

Tugas Keamanan Informasi

Kriptografi

Biometric Authentication

Public Key Infrastructure

Intruksi Tugas :

- ☐ Buat persentasi sesuai dengan tugas yang didapat,
- ☐ Jelaskan dengan jelas apa dan bagaimana maksud dari tugas tersebut.
- ☐ Berikan studi kasus minimal 2 kemudian Hitunglah sesuai tugas yang didapat.
- ☐ Tuliskan juga cara penyelesaian dari kasus tersebut.
- ☐ Tugas dikerjakan sesuai dengan kelompok masing-masing
- ☐ Semua anggota kelompok harus paham apa dan maksud tugas yang didapat.
- ☐ **Urutan tugas sesuai kelompok UTS/absensi.**



Tugas 1 – Point tentang

□ Algoritma kriptografi klasik:

- Cipher Substitusi (Substitution Ciphers)
- Cipher Transposisi (Transposition Ciphers)
- Permutasi

Tugas 2 – Point tentang

- ❑ Algoritma Kriptografi Modern yang Beroperasi dalam mode bit.
- ❑ Algoritma Enkripsi dengan rangkaian bit, Bit I dan Bit II.
- ❑ kriptosistem :
 - One-Time-Pad
 - CodeBook
 - Per-Bit Encryption dengan XoR

Tugas 3 - Point tentang

☐ Algoritma Simetri

☐ Blok Chiper : **DES, IDEA, AES**

☒ ~~Stream Chiper : OTP, A5 dan RC4~~

☒ ~~Algoritma Asimetri : RSA, DH, ECC, DSA~~

☒ ~~Fungsi Hash : MD5, SHA1~~

☐ Algoritma Simetri

Tugas 4 - Point tentang

☐ Algoritma Simetri

☒ ~~Blok Chiper : DES, IDEA, AES~~

☐ Stream Chiper : **OTP, A5** dan ~~RC4~~

☒ ~~Algoritma Asimetri : RSA, DH, ECC, DSA~~

☒ ~~Fungsi Hash : MD5, SHA1~~

Tugas 5 - Point tentang

☐ Algoritma Simetri

☒ ~~Blok Chiper : DES, IDEA, AES~~

☒ ~~Stream Chiper : OTP, A5 dan **RC4**~~

☐ Algoritma Asimetri : **RSA**, ~~DH, ECC, DSA~~

☒ ~~Fungsi Hash : MD5, SHA1~~

Tugas 6 - Point tentang

☐ Algoritma Simetri

☒ ~~Blok Chiper : DES, IDEA, AES~~

☒ ~~Stream Chiper : OTP, A5 dan RC4~~

☐ Algoritma Asimetri : RSA, DH, ECC, ~~DSA~~

☒ ~~Fungsi Hash : MD5, SHA1~~

Tugas 7 - Point tentang

☐ Algoritma Simetri

☐ ~~Blok Chiper : DES, IDEA, AES~~

☐ ~~Stream Chiper : OTP, A5 dan RC4~~

☐ Algoritma Asimetri : ~~RSA, DH, ECC,~~ DSA

☐ Fungsi Hash : MD5, ~~SHA1~~

Tugas 8 - Point tentang

☒ ~~Algoritma Simetri~~

☒ ~~Blok Chiper : DES, IDEA, AES~~

☒ ~~Stream Chiper : OTP, A5 dan RC4~~

☒ ~~Algoritma Asimetri : RSA, DH, ECC, DSA~~

☐ **Fungsi Hash : MD5, SHA1, SHA-2, SHA-3, Tiger Hash**

Tugas 9 - Point tentang

☒ ~~Algoritma Simetri~~

☒ ~~Blok Chiper : DES, IDEA, AES~~

☒ ~~Stream Chiper : OTP, A5 dan RC4~~

☒ ~~Algoritma Asimetri : RSA, DH, ECC, DSA~~

☐ **Fungsi Hash : MD5, SHA1, SHA-2, SHA-3, Tiger Hash**



Tugas 10 - Point tentang

- ☐ Infrastruktur Kunci Publik
- ☐ Konsep :
 - ☐ CA (Certification Authority)
 - ☐ Digital Certificate
 - ☐ RA (Registration Authority)
 - ☐ Certification Revocation List (CRL)



Tugas 11 - Point tentang

- ☐ Biometrics Authentication
- ☐ Sidik Jari
- ☐ feature extraction
- ☐ Hand Geometry
- ☐ Pola Iris
- ☐ Hamming Distance
- ☐ Pengenalan Wajah