

DESAIN PROTOKOL XXX-YYY SEBAGAI PENGAMANAN DALAM PENGIRIMAN JAWABAN SISTEM UJIAN AKHIR NASIONAL (UAN) ONLINE

Sofu Risqi Y.S.¹⁾, Muhamad Al Fikri²⁾, Dimas Dwiki Ismoyo³⁾

Sekolah Tinggi Sandi Negara

Jl.H.Usa Putat Nutug Ciseeng - Bogor, 16120

Telp : 085642863390

E-mail : sofurizky@yahoo.com¹⁾, malfikri87@gmail.com²⁾, dimasismoyo@gmail.com³⁾

Abstrak

Ujian Akhir Nasional (UAN) merupakan salah satu tahapan evaluasi yang diselenggarakan oleh pemerintah untuk mengetahui tingkat keberhasilan dari proses belajar mengajar. Sistem ujian konvensional dengan media kertas membutuhkan biaya, sumber daya waktu dan tenaga yang besar. Oleh karena itu, perlu adanya metode alternatif untuk dapat melaksanakan ujian dengan baik, cepat, akurat, dan efisien. Salah satu metode alternatif tersebut adalah sistem ujian yang dilakukan secara online, melalui media komputer dan koneksi internet. Dengan cara ini, pemerintah dapat menekan baik biaya, waktu, dan sumber daya yang diperlukan untuk melaksanakan ujian. Suatu sistem ujian secara online menuntut ketersediaan data yang jelas dan akurat serta hanya dapat diakses oleh pihak yang sah. Teknik yang banyak digunakan untuk menjaga keamanan data yang tersimpan dalam sebuah sistem melalui media internet adalah kriptografi. Penelitian ini bertujuan untuk menghasilkan rancangan protokol yang dapat digunakan untuk mengamankan data dalam sistem ujian online. Rancangan protokol keamanan data diimplementasikan dengan program simulasi sederhana menggunakan bahasa pemrograman C. Hasil dari penelitian ini adalah sebuah protokol keamanan data yang memenuhi kebutuhan keamanan dari Sistem Ujian Online.

Kata kunci: Kriptografi, Protoko, Keamanan, Sistem Ujian Online

Abstract

National Final Examination is one of the evaluation stages organized by the government to assess the success of the student learning process. Conventional test systems by using papers cost significant amount of time, money, and resources. Therefore, the government needs for alternative methods to be able to conduct the test well, quickly, accurately, and efficiently. One alternative method is the method by using computer and internet connection called Online Examination System. In this way, the government can reduce the cost, time, and resources required to conduct the exam. An online examination system requires the availability of clear and accurate data and can only be accessed by unauthorized parties. Cryptography is a widely used technique for maintaining the security of data stored in a system via the Internet. This research aims to propose a data security protocol design that can be used to secure data in the online examination system. The data security protocol design in this research is implemented by a simple simulation program using the C programming language. The result is a data security protocol that meets the security needs of Online Examination System.

Kata kunci: Cryptography, Protocol, Security, Online Examination System