UNIVERSITAS
GADJAH MADA
Kriptografi Berdasar Multivariat: Skema Tanda Tangan Digital Hidden Product of Polynomial Composition (HPPC)
Saifullah Ali, Prof. Dr.rer.nat. Indah Emilia Wijayanti, S.Si., M.Si. ; Uha Isnaini, S.Si., M.Sc., Ph.D.
Universitas Gadjah Mada, 2024 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR ISI

HALAMAN JUDUL . . . . . **i**
HALAMAN PENGESAHAN . . . . . **iii**
HALAMAN PERNYATAAN . . . . . **iii**
HALAMAN PERSEMBAHAN . . . . . **iv**
HALAMAN MOTTO . . . . . **v**
PRAKATA . . . . . **vi**
DAFTAR ISI . . . . . **ix**
DAFTAR TABEL . . . . . **xi**
DAFTAR LAMBANG . . . . . **xii**
INTISARI . . . . . **xiii**
ABSTRACT . . . . . **xiv**
I PENDAHULUAN **1**
1.1 Latar Belakang Masalah 1
1.2 Perumusan Masalah 3
1.3 Tujuan dan Manfaat Penelitian 3
1.4 Tinjauan Pustaka 3
1.5 Metode Penelitian 5
1.6 Sistematika Penulisan 5
II DASAR TEORI **6**
2.1 Lapangan Hingga 6
2.1.1 Konstruksi Lapangan Hingga 6
2.1.2 Lapangan Perluasan 9
2.2 Transformasi Affine 19
2.3 Ring Polinomial Multivariat 26
2.4 Kriptografi 35
2.4.1 Skema Enkripsi 36
2.4.2 Fungsi Hash 38
2.4.3 Tanda Tangan Digital 40
III KRIPTOGRAFI BERDASAR MULTIVARIAT **44**
3.1 Permasalahan Multivariat Kuadratik 44
3.2 Pintu Jebakan Permasalahan Multivariat Kuadratik 54
3.3 Modifikasi pada Permasalahan Multivariat Kuadratik 61

UNIVERSITAS
GADJAH MADA
Kriptografi Berdasar Multivariat: Skema Tanda Tangan Digital Hidden Product of Polynomial Composition (HPPC)
Saifullah Ali, Prof. Dr.rer.nat. Indah Emilia Wijayanti, S.Si., M.Si. ; Uha Isnaini, S.Si., M.Sc., Ph.D.
Universitas Gadjah Mada, 2024 | Diunduh dari http://etd.repository.ugm.ac.id/

IV PRODUK DARI KOMPOSISI POLINOMIAL TERSEMBUNYI (*HIDDEN PRODUCT OF POLYNOMIAL COMPOSITION*/HPPC) 67
4.1 Matriks Kompanion dan Representasi Lapangan Hingga 67
4.2 Tensor 77
4.3 Representasi Tensor 82
4.4 Skema *Hidden Product of Polynomial Composition* (HPPC) 86
V KESIMPULAN 99
DAFTAR PUSTAKA 101
A LAPANGAN HINGGA $\mathbb{F}_{2^4}$ 104
B SKRIP PROGRAM SAGEMATH TANDA TANGAN DIGITAL HPPC 105
C CONTOH TANDA TANGAN DIGITAL HPPC $(2, 16, 33, 9)$ 111