

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
HALAMAN PERNYATAAN BEBAS PLAGIASI	iv
HALAMAN PERSEMBAHAN	v
HALAMAN MOTTO	vi
PRAKATA	vii
DAFTAR ISI	x
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
DAFTAR LAMBANG	xiv
INTISARI	xvi
ABSTRACT	xvii
I PENDAHULUAN	1
1.1. Latar Belakang Masalah	1
1.2. Tujuan dan Manfaat Penelitian	1
1.3. Tinjauan Pustaka	2
1.4. Metodologi Penelitian	3
1.5. Sistematika Penulisan	4
II DASAR TEORI	6
2.1. Kronecker Product	6
2.2. Grup dan Subgrup	8
2.2.1. Grup	8
2.2.2. Subgrup	11
2.3. Ring, Subring, Ideal, dan Ring Faktor	14
2.3.1. Ring dan Subring	14
2.3.2. Ideal	16
2.3.3. Ring Faktor	16
2.4. Daerah Integral dan Lapangan	20
2.5. Ruang Vektor	26
2.5.1. Ruang Vektor dan Subruang	26
2.5.2. Himpunan Pembangun dan Kebebas Linear	29
2.5.3. Basis dan Dimensi	31
2.6. Ring Polinomial	35

2.7. Lapangan Hingga	37
2.7.1. Struktur Lapangan Hingga	37
2.7.2. Elemen Primitif dan Residu Kuadratik	41
2.8. Matriks <i>Circulant</i>	44
2.9. Matriks Ortogonal Tipe-I	46
2.10. Matriks Eksponensial	52
III Matriks Hadamard	60
3.1. Matriks Hadamard	60
3.2. Kelas Ekuivalensi Matriks Hadamard	61
3.3. Eksistensi Matriks Hadamard	66
IV Beberapa Metode Pengonstruksian Matriks Hadamard	68
4.1. Penggunaan Metode Sylvester dalam Pengonstruksian Matriks Hadamard	68
4.2. Penggunaan Metode Paley dalam Pengonstruksian Matriks Hadamard	69
4.3. Penggunaan Metode Williamson dalam Pengonstruksian Matriks Hadamard	79
V Aplikasi Matriks Hadamard pada Kriptografi	83
5.1. Kriptografi	83
5.2. Algoritma Pertama	85
5.2.1. Proses Enkripsi	86
5.2.2. Proses Dekripsi	87
5.3. Algoritma Kedua	90
5.3.1. Proses Enkripsi	90
5.3.2. Proses Dekripsi	91
5.4. Algoritma Ketiga	93
5.4.1. Proses Enkripsi	94
5.4.2. Proses Dekripsi	95
VI KESIMPULAN	102
DAFTAR PUSTAKA	104
A LAMPIRAN SKRIP PROGRAM	106