LAPORAN

KEAMANAN PERANGKAT LUNAK

DelApotek – Aplikasi Penyediaan Obat-obat Mahasiswa Del

Menggunakan Penerapan Applied Cryptography

DISUSUN OLEH :

11S19017 Montana Gurning
11S19020 Talenta Maria Sihotang
11S19021 Trivena Yuli Necia Panjaitan
11S19037 Rio Efraim Simanjuntak
11S19043 Hari D.S.J Siburian
11S19045 Josua Gaolus Nainggolan

PROGRAM STUDI SARJANA INFORMATIKA

FAKULTAS INFORMATIKA DAN TEKNIK ELEKTRO

INSTITUT TEKNOLOGI DEL

T.A. 2021/2022

CRYPTOGRAPHY

Cryptography adalah salah satu aspek di dunia cyber security yang memiliki peran penting dalam melindungi data-data informasi dan juga saluran komunikasi. Secara mendasar, cryptography adalah metode yang sangat erat kaitannya dengan enkripsi, yakni proses konversi data ke dalam format atau kode tertentu. Cryptography merupakan suatu cara untuk keamanan informasi. Crypto berasal dari dua kata yaitu crypto dan graphen. crypto berarti secret atau rahasia dan graphien berarti writing atau menulis. Jadi Cryptography merupakan ilmu-ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan, dan informasi seperti kerahasiaan,integritas data, dan otentikasi. Ada beberapa kategori dimana aplikasi dikatakan aman yaitu :

1. Confidentiality

   Confidentiality berarti bagaimana terjaganya kerahasiaan informasi yang aman. Disini berbicara bagaimana agar pihak-pihak yang tidak terkait tidak bisa mengakses pesan yang ada pada aplikasi. Pada **proyek** yang telah kami buat, **confidentiality** dapat dilihat dari terjaganya kerahasiaan password yang tersimpan pada database sehingga password tidak diketahui oleh orang lain dan juga kerahasiaan notes-notes yang dibuat oleh user sehingga notes tersebut aman dan tidak bisa dilihat oleh orang lain.

2. Data Integrity

   Data Integrity maksudnya adalah terjaganya keaslian data dan pesan tidak bisa dimanipulasi oleh pihak yang tidak bertanggung jawab. Pada **proyek** Buddyject yang telah kami buat, dapat dilihat pada fitur-fitur seperti my notes, sticky notes, dan To do list. Ketika user melakukan login dan berhasil mengakses website, tentunya user bisa mengakses fitur-fitur yang ada seperti membuat catatan. Ketika user membuat catatan, maka catatan tersebut akan tersimpan secara otomatis dan dapat dipastikan bahwa data tersebut asli dibuat oleh user yang telah melakukan login dan catatan tersebut tidak bisa dimanipulasi oleh pihak-pihak yang tidak bersangkutan atau pihak yang tidak berwenang.

3. Authentication

   Authentication adalah bagaimana meyakinkan dan mengetahui bahwa pengirim pesan adalah asli dan bukan merupakan pihak ketiga yang sedang menyamar atau bisa

dibilang hacker. Disini harus bisa dipastikan bahwa pihak-pihak yang berkomunikasi benar adanya untuk mencegah adanya hacker. Dalam Buddyject sendiri hal ini dapat dipastikan dengan proses registrasi dan login yang telah dilakukan sebelum mengakses fitur. Dimana, pada proses registrasi user wajib mengisi email dan password yang pastinya berbeda untuk setiap user yang mana nantinya datanya juga akan langsung tersimpan pada database dari proyek.

4. Non Repudiation

   Non Repudiation adalah memastikan bahwa pengirim pesan ketika melakukan suatu aktivitas pada aplikasi, dapat dipastikan bahwasanya dia lah yang melakukan hal tersebut sehingga si pengirim pesan tidak dapat menyangkal bahwa hal yang dilakukannya memang merupakan dia yang mengerjakan.Pada Proyek Buddyject ini ketika user membuat catatan pada sticky notes maka akan tersimpan tanggal dan waktu kapan user membuat catatan tersebut. Tentunya sebelum mengakses fitur sticky notes tersebut, user harus melakukan login sehingga user tidak bisa menyangkal bahwa dia lah yang membuat catatan tersebut.

   Salah satu proses bisnis yang dapat dilakukan dengan penerapan algoritma Kriptografi yaitu dengan Terminologi. Adapun bagian-bagian yang termasuk dalam Terminologi adalah sebagai berikut:

   A. Pesan, Plainteks, dan Cipherteks

      Pesan (message) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah plainteks (plaintext) atau teks-jelas (cleartext). Pesan tidak hanya berupa teks, tetapi juga dapat berbentuk gambar (image), suara (audio), video, atau berkas biner lainnya.Pesan perlu disandikan ke bentuk lain yang tidak dipahami agar tidak dapat dimengerti maknanya oleh pihak lain. Bentuk pesan yang tersandi disebut cipherteks (ciphertext) atau kriptogram (cryptogram). Cipherteks harus dapat ditransformasikan kembali menjadi plainteks semula agar pesan yang diterima bisa dibaca.

   B. Pengirim dan Penerima

      Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (sender) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima

(receiver) adalah entitas yang menerima pesan. Entitas di sini dapat berupa orang, komputer, kartu kredit, dan sebagainya.

C. Enkripsi dan Dekripsi

Proses menyandikan plainteks menjadi cipherteks disebut enkripsi (encryption) atau enciphering (standar nama menurut ISO 7498-2). Sedangkan proses mengembalikan cipherteks menjadi plainteks semula disebut dekripsi (decryption) atau deciphering Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Keuntungan dari enkripsi adalah kode asli kita tidak dapat dibaca oleh orang lain.

Dekripsi adalah proses mengembalikan suatu informasi dengan cara tertentu dan sesuai dengan algoritma enkripsi yang dipakai. Dekripsi merupakan proses kebalikan dari proses enkripsi, mengubah ciphertext kembali ke dalam bentuk plain text. Proses utama dalam suatu algoritma kriptografi adalah enkripsi dan deskripsi.

D. Cipher dan kunci

Cipher atau algoritma kriptografi adalah aturan untuk enchipering dan deciphering, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa cipher memerlukan algoritma yang berbeda untuk enchipering dan deciphering. Kunci (key) adalah parameter yang digunakan untuk transformasi enchipering dan deciphering. Kunci biasanya berupa string atau deretan bilangan.

E. Penyadap

Penyadap (eavesdropper) adalah orang yang mencoba menangkap pesan selama ditransmisikan. Tujuan penyadap adalah untuk mendapatkan informasi sebanyak-banyaknya mengenai sistem kriptografi yang digunakan untuk berkomunikasi dengan maksud untuk memecahkan cipherteks.

F. Kriptanalisis dan Kriptologi

Kriptanalisis (cryptanalysis) adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui kunci yang digunakan.

Pelakunya disebut kriptanalis. Kriptologi (cryptology) adalah studi mengenai kriptografi dan kriptanalisis.

Pada Proyek BuddyJect kami menggunakan terminologi enkripsi. Seperti yang telah dibahas sebelumnya, Enkripsi merupakan proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Pada website Buddy Ject, password disimpan pada database SQL yog dan password yang telah disimpan tersebut akan diubah ke dalam huruf-huruf tertentu. Tujuan pengubahan password dalam database yang berbeda dengan aslinya adalah agar hacker tidak dengan mudah meretas password dari user dan menghindari kejahatan yang akan dilakukan oleh user.Penyimpanan password tersebut disimpan dengan menggunakan teknik MD5 yaitu salah jenis enkripsi satu arah yang banyak digunakan pada aplikasi website untuk keperluan seperti menyimpan password user/member yang tergabung ke dalam website. Dengan menggunakan MD5 tentunya kerahasiaan password user lebih aman dan bisa terjaga dengan baik.

id	email	password	name
1	laura@yahoo.com	$2y$10$xxIYPdrKKGCf8Q6zaakF4O8aGar0wWnnMeBjsCJKsX5LRNvVR0qDm	Laura
2	dg@gmail	$2y$10$D06.pQ1Y2DyC1eDBb65CNOTS3.wG1bRsm28YsFV1rM0QsHzJsGJMG	saya
3	okee@gmail.com	$2y$10$7isdVq4irEoVCPdqMdUOE.qpTQBmEp9tGcwMttc8RE9LY7MiBak0u	saya
4	laurasinagaa@yahoo.com	$2y$10$Sx8Ov8Re2gHUwUbumseYjOeFtxU3t0Dn2maGGc5G6MmWMLrvVhWJi	laura sinaga
5	laurasinaga99@yahoo.com	$2y$10$81Vq7kca.rZ3Kz9cmnJZoOiV298hP1PJyRG1usdtBBNhi843/uiG2	laura sinaga
6	estermartogi@gmail.com	$2y$10$/D2z19k35/3LvU8g5yYTN.QCPkGBAKg2wQB6LRywcU5AOTi5QqyAu	Ester martogi
7	rinanose@gmail.com	$2y$10$QPXiVjOSQ/0LKq2HCohi4eKqGhwyGOOavUChdWVfCDbebD.eHumGq	rina