

# IMPLEMENTASI TANDA TANGAN DIGITAL PADA TRANSKRIP DIGITAL MENGUNAKAN METODE DSA (DIGITAL SIGNATURE ALGORITM)

(STUDI KASUS : FAKULTAS SAINS DAN TEKNOLOGI  
UNIVERSITAS ISLAM NEGERI BANDUNG)

Oleh:

**LIAWATI NUGRAHA**

**NIM. 207700412**

## ABSTRAK

Tanda tangan digital adalah kriptografi pada transkrip digital dan pengirim. Tanda tangan digital digunakan untuk integritas data. Selain itu, dapat digunakan untuk authentication pesan (legalitas pengirim) dan untuk tujuan non repudiation. Dengan demikian, penelitian ini dilakukan untuk membuat kunci publik dengan menggunakan algoritma yang di khususkan untuk membuat tanda tangan digital, yaitu DSA (Digital Signature Algorithm) dan menggunakan bahasa pemrograman Java.

Algoritma DSA menggunakan dua kunci, yaitu kunci *private* dan kunci *public*. Fungsi kunci private untuk membuat tanda tangan digital dan kunci public untuk memverifikasi tanda tangan digital. DSA menggunakan nilai yang besar sehingga sulit untuk di palsukan.

Tahapan penelitian adalah di mulai dari analisis kebutuhan sistem, merancang sistem, dan pengujian sistem. DSA dirancang menggunakan metode berorientasi objek. Desain sistem menghasilkan kelas perencanaan, paket dan antarmuka pengguna untuk pelaksanaan program dengan bahasa pemrograman java.

Aplikasi DSA memiliki kemampuan untuk menghasilkan pasangan kunci, menghasilkan tanda tangan digital, dan verifikasi tanda tangan digital. Aplikasi ini juga dapat menunjukkan pesan yang dimodifikasi oleh orang lain terhadap keabsahan tanda tangan digital. Aplikasi ini dapat memberikan pelayanan keamanan integritas dan otentikasi data.

**Kata kunci** : kriptografi, DSA, Java