



# TEKNIK CRYPTOGRAPHY (KRIPTOGRAFI) BAGIAN 3

PERTEMUAN 6

# TRANSPOSITION CIPHER

- Railfence Cipher
- Redefence Cipher
- Reverse Cipher

# RAILFENCE CIPHER

- Plainteks dapat dimulai pada titik manapun pada setiap siklus, ditulis dengan cara zigzag
- Contoh: “3 0” ini menandakan bahwa 3 baris dan tidak ada offset. Offset berjalan dari 0 sampai  $2R-3$ , dimana  $R$  adalah jumlah baris

# CONTOH RAILFENCE CIPHER

Plainteks: sirik tanda tak mampu, Kunci 3

S		K		D		K		P	
I	I	T	N	A	A	M	M	U	
	R		A		T		A		X

Ciperteks: SKDKP IITNAAMMU RATA X

# CONTOH LAIN

Diketahui cipherteks TKAKDAG IAKNLAAIASYN DEMTKA,  
Kunci 3

Plainteks?

T            K            A            K            D            A            G  
I    A            K    N            L    A            A    I            A    S            Y    N  
D            E            M            T            K            A

Plainteks= TIDAK KENAL MAKA TIDAK SAYANG

# REDEFENCE CIPHER

- Plainteks dapat dimulai pada titik manapun pada setiap siklus
- Ditulis dengan zig-zag

# CONTOH REDEFENCE CIPHER

Plainteks: Sirik Tanda Tak Mampu, Kunci [2, 1, 3]

2: S K D K P

1: I I T N A A M M U

3: R A T A X

Cipherteks: IITNAAMMU SKDKP RATA X

# REVERSE CIPHER

- Cara kerja dari sandi ini adalah dengan cara mengganti satu huruf dengan huruf yang lain
- Sandi ini adalah contoh yang paling sederhana dari transposisi yaitu dengan mengubah suatu kalimat dengan cara menuliskan setiap kata secara terbalik (reverse)



# CONTOH REVERSE CIPHER

Plainteks : B E L A J A R K R I P T O G R A F I

Cipherteks: R A J A L E B I F A R G O T P I R K

# ONE-TIME PAD CIPHER

- Secara teoritis 100% aman dan merupakan sandi yang mudah untuk dilakukan secara manual
- Pertama diperkenalkan oleh Frank Miller pada tahun 1882, dan ditemukan Kembali pada tahun 1917.
- Mirip dengan sandi Vigenère, tetapi tanpa pengulangan kunci
- Persyaratan one-time pad: kunci harus random, jumlah kunci sama atau lebih dari plainteks, kunci tidak dapat digunakan kembali, kunci harus tetap rahasia
- Contoh one-time pad:
  - Plainteks: ONE TIME PAD
  - Kunci: PERFECTSECRECY
  - Cipherteks: DRVXKFWRRH