

ABSTRAK

Nama : Devi Heryani
NIM : 2014081042
Prodi : Teknik Informatika
Judul : Implementasi Algoritma *Rivest Shamir Adleman* (RSA) Berbasis QR-Code pada Aplikasi Pengaman Keaslian Sertifikat TOEFL

Perguruan Tinggi merupakan institusi yang berperan penting dalam mencetak sumber daya manusia (SDM) yang berkualitas. Hal ini juga yang dilakukan oleh Universitas Kuningan sebagai Perguruan Tinggi swasta yaitu dengan menjadikan kelulusan ujian TOEFL sebagai salah satu prasyarat kelulusan jenjang sarjana. Sulitnya ujian TOEFL menyebabkan mahasiswa selalu mencari celah untuk mendapatkan sertifikat tanpa harus mengikuti ujian nya, seperti melakukan pemalsuan sertifikat. Pemalsuan dapat dilakukan karena belum adanya pengaman keaslian pada sertifikat TOEFL yang sedang berjalan, hal ini menyebabkan sulitnya untuk membedakan sertifikat yang asli dan palsu. Maka dari itu, tujuan dari penelitian ini adalah untuk membuat pengaman keaslian menggunakan algoritma RSA berbasis QR-Code. Metode pengembangan perangkat lunak yang digunakan adalah Rational Unified Process (RUP) yang memiliki 4 tahapan : Inception, Elaboration, Construction, dan Transition. Algoritma RSA merupakan algoritma kriptografi asimetris atau algoritma kunci publik yang digunakan untuk penyandian pesan. Algoritma ini terdiri dari 3 tahapan, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Data yang digunakan dalam proses kriptografi adalah nomor sertifikat, yang kemudian disimpan ke dalam bentuk QR-Code dan dicetak pada sertifikat. Pemindaian QR-Code dilakukan menggunakan QR-Code Reader dan hasil dari pemindaian QR-Code ini adalah data keaslian sertifikat sesuai dengan yang tercetak pada sertifikat. Aplikasi ini dibangun menggunakan bahasa pemrograman PHP, database MySQL notepad++ untuk editor, serta Android Studio untuk QR-Code Reader. Dengan menerapkan QR-Code pada sertifikat TOEFL dengan data yang terenkripsi algoritma RSA, sertifikat akan sulit dipalsukan.

Kata Kunci : Pemalsuan, Sertifikat, Algoritma RSA, *Rational Unified Process* (RUP), MySQL, QR-Code.