

## **ABSTRAK**

*Pada kriptografi terdapat sebuah fungsi checksum yang sesuai untuk aplikasi keamanan seperti otentikasi dan integritas pesan yang disebut dengan fungsi Hash. MD5 merupakan salah satu fungsi dari kriptografi yang dapat membangkitkan kode unik dari suatu file dan dapat mendeteksi perubahan isi dari suatu file walaupun perubahan tersebut sangat kecil. Perubahan dapat terdiri dari penambahan, pengurangan atau penggantian isi dari suatu file. MD5 merupakan hash satu arah sehingga kode yang dihasilkan dari suatu data sangat sulit untuk dikembalikan ke kode sumbernya. Saat ini keamanan terhadap data yang tersimpan dalam perangkat seperti komputer dan smartphone Android sudah menjadi persyaratan mutlak. Dalam hal ini sangat terkait dengan betapa pentingnya data tersebut bagi orang-orang yang berkepentingan, apakah data tersebut masih asli. Data tersebut tidak berguna lagi apabila telah disadap oleh orang yang tidak berhak, atau telah termodifikasi tanpa sadar saat transfer data. Internet sebagai merupakan salah satu media teknologi informasi yang dapat memberikan data dan informasi dengan luas, lengkap dan terbaru. Pengguna dapat saling bertransfer data seperti file dokumen, aplikasi, kompresi dan teks melalui jaringan Internet. Seringkali, keamanan terhadap file tersebut juga menjadi perhatian, khususnya keaslian dan keutuhan file. Gagal dalam mengunduh file serta banyaknya malware seperti virus, trojan dan worm dapat mengancam integritas file. Dengan meningkatnya mobilitas masyarakat serta meningkatnya pengguna perangkat Android yang memanfaatkannya sebagai media komunikasi dan transfer data, pengguna dapat memanfaatkan aplikasi ini di perangkat Android mereka agar dapat langsung memverifikasi data-data yang mereka dapatkan/miliki di perangkat Android.*

**Kata kunci :** integritas data, verifikasi, hash, MD5, android.

## ABSTRACT

*In cryptography there is a checksum function that is suitable for security applications such as authentication and message integrity called Hash function. MD5 is one of the cryptographic functions that can generate a unique code (hash) from a file and can detect changes in the contents of a file, even though in very small changes. Changes may consist of addition, subtraction, or replacement of the contents of a file. MD5 is a one-way hash so that the code generated from the data is very difficult to be returned even impossible to its source code. With the increase of peoples mobility and the increase of Android handheld users using it for communication and data transfer media, Android users can use this application so they can quickly verify their stored data within their Android handheld. For now, the security of the data that stored in computer and android handheld becomes more absolute matter. In that case, users will think how important was their data, whether the data still authentic or not. The data is out of use if it have been accessed by people who have no right to it, or modified by data transferring process. Internet is one of information technology media which can provide data and information completetely and up to date. Users can transferring data such as credential document, application files, compressed files, and text via the Internet. Mostly, security of files are also a concern, especially authenticity and integrity of the file. Failure in downloading, not to mention many malware such as viruses, trojans and worms can be a threat for the integrity of files.*

**Keywords :** *data integrity, verification, hash, MD5, android.*