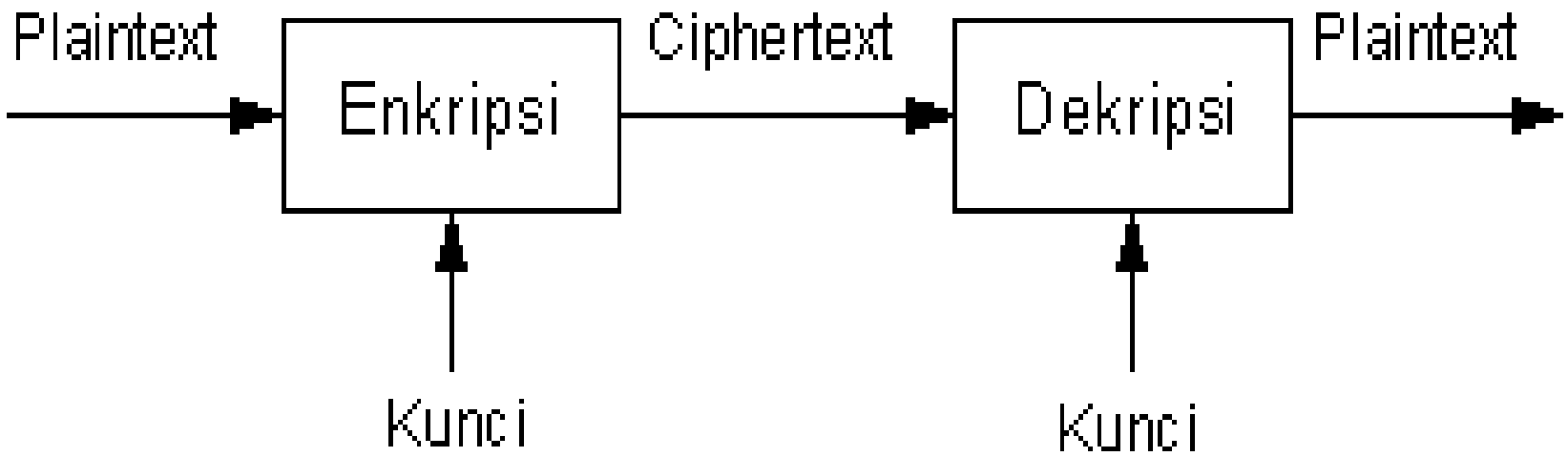
KRIPTOGRAFI, ENKRIPSI DAN DESKRIPSI

PENDAHULUAN

1. Kriptografi dapat diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan.
2. Orang yang melakukan kriptografi disebut *cryptographer*
3. Kriptanalisis (cryptanalysis) adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui kunci yang diberikan.
4. Pelakunya disebut kriptanalis
5. Tujuan Kriptografi yaitu sebagai berikut: Kerahasiaan, Integritas data, Autentikasi

6. Enkripsi merupakan proses untuk mengubah plainteks menjadi chiperteks
7. Planteks sendiri adalah data atau pesan asli yang ingin dikirim
8. Chiperteks adalah data hasil enkripsi
9. Deskripsi adalah kebalikan dari enkripsi yaitu proses mengubah chiperteks menjadi plainteks


Plaintext
Enkripsi
Ciphertext
Dekripsi
Plaintext
Kunci
Kunci

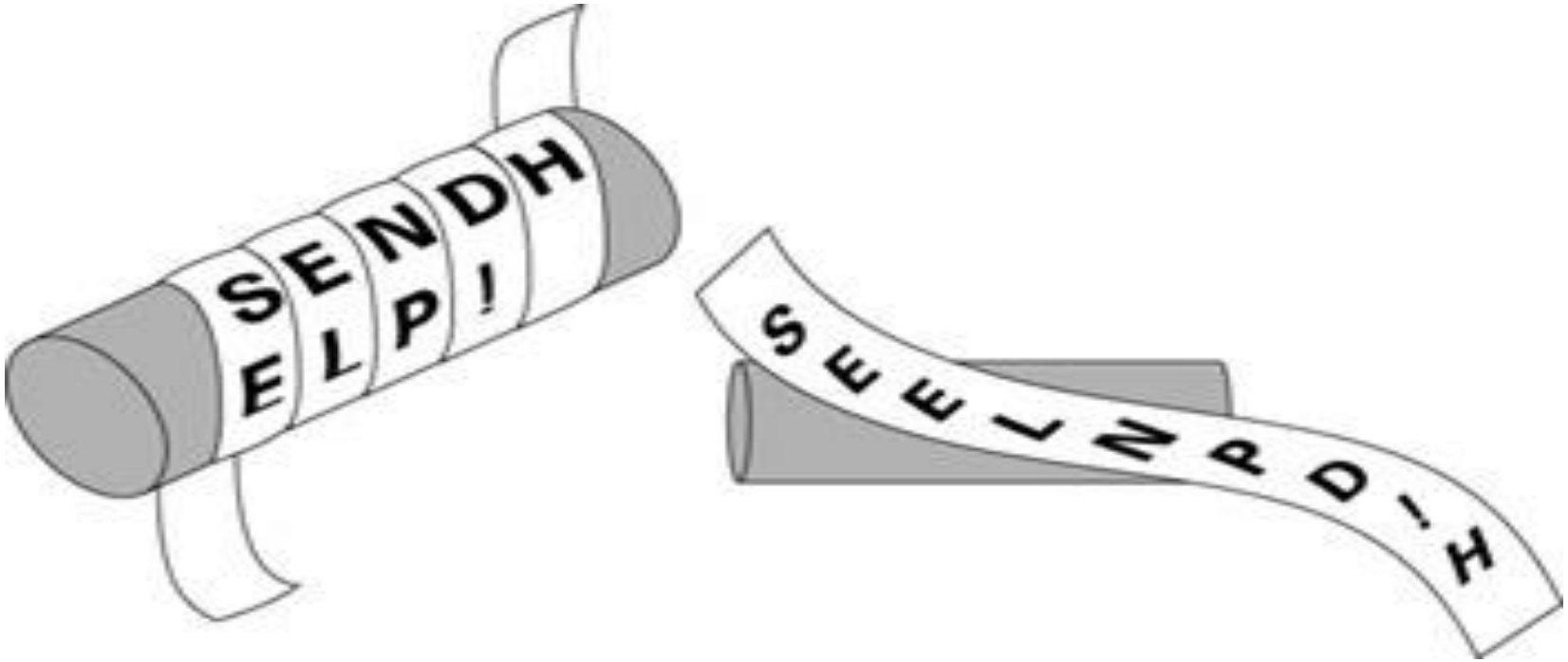
TUJUAN KRIPTOGRAFI

1. Kerahasian
2. Integritas Data
3. Autentikasi

SYARAT KRIPTOGRAFI

1. Keamanan sistem terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan.
2. Kriptografi yang baik memiliki ruang kunci (keyspace) yang besar.
3. Kriptografi yang baik akan menghasilkan ciphertext yang terlihat acak dalam seluruh tes statistik yang dilakukan terhadapnya.
4. Kriptografi yang baik mampu menahan seluruh serangan yang telah dikenal sebelumnya

SCYTALE



CAESAR CIPHER

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Pesan : INI ADALAH KATA SANDI YANG BENAR

Hasil enkripsi : LQL DGDODK NDWD VDQGL BDQJ EHQDU

TABEL SUBSTITUSI

A-B-C-D-E-F-G-H-I-J-K-L-M-N-O-P-Q-R-S-T-U-V-W-X-Y-Z-1-2-3-4-5-6-7-8-9-0-.-,
B-F-1-K-Q-G-A-T-P-J-6-H-Y-D-2-X-5-M-V-7-C-8-4-I-9-N-R-E-U-3-L-S-W-,-.-O-Z-0

Plainteks : SISTEM

Cipherteks : VPVCQY

ROT13

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Contoh:

Pesan : **KOMPUTER**

Hasil Enkripsi : **XBZCHGRE**

CIPHER POLIALFABETIK

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Pesan : KOMPUTER

Key : DEF

Enkripsi : NSRSYYHV

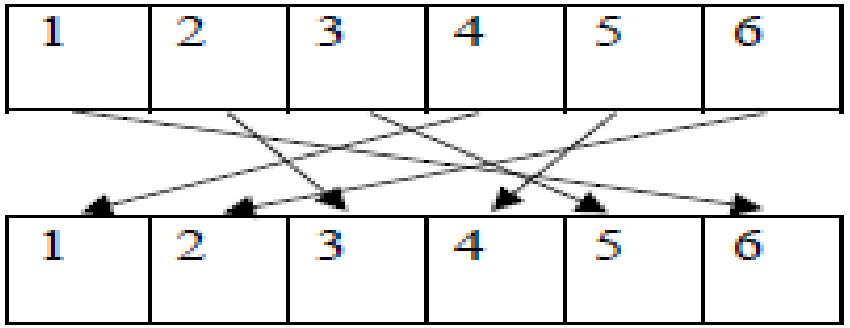
BLOCKING

S	K	N	T	BLOK 1
I	E		E	BLOK2
S	A	K	R	BLOK 3
T	M	O		BLOK 4
E	A	M		BLOK 5
M	N	P		BLOK 6
	A	U		BLOK 7

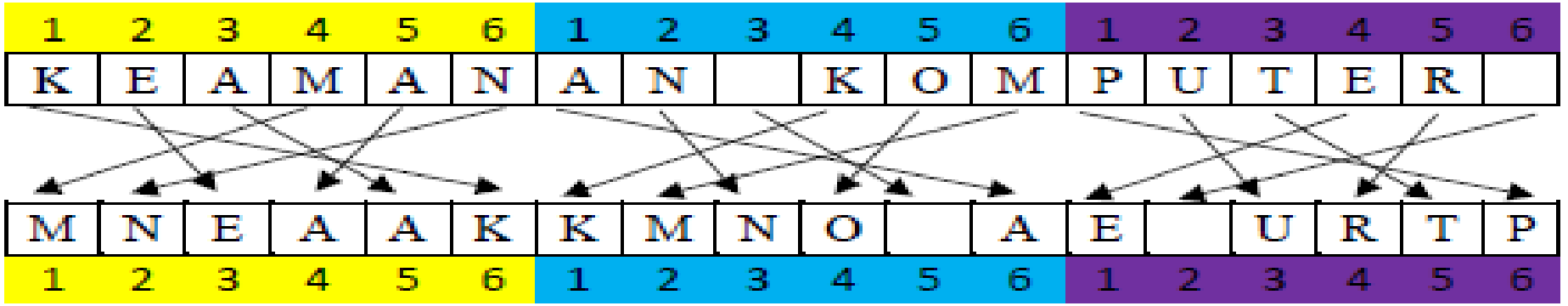
Jadi ciphertext yang dihasilkan dengan teknik ini adalah

"SKNTIE ESAKRTMO EAM MNP AU"

PEMUTASI



Pesan : **KEAMANAN KOMPUTER**



Enkripsi : **MNEAAKKMNO AE URTP**

EKSPANSI

Pesan : 7 KEAMANAN KOMPUTER

7		K	E	A	M	A	N	A	N		K	O	M	P	U	T	E	R	

7	A	N		E	A	M	A	N	A	N	K	A	N		O	M	P	U	T	E	R	K	A	N

Enkripsi : 7AN EAMANANKAN OMPUTERKAN

PEMAMPATAN

Pesan : KEAMANAN KOMPUTER

K	E	A	M	A	N	A	N		K	O	M	P	U	T	E	R

A	N		M	T

K	E	M	A	A	N	K	O	P	U	E	R

&

A	N		M	T

Huruf Yang Hilang : AN MT

Enkripsi : KEMAANKOPUER&AN MT

DATA ENCRYPTION STANDAR

1. Algoritma DES dikembangkan di IBM dibawah kepemimpinan W.L. Tuchman pada tahun 1972. Algoritma ini didasarkan pada algoritma Lucifer yang dibuat oleh Horst Feistel.
2. lgoritma ini telah disetujui oleh National Bureau of Standard (NBS) setelah penilaian kekuatannya oleh National Security Agency (NSA) Amerika Serikat.

DATA ENCRYPTION STANDAR

Data Encryption Standard (DES) adalah sebuah algoritma enkripsi sandi block kunci simetrik dengan ukuran blok 64-bit dan ukuan kunci. DES adalah tipikal blok chiper suatu algoritma yang membutuhkan tetap serangkaian panjang dan mengubah bit plaint text melalui serangkaian operasi rumit ke bitstring cipherteks lain yang sama panjang

DATA ENCRYPTION STANDAR

1. Panjang kunci eksternal DES hanya 64 bit atau 8 karakter, itupun yang dipakai hanya 56 bit
2. dengan panjang kunci 56 bit akan terdapat 2^{56} atau 72.057.594.037.927.936 kemungkinan kunci
3. diperlukan 1142 tahun untuk menemukan kunci yang benar
4. Tahun 1998, Electronic Frontier Foundation (EFE) dapat menemukan kunci selama 5 hari
5. Tahun 1999EFE dapat menemukan kunci DES kurang dari 1 hari

ADVANCED ENCRYPTION STANDARD

Pada tahun 1997, *National Institute of Standard and Technology* (NIST) *of United States* mengeluarkan *Advanced Encryption Standard (AES) untuk menggantikan Data Encryption Standard (DES)*. Pada tanggal 2 Maret tahun 2001 ditetapkanlah algoritma baru Rijndael sebagai AES. Kriteria pemilihan AES didasarkan pada 3 kriteria utama yaitu: keamanan, harga, dan karakteristik algoritma beserta implementasinya

ADVANCED ENCRYPTION STANDARD

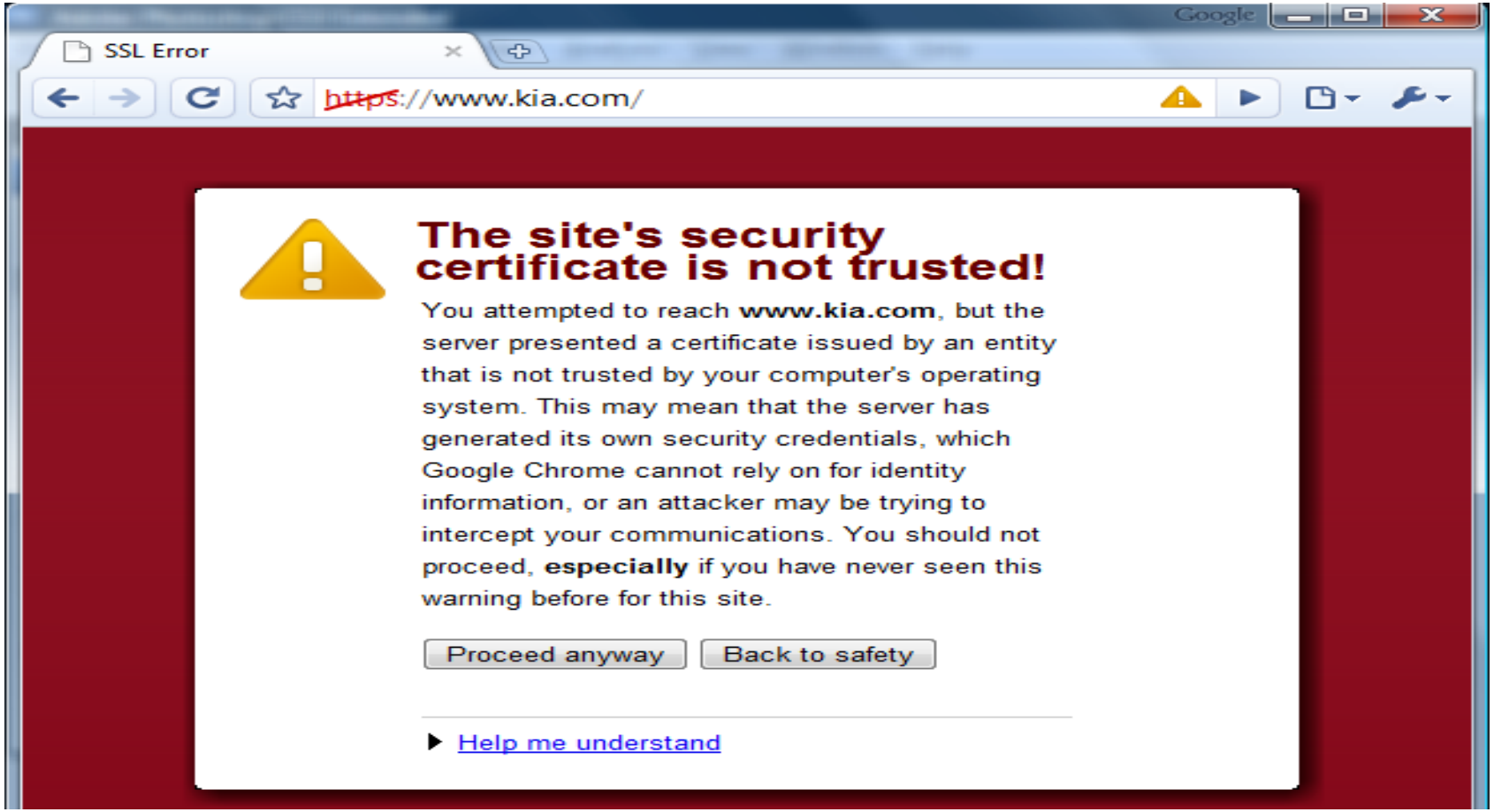
Dalam kriptografi, Advanced Encryption Standard (AES) merupakan standar enkripsi dengan kunci-simetris yang diadopsi oleh pemerintah Amerika Serikat

AES dibangun dengan maksud untuk mengamankan pemerintahan diberbagi bidang. Algoritma AES di design menggunkan blok chiper minimal dari blok 128 bit input dan mendukung ukuran 3 kunci (3-key-sizes), yaitu kunci 128 bit, 192 bit, dan 256 bit

ADVANCED ENCRYPTION STANDARD

Salah satu contoh penggunaan AES adalah pada kompresi 7-Zip. Salah satu proses di dalam 7-Zip adalah mengenkripsi isi dari data dengan menggunakan metode AES-256

DIGITAL CERTIFICATE SERVER



METODE ENKRIPSI LAINNYA

1. IP Security (IPSec)
2. Kerberos
3. Point to point Tunneling Protocol (PPTP)
4. Remote Access Dial-in User Service (RADIUS)
5. Security Token
6. Secure Socket Layer (SSL)
7. Secure Shell (SSH)
8. MD5
9. Secure Hash Algoritm (SHA)
10. RSA Encryption
11. Simple Key Management for Internet Protocol

APLIKASI YANG MEMERLUKAN ENKRIPSI

1. Jasa telekomunikasi
2. Militer dan pemerintahan
3. Data Perbankan
4. Pengamanan electronic mail
5. Data konfidensial perusahaan
6. Kartu Plastik

METODE ENKRIPSI PADA KOMPUTER

1. Enkripsi File
2. Enkripsi Folder
3. Enkripsi Full Disk
4. Shredder

APP ENKRIPSI

1. AxCrypt
2. DiskCryptor
3. VeraCrypt
4. Dekart Private Disk
5. 7-Zip
6. Gpg4Win
7. Synmantec Drive Encryption
8. BitLocker

TUGAS

- Buat aplikasi enkripsi dan deskripsi
- Jelaskan ancaman jika tidak menggunakan enkripsi
- Jelaskan algoritma yang dipakai
- Jelaskan pemilihan bahasa pemograman
- Jelaskan aplikasinya