Satya Dharma: Jurnal Ilmu Hukum
Vol 3 No.2 Tahun 2020
ISSN 2548-6055(print), ISSN (online)
https://ejournal.iahntp.ac.id/index.php/satya-dhamat

PEMANFAATAN TEKNOLOGI KRIPTOGRAFI DALAM MENGATASI KEJAHATAN *CYBER*

Oleh
Ni Putu Eka Merliana
Institut Agama Hindu Negeri Tampung Penyang Palangka Raya
putuekamerliana@iahntp.ac.id

Abstrak

Teknologi menjadi hal yang tidak bisa dihindari perkembangannya, karena sebagian besar masyarakat sudah menggunakan untuk memenuhi kebutuhan hidup sehari-hari. Merembaknya penggunakan teknologi menjadi kesempatan para pelaku kejahatan untuk menggunakan teknik yang memanfaatkan teknologi agar mendapatkan keuntungan dan kejahatan itu disebut kejahatan siber (*cyber crime*). Tujuan dari tulisan ini adalah memberikan gambaran mengenai kejahatan siber yang sudah terjadi serta perangkat hukum dan teknologi kriptografi sebagai bentuk pemecahan masalah dalam kejahatan siber. Walaupun teknologi yang digunakan dalam bentuk kriptografi, akan tetapi tidak bisa terlepas dari perangkat hukum yang sudah diterapkan oleh pemerintah dan ini dijadikan landasan bagi masyarakat untuk tetap berhati-hati dalam melakukan tindakan yang berhubungan dengan pemanfaatan teknologi.
Kata kunci : Kejahatan Cyber, Teknologi Kriptografi

I. PENDAHULUAN

Perkembangan teknologi sudah memberikan efek terhadap perilaku dalam kehidupan masyarakat saat ini, sehingga masyarakat secara tidak langsung sudah ketergantungan dalam penggunaan teknologi sebagai pemenuhan kehidupan sehari-hari. Berbagai bidang seperti bidang agama, sosial, pendidikan, budaya dan lainnya sudah memanfaatkan teknologi sebagai media pendukung dalam melakukan dan menyelesaikan pekerjaan yang dibuat. Masyarakat secara awam sebagai pengguna tidak memahami bahwa pentingnya keamanan data maupun informasi dalam menggunakan teknologi informasi dan komunikasi. Penetrasi teknologi informasi yang berada pada segala aspek bidang sudah dirasakan oleh masyarakat secara umum baik itu

dalam kehidupan sehari-hari secara tidak langsung maupun secara langsung berinteraksi dengan memanfaatkan teknologi sebagai alat bantu dalam memenuhi kebutuhan hidup masyarakat. Berbagai jenis kegiatan yang dilakukan dengan pemanfaatan media elektronik perlu adanya dukungan hukum dalam memanfaatkannya sehingga dapat melindungi masyarakat secara global. Perlunya hukum dalam melindungi masyarakat dalam memanfaatkan teknologi dikarenakan kesempatan untuk melakukan kejahatan dalam memanfaatkan teknologi bisa menjadi alat oleh para pelaku kejahatan untuk mendapatkan keuntungan (Ersya, 2018:50).

Bentuk teknologi yang trend dan banyak dipergunakan adalah adanya teknologi internet yang sangat memberikan pengaruh besar terhadap kehidupan masyarakat baik itu dalam hal pengaksesan informasi maupun pemberian data untuk memenuhi kebutuhan sehari-hari. Internet merupakan jaringan yang luas dari perangkat komputer dengan memafaatkan teknologi wide network sehingga sering disebut dengan worldwide network. Berbagai bentuk teknologi jaringan internet yang antara lain seperti serat optic, gelombang atau frekuensi serta kabel telepon, dan teknologi ini sudah berkombinasi dengan media komunikasi yang biasa hadir dalam bentik telepon seluler atau smartphone (Ersya, 2018). Kehadiran teknologi internet menurut Ardianti memberikan gambaran bahwa manusia tidak mampu lepas dari adanya arus komunikasi dan informasi sehingga menyebabkan terjadinya suatu loncatan besar bagi kehidupan masyarakat terutama dalam hal perilaku dan gaya hidup masyarakat. Teknologi akan memberikan perhatian khusus dalam penggunaanya adalah karena disesuaikan dengan nilai-nilai sosial yang dapat beradaptasi terhadap kehidupan masyarakat sehingga mau tidak mau pemerintah harus menetapkan suatu aturan dan etika yang dapat menangkal

munculnya dampak negatif dari penggunaan teknologi tersebut (Ardiyanti, 1986:1).

Pada aplikasi pemanfaatan teknologi digital yang digunakan dalam memenuhi kebutuhan hidup masryarakat secara umum, dapat memberikan dampak baik itu positif maupun negatif. Dampak positifnya adalah dapat mempermudah semua pekerjaan sehingga dapat meningkatkan kesejahteraan dan kemajuan hidup masyarakat secara umum. Misalnya dalam penggunaan aplikasi *e-banking, e-commerce, education*, via sms dan masih banyak lagi aplikasi yang lain. Sedangkan dampak negatifnya terdapat beberapa tindak kejahatan yang memanfaatkan teknologi digital sebagai transaksi elektronik yang sangat meresahkan masyarakat atau yang sering dikenal dengan istilah *cybercrime*. Pelaku kejahatan dapat membobol atau memecahkan kata sandi atau kata kunci dari data digital korban untuk mendapatkan keuntungan dari hal tersebut. Menurut Sari, bentuk kejahatan dengan menggunakan teknik *cyber* adalah dengan memanfaatkan teknologi internet untuk mengambil keuntungan dengan motif berbagai jenis misalnya motif intelektual dimana kejahatan yang digunakan untuk kepuasan sendiri dengan cara merekayasa serta mengaplikasikan pemanfaatan teknologi informasi dalam dunia kejahatan, selain itu motif ekonomi yang mana bentuk kejahatan yang beredar adalah dengan mencari keuntungan pribadi dan kelompok yang dapat merugikan orang lain secara ekonomi (Sari, 2018).

Memahami kejahatan *cyber* perlu adanya suatu hukum *cyber* yang dapat mengendalikan kejahatan *cyber* yang sudah menyerang penggunaan teknologi informasi di masyarakat. Hukum *cyber* yang menjadi hukum multidispliner merangkul berbagi macam jenis cabang ilmu seperti hukum pidana, hukum perdata, perlindungan konsumen, ekonomi, serta administrasi yang diperoleh dengan memanfaatkan teknologi, sosial budaya dan hukum. Pentingnya

menerapkan hukum *cyber* menjadikan perhatian bagi pemerintahan di berbagai negara di seluruh dunia, hal tersebut dikarenakan sebagaian besar besar masyarakat sudah menggunakan teknologi sebagai kebutuhannya (Ersya, 2018). Selain itu yang menjadi perhatian adalah memahami bentuk perkembangan kejahatan *cyber* yang sudah dilakukan oleh oknum yang tidak bertanggung jawab. Seperti yang diungkapkan oleh Handayani bahwa kejahatan *cyber* yang dilakukan oleh oknum dengan menggunakan sarana teknologi indormasi baik itu dalam bentuk sebagai programmer, analisi sistem, manager, kasir yang mampu melakukan kejahatan *cyber*. Faktor yang mengakibatkan adanya kejahatan tersebut adalah adanya dorongan yang mendominasikan pesatnya perkembangan teknologi baik itu handphone maupun smartphone yang mana pada oknum yang akan melakukan hal tersebut mencari celah dan mendapatkan cara untuk mencuri data maupun merusak data yang mana hal tersebut dapat digunakan untuk keuntungan pihak tertentu .

Memahami tentang kejahatan *cyber* harus ada cara yang digunakan untuk menangkal kejahatan berbasis digital tersebut, salah satunya adalah dengan menggunakan dan memanfaatkan teknologi kriptografi. Berbagai bentuk teknik kriptografi sudah banyak diterapkan dalam mengimplementasikan dan mengamankan bentuk transaksi digital yang sudah digunakan. Ungkapan yang disampaikan dalam buku tentang security managemen terdapat tiga (3) aspek yang harus dilakukan dalam penggunaan dan pengimplementasian keamanan informasi antra lain kerahasiaan, keutuhan data serta ketersediaan. Pelaksanaan dan penerapan teknologi kriptografy memberikan gambaran untuk menjamin kerahasiaan yang dikomunikasikan (Agustina & Kurniati, 2009). Pengembangan ilmu pengetahuan yang digunakan dalam memberikan keamanan bagi penggunaan teknologi perlu

ditingkatkan agar para masyarakat merasa nyaman dan aman pada saat memanfaatkannya, dan salah satu cara atau teknik yang digunakan adalah dengan memanfaatkan teknologi kriptografi. Teknik ini merupakan salah satu teknik untuk menyandikan data maupun informasi sebelum dikirim dengan menggunakan teknologi internet. Selain itu teknik ini memberikan kemudahan dalam pengamanan informasi dikarenakan proses enkripsi yang dilakukan dengan proses pengacakan data informasi agar sulit untuk ditemukan.

Tulisan akan mengulas penggunaan teknik kriptografi dalam mengamankan teknologi informasi dari kejahatan *cyber*crime. Selain itu tulisan ini menggambarkan Teknik kriptografy yang digunakan dalam membantu penanganan kejahatan *cyber* secara digital. Tujuan dalam tulisan ini adalah untuk memahami cara kerja dan peran serta tindakan yang dapat dilakukan dalam menangani kejahatan *cyber*. Teknik kriptografi yang dibahas dalam artikel ini nantinya dapat memberikan gambaran dan membantu para penegak hukum dalam memberantas kejahatan *cyber* yang lagi marak saat ini.

II. PEMBAHASAN

A. Kejahatan *Cyber* (*Cyber crime*)

Era globalisasi tidak lagi menunjukan cara persaingan yang dilakukan tidak secara tradisional dan konvesional dengan melakukan peperangan yang menggunakan kekuatan senjata, akan tetapi persaingan yang dilakukan pada bidang budaya, perekonomian, politik serta teknologi yang mana persaingan ini tidak menunjukan hal yang dibatasi oleh suatu cara. Sasaran ancaman kejahatan siber (*cyber*crime) dapat terjadi pada saat penyadapan komunikasi yang melibatkan beberapa pejabat tinggi negara. Peningkatan terhadap ancaman kejahatan siber (*cyber*crime) dapat dilakukan oleh beberapa oleh negara atau actor non negara (non state actor)

berdampak terhadap terjadinya *cyber* warfare atau gangguan *cyber* (*cyber* violence) (Rahmawati, 2017). Menurut Sudarwanto mengemukakan bahwa bentuk kejahatan yang dilakukan siber adalah dengan melakukan penyerangan yang terjadi pada teknologi digital seperti content, computer system dan communication techonology yang dimiliki oleh masyarakat secara umum yang berada di dalam *cyber*space. Bentuk penyerangan tersebut biasanya terjadi pada jaringan komputer yang mana si pelaku akan memperoleh pengaksesan terhadap akun pribadi pengguna yang kemudian menggunakan interface yang dimiliki oleh korban untuk menyerang situs lain (Sudarwanto, 2009). Terdapat beberapa jenis kejahatan *cyber crime* yang terjadi antara lain :

1. Unauthorized Access to Computer System and Service

   Bentuk kejahatan yang dilakukan dengan masuk ke dalam sistem jaringan yang dimiliki oleh seseorang tanpa sepengetahuan atau ijin dari akses suatu jaringan komputer tersebut yang mana motif yang dilakukan dapat berupa pencurian, pembobolan, sabotase atau yang lainnya sehingga pelaku akan mendapatkan keuntungan dari kejahatan tersebut.

2. Illegal Contents

   Bentuk kejahatan yang dilakukan adalah dengan cara memasukan beberapa data maupun informasi yang tidak benar ataupun tidak etis ke dalam teknologi internet yang mana dapat melanggar hukum sehingga masyarakat umum dapat bebas mengaksesnya dan akan mengakibatkan dampak negatif bagi lingkungan masyarakat. Sebagai contoh adalah kejahatan dengan membuat hoax atau berita tidak benar, pornografi.

3. Data Forgery

Bentuk kejahatan yang dilakukan dengan cara menyimpan data-data dokuman yang palsu melalui penggunaan teknologi internet.

4. *Cyber* Espionage

   Bentuk kejahatan yang memanfaatkan jaringan dari teknologi internet dikarenakan penyebarannya sangat mudah dan cepat serta dapat diakses oleh siapa saja yang mana pelaku kejahatan memasukan mata-mata atau pendeteksi kedalam jaringan komputer (computer network system) ke korban yang dituju. Biasanya kejahatan ini digunakan untuk persaingan bisnis dalam hal penyimpanan data dan dokuman yang tersimpan dalam suatu sistem komputer yang terhubung dengan jaringan komputer.

5. *Cyber* Sabotage and Extortation

   Bentuk kejahatan yang dilakukan adalah dengan melakukan pengrusakan, mengganggu maupun penghacuran terhadap informasi, program komputer maupun sistem jaringan komputer yang terhubung melalui internet. Penyusupan dengan memasukan virus komputer melalui sistem jaringan komputer dilakukan pada modus kejahatan ini sehingga mengakibatkan data maupun informasi dan program komputer yang digunakan oleh korban tidak dapat diakses lagi. Bentuk kejahatan ini sering disebut dengan *cyber* terrorism.

6. Offence Againts Intellectual Property

   Bentuk kejahatan pada modus ini adalah dengan mengarah pada HKI atau Bentuk Hak Kekayaan Intelektual yang dimiliki oleh pihak lain dengan memasukannya ke dalam sistem teknologi internet. Sebagai contoh kejahatan yang dilakukan adalah dengan cara meniru

gambaran dari tampilan website tertentu dengan menyiarkan rahasia dagang yang merupakan rahasia dagang yang dimiliki oleh korban.

7. Infrringemts of Pryvacy

   Modus kejahatan ini yang dilakukan sasarannya adalah informasi yang dimiliki oleh seseorang yang bersifat rahasia dan sangat pribadi. Cara yang dilakukan adalah membobol data pribadi tersebut untuk mendapat keuntungan bagi si pelaku, sebagai contoh data yang dicari adalah nomor PIN yang ada di ATM, nomor kartu kredit (Handayani, 2016).

B. *Cyber crime* di Indonesia

Kejadian *cyber crime* yang ada di Indonesia menjadi perbincangan dan perhatian bagi para pakar hukum karena kejahatan dalam bentuk seperti ini sangat sering terjadi hal ini disebabkan karena sebagaian besar kehidupan serta transaksi yang dilakukan oleh masyarakat tidak lepas dari pemanfaatan maupun penggunaan dari teknologi. Sebagai contoh para aparat hukum, penegang hukum maupun akademisi selalu mencari dan mendesak pemerintah untuk menyusun aturan perundang-undangan yang mengatur tentang *cyber crime* (Handayani, 2016). Biasanya para pelaku kejahatan *cyber* merupakan orang-orang yang memiliki kemampuan dan pengetahuan dalam mengoperasikan komputer terutama dalam hal melakukan pembobolan sistem informasi maupun jaringan komputer. Kebanyakan para pelaku paham dan sangat ahli dalam pembuatan bahasa pemrograman, selain itu para pelaku juga dapat melakukan analisa sistem kerja yang ada pada komputer sehingga dapat menemukan celah yang ada pada sistem dan kemudian melakukan tindakan kejahatan (Sari, 2018). Menurut Abidin *cyber*crime merupakan tindakan yang melawan hukum dengan memanfaatkan teknologi internet dan jaringan komputer berbasis teknologi komputer dan telekomunikasi. Terdapat 2

karakterisitik *cyber*crime yaitu kejahatan kerah biru (*blue collar crime*) yang mana kejahatan yang dilakukan secara konvensional seperti perampokan, pembunuhan, serta pencurian dan kejahatan kerah putih (*white collar crime*) (Abidin, 2015).

Berdasarkan pendapat dari Joann L. Miller terdapat 4 (empat) kategori dari white collar crime yaitu :

a. *Organizational occupational crime* merupakan jenis kejahatan yang sasarannya lebih ke suatu oragnisasi atau sering disebut dengan kejahatan korporasi

b. *Government occupational crime* merupakan kejahatan yang sasarannya adalah pekerjaab yang dilakukan oleh instansi pemerintahan.

c. *Profesional occupational crime* merupakan kejahatan yang sasarannya adalah suatu pekerjaan yang dilakukan oleh seorang pakar atau suatu pekerjaan yang dilakukan secara profesional

d. *Individual occupational crime* merupakan kejahatan yang resikonya diperoleh dari pekerjaan yang dilakukan oleh seorang individu.

Negara Indonesia menjadi negara yang memiliki kasus tertinggi dalam bidang *cybercrime*, hal tersebut memberikan prestasi bagi para hacker, cracker dan carder lokal. Kasus *cyber* yang paling banyak di Indonesia adalah kasus pornografi, yang mana pelaku membuat serta menyebarkan data dan informasi dalam bentuk pornografi melalui perangkat teknologi informasi dan komunikasi. Salah satu contohnya adalah pada kasus Ariel, Luna dan Cut Tari yang mana video porno yang dilakukan artis tersebut disebar oleh pelaku melalui teknologi internet. Modus kejahatan tersebut sasarannya adalah perorang atau invidu sesuai dengan tujuan tertentu. Karena penyebaran sengaja dilakukan maka kasus ini dijerat oleh Pasal 29 UURI No. 44 tahun 2008

tentang Pornografi Pasal 56 dengan hukuman minimal 6 bulan sampai 12 tahun atau denda minimal 250 juta hingga 6 miliyar rupiah (Ketaren, 2016).

Maraknya kejahatan di dunia maya tergantung dari pemanfaatan sumber daya perangkat keras (hardware) dan perangkat lunak (software) serta penggunanya yang harusnya memiliki kesadaran penting sistem pengamanan komputer di dunia maya. Setiap penyedia layanan internet serta pelanggan internet akan menjadi target para pelaku *cyber crime* untuk mendapatkan keuntungan bagi mereka dan merugikan para pengguna internet. Bentuk kejahatan siber yang dilakukan tidak memerlukan interaksi langsung antara korban dan para pelaku kejahatan, karena modusnya adalah dengan menggunakan layanan teknologi internet. Sasaran yang menjadi modus kejahatan ini adalah kartu ATM, kartu kredit, website jual beli online, layanan keuangan yang dilakukan secara online, dan segala bentuk transaksi atau kegiatan yang dilakukan melalui jasa online atau elektronik.

C. Penanggulangan *Cyber Crime* di Indonesia

Cyber crime adalah tindakan pelanggaran hukum yang secara khusus diatur dalam Undang-undang Nomor 11 Tahun 2008 yang mengatur tentang Informasi dan Transaksi Elektronik untuk mengembangkan pengetahuan dan kemampuan penyidik dalam dunia cyber (Suhendar, 2013) . Kejahatan cyber yang memanfaatkan teknologi informasi sebagai medianya pengaturan hukumnya diatur dalam Undang-undang nomor 11 Tahun 2008 yang sekarang sudah diubah oleh Undang-undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-undang nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Terdapat beberapa pasal yang menjelaskan mengenai kejahatan yang dilakukan dengan memanfaatkan teknologi internet dan jaringan

komputer seperti transimis, disribusi atau penyebaran yang dapat diakses pada konten yang illegal yang terdiri dari :

1) Kesusilaan (pasal 27 ayat 1 UU ITE)
2) Perjudian (pasal 27 ayat 2 UU ITE)
3) Penghinaan dan pencemaran nama baik (pasal 27 ayat 3 UU ITE)
4) Pemerasan dan pengancaman (Pasal 27 ayat 4 UU ITE)
5) Adanya berita bohong yang menyesatkan dan merugikan konsumen (Pasal 28 ayat 1 UU ITE)
6) Menimbulkan rasa benci yang didasari pada SARA (pasal 28 ayat 2 UU ITE)
7) Mengirimkan informasi yang berisikan ancaman kekerasan serta menakut-nakuti seseorang (pasal 29 UU ITE) (Sari, 2018).

Berdasarkan paparan peraturan yang disebutkan di atas terdapat beberapa hal yang perlu dilakukan agar dapat meminimalisir kejahatan cyber di Indonesia antara lain

a. Perlu adanya kesadaran masyarakat untuk dapat mengatasi dan menggunakan teknologi informasi dan komunikasi secara dengan tetap menerapkan UU ITE dalam melakukan transaksi elektronik (Ketaren, 2016)
b. Pemerintah harus mampu menyampaikan peraturan dan penggunaan teknologi informasi yang baik dan benar dalam bentuk penyuluhan dan sosialisasi kepada masyarakat. Pemerintah juga harus mampu dengan tegas dalam menerapkan hukum yang sudah ditentukan terhadap para pelaku kejahatan siber
c. Aparat hukum harus lebih memahami tentang hukum cyber (cyber law) sebagai tameng atau pelindung dari kejahatan cyber agar tidak semakin meluas dan merajalela dalam kehidupan masyarakat (Sari, 2018).

D. Teknologi Kriptografi

Selain dengan menggunakan peraturan yang sudah diterapkan dalam mengatur penggunaan Teknologi Informasi khususnya dalam teknologi internet, terdapat beberapa teknologi yang dapat menangkal kejahatan cyber. Salah satunya adalah teknologi Kriptografi yang mana asal kata dari kata Kriptografy (Cryptography) memiliki dua suku kata antara lain kripto artinya menyembunyikan sedangkan graphia adalah tulisan. Sehingga dari dua suku kata tersebut diperoleh pengertian dari Kriptografy yaitu teknik-teknik matematika yang memiliki hubungan dengan aspek keamanan informasi dalam bentuk kerahasiaan data, integrasi data, autentifikasi data maupun keabsahan data (Amin, 2017). Terdapat beberapa pengertian tentang teknologi kriptografi, seperti yang diungkapkan oleh Pabokory dkk adalah suatu ilmu seni yang diguankan untuk memproteksi pengiriman data dengan merubah data tersebut menjadi suatu kode tertentu yang nantinya dapat dijadikan alat melindunginya sehingga pada saat data tersebut akan dibuka diperlukan suatu kunci dalam mengubah kode tersebut (Pabokory et al., 2016). Asal mulanya teknologi kriptografi diperoleh dari cara atau metode dengan enkripsi klasik dengan memanfaatkan pensil dan kertas, atau bahan lain yang merupakan alat mekanik sederhana. Metode pada teknologi ini dikelompokan menjadi dua jenis yaitu algoritma transposisi (transposisition cipher) cara yang digunakan untuk merubah posisi susunan huruf baik besar maupun kecil dan algoritma substitusi (substitution cipher) mengganti setiap huruf yang yang ada pada suatu kelompok ke sebuah huruf dari kelompok yang lainva (Pabokory et al., 2016).

a. Sejarah Kriptografi

Penggunaan kriptografi sudah dimanfaatkan oleh masyarakat sejak 4000 tahun yang lalu oleh masyarakat Mesir dengan bentuk hieroglyph. Bentuk dari tulisan ini bukanlah menjadi dasar dalam menulis suatu pesan yang ada pada jaman itu. Awalnya Julius Cesar saat itu ingin mengirimkan pesan rahasia kepada seorang jendral yang waktu itu terjadi peperangan, dan pesan tersebut dikirimkan melalui seorang kurir. Kemudian Julius Caesar melakukan strategi dengan cara mengacak huruf yang ada dipesan tersebut agar tidak mudah dipahami oleh musuhnya dan yang hanya bisa memahami adalah si penerima pesan yaitu jendralnya. Jendral sudah diberikan cara untuk memahami dalam membaca tulisan tersebut, yang dilakukan oleh Julius Caesar adalah dengan mengganti semua huruf a, b, c menjadi d, e,f dan seterusnya (Ariyus, 2008).

b. Istilah yang dimiliki dalam Kriptografi

Terdapat beberapa istilah atau terminology yang digunakan dalam teknik kriptografy antara lain :

1. Pesan, plaintext dan ciphertext

   Bentuk pesan yang disampaikan dalam data dan informasi yang mana bentuk ciphertext merupakan bentuk lain yang tidak dapat dipahami oleh orang yang tidak berkepentingan atau dalam pesan yang tersandi.

2. Pengirim dan penerima

   Pengirim atau sender merupakan entitas atau seseorang yang menyampaikan informasi kepada orang lain. Penerima atau receiver merupakan seseorang atau orang yang menerima pesan atau informasi yang disampaikan.

3. Enkripsi dan deskripsi

Suatu proses yang digunakan untuk menyandikan dan mengembalikan kata sandi yang sudah di acak untuk dapat dipahami oleh si penerima pesan.

4. Alogoritma Kriptografi dan Kunci

   Kriptografi yang digunakan untuk melakukan dan mengatasi masalah keamanan dengan penggunaan kunci. Kunci yang digunakan adalah parameter yang berupa string atau deretan bilangan.

5. Sistem Kriptografi

   Kumpulan algoritma kriptografi yang digunakan baik itu dalam plainteks maupun chiperteks dimana disertai dengan adanya kunci untuk membacanya.

6. Kriptanalisis dan kriptografi

   Ilmu atau seni yang digunakan dalam memecahkan chiperteks yang sudah dijadikan plainteks tanpa mengetahui kunci yang diberikan (Natsir, 2016).

E. Penanganan Cyber Crime dengan teknik Kriptografi

Bentuk pertukaran antara informasi dan data yang dilakukan dalam proses komunikasi memerlukan keamanan dan kerahasiaan yang menjadi hal penting, misalnya komunikasi yang disampaikan kepada penerima merupakan informasi yang benar atau sesuai dengan apa yang disampaikan oleh pengirim pesan dapat dirubah datanya oleh oknum tertentu sehingga dapat menimbulkan kesalahpahaman dan menjatuhkan pihak dari si pengirim pesan. Selain itu bentuk pesan yang memiliki sifat rahasia dapat dimanfaatkan oleh pihak lain untuk kepentingannya sendiri. Sebagai contoh pada saat dunia perbankan mengalami suatu kasus yang dilakukan oleh seorang Steven Haryanto dimana Steven menciptakan

sebuah situs asli tetapi palsu yang memiliki kesamaan dalam melakukan layanan lewat internet BCA. Situs tersebut dimanfaatkan oleh nasabah yang mana nasabah akan mengetik situs asli internet BCA akan tetapi directnya (akses) ke situs yang dibuat oleh Steven, sehingga pada saat nasabah melakukan transaksi dengan memasukan identitas pengguna (user ID) dan nomor identifikasi personal (PIN) maka akan tersimpan sebagai histori dari situs tersebut. Terdapat 130 nasabah yang mengalami pencurian dari data-data yang dimilikinya namun, berdasarkan pengakuan dari Steven dimana membuat situs tersebut adalah sebagai bentuk agar public member memiliki perhatian pada saat melakukan kesalahan dalam pengetikan alamat situs, bukan untuk mendapatkan keuntungan pribadi. Akan tetapi para nasabah BCA merasa memiliki kehilangan uang yang dimiliki padahal para nasabah tidak melakukan transaksi. Nasabah merasa kebobolan dikarenakan para nasabah menggunakan fasilitas internet banking yang dilakukan melalui situs klik BCA, pada saat user ID dan PIN yang dimiliki nasabah mengakses situs tersebut akan ditangkap oleh situs asli tapi palsu yang dimiliki oleh si pelaky sehingga akan lebih mudah disalahgunakan dalam penggunaan data pribadi yang dimiliki oleh nasabah (Sari, 2018).

Teknik yang digunakan untuk mengintegrasikan dan mengauthetikasikan suatu data ID sangat diperlukan demi penyelidikan serta pembuktian dalam kejadian kejahatan cyber. Teknik yang dapat mengamankan dan menjamin proses autentifikasi (verifikasi) dari data yang dimiliki adalah dengan cara teknik kriptografi yang mana dengan menggunakan dua proses yaitu enkripsi (dengan mengacak data yang ada dan tidak dapat terbaca oleh orang-orang yang tidak berhak mengetahui isi informasi tersebut) dan deskripsi (menjadikan data yang sudah di enkripsi dapat diketahui dan dibaca oleh si penerima pesan)

Konsep yang ada dari proses algoritma ini adalah adanya relasi atau hubungan antara dua himpunan yang berisikan chipherteks dan plainteks, yang mana mejadikan fungsi enkripsi dan deskripsi sebagai pemetaan dalam himpunan data tersebut. Misalnya adalah P yang menyatakan plainteks dan C yang merupakan cipherteks sehingga fungsi dari enkripsi E akan memetakan P ke C dengan kode atau symbol sebagai berikut (Pabokory et al., 2016):

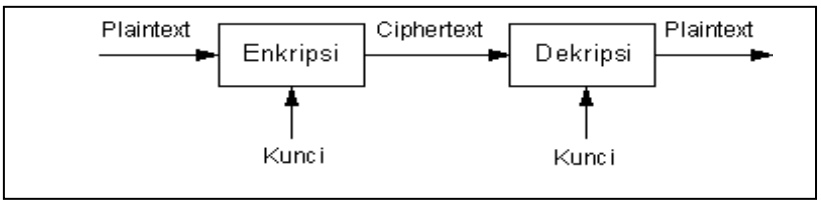
E(P) = C ➔ memetakan P ke C dengan menggunakan fungsi enkripsi,

D(C) = P ➔ memetakan C ke P dengan menggunakan fungsi deskripsi

Proses enkripsi sudah dilakukan sehingga perlu dilakukan deskripsi agar pesan yang sudah diacak dapat dikembalikan ke bentuk awal dengan persamaan sebagai berikut :

D(E(P)) = P

Secara sederhana berikut ini gambar proses enkripsi/dekripsi dari teknik kriptografi



Gambar 1 : Alur proses enkripsi dan deskripsi dengan menggunakan elemen kunci

Hal yang perlu dilakukan dalam mengubah plainteks ke ciperteks disebut sebagai enkripsi atau enciphement. Untuk mengubah cipherteks menjadi plainteks menggunakan fungsi decryption atau decipherment.

Terdapat beberapa teknik dasar yang digunakan dalam kriptografi seperti yang diungkapkan oleh Mukodim antara lain :

a. Substitusi

Pada teknik ini yang pertama dilakukan adalah dengan membuat tabel subsitusi, kemudian tabel tersebut dibuat sesuai dengan keinginan dari pengguna dengan catatan bahwa penerima pesan harus memiliki tabel yang dibuat yang nantinya akan digunakan pada saat deskripsi data. Bila tabel subsitusi yang dibuat ditampilkan secara acak, maka orang tidak berhak mengalami kesulitan dalam memecahkan ciphertext.

b. Blocking

Sistem enkripsi terkadang membagi plaintext menjadi blok-blok yang terdiri dari beberapa karakter yang kemudian dienkripsikan secara independen. Dengan menggunakan enkripsi blocking dipilih jumlah lajur dan kolom untuk penulisan pesan. Jumlah lajur atau kolom menjadi kunci bagi kriptografi dengan teknik ini. Plaintext dituliskan secara vertical ke bawah berurutan pada lajur, dan dilanjutkan pada kolom berikutnya sampai seluruhnya tertulis. Ciphertext-nya adalah hasil pembacaan plaintext secara horizontal berurutan sesuai dengan bloknya.

c. Permutasi

Salah satu teknik enkripsi yang terpenting adalah permutasi atau sering disebut transposisi. Teknik ini memindahkan atau merotasikan karakter dengan aturan tertentu. Prinsipnya adalah berlawanan dengan teknik substitusi. Pada teknik permutasi, identitas karakternya tetap, namun psosisinya yang diacak. Sebelum dilakukan permutasi, umumnya plaintext terlebih dahulu dibagi menjadi blok-blok dengan panjang yang sama

d. Ekspansi

Metode sederhana yang dilakukan dengan cara mengacak pesan yang akan dikirim dengan cara melebarkan pesan tersebut dengan aturan tertentu.

e. Penempatan

Metode ini dilakukan dengan cara mengurangi panjang atau jumlah blok yang akan dikirim yang kemudian akan disembunyikan termasuk isi pesan (Mukodim, 2002).

III. KESIMPULAN

Pengamanan informasi dan data dari kejahatan dengan menggunakan teknik kriptografi sangat membantu para pengguna teknologi informasi saat ini. Karena teknik ini akan melindungi data yang kemudian disandikan sehingga para penyadap data tidak dapat mengeri isi data tersebut. Dalam teknik kriptografi ini terdapat dua proses yaitu enkripsi dan dekripsi. Proses enkripsi adalah proses yang mengubah data asli menjadi data sandi, sedangkan proses dekripsi adalah proses mengembalikan data sandi menjadi data aslinya. Kriptografi menjadi salah satu teknik yang sedang dikembangkan untuk peningkatan proses pengamanan data dan informasi agar pengguna teknologi selalu merasa nyaman dan aman. Selain itu walaupun menggunakan teknik kriptografi, tetap perlu adanya penguatan hukum yang diterapkan dalam mengatur kejahatan siber agar para pengguna yaitu masyarakat akan tetap terlindungi terutama dalam hal data transaksi elektronik.

DAFTAR PUSTAKA

Abidin, D. Z. (2015). Kejahatan dalam Teknologi Informasi dan Komunikasi. Jurnal Ilmiah Media Processor, 10(2), 1–8. http://ejournal.stikom-db.ac.id/index.php/processor/article/view/107/105

Agustina, E. R., & Kurniati, A. (2009). Pemanfaatan Kriptografi dalam Mewujudkan Keamanan Informasi pada e-Voting di Indonesia. Seminar Nasional Informatika, 2009(semnasIF), 22–28.

Amin, M. M. (2017). Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks. Pseudocode, 3(2), 129–136. https://doi.org/10.33369/pseudocode.3.2.129-136

Ardiyanti, H. (1986). Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. 95–110.

Ariyus, D. (2008). Pengantar Ilmu Kriptografi (Teori, Analisisi dan Implementasi.

Ersya, M. P. (2018). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. Moral and Civic Education, 1(1), 50–62. https://doi.org/10.24036/8851412020171112

Handayani, P. (2016). Penegakan Hukum Terhadap Kejahatan Teknologi Informasi (Cyber Crime). Jurnal Dimensi, 1–8.

Ketaren, E. (2016). Cybercrime, Cyber Space, dan Cyber Law. Times, 5(2), 35–42. http://stmik-time.ac.id/ejournal/index.php/jurnalTIMES/article/viewFile/556/126

Mukodim, D. (2002). Tinjauan Tentang Enkripsi dan Dekripsi, Suatu Teknik Pengamanan Data dengan Penyandian RSA. Komputer Dan Sistem Intelijen (KOMMIT), 92–100.

Natsir, M. (2016). Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office. Jurnal Format, 6(2).

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2016). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer, 10(1), 20. https://doi.org/10.30872/jim.v10i1.23

Rahmawati, I. (2017). the Analysis Ofcyber Crime Threat Risk Management To Increase Cyber Defense. Jurnal Pertahanan & Bela Negara, 7(2), 51–66. https://doi.org/10.33172/jpbh.v7i2.193

Sari, N. W. (2018). Kejahatan Cyber dalam Perkembangan Teknologi Informasi Berbasis Komputer. Jurnal Surya Kencana Dua: Dinamika Masalah Hukum Dan Keadilan, 5(2), 577–593. http://openjournal.unpam.ac.id/index.php/SKD/article/download/2340/1887

Sudarwanto, A. S. (2009). Cyber-Bullying Kejahatan Dunia Maya Yang "Terlupakan." In Jurnal Hukum PRO JUSTITIA (Vol. 27, Issue 1, pp. 1–16).

Suhendar, A. (2013). Keterkaitan antar bidang pembinaan ketahanan nasional/ pembinaan gatra (+). Keterkaitan Antar Bidang Pembinaan Ketahanan Nasional/Pembinaan Gatra.