

PRAKTIKUM KRIPTOGRAFI





Disusun Oleh:

140810210059 - Prames Ray Lopian

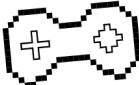
**PROGRAM STUDI S-1 TEKNIK INFORMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PADJADJARAN JATINANGOR**

2023

Soal



Tugas



1. Cari penjelasan dan perbedaan lebih lanjut terkait perbedaan kriptografi Klasik dan Modern, termasuk jenis/tipe dari masing-masing kriptografi!
2. Cari 3 (atau lebih) contoh lain dari aplikasi/penerapan kriptografi, dan jelaskan secara singkat peran dan logika kriptografi dalam penerapan tersebut! **(Selain yang sudah disebutkan di slide sebelumnya)**
3. Cari contoh algoritma kriptografi klasik dan 1 contoh algoritma modern, lalu berikan penjelasan singkatnya!
4. Pilih algoritma dari slide 16, coba eksplorasi terkait algoritma tersebut, lalu tuliskan penjelasan hasil eksplorasi kalian!

Format: Tugas1_NPM.pdf

Deadline: H-1 Praktikum Berikutnya

JAWABAN

1. Perbedaan Kriptografi Klasik dan Modern

- Kriptografi Klasik

Algoritma kriptografi klasik digunakan sejak sebelum era komputerisasi dan kebanyakan menggunakan teknik kunci simetris. Metode menyembunyikan pesannya adalah dengan teknik substitusi atau transposisi atau keduanya.

Teknik substitusi adalah menggantikan karakter dalam plaintext menjadi karakter lain yang hasilnya adalah ciphertext. Sedangkan transposisi adalah teknik mengubah plaintext menjadi ciphertext dengan cara permutasi karakter. Kombinasi keduanya secara kompleks adalah yang melatarbelakangi terbentuknya berbagai macam algoritma kriptografi modern. Contoh algoritma kriptografi klasik yaitu: *Caesar Cipher*, *Vigenere Cipher*, dan *Hill Cipher*.

- Kriptografi Modern

Algoritma kriptografi modern merupakan suatu perbaikan yang mengacu pada kriptografi klasik. Algoritma ini menggunakan pengolahan simbol biner yang dibentuk dari kode ASCII (*American Standard Code for Information Interchange*) karena berjalan mengikuti operasi komputer digital, sehingga membutuhkan pengetahuan dasar matematika untuk menguasainya. Algoritma ini memiliki tingkat kesulitan yang kompleks yang menyebabkan kriptanalisis sangat sulit memecahkan ciphertext tanpa mengetahui kuncinya.

Adapun jenis kunci dalam kriptografi modern terdiri dari 3 yaitu: simetri, asimetri, dan hibrida. Pada kriptografi modern terdapat berbagai macam algoritma yang dimaksudkan untuk mengamankan informasi yang dikirim melalui jaringan komputer. Contoh kriptografi modern yaitu MD5, RC4, AES dan lain-lain.

- Perbandingan

Dilihat dari algoritma kriptografi klasik dan modern yang telah dipaparkan di atas, ternyata cara kerjanya sangat jauh berbeda. Kriptografi klasik prosesnya sangat sederhana dan umumnya menggunakan karakter huruf A sampai Z, sehingga sangat memungkinkan untuk dipecahkan dengan mudah sekalipun dengan cara manual. Sementara kriptografi modern menggunakan mode bit biner yang dibentuk dari kode ASCII dengan sangat kompleks sehingga susah dipecahkan walaupun menggunakan alat.

Dari segi kerahasiaan, integritas data, otentikasi, dan ketiadaan penyangkalan pesan, algoritma kriptografi modern jauh lebih terjaga daripada kriptografi klasik, sehingga memungkinkan digunakan sekalipun pesan tersebut sangat rahasia. Kriptografi modern lebih efektif, efisien, dan praktis digunakan dalam kehidupan sehari-hari dari pada kriptografi klasik. Namun, walaupun banyak kelebihan kriptografi modern dari pada kriptografi klasik, tidak tertutup ada kelemahannya yakni sangat tergantung dengan teknologi. Ketika teknologi tidak bisa digunakan maka kriptografi modern tidak akan berfungsi, sementara kriptografi klasik akan tetap berfungsi sekalipun tidak menggunakan teknologi.

2. 3 Contoh pengaplikasian Kriptografi beserta penjelasan dan logika cara kerjanya.

- VPN (*Virtual Private Network*)

VPN adalah layanan yang memungkinkan penggunanya untuk mengakses internet melalui jaringan pribadi virtual yang aman, bahkan ketika terhubung ke jaringan internet publik seperti Wifi umum atau jaringan seluler. Tujuan utama dari VPN adalah meningkatkan privasi dan keamanan online penggunanya.

VPN menggunakan kriptografi untuk menyembunyikan lalu lintas internet Anda, sehingga tidak ada yang bisa melihat data yang Anda kirim atau terima saat terhubung ke internet melalui VPN. Ini membantu melindungi privasi online Anda.

- Sertifikasi SSL (*Secure Sockets Layer*)

Sertifikat SSL adalah tanda keamanan digital yang dikeluarkan oleh otoritas sertifikat (*Certificate Authorities*) yang dapat dipercaya. Sertifikat ini digunakan oleh situs web untuk mengenkripsi data yang dikirimkan antara browser pengguna dan server web. Ketika situs web memiliki sertifikat SSL, Anda dapat mengidentifikasinya melalui protokol "https://" dan simbol gembok yang muncul di bilah alamat browser.

Ketika pengguna mengunjungi situs web yang menggunakan sertifikat SSL, kriptografi digunakan untuk mengenkripsi data yang dikirimkan antara browser pengguna dan server situs web. Ini melindungi informasi pribadi pengguna ketika berinteraksi dengan situs web tersebut.

- IoT (*Internet Of Things*)

IoT, yang merujuk pada jaringan perangkat fisik yang terhubung ke internet. Ini termasuk perangkat seperti lampu pintar, kamera keamanan, termostat pintar, kendaraan otonom, dan banyak lagi. Perangkat IoT ini dapat mengumpulkan data, berkomunikasi satu sama lain, dan dengan server di internet.

Keamanan IoT sangat penting karena perangkat ini mengumpulkan, mengirimkan, dan mengakses data yang mungkin sangat sensitif. Jika perangkat IoT tidak aman, ini dapat membuka celah bagi serangan yang merugikan, seperti pencurian data, pengendalian perangkat oleh pihak yang tidak berwenang, atau serangan terhadap jaringan lebih besar. Untuk itu kriptografi digunakan untuk mengenkripsi data antara perangkat dan server, memastikan otentikasi perangkat IoT tersebut, menjaga integritas data, dan peran keamanan lainnya.

3. Contoh algoritma Kriptografi Klasik dan Modern:

- Kriptografi Klasik: Caesar Cipher

Metode penyandian ini dinamakan Caesar Cipher, setelah digunakan Julius Caesar untuk berkomunikasi dengan para panglimanya. Dalam kriptografi

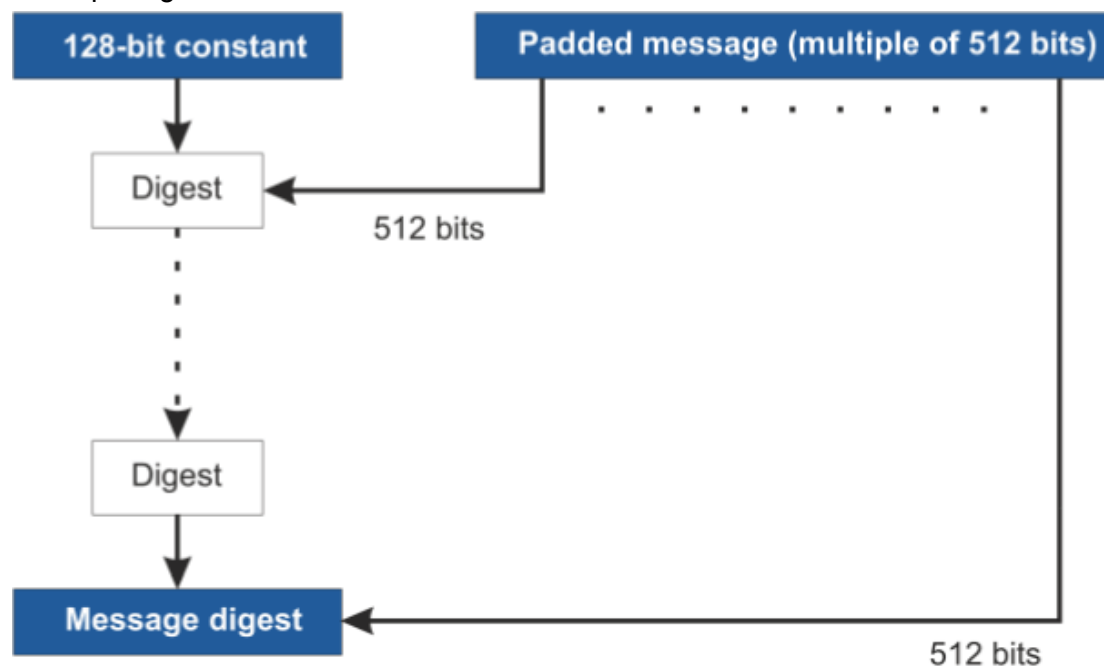
Caesar Cipher dikenal dengan beberapa nama seperti: shift cipher, Caesar's code atau Caesar shift. Caesar Cipher merupakan teknik enkripsi yang paling sederhana dan banyak digunakan. Cipher ini berjenis cipher substitusi, dimana setiap huruf pada plaintextnya digantikan dengan huruf lain yang tetap pada posisi alfabet [4]. Misalnya diketahui bahwa pergeseran = 3, maka huruf A akan digantikan oleh huruf D, huruf B menjadi huruf E, dan seterusnya.

- Kriptografi Modern: Algoritma Simetris

Algoritma Simetris adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Algoritma kriptografi simetris sering disebut algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci, dan mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu. Kelebihan dari algoritma kriptografi simetris adalah waktu proses untuk enkripsi dan dekripsi relatif cepat. Hal ini disebabkan efisiensi yang terjadi pada pembangkit kunci. Karena prosesnya relative cepat maka algoritma ini tepat untuk digunakan pada sistem komunikasi digital secara real time seperti GSM. Aplikasi dari algoritma simetris digunakan oleh beberapa algoritma di seperti: *Data Encryption Standard* (DES); *Advance Encryption Standard* (AES); *International Data Encryption Algorithm* (IDEA); A5; dan RC4.

4. Eksplorasi salah satu algoritma Kriptografi.

- Deskripsi algoritma:



MD5 Algorithm Structure

Algoritme hashing MD5 (Message-Digest algorithm) adalah fungsi kriptografi satu arah yang menerima pesan dengan panjang berapa pun sebagai

masukan dan mengembalikan sebagai keluaran nilai intisari dengan panjang tetap yang akan digunakan untuk mengautentikasi pesan asli.

Fungsi hash MD5 pada awalnya dirancang untuk digunakan sebagai algoritma hash kriptografi yang aman untuk mengautentikasi tanda tangan digital. Namun MD5 sudah tidak digunakan lagi selain sebagai checksum non kriptografi untuk memverifikasi integritas data dan mendeteksi kerusakan data yang tidak disengaja.

Message-Digest, juga dikenal sebagai fungsi hash, adalah fungsi satu arah; mereka menerima pesan dengan ukuran berapa pun sebagai masukan dan menghasilkan Message-Digest dengan panjang tetap sebagai keluaran.

MD5 adalah algoritma Message-Digest ketiga yang dibuat Rivest. MD2, MD4 dan MD5 memiliki struktur serupa, namun MD2 dioptimalkan untuk mesin 8-bit, dibandingkan dengan dua algoritma selanjutnya, yang dirancang untuk mesin 32-bit. Algoritma MD5 merupakan perpanjangan dari MD4, yang menurut tinjauan kritis cepat namun berpotensi tidak aman. Sebagai perbandingan, MD5 tidak secepat algoritma MD4, namun menawarkan lebih banyak jaminan keamanan data.

Perhitungan nilai intisari MD5 dilakukan dalam tahapan terpisah yang memproses setiap blok data 512-bit beserta nilai yang dihitung pada tahap sebelumnya. Tahap pertama dimulai dengan nilai Message-Digest yang diinisialisasi menggunakan nilai numerik heksadesimal yang berurutan. Setiap tahap mencakup empat lintasan Message-Digest, yang memanipulasi nilai dalam blok data saat ini dan nilai yang diproses dari blok sebelumnya. Nilai akhir yang dihitung dari blok terakhir menjadi intisari MD5 untuk blok tersebut.

- Kekurangan:

Keamanan fungsi hash MD5 dianggap sangat terganggu. Tabrakan dapat ditemukan dalam hitungan detik, dan dapat digunakan untuk tujuan jahat.

Faktanya, pada tahun 2012, spyware Flame yang menyusup ke ribuan komputer dan perangkat di Iran dianggap sebagai salah satu masalah keamanan paling menyusahkan tahun ini. Flame menggunakan tabrakan hash MD5 untuk menghasilkan sertifikat pembaruan Microsoft palsu yang digunakan untuk mengautentikasi sistem penting. Untungnya, kerentanan tersebut ditemukan dengan cepat, dan pembaruan perangkat lunak dikeluarkan untuk menutup lubang keamanan ini. Hal ini melibatkan peralihan penggunaan SHA-1 untuk sertifikat Microsoft.

- Kelebihan:

Meskipun diketahui memiliki masalah keamanan, MD5 masih digunakan untuk hashing kata sandi dalam perangkat lunak. MD5 digunakan untuk menyimpan kata sandi dengan hash kata sandi satu arah, tetapi ini bukan salah satu hash yang direkomendasikan untuk tujuan ini. MD5 umum dan mudah digunakan, dan pengembang sering kali masih memilihnya untuk hashing dan penyimpanan kata sandi.

MD5 juga masih digunakan dalam keamanan siber untuk memverifikasi dan mengautentikasi tanda tangan digital. Dengan menggunakan MD5, pengguna dapat memverifikasi bahwa file yang diunduh adalah asli dengan mencocokkan kunci publik dan privat serta nilai hash. Namun, karena tingginya tingkat tabrakan MD5, algoritma intisari pesan ini tidak ideal untuk memverifikasi integritas data atau file karena pelaku ancaman dapat dengan mudah mengganti nilai hash dengan nilai hash mereka sendiri.

Algoritma message-digest MD5 dapat digunakan untuk memastikan bahwa data sama seperti aslinya dengan memeriksa apakah outputnya sama dengan inputnya. Jika file diubah secara tidak sengaja, masukan akan menghasilkan nilai hash yang berbeda, yang kemudian tidak lagi cocok. Ini memberitahu Anda bahwa file tersebut rusak. Namun, ini hanya efektif jika data telah rusak secara tidak sengaja, dan tidak jika terjadi gangguan yang berbahaya.

- Contoh

Biasanya MD5 digunakan untuk meng-enkripsi data yang bersifat rahasia dan tidak ingin diketahui oleh orang lain. contoh nya yang paling sering adalah dalam membuat sebuah login. biasanya data password pada database, akan di enkripsi terlebih dahulu. agar jika pun ada orang yang tidak bertanggung jawab yang masuk dan dapat melihat isi database, maka ia tidak akan bisa menebak password yang tersimpan di sana.(karena sudah di enkripsi dengan MD5).

REFERENSI

1. <http://seminar.uny.ac.id/semnasmatematika/sites/seminar.uny.ac.id.semnasmatematika/files/full/T-37.pdf>
2. <https://www.techtarget.com/searchsecurity/definition/MD5>
3. <https://www.okta.com/identity-101/md5/>
4. <https://www.malasngoding.com/pengertian-penggunaan-dan-cara-membuat-md5-pada-php/>