enkripsi dan Deskripsi

Salah satu metode buat tingkatkan keamanan merupakan dengan memakai teknologi enkripsi. Data- data yang dikirimkan diganti sedemikian muka alhasil tidak gampang disadap. Jadi enkripsi merupakan cara yang dicoba buat mengamankan suatu catatan(yang diucap *plaintext*) jadi catatan yang tersembunyi(diucap *ciphertext*) merupakan enkripsi(*encryption*). *Ciphertext* merupakan catatan yang telah tidak bisa dibaca dengan gampang. Terminologi yang lebih pas dipakai merupakan" *encipher*". Cara kebalikannya, buat mengganti *ciphertext* jadi *plaintext*, diucap dekripsi(*decryption*). Terminologi yang lebih pas buat prosedur ini ialah" *decipher*" (Hayaty and Putra 2018).

Bersumber pada metode mengerjakan bacaan(*plaintext*), *cipher* bisa dikategorikan jadi 2 tipe: *block cipher and stream cipher*. *Block cipher* bertugas dengan mengerjakan informasi dengan cara kelompok, dimana sebagian karakter atau informasi digabungkan jadi satu kelompok. Tiap cara

satu kelompok menciptakan keluaran satu kelompok pula. Sedangkan itu *stream cipher* bertugas mengerjakan masukan(karakter ataupun informasi) dengan cara terus menerus serta menciptakan informasi pada saat yang beriringan.

G. Koperasi Syariah

Koperasi syariah merupakan koperasi yang melaksanakan upaya di aspek simpan pinjam serta pembiayaan yang berpinsip syariah. Koperasi syariah serupa dengan baitul maal watamwi (BMT). Perkembangan koperasi syariah berkembang dengan aktivitas upaya yang tidak sejenis, antara lain mempunyai sebagian tipe julukan semacam Koperasi Simpan Pinjam Pembiayaan Syariah (KSPPS), serta Bagian Usaha Simpan Pinjam serta Pembiayaan Syariah (UPPS)(Apriyana and Hasbi 2020; Kementerian Koperasi dan Usaha Kecil dan Menengah 2017).