LAPORAN PRAKTIKUM

CRYPTOGRAPHI

DISUSUN OLEH **:**

Nama	: Diki Candra
Nim	: 2022903430010
Kelas	: TRKJ 2B
Jurusan	: Teknologi Informasi dan Komputer
Program Studi	: Teknologi Rekayasa Komputer Jaringan
Dosen Pengajar	: Aswandi, S.Kom, M.Kom.

JURUSAN TEKNOLOGI INFORMASI DAN KOMUNIKASI

PRODI TEKNOLOGI REKAYASA KOMPUTER DAN JARINGAN

POLITEKNIK NEGERI LHOKSEUMAWE

TAHUN 2022/2023

LEMBARAN PENGESAHAN

Laporan Yang Berjudul	: Cryptographi
Disusun Oleh	: Diki Candra
NIM	: 2022903430010
Jurusan	: Teknologi Informasi & Komputer
Program Studi	: Teknologi Rekayasa Komputer Jaringan
Mata Kuliah	: Ethical Hacking
Tabel Penilaian	:

Mengetahui,

Dosen Pembimbing,

Aswandi, S.Kom, M.Kom
NIP. 197209242010121001

Penyusun,

Diki Candra
NIM. 2022903430010

Dasar Teori

Dasar-dasar teori kriptografi melibatkan konsep-konsep matematika dan teknik yang membentuk dasar bagi pengembangan metode penyandian dan perlindungan informasi. Beberapa konsep dasar dalam teori kriptografi meliputi:

Enkripsi dan Dekripsi:

Enkripsi: Proses mengubah teks atau data asli menjadi bentuk yang tidak dapat dimengerti tanpa kunci khusus.

Dekripsi: Proses mengembalikan teks atau data yang telah dienkripsi menjadi bentuk aslinya menggunakan kunci.

Kunci Kriptografi:

Kunci adalah nilai yang digunakan dalam algoritma kriptografi untuk mengontrol proses enkripsi dan dekripsi. Ada dua tipe utama kunci:

Kunci Simetris: Kunci yang sama digunakan untuk enkripsi dan dekripsi. Algoritma seperti DES, AES, dan 3DES menggunakan kunci simetris.

Kunci Asimetris (atau Kunci Publik-Privat): Pasangan kunci yang terdiri dari kunci publik yang digunakan untuk enkripsi dan kunci pribadi yang digunakan untuk dekripsi. RSA adalah contoh algoritma kunci publik.

Kriptografi Kunci Publik (Public Key Cryptography):

Konsep yang melibatkan dua kunci terpisah, yaitu kunci publik dan kunci pribadi. Kunci publik dapat dibagikan secara terbuka, sementara kunci pribadi harus dijaga dengan ketat. Pesan yang dienkripsi dengan kunci publik hanya dapat di-dekripsi oleh pemilik kunci pribadi yang sesuai.

Fungsi Hash:

Fungsi hash mengubah data menjadi nilai hash tetap panjang. Ini digunakan untuk memeriksa integritas data dan menciptakan tanda tangan digital. Algoritma hash populer termasuk SHA-256 dan MD5.

Tanda Tangan Digital:

Tanda tangan digital digunakan untuk memverifikasi keaslian pesan atau data. Ini melibatkan penggunaan kunci pribadi untuk menghasilkan tanda tangan yang dapat diverifikasi menggunakan kunci publik yang sesuai.

Protokol Kunci:

Protokol kunci menyusun aturan dan langkah-langkah yang digunakan untuk berkomunikasi secara aman melalui jaringan. Contoh protokol kunci termasuk TLS/SSL untuk keamanan komunikasi web dan protokol kunci pertukaran kunci seperti Diffie-Hellman.

Teori Informasi:

Konsep dari teori informasi, seperti entropi, digunakan untuk mengukur ketidakpastian dan kompleksitas informasi dalam konteks kriptografi.

Kerapatan (Cryptographic Security):

Kerapatan mengacu pada sejauh mana sistem kriptografi dapat memberikan keamanan terhadap berbagai jenis serangan, termasuk serangan brute-force, serangan kunci, dan serangan lainnya.

Tujuan Praktikum

Implementasi Algoritma:

Memahami dan menerapkan algoritma kriptografi seperti AES, DES, atau RSA.

Pemahaman Kunci dan Manajemen:

Mengelola dan mengamankan pertukaran kunci simetris dan asimetris.

Analisis Keamanan:

Mengidentifikasi potensi kerentanan atau celah keamanan dalam implementasi kriptografi.

Penerapan Protokol Keamanan:

Menerapkan protokol keamanan seperti SSL/TLS dalam komunikasi jaringan.

Tanda Tangan Digital:

Membuat dan memverifikasi tanda tangan digital untuk menjaga integritas dan keaslian data.

Peralatan Kriptografi:

Menggunakan perangkat keras dan perangkat lunak kriptografi yang umum.

Kesadaran Etika dan Hukum:

Memahami aspek etika dan hukum dalam penggunaan kriptografi.

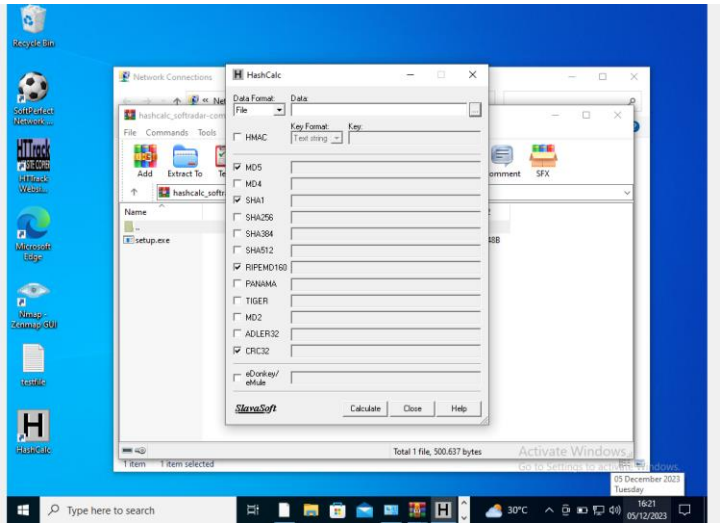
Proyek Kriptografi:

Terlibat dalam proyek-proyek kecil untuk merancang dan menerapkan solusi keamanan menggunakan kriptografi.

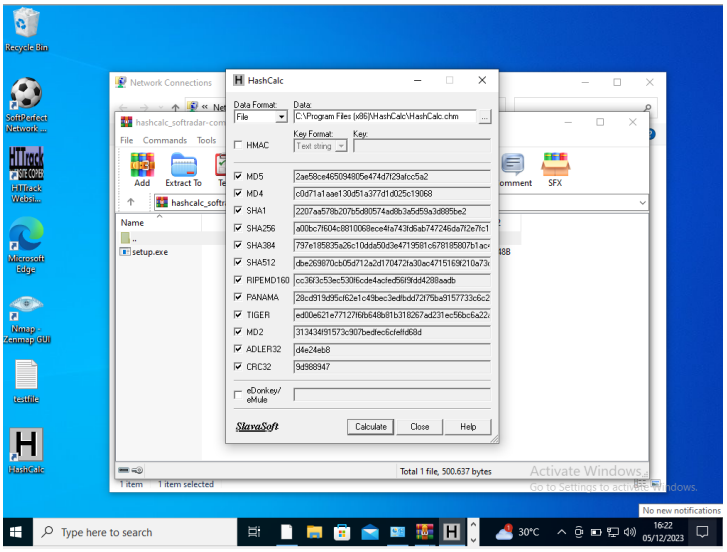
Alat dan Bahan

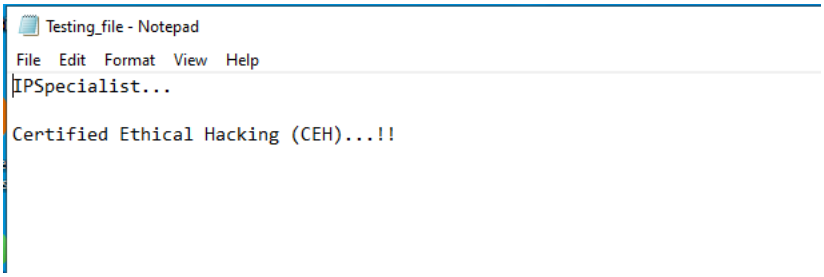
1. VMware
2. OS Server
3. Hashcalc
3. Hashcalc
4. Advanced encryption package

1. Buka alat HashCalc.

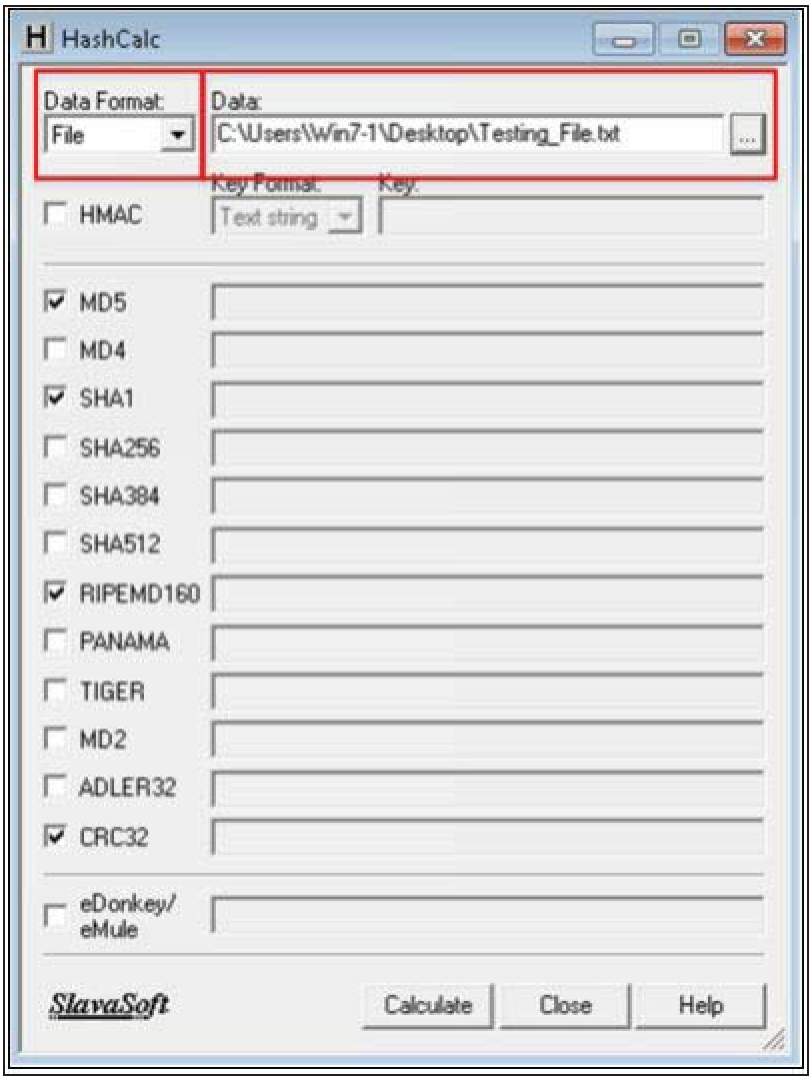


2. Buat file baru dengan beberapa konten di dalamnya seperti yang ditunjukkan di bawah ini.

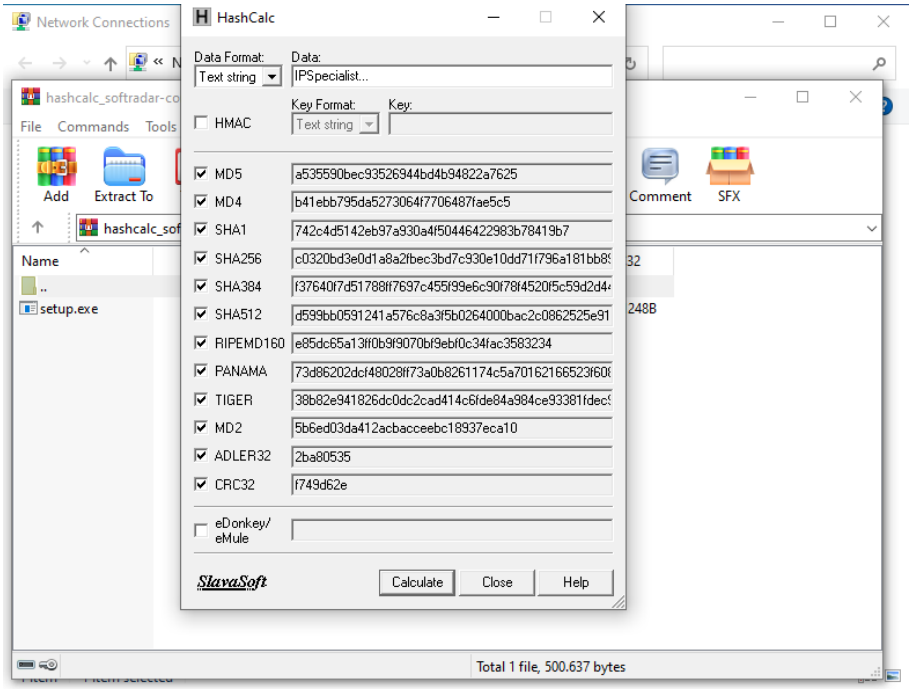




. Pilih Format Data sebagai "File" dan unggah file Anda



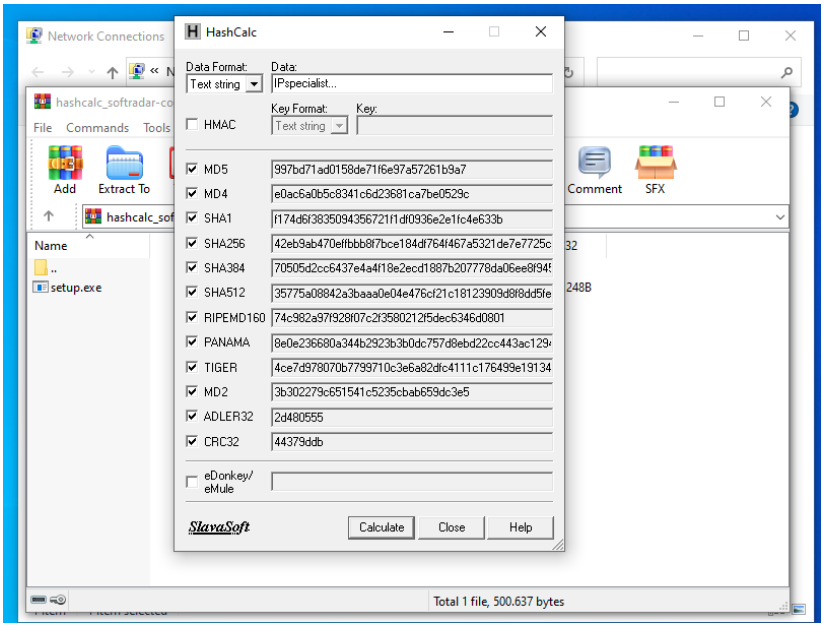
Pilih Algoritma Hashing dan Klik Hitung



Sekarang Pilih Format Data ke "String Teks" dan Ketik "IPSpecialist..." ke dalam Data yang diajukan dan dihitung MD5.

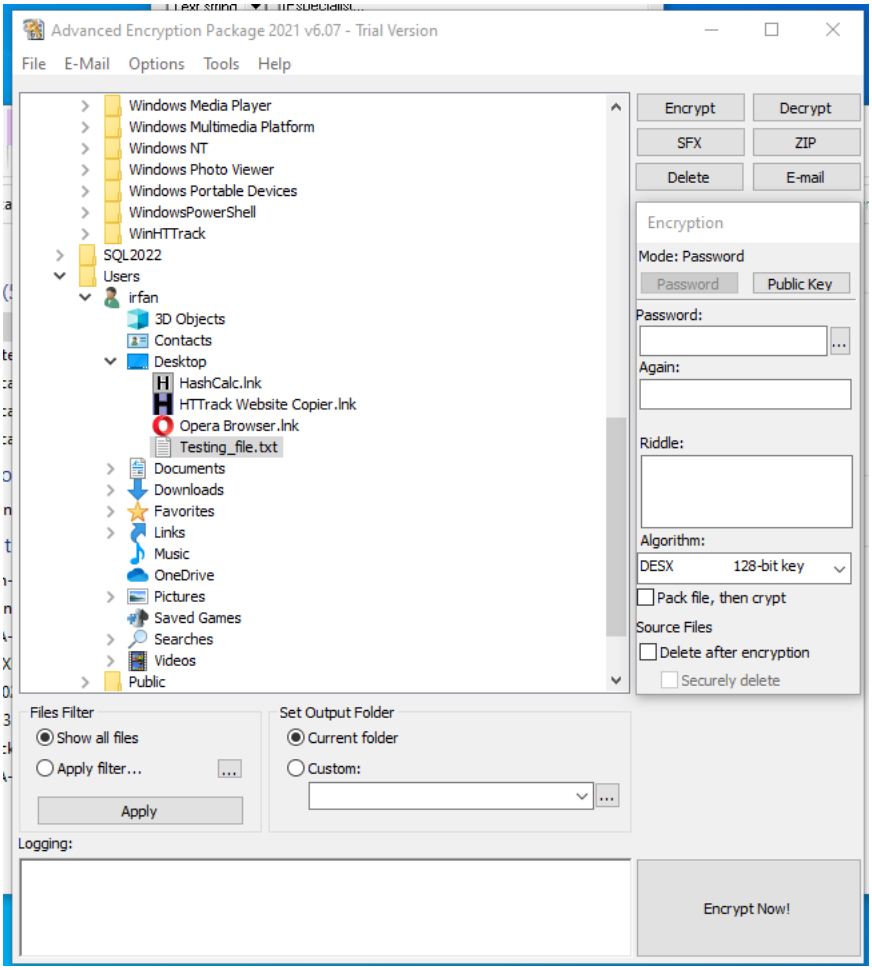
MD5 Dihitung untuk string teks “IPSpecialist…” adalah “a535590bec93526944bd4b94822a7625”

Sekarang, mari kita lihat bagaimana nilai MD5 berubah dari perubahan kecil.

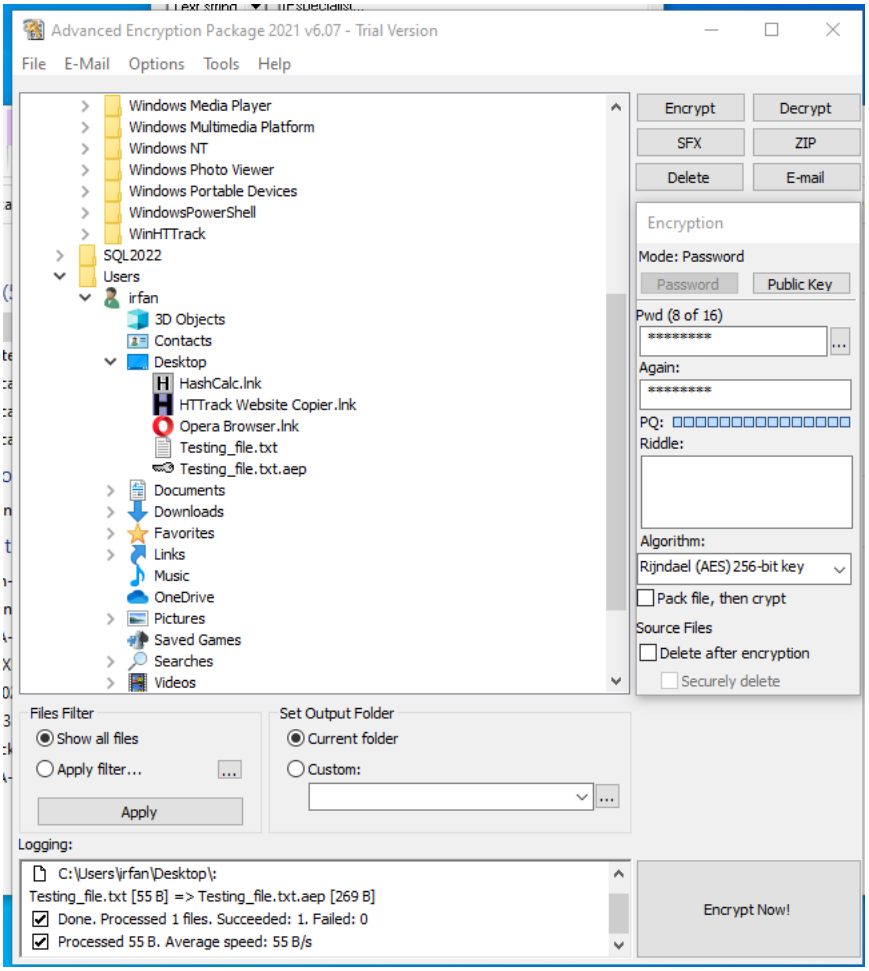


Menurunkan huruf besar/kecil saja akan mengubah seluruh nilai hashing. MD5 Dihitung untuk string teks “IPspecialist…” adalah “997bd71ad0158de71f6e97a57261b9a7”

Rangkaian	MD5
Spesialis IPS…	a53559Obec93526944bd4b94822a7625
Spesialis IP…	997bd71adO158de71f6e97a57261b9a7

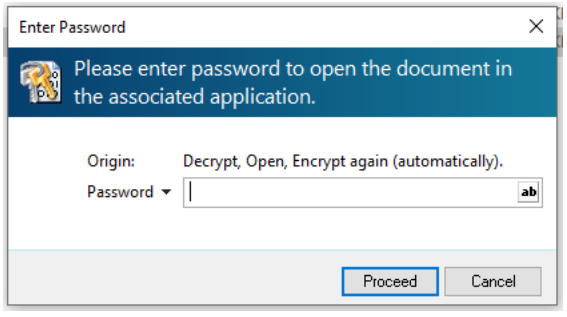


1. Pilih File yang ingin Anda Enkripsi.
2. Tetapkan kata sandi
3. Pilih Algoritma



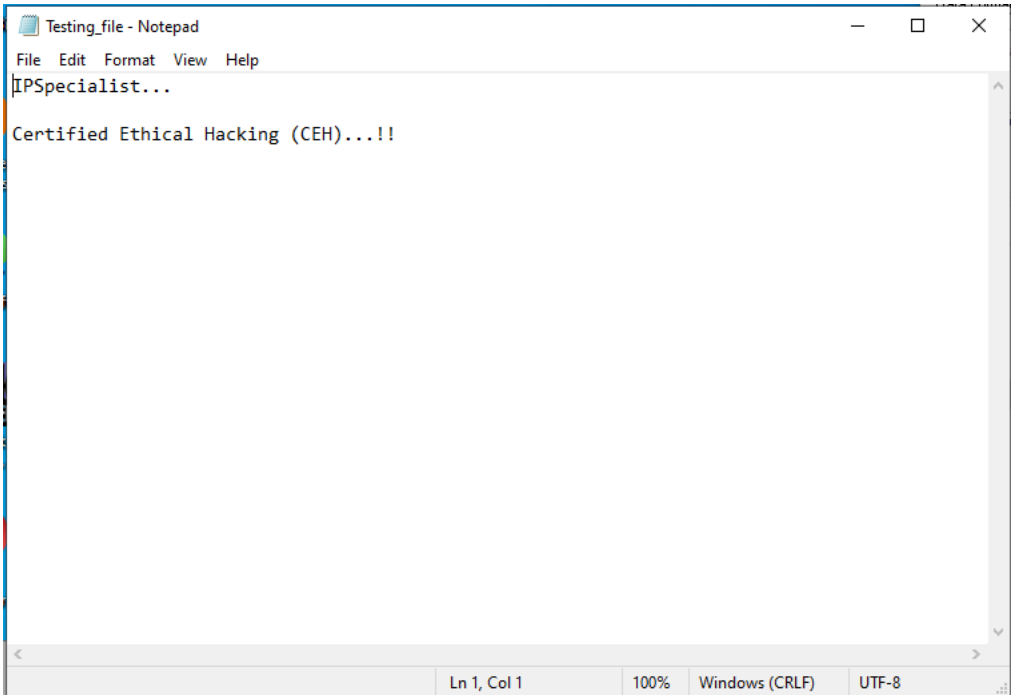
Klik Enkripsi

Bandingkan kedua File



File berhasil didekripsi.

Masukkan kata sandi untuk memasuki file



Analisa dan kesimpulan

Analisa:

Kriptografi memainkan peran kunci dalam melindungi informasi sensitif dan komunikasi. Dengan adanya teknik penyandian yang kuat, informasi dapat dijaga dari akses yang tidak sah.

Evolution of Technology:

Kriptografi telah mengalami evolusi yang signifikan seiring dengan kemajuan teknologi. Dari metode sederhana seperti penyandian Caesar hingga algoritma kunci publik dan protokol kunci modern, kriptografi terus beradaptasi dengan tantangan baru.

Kunci Simetris vs. Kunci Asimetris:

Kunci simetris efisien untuk enkripsi dan dekripsi cepat, tetapi menimbulkan tantangan dalam pertukaran kunci yang aman. Kunci asimetris, meskipun lebih aman dalam pertukaran kunci, memerlukan daya komputasi yang lebih tinggi.

Pentingnya Protokol Kunci:

Protokol kunci seperti TLS/SSL adalah elemen penting dalam keamanan komunikasi online. Mereka menyediakan saluran aman untuk pertukaran informasi dalam lingkungan yang mungkin tidak aman, seperti internet.

Teori Informasi dan Keamanan:

Konsep dari teori informasi, seperti entropi, membantu memahami sejauh mana kriptografi dapat memberikan keamanan. Semakin tinggi entropi, semakin sulit untuk menebak kunci atau informasi yang terenkripsi

Kesimpulannya, kriptografi adalah landasan utama keamanan dalam era digital. Dengan pemahaman yang baik tentang konsep-konsep dasarnya, penerapan yang bijaksana dari teknik-teknik kriptografi dapat membantu melindungi informasi dan mendukung pertumbuhan keamanan dalam berbagai konteks. Namun, tantangan baru akan terus muncul, dan inovasi dalam kriptografi tetap penting untuk menjawab ancaman keamanan yang berkembang.