PENGAMANAN KUNCI JAWABAN SERTIFIKASI CCNA MENGGUNAKAN ADVANCED ENCRYPTION STANDARD (AES) DAN MODE OPERASI CIPHER BLOCK CHAINING (CBC)

MIKO PRASETYA WIDI
Program Studi Teknik Informatika - S1, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
URL : http://dinus.ac.id/
Email : 111201005551@mhs.dinus.ac.id

ABSTRAK

Perkembangan teknologi yang semakin pesat dapat membantu pekerjaan dapat diselesaikan dengan cepat dan efisien. Namun tidak semua dengan kecanggihan teknologi sekarang ini memberikan dampak positif bagi pengguna. Dampak negatif yang bisa terjadi adalah masalah keamanan data, pesan, ataupun informasi. Untuk mengurangi atau mencegah tindakan tersebut dibutuhkan metode keamanan data atau lebih dikenal dengan istilah kriptografi.Kriptografi mendukung kebutuhan untuk menjaga aspek keamanan seperti integritas data, keaslian entitas dan keaslian data. Dalam kriptografi mengenal beberapa teknik dalam pengamanan data, namun dalam penelitian ini kriptografi yang digunakan adalah Algoritma AES dan mode operasi CBC.Kedua metode ini dipilih karena menggunakan cukup banyak kunci dalam enkripsi dan dekripsi. Dengan banyaknya kunci yang digunakan akan memperkuat algoritma kriptografi dan dapat menambah kesulitan bagi kriptanalis dalam memecahkan hasil enkripsi tersebut.Salah satu dokumen yang perlu diperhatikan adalah pada sertifikasi CCNA.CCNA merupakan sertifikasi dalam bidang Computer Networking. Dalam hal ini banyak kunci jawaban yang tersebar di media untuk tiap-tiap chapter yang diberikan, dengan demikian dikhawatirkan akan mempermudah peserta untuk mencari jawaban tanpa harus berfikir lebih untuk menyelesaikan soal yang diujikan dan hal ini akan mengurangi kualitas dari pemegang sertifikasi itu sendiri dalam hal pengetahuan tentang mengoperasikan dan memecahkan permasalahan.

Kata Kunci : Kriptografi, Algoritma AES, Mode Operasi CBC, CCNA

SECURING CCNA CERTIFICATION ANSWER KEY USING ADVANCED ENCRYPTION STANDARD (AES) AND CIPHER BLOCK CHAINING (CBC) OPERATION MODE

MIKO PRASETYA WIDI
Program Studi Teknik Informatika - S1, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
URL : http://dinus.ac.id/
Email : 111201005551@mhs.dinus.ac.id

ABSTRACT

Rapid technological developments can help the work can be completed quickly and efficiently. But not all the sophistication of today's technology a positive impact on users. The negative impact that may occur is a matter of security of data, messages, or information. To reduce or prevent the action takes data security methods or better known as kriptografi.Kriptografi support the need to maintain the security aspects such as data integrity, authenticity and originality of the data entities. In cryptography to know some techniques in data security, but in this study the cryptographic algorithm used is AES and mode of operation have been CBC.Kedua method uses quite a lot of keys in encryption and decryption. With so many keys that are used to strengthen cryptographic algorithms and can add to the difficulty in solving encrypted cryptanalyst tersebut.Salah a document that needs to be considered is the CCNA.CCNA certification is a certification in the field of Computer Networking. In this case a lot of the key answers are scattered in the media for each chapter are given, thus it is feared will facilitate participants to find the answer without having to think much to solve problems that are tested and this will reduce the quality of the certification holder itself in terms of knowledge about operate and solve problems.

Keyword : Cryptography, AES Algorithms, Operating Mode CBC, CCNA