

## KRIPTOGRAFI PADA PERANG DUNIA I: SANDI PLAYFAIR

Oleh: M. Zaki Riyanto

Email: [zaki@mail.ugm.ac.id](mailto:zaki@mail.ugm.ac.id)

<http://zaki.math.web.id>

### Sandi Playfair

Sandi Playfair digunakan oleh Tentara Inggris pada saat Perang Boer II dan Perang Dunia I. Ditemukan pertama kali oleh Sir Charles Wheatstone dan Baron Lyon Playfair pada tanggal 26 Maret 1854.

Playfair merupakan *digraphs cipher*, artinya setiap proses enkripsi dilakukan pada setiap dua huruf. Misalkan plainteknya “KRIPTOLOGI”, maka menjadi “KR IP TO LO GI”. Playfair menggunakan tabel 5x5. Semua alfabet kecuali J diletakkan ke dalam tabel. Huruf J dianggap sama dengan huruf I, sebab huruf J mempunyai frekuensi kemunculan yang paling kecil. Kunci yang digunakan berupa kata dan tidak ada huruf sama yang berulang. Apabila kuncinya “MATAHARI”, maka kunci yang digunakan adalah “MATHRI”. Selanjutnya, kunci dimasukkan ke dalam tabel 5x5, isian pertama adalah kunci, selanjutnya tulis huruf-huruf berikutnya secara urut dari baris pertama dahulu, bila huruf telah muncul, maka tidak dituliskan kembali.

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

Berikut ini aturan-aturan proses enkripsi pada Playfair.

- 1) Jika kedua huruf tidak terletak pada baris dan kolom yang sama, maka huruf pertama menjadi huruf yang

sebaris dengan huruf pertama dan sekolom dengan huruf kedua. Huruf kedua menjadi huruf yang sebaris dengan huruf kedua dan sekolom dengan huruf pertama. Contohnya, SA menjadi PH, BU menjadi EP.

- 2) Jika kedua huruf terletak pada baris yang sama maka huruf pertama menjadi huruf setelahnya dalam baris yang sama, demikian juga dengan huruf kedua. Jika terletak pada baris kelima, maka menjadi baris pertama, dan sebaliknya. Arahnya tergantung dari posisi huruf pertama dan kedua, pergeserannya ke arah huruf kedua. Contohnya, AH menjadi TR, LK menjadi KG, BE menjadi CI.
- 3) Jika kedua huruf terletak pada kolom yang sama maka huruf pertama menjadi huruf setelahnya dalam kolom yang sama, demikian juga dengan huruf kedua. Jika terletak pada kolom kelima, maka menjadi kolom pertama, dan sebaliknya. Arahnya tergantung dari posisi huruf pertama dan kedua, pergeserannya ke arah huruf kedua. Contohnya, DS menjadi LY, PA menjadi GW, DH menjadi HY.
- 4) Jika kedua huruf sama, maka letakkan sebuah huruf di tengahnya (sesuai kesepakatan).
- 5) Jika jumlah huruf plainteks ganjil, maka tambahkan satu huruf pada akhirnya, seperti pada aturan ke-4.

Sedangkan proses dekripsinya adalah kebalikan dari proses enkripsi. Contohnya, HR didekrip menjadi HT, BS didekrip menjadi DP, ZU didekrip menjadi RZ.

**Contoh Soal.**

Enkrip pesan “ATTACK TOMORROW” menggunakan kunci dan tabel di atas.

*Jawab:* Plainteksnya AT TA CK TO MO RR OW. Karena ada digraph RR, tambahkan sebuah huruf, misalkan Q, maka plainteksnya menjadi AT TA CK TO MO RQ RO WQ. Sehingga diperoleh bahwa cipherteksnya adalah “TH AM KQ QM IV UT UM TO”.

**Soal Latihan Sandi Playfair**

1) Enkrip “SUPPORT ARMY URGENTLY” menggunakan kunci “MIDNIGHT”.

Jawab:


Plainteks: 


  
 Cipherteks: 



2) Enkrip “THE FIRST WORLD WAR” menggunakan kunci seperti pada soal 1 di atas.

Jawab:

Plainteks: 


  
 Cipherteks: 



3) Enkrip “DATANG JAM EMPAT SORE” menggunakan kunci seperti pada soal 1 di atas.

Jawab:

Plainteks: 


  
 Cipherteks: 



4) Dekrip “FD FS FB EP FD GM CF GE SR UK IW” menggunakan kunci seperti pada soal 1 di atas.

Jawab:

Plainteks: 


  
 Cipherteks: 



Pesan Asli : .....

5) Dekrip “MI GB QL CI BP GQ AO VO GQ CL QL EI GK” menggunakan kunci “CRYPTOLOGY”.

Jawab:


Plainteks: 


  
 Cipherteks: 



Pesan Asli : .....

6) Dekrip “QH PL CQ VK CX GO IM DU PL OZ ED  
 QO QR ZK” menggunakan kunci soal 5 di atas.

Jawab:

Plainteks: 


Cipherteks: 



Pesan Asli : .....

.....

7) Dekrip “YD IP BA TQ HM SD HM QT EO FN SD  
 UE BA TM UA KA DS MT HM QT QB UE EH  
 MN TQ BW” (Hint. Pasal 15 Ayat 1 RUU Rahasia  
 Negara). Gunakan kunci “MATEMATIKA”.

Jawab:


Plainteks: 


Cipherteks: 




Plainteks: .....

.....

.....

### Daftar Pustaka

Churchhouse, Robert, 2001, *Codes and Ciphers, Julius Caesar, the Enigma, and the Internet*, Cambridge University Press, UK.

Spillman, Richard, 2005, *Classical and Contemporary Cryptology*, Pearson Education, Inc, New Jersey.