



01 0 1

**PEMBAHASAN SOAL
DASAR DASAR BAGIAN**

Kriptography

Gerry Italiano Wowiling, S.Tr.Kom., M.T. | Sari Muthia Silalahi, S.Pd., M.Ed | Haratama Felix Tamba
Nova Evelyn Sirait | Merry Wijaya Tamba | Jessica Panjaitan | Agnes Yolanda Siahaan
Necia Gloria Amanda Sitohang | Asita M.K. Tambunan | Sinta Simbolon
Brian Daniel Napitupulu

PEMBAHASAN SOAL
DASAR DASAR BAGIAN

Kriptography



eureka
media aksara
Anggota IKAPI
No. 225/ITE/2021

☎ 0858 5343 1992
✉ eurekaediaaksara@gmail.com
📍 Jl. Banjaran RT.20 RW.10
Bojongsari - Purbalingga 53362

ISBN 978-623-520-257-4



9

786231

202574

PEMBAHASAN SOAL DASAR DASAR BAGIAN KRIPTOGRAPHY

Gerry Italiano Wowiling, S.Tr.Kom., M.T.

Sari Muthia Silalahi, S.Pd., M.Ed

Haratama Felix Tamba

Nova Evelyn Sirait

Merry Wijaya Tamba

Jesica Panjaitan

Agnes Yolanda Siahaan

Necia Gloria Amanda Sitohang

Asita M.K. Tambunan

Sinta Simbolon

Brian Daniel Napitupulu



eureka
media aksara

PENERBIT CV.EUREKA MEDIA AKSARA

**PEMBAHASAN SOAL DASAR DASAR BAGIAN
KRIPTOGRAPHY**

Penulis : Gerry Italiano Wowiling, S.Tr.Kom., M.T.
Sari Muthia Silalahi, S.Pd., M.Ed
Haratama Felix Tamba
Nova Evelyn Sirait
Merry Wijaya Tamba
Jessica Panjaitan
Agnes Yolanda Siahaan
Necia Gloria Amanda Sitohang
Asita M.K. Tambunan
Sinta Simbolon
Brian Daniel Napitupulu

Desain Sampul : Eri Setiawan

Tata Letak : Rizki Rose Mardiana

ISBN : 978-623-120-257-4

Diterbitkan oleh : **EUREKA MEDIA AKSARA, FEBRUARI 2024**
ANGGOTA IKAPI JAWA TENGAH
NO. 225/JTE/2021

Redaksi:

Jalan Banjaran, Desa Banjaran RT 20 RW 10 Kecamatan Bojongsari
Kabupaten Purbalingga Telp. 0858-5343-1992

Surel : eurekamediaaksara@gmail.com

Cetakan Pertama : 2024

All right reserved

Hak Cipta dilindungi undang-undang

Dilarang memperbanyak atau memindahkan sebagian atau seluruh isi buku ini dalam bentuk apapun dan dengan cara apapun, termasuk memfotokopi, merekam, atau dengan teknik perekaman lainnya tanpa seizin tertulis dari penerbit.

KATA PENGANTAR

Puji syukur kami panjatkan kehadirat Allah SWT atas segala rahmat dan kasih-Nya, yang telah memberi petunjuk dan keberkahan sehingga kami berhasil menyusun buku pembelajaran ini dengan judul "Dasar-Dasar Bagian Kriptografi". Kami dengan senang hati mempersembahkan buku ini kepada para pembaca, terutama bagi mereka yang ingin mendalami pengetahuan dasar-dasar kriptografi.

Buku pembelajaran ini bertujuan memberikan pemahaman yang mendalam mengenai dasar-dasar kriptografi, membahas soal-soal yang relevan, dan memberikan panduan praktis untuk memahami konsep-konsep tersebut. Dengan fokus pada pembahasan soal, diharapkan buku ini dapat menjadi alat bantu yang efektif bagi pembaca dalam meningkatkan pemahaman mereka terhadap kriptografi.

Kami berterima kasih kepada semua pihak yang telah turut membantu penulis dalam penyusunan buku ini. Kontribusi mereka bukan hanya memperkaya isi modul, tetapi juga mendukung terwujudnya buku yang komprehensif dan bermanfaat.

Semoga "Pembahasan Soal Dasar-Dasar Bagian Kriptografi" dapat memberikan manfaat yang signifikan dan memenuhi kebutuhan pembaca, khususnya mereka yang ingin menggali lebih dalam konsep-konsep dasar dalam bidang kriptografi. Harapan kami adalah agar buku ini tidak hanya menjadi referensi sekali baca, melainkan menjadi panduan yang terus-menerus memberikan pemahaman yang mendalam. Terima kasih atas dukungan dan antusiasme Anda dalam mengikuti perjalanan pembelajaran ini.

DAFTAR ISI

KATA PENGANTAR.....	iii
DAFTAR ISI.....	iv
DAFTAR TABEL	v
DAFTAR GAMBAR.....	vii
BAB 1 INTRODUCTION TO NUMBER THEORY	1
A. Modular Arithmetic Operations	1
B. Properties of Modular Arithmetic	10
C. Properties Modular Arithmetic for Integers In Z_n	22
D. Fermat's Theorem.....	34
BAB 2 SYMMETRIC CIPHERS	43
A. Hill Chipper	44
B. Hill Chipper Mariks 3×3	55
C. Transposition Technique dengan Kedalaman	65
D. Transposition Techniques dengan Kolom Matrix	98
E. Playfair Chiper.....	105
F. RSA(Rivest Shamir Adleman).....	125
DAFTAR PUSTAKA.....	163

DAFTAR TABEL

Tabel 1. 1	Multiplication Modulo 3.....	11
Tabel 1. 2	Additional Modulo 3.....	11
Tabel 1. 3	Additional Modulo 3.....	11
Tabel 1. 4	Multiplication Modulo 3.....	11
Tabel 1. 5	Addition Modulo 16.....	12
Tabel 1. 6	Multiplication Modulo 16.....	12
Tabel 1. 7	Addition Modulo 17.....	12
Tabel 1. 8	Multiplication Modulo 17.....	13
Tabel 1. 9	Addition Modulo 3.....	13
Tabel 1. 10	Multiplication Modulo 3.....	13
Tabel 1. 11	Addition Modulo 20.....	14
Tabel 1. 12	Multiplication Modulo 20.....	14
Tabel 1. 13	Addition Modulo 21.....	14
Tabel 1. 14	Multiplication Modulo 21.....	15
Tabel 1. 15	Multiplication Modulo 22.....	15
Tabel 1. 16	Addition Modulo 22.....	15
Tabel 1. 17	Addition Modulo 27.....	16
Tabel 1. 18	Multiplication Modulo 27.....	16
Tabel 1. 19	Addition Modulo 6.....	16
Tabel 1. 20	Multiplication Modulo 28.....	17
Tabel 1. 21	Addition Modulo 30.....	17
Tabel 1. 22	Multiplication Modulo 30.....	18
Tabel 1. 23	Addition Modulo 31.....	18
Tabel 1. 24	Multiplication Modulo 8.....	19
Tabel 1. 25	Addition Modulo 33.....	19
Tabel 1. 26	Multiplication Modulo 33.....	19
Tabel 1. 27	Addition Modulo 8.....	20
Tabel 1. 28	Multiplication Modulo 45.....	20
Tabel 1. 29	Addition Modulo 52.....	20
Tabel 1. 30	Multiplication Modulo 52.....	21
Tabel 1. 31	Addition Modulo 60.....	21
Tabel 1. 32	Multiplication Modulo 60.....	21
Tabel 2. 1	Kata Kunci "CHIPER"	106
Tabel 2. 2	Metode Playfair cipher.....	108

Tabel 2. 3	Keyword Pakniotims.....	108
Tabel 2. 4	Tabel Subtitusi Pergeseran dari Plaintext.....	113
Tabel 2. 5	Table Caesar chiper	117
Tabel 2. 6	Substitusi Caesar Chipper Bergeser 4 Huruf.....	117
Tabel 2. 7	Substitusi Caesar Chipper Bergeser 5 Huruf.....	118

DAFTAR GAMBAR

Gambar 2. 1 Algoritma Playcipher	107
--	-----



**PEMBAHASAN SOAL DASAR DASAR BAGIAN
KRIPTOGRAPHY**

**Gerry Italiano Wowiling, S.Tr.Kom., M.T.
Sari Muthia Silalahi, S.Pd., M.Ed
Haratama Felix Tamba
Nova Evelyn Sirait
Merry Wijaya Tamba
Jesica Panjaitan
Agnes Yolanda Siahaan
Necia Gloria Amanda Sitohang
Asita M.K. Tambunan
Sinta Simbolon
Brian Daniel Napitupulu**



BAB 1

INTRODUCTION TO NUMBER THEORY

Teori bilangan tersebar luas dalam algoritma kriptografi. Bab ini menyediakan cakupan yang cukup luas dan mendalam dari topik teori bilangan yang relevan untuk memahami berbagai aplikasi dalam kriptografi. Pembaca akrab dengan ini topik dapat dengan aman melewati bab ini. Pada bagian pertama memperkenalkan konsep dasar teori bilangan yaitu diperlukan untuk memahami bidang yang terbatas; ini termasuk Modular Arithmetic Operations, Properties of Modular Arithmetic, Properties Modular Arithmetic for Integers In \mathbb{Z}_n , dan Fermat's Theorem. Konsep dan teknik teori bilangan cukup abstrak, dan seringkali memang demikian sulit untuk memahaminya secara intuitif tanpa contoh. Oleh karena itu, bab ini mencakup sejumlah contoh.

A. Modular Arithmetic Operations

Dalam konteks matematika, Operasi Aritmetika Modular merupakan suatu sistem aritmatika yang diterapkan pada bilangan bulat, di mana angka-angka "wrap around" saat mencapai nilai tertentu yang disebut modulus. ide utama dalam aritmatika modular adalah mengarahkan perhatian pada sisa hasil pembagian angka dengan modulus. Pada dasarnya, Modular arithmetic melibatkan operasi matematika dengan nilai yang direset ke nol setiap kali mencapai bilangan bulat tertentu N , yang disebut modulus (mod). Contoh penggunaan konsep ini dapat ditemui pada jam digital dalam sistem 24 jam, yang mengalami reset kembali ke nol pada tengah malam ($N = 24$),

BAB 2

SYMMETRIC CIPHERS

Pada bab ini, terdapat penjelasan tentang latar belakang pemilihan symmetric ciphers dan Hill cipher sebagai fokus pembahasan. Keberadaan modul pembelajaran ini dimaksudkan untuk memberikan pemahaman yang lebih mendalam mengenai cara pesan-pesan dijamin keamanannya. Symmetric ciphers, yang sering disebut sebagai sandi simetris, menjadi pilihan utama karena menggunakan kunci yang sama untuk mengamankan dan mengembalikan pesan, praktis digunakan dalam berbagai konteks seperti obrolan online dan penyimpanan file penting. Algoritma populer seperti AES, DES, dan 3DES akan dijelaskan untuk memperkaya pemahaman.

Sementara itu, Hill cipher, sebuah teknik klasik yang memanfaatkan matriks untuk merahasiakan teks, juga dipilih sebagai topik pembahasan. Ditemukan oleh Lester S. Hill pada tahun 1929, Hill cipher memberikan keunikan dengan menggunakan matriks sebagai kunci rahasia, dan setiap huruf dalam pesan diubah melalui operasi matriks. Kemampuannya mengatasi kelemahan sandi yang lebih sederhana membuatnya menarik untuk dipelajari. Dengan memahami baik symmetric ciphers dan Hill cipher, pembaca akan dapat mengembangkan dasar keamanan data yang solid. Penjelasan ini diharapkan memberikan pemahaman yang lebih baik tentang pemilihan topik dan tujuan modul pembelajaran ini.

DAFTAR PUSTAKA

W. Stallings, *Cryptography and Network Security: Principles and Practice*. Pearson, 2020.