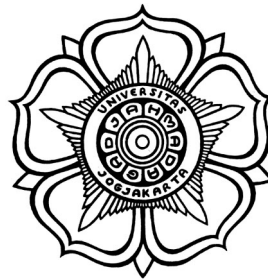


SKRIPSI

***PROOF OF CONCEPT SERANGAN PADDING ORACLE PADA
PENYANDIAN AES DENGAN MODE PCBC***

***PROOF OF CONCEPT ORACLE PADDING ATTACK ON AES
ENCRYPTION WITH PCBC MODE***



Rafie Muhammad
16/398524/PA/17485

**PROGRAM STUDI S1 ILMU KOMPUTER
DEPARTEMEN ILMU KOMPUTER DAN ELEKTRONIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS GADJAH MADA
YOGYAKARTA**

2020