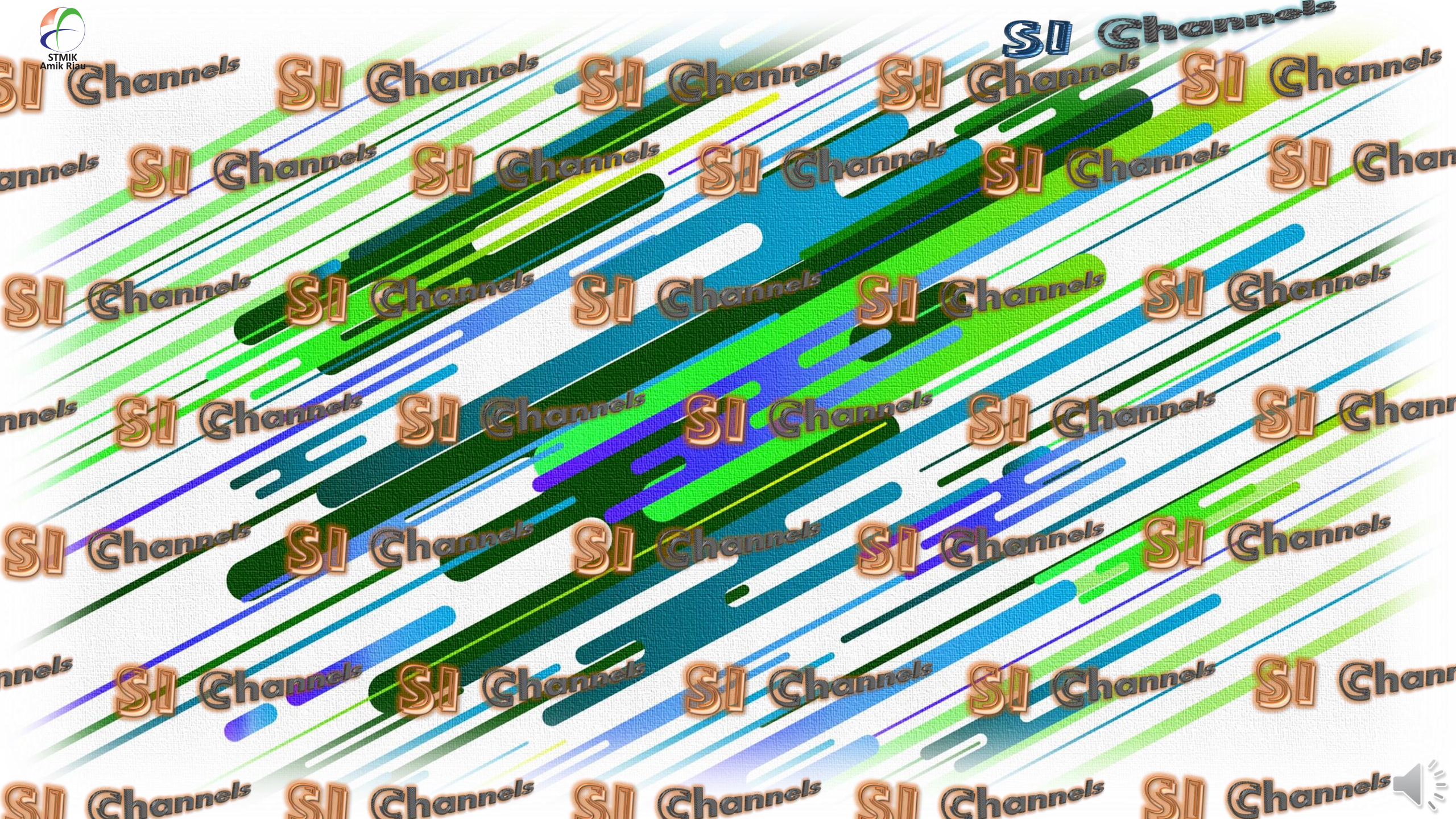
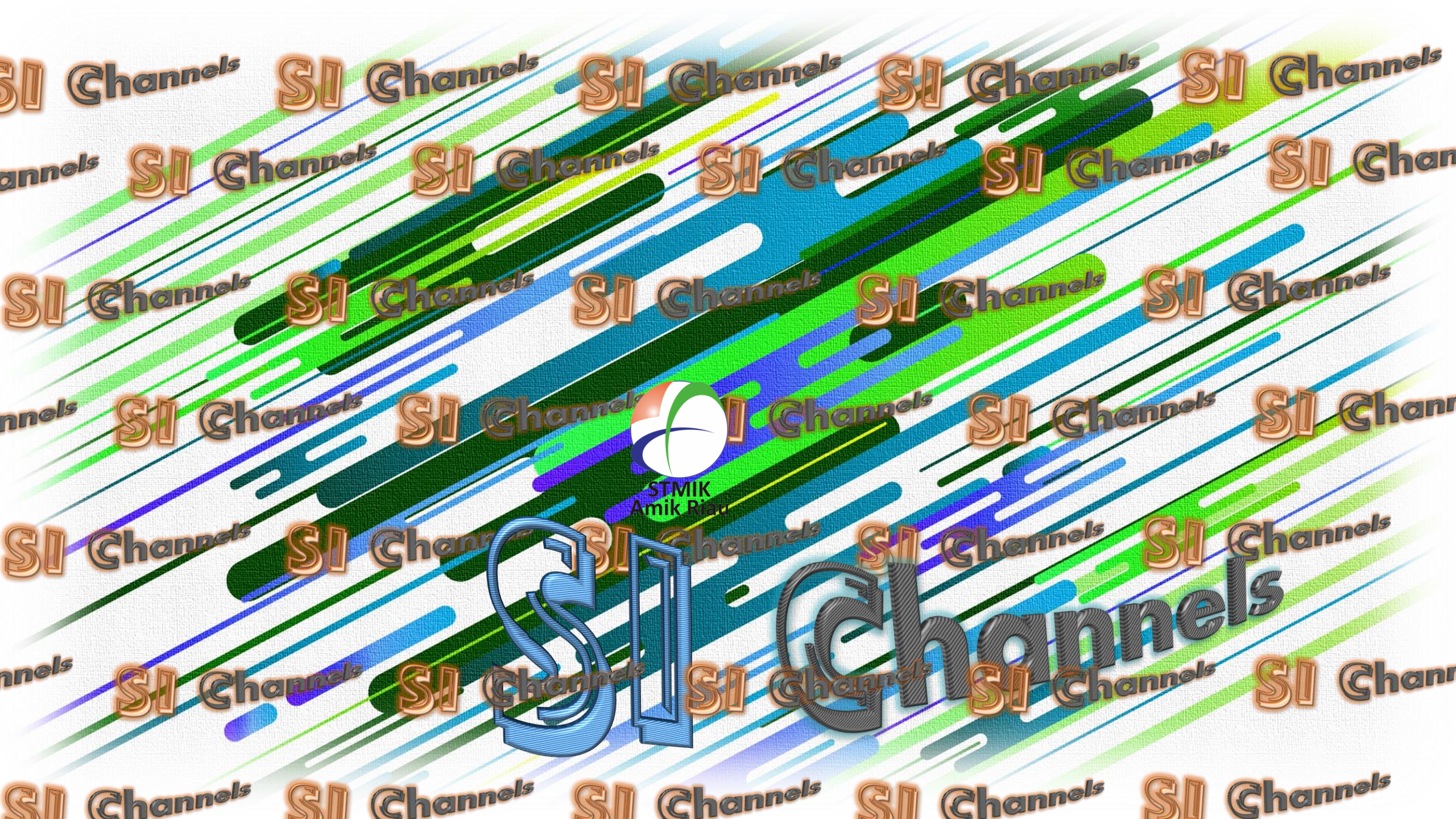

STMIK
Amik Riau
SI Channels


SI Channels
STMIK
Amik Riau

STMIK
Amik Riau

MATAKULIAH
KEAMANAN PERANGKAT LUNAK

Syahrul Imardi Channels

Pertemuan 10

Praktikum Kriptografi Klasik

SYAHRUL IMARDI, M.T

MATAKULIAH

KEAMANAN PERANGKAT LUNAK

SI

Channels

Pertemuan 10

Praktikum Kriptografi Klasik

SYAHRUL IMARDI, M.T

STMIK Amik Riau

#10

Syahrul Imardi, MT

STMIK Amik Riau

MATAKULIAH

KEAMANAN PERANGKAT LUNAK

Praktikum KRIPTOGRAFI KLASIK

P7

STMIK
Amik Riau

MATAKULIAH
KEAMANAN PERANGKAT LUNAK

Syahrul Imardi, MT

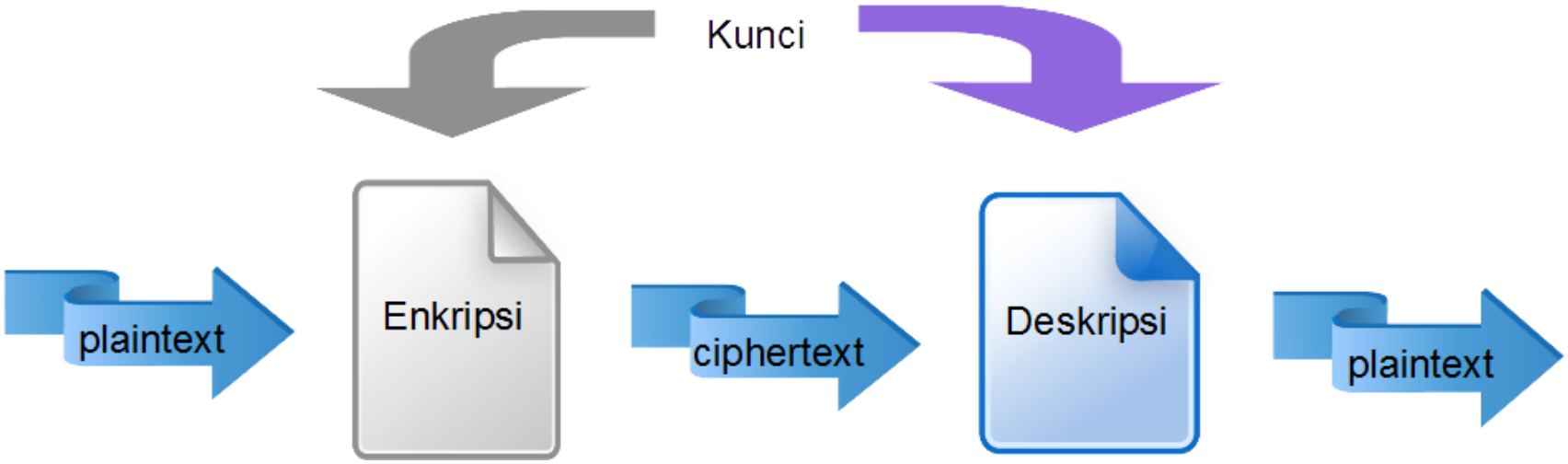
P10 : Praktikum **Kriptografi Klasik**

Algoritma Kriptografi

- Algoritma kriptografi harus memiliki kekuatan untuk melakukan proses enkripsi ***(Shannon)*** :
  - **Konfusi/pembingungan** (*confusion*), dari teks terang sehingga sulit untuk direkonstruksikan secara langsung tanpa menggunakan algoritma dekripsinya.
  - **Difusi/peleburan** (*difusion*), dari teks terang sehingga karakteristik dari teks terang tersebut hilang.

- Ada 3 macam atau jenis algoritma
  - Algoritma Hash (*Hashing algorithm*)
  - Algoritma Kunci Simetris (*Symmetric key algorithm*)
  - Algoritma Kunci Asimetris (*Asymmetric key algorithm*)

Symmetric Key

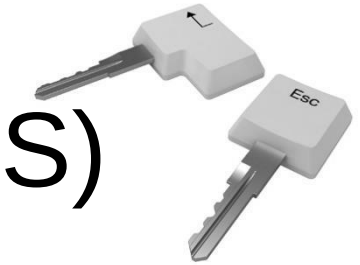


Algoritma Kunci Simetris

- Menggunakan kunci sama dalam proses enkripsi dan deskripsi (sampai Juni 1976.)
- Algoritma :
  - OTP, DES (*Data Encryption Standard*), 3DES, Rivest cipher (RC2, RC4, RC5, RC6), IDEA (*International Data Encryption Algorithm*), AES (*Advanced Encryption Standard*), blowfish, twofish, MARS, dll
- Kelebihan :
  - Kecepatan proses enkripsi dan deskripsi
- Kelemahan :
  - Karena menggunakan kunci yang sama sehingga timbul permasalahan kerahasiaan pada saat pengiriman kunci

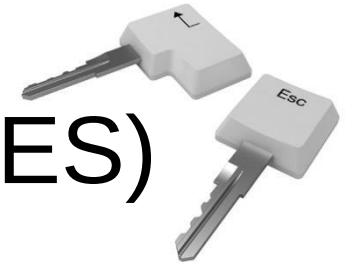
- Implementasi ada 2 macam :
  - ***Block Cipher***
    - Skema algoritma sandi yang akan membagi-bagi teks terang yang akan dikirimkan dengan ukuran tertentu (disebut blok) dengan panjang t (56/64/128/256/512 *bit* dst),
    - Setiap blok dienkripsi dengan menggunakan kunci yang sama.
  - ***Stream Cipher***
    - Algoritma sandi yang mengenkripsi data persatuan data, seperti *bit, byte, nible* atau per 5 *bit* (saat data yang di enkripsi berupa data *Boudout*).
    - Setiap mengenkripsi satu satuan data digunakan kunci yang merupakan hasil pembangkitan dari kunci sebelum.

Data Encryption Standard (DES)



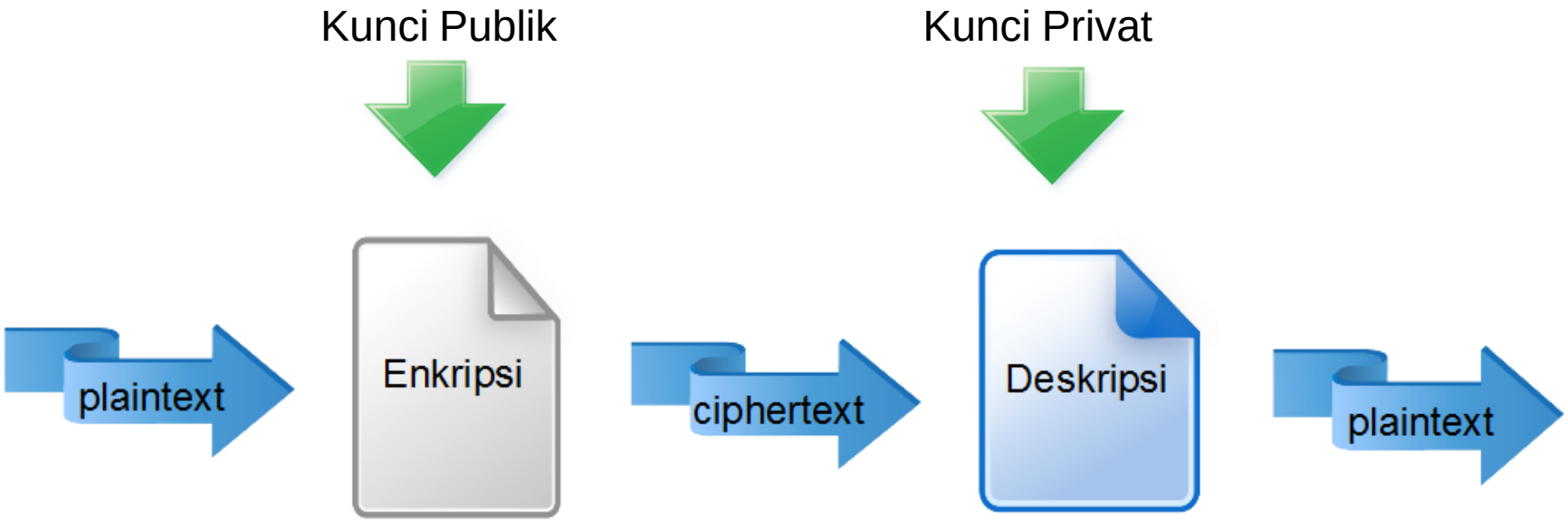
- Nama lain : DEA (*Data Encryption Algorithm*) atau DEA-1 atau Lucifer, dikembangkan awal 1970-an.
- Menggunakan *key* 56-*bit*, sehingga ada 2^{56} (72.057.594.037.927.936) kemungkinan kunci yg bisa dipakai.
- Setelah konsultasi dengan NSA (*National Security Agency*) tahun 1976, akhirnya dijadikan standard sejak tahun 1977 di USA.
- Meski sempat digunakan luas, kini dianggap kurang aman, tahun 1999 *distributed.net & Electronic Frointier Foundation* berhasil membongkar enkripsi DES dalam 22 jam 15 menit.
- Pada 26 May 2002 DES digantikan dengan AES (*Advanced Encription Standard*).
- 3 DES oleh NIST (*National Institute of Standards and Technology*) tetap disetujui sampai 2030 untuk informasi pemerintah yang sensitif.

Advanced Encryption Standard (AES)



- Spesifikasi enkripsi untuk data elektronik yang diterbitkan oleh NIST tahun 2001, menggantikan DES (aslinya disebut *Rijndael*)
- Diadopsi pemerintah USA dan digunakan secara luas di dunia.
- Menggunakan ukuran kunci 128, 192 atau 256-*bit*.
  - *Key* 128-*bit* digunakan pemerintah USA untuk kategori informasi *SECRET*, dan
  - *Key* 192-*bit* / 256-*bit* untuk kategori *TOP SECRET*.

Asymmetric Key



- Kunci deskripsi dan enkripsi berbeda
  - Enkripsi → *public key*
  - Deskripsi → *private key*
- Kunci publik yang akan didistribusikan, sehingga dapat mengatasi permasalahan pada algoritma simetris.
- Algoritma : RSA, DSA, DH, ECC

Pendahuluan

- Algoritma kriptografi klasik berbasis karakter
- Menggunakan pena dan kertas saja, belum ada komputer
- Termasuk ke dalam kriptografi kunci-simetri
- Algoritma kriptografi klasik:
  - *Cipher* Substitusi (*Substitution Ciphers*)
  - *Cipher* Transposisi (*Transposition Ciphers*)

1. Cipher Substitusi

- Monoalfabet : setiap karakter chipertext menggantikan satu macam karakter plaintext
- Polyalfabet : setiap karakter chipertext menggantikan lebih dari satu macam karakter plaintext
- Monograf /unilateral: satu enkripsi dilakukan terhadap satu karakter plaintext
- Polygraf /multilateral: satu enkripsi dilakukan terhadap lebih dari satu karakter plaintext

1. Cipher Substitusi - Caesar Cipher

- Tiap huruf alfabet digeser 3 huruf ke kanan

p_i : 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

c_i : **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**

- Contoh:

  Plainteks: AWASI ASTERIX DAN TEMANNYA OBELIX

  Cipherteks: **DZDVL DVWHULA GDQ WHPDQQBA REHOLA**

1. Cipher Substitusi - Caesar Cipher

- Dalam praktek, cipherteks dikelompokkan ke dalam kelompok n-huruf, misalnya kelompok 4-huruf:

  DZDV LDVW HULA GDQW HPDQ QBAR EHOL A

- Atau membuang semua spasi:

  DZDVLDVWHULAGDQWHPDQQBAREHOLA

- Tujuannya agar kriptanalisis menjadi lebih sulit

1. Cipher Substitusi - *Vigènere Cipher*

- Termasuk ke dalam cipher abjad-majemuk (polyalpabetic substitution cipher).
- Algoritma tersebut baru dikenal luas 200 tahun kemudian yang oleh penemunya cipher tersebut kemudian dinamakan Vigènere Cipher.
- Vigènere Cipher menggunakan Bujursangkar Vigènere untuk melakukan enkripsi.
- Setiap baris di dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan Caesar Cipher.

1. Cipher Substitusi - *Vigènere Cipher*

Kunci \ Plainteks	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

Gambar 4.2 Bujursangkar *Vigènere*

1. Cipher Substitusi - *Vigènere Cipher*

- Contoh penerapan Vigènere Cipher :

  Plainteks : THIS PLAINTEXT

  Kunci : amik amikamika

  Cipherteks : **TTTC PXLSNFRHT**

- Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang secara periodik. Dalam hal ini Kunci “amik” diulang sebanyak panjang plaintext-nya
- Pada dasarnya, setiap enkripsi huruf adalah *Caesar cipher* dengan kunci yang berbeda-beda.

  c(‘T’) = (‘T’ + ‘a’) mod 26 = L

  T = 20 dan a= 1 → (20+1)%26=19 → T

  c(‘H’) = (‘H’ + ‘m’) mod 26 = T, dst

2. Cipher Transposisi

- Cipherteks diperoleh dengan mengubah posisi huruf di dalam plainteks.
- Dengan kata lain, algoritma ini melakukan *transpose* terhadap rangkaian huruf di dalam plainteks.
- Nama lain untuk metode ini adalah **permutasi**, karena *transpose* setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.

2. Cipher Transposisi (Contoh)

Contoh: Misalkan plainteks adalah

```
TEKNIK INFORMATIKA STMIK AMIK RIAU
```

Enkripsi:

```
TEKNIK
INFORM
ATIKAS
TMIKAM
IKRIAU
```

Cipherteks: (baca secara vertikal)

TIATIENTMKKFIIRNOKKIIRAAAKMSMU

TIAT IENT MKKFI IRNO KKII RAAA KMSMU

Referensi utama :

>> Michael Felderer , Riccardo Scandariato (editor) - Exploring Security in Software Architecture and Design, 2018.

>> Nancy R. Mead, Carol Woody - Cyber Security Engineering_ A Practical Approach for Systems and Software Assurance-Addison-Wesley Professional (2016)

>> James Helfrich - Security for Software Engineers-CRC Press (2019)

>> Pete Loshin - Simple Steps to Data Encryption_ A Practical Guide to Secure Computing-Syngress (2013)

>> Tevfik Bultan,Fang Yu,Muath Alkhalaf,Abdulbaki Aydin (auth.) - String Analysis for Software Verification and Security (2017)


Any
Questions?