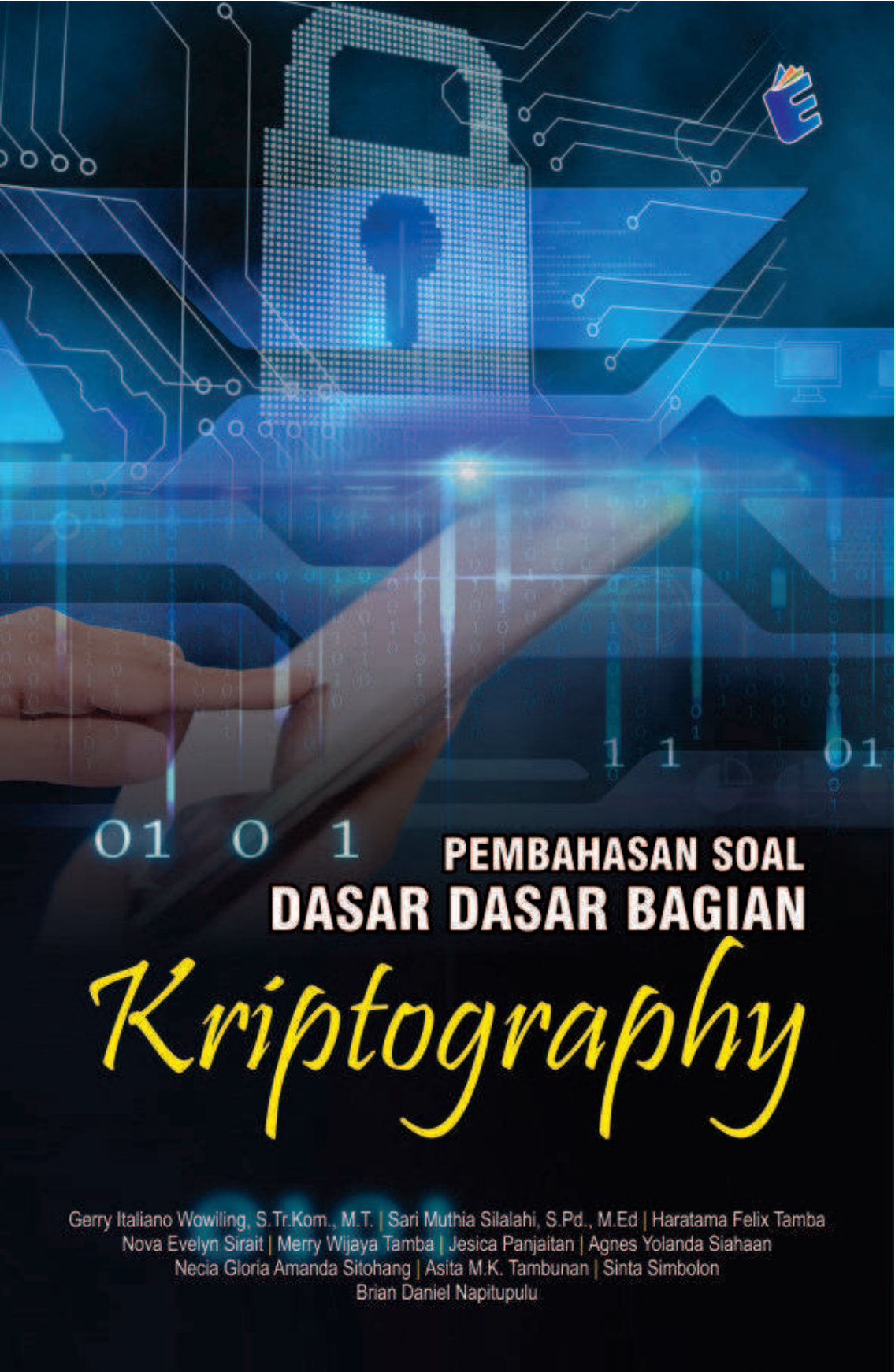

PEMBAHASAN SOAL DASAR DASAR BAGIAN Kriptography

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

PEMBAHASAN SOAL
DASAR DASAR BAGIAN
Kriptography

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

0858 5343 1992
eurekamediaaksara@gmail.com
Jl. Banjaran RT.20 RW.10
Bojongsari - Purbalingga 53362

ISBN 978-623-120-257-4

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

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
Jesica 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

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

DAFTAR TABEL

DAFTAR GAMBAR

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 Arithmatic, Properties Modular Arithmetic for Intergers In Zn, 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.