KRIPTOGRAFI – PERTEMUAN 6

TEKNIK TRANSPOSISI

Sindhu Rakasiwi, M.Kom
sindhu.rakasiwi@dsn.dinus.ac.id

Content

1. Transposisi Rail Fence
2. Transposisi Kolom
3. Transposisi Ganda
4. Transposisi Myszkowski

Teknik Transposisi

- Metode penyandian transposisi adalah metode penyandian dengan cara mengubah letak dari teks pesan yang akan disandikan.
- Untuk membaca pesan aslinya kembali, cukup dengan mengembalikan letak dari pesan tersebut berdasarkan kunci dan algoritma pergeseran huruf yang telah disepakati.

Teknik Transposisi

- Terdapat beberapa algoritma dalam metode penyandian transposisi yaitu :
  - *Transposisi Rail Fence*
  - *Transposisi Kolom*
  - *Transposisi Ganda*
  - *Transposisi Myszkowski*

Transposisi Rail Fence

- *Rail Fence* atau bisa juga disebut alur pagar adalah bentuk penyandian transposisi dengan cara menuliskan huruf-huruf teks asli secara turun naik dalam sebuah pagar imajiner.
- Teks sandinya dibaca secara baris per baris.

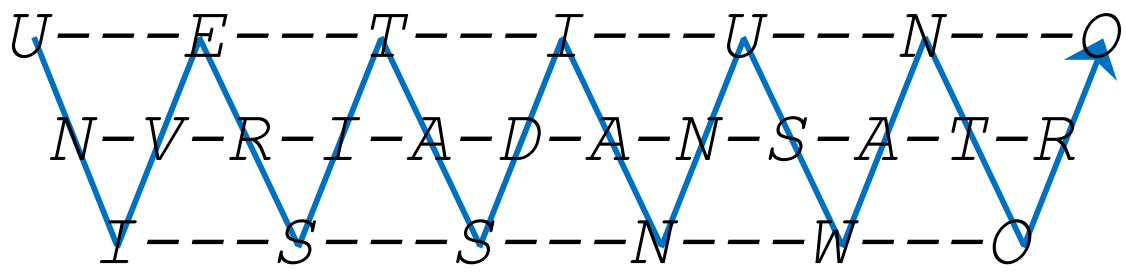
Transposisi Rail Fence

- Contoh:

  Plaintext : *UNIVERSITAS DIAN NUSWANTORO*

  Kunci : *3 baris*

  Proses penyandian



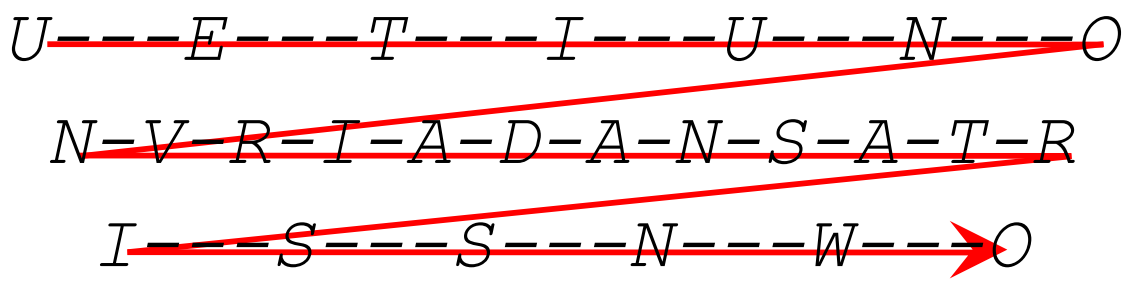
Transposisi Rail Fence

- Contoh:

  Plaintext : *UNIVERSITAS DIAN NUSWANTORO*

  Kunci : *3 baris*

  Proses penyandian



  Ciphertext:

  UETIUNONVRIADANSATRISSNWO

Transposisi Kolom

- Penyandian Transposisi Kolom dituliskan secara baris (biasa) dengan panjang yang telah ditentukan sebagai kunci-nya.
- Teks sandi-nya dibaca secara kolom demi kolom dengan pengacakan melalui permutasian angka kuncinya.
- Panjang baris dan permutasian kolomnya disebut sebagai “kata kunci”.
- Dalam prosesnya, kata kunci tersebut didefinisikan dahulu dengan angka sesuai urutan abjad.
- Sedangkan proses untuk mengembalikan ke teks sandi ke teks aslinya dilakukan langkah kebalikan darinya.

Transposisi Kolom

- Contoh:
  - *Plaintext:*

    UNIVERSITAS DIAN NUSWANTORO UDINUS POLKE
  - *Kunci:*

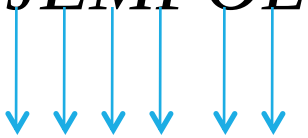
    JEMPOL
  - *Ciphertext: ???*

Transposisi Kolom

- Contoh:
  - *Plaintext:*

    UNIVERSITAS DIAN NUSWANTORO UDINUS POLKE
  - *Kunci:*

    JEMPOL

    214 6 5 3

  - *Ciphertext:*

Transposisi Kolom

- Contoh:
  - *Plaintext:*

    UNIVERSITAS DIAN NUSWANTORO UDINUS POLKE
  - *Kunci:*

    JEMPOL

    214 6 5 3

U	N	I	V	E	R
S	I	T	A	S	D
I	A	N	N	U	S
W	A	N	T	O	R
O	U	D	I	N	U
S	P	O	L	K	E

  - *Ciphertext:*

Transposisi Kolom

- Contoh:
  - *Plaintext:*

    UNIVERSITAS DIAN NUSWANTORO UDINUS POLKE

  - *Kunci:*

    JEMPOL

    214653

    2 1 4 6 5 3

U	N	I	V	E	R
S	I	T	A	S	D
I	A	N	N	U	S
W	A	N	T	O	R
O	U	D	I	N	U
S	P	O	L	K	E

  - *Ciphertext:*

Transposisi Kolom

- Contoh:
  - *Plaintext:*

    UNIVERSITAS DIAN NUSWANTORO UDINUS POLKE
  - *Kunci:*

    JEMPOL

    214653
  - *Ciphertext:*

    NIAAUP

2	1	4	6	5	3
U	N	I	V	E	R
S	I	T	A	S	D
I	A	N	N	U	S
W	A	N	T	O	R
O	U	D	I	N	U
S	P	O	L	K	E

Transposisi Kolom

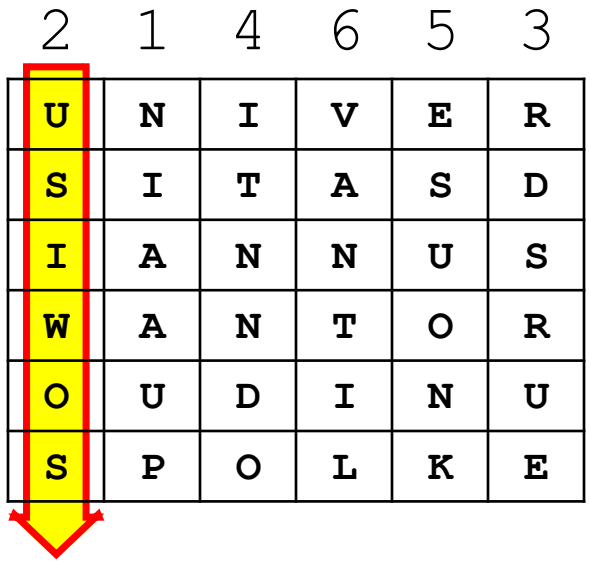
- Contoh:
  - *Plaintext:*

    UNIVERSITAS DIAN NUSWANTORO UDINUS POLKE

  - *Kunci:*

    JEMPOL

    214653



  - *Ciphertext:*

    *NIAAUP**USIWOS***

Transposisi Kolom

- Contoh:
  - *Plaintext:*

    UNIVERSITAS DIAN NUSWANTORO UDINUS POLKE

  - *Kunci:*

    JEMPOL

    214 6 5 3

2	1	4	6	5	3
U	N	I	V	E	R
S	I	T	A	S	D
I	A	N	N	U	S
W	A	N	T	O	R
O	U	D	I	N	U
S	P	O	L	K	E

  - *Ciphertext:*

    *NIAAUPUSIWOS**RDSRUE***

Transposisi Kolom

- Contoh:
  - *Plaintext:*

    UNIVERSITAS DIAN NUSWANTORO UDINUS POLKE
  - *Kunci:*

    JEMPOL

    214653

2	1	4	6	5	3
U	N	I	V	E	R
S	I	T	A	S	D
I	A	N	N	U	S
W	A	N	T	O	R
O	U	D	I	N	U
S	P	O	L	K	E
  - *Ciphertext:*

    NIAAUPUSIWOSRDSRUEITNNDOESUONKVANTIL

Transposisi Ganda

- Penyandian transposisi ganda adalah metode penyandian transposisi kolom yang dilakukan dua kali.
- Dua kali proses penyandian ini dilakukan untuk mempersulit upaya pemecahan teks sandi transposisi kolom yang biasanya dapat dengan mudah dilakukan dengan metode tertentu.
- Proses penyandian yang kedua ini bisa menggunakan kunci yang sama atau dua kunci yang berbeda.

Transposisi Ganda

- Latihan:
  - *Plaintext:*

    UNIVERSITAS
  - *Kunci #1:*

    OKE
  - *Ciphertext #1 / Plaintext Baru:*

    IRTNEISUVSA
  - ***Kunci #2:***

    SAYA
  - ***Ciphertext #2:***

    ???

    RISNUIEVTSA

Transposisi Myszkowski

- Émile Victor Théodore **Myszkowski** di tahun 1902 memperkenalkan variasi dari metode penyandian transposisi kolom, yang dibedakan dalam pendefinisian dan permutasian kata kunci-nya.
- Dalam metode penyandian transposisi kolom, kata kunci misalnya BOROBUDUR di definisikan menjadi 1 4 6 5 2 8 3 9 7
- Sedangkan dalam metode Myszkowski menjadi 1 3 4 3 1 5 2 5 4

Transposisi Myszkowski

- Teks sandinya dibaca secara urutan nomor kolom, bila nomor urut kolomnya sama dibaca secara bersamaan dimulai dari sebelah kiri

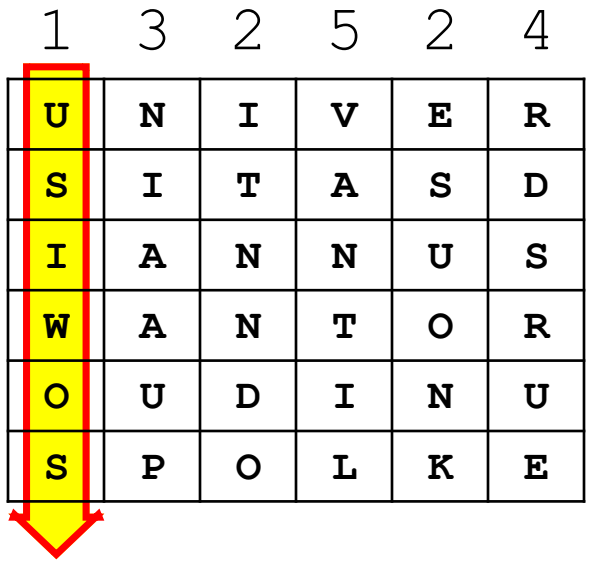
Transposisi Myszkowski

- Contoh:
  - *Plaintext:*

    UNIVERSITAS DIAN NUSWANTORO UDINUS POLKE
  - *Kunci:*

    CLEVER

    132 5 24



  - *Ciphertext:*

    USIWOS

Transposisi Myszkowski

- Contoh:
  - *Plaintext:*

    UNIVERSITAS DIAN NUSWANTORO UDINUS POLKE
  - *Kunci:*

    CLEVER

    132 5 24

1	3	**2**	5	**2**	4
U	N	**I**	V	**E**	R
S	I	**T**	A	**S**	D
I	A	**N**	N	**U**	S
W	A	**N**	T	**O**	R
O	U	**D**	I	**N**	U
S	P	**O**	L	**K**	E

  - *Ciphertext:*

    *USIWOS**IETSNUNODNOK***

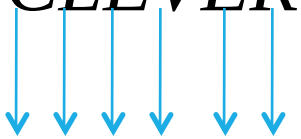
Transposisi Myszkowski

- Contoh:
  - *Plaintext:*

    UNIVERSITAS DIAN NUSWANTORO UDINUS POLKE

  - *Kunci:*

    CLEVER

    132 5 24

1	3	2	5	2	4
U	N	I	V	E	R
S	I	T	A	S	D
I	A	N	N	U	S
W	A	N	T	O	R
O	U	D	I	N	U
S	P	O	L	K	E

  - *Ciphertext:*

    USIWOSIETSNUNODNOKNIAAUPRDSRUEVANTIL

Latihan Soal

- Soal 1 : (point 40)

Plainteks : Kampus Biru Universitas Dian Nuswantoro Jaya Raya

Kunci : Semangat

Algoritma : a)Transposisi Kolom

b) Transposisi Myszkowski

- Soal 2 : (point :20)

Transposisi Rail Fence

Plaintext : Kampus Biru Ceria

Kunci : 3 Baris

- Soal 3 : (point 40)
  - *Plaintext:*

    UNIVERSITAS DIAN NUSWANTORO UDINUS POLKE
  - *Kunci #1:*

    JEMPOL
  - *Kunci #2:*

    UDINUS

TERIMAKASIH