

KRIPTOGRAFI PADA PERANG DUNIA I: SANDI ADFGVX

Oleh: M. Zaki Riyanto

Email: zaki@mail.ugm.ac.id

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

Sandi ADFGVX

Sandi ADFGVX digunakan oleh Tentara Jerman pada Perang Dunia I. Ditemukan pertama kali oleh Kolonel Fritz Nobel pada Maret 1918. ADFGVX menggunakan tabel 6x6 yang berisi 26 huruf dan 10 angka (0-9). Enkripsinya terdiri dari dua proses, yaitu proses substitusi dan proses transposisi. Setiap proses membutuhkan sebuah kunci. Huruf A, D, F, G, V, dan X dipilih karena mudah dikirimkan menggunakan Sandi Morse.

Berikut ini aturan-aturan dalam Sandi ADFGVX yang disertai dengan contoh.

- (1) Tentukan kunci pertama yang terdiri dari huruf dan angka, misalkan "math08". Jika ada huruf yang berulang, maka cukup satu huruf yang muncul pertama yang dituliskan.
- (2) Buatlah sebuah tabel 6x6 dengan bentuk berikut ini. Isian pertama adalah kunci, kemudian huruf-huruf berurutan yang belum muncul, dan selanjutnya angka-angka berurutan yang belum muncul.

	A	D	F	G	V	X
A	m	a	t	h	0	8
D	b	c	d	e	f	g
F	i	j	k	l	n	o
G	p	q	r	s	u	v
V	w	x	y	z	1	2
X	3	4	5	6	7	9

- (3) Selanjutnya, setiap huruf dalam plainteks disubstitusi menjadi dua huruf yang ditentukan oleh posisi baris dan kolom. Contohnya huruf k menjadi FF, huruf g menjadi DX. Misalkan plainteksnya "belajar sandi", maka hasil substitusinya adalah "DA DG FG AD FD AD GF GG AD FV DF FA".
- (4) Tentukan kata kunci kedua, terdiri dari huruf saja, dan boleh muncul berulang. Kunci ini digunakan dalam proses transposisi. Pertama buatlah tabel, tulis kunci di atasnya, kemudian tulis hasil substitusi (3) di bawahnya berurutan. Jika ada sisa, diisi dengan huruf X atau sesuai dengan kesepakatan. Perhatikan tabel di bawah ini. Misalkan kuncinya "kunci".

1 2 3 4 5
k u n c i

D	A	D	G	F
G	A	D	F	D
A	D	G	F	G
G	A	D	F	V
D	F	F	A	X
X	X	X	X	X

- (5) Selanjutnya, urutkan huruf pada kunci. Contohnya, jika kuncinya "matahari" (1-2-3-4-5-6-7-8), menjadi "aaahimrt" (2-4-6-5-8-1-7-3). Jadi, untuk kunci "kunci" menjadi "ciknu" (4-5-1-3-2). Sehingga tabel menjadi:

4 5 1 3 2
c i k n u

G	F	D	D	A
F	D	G	D	A
F	G	A	G	D
F	V	G	D	A
A	X	D	F	F
X	X	X	X	X

(6) Ciphertekstnya adalah huruf-huruf yang berada di kolom pertama, dan seterusnya. Jadi, ciphertekstnya adalah "GFFFFX FDGVXX DGAGDX DDGDFX AADAFX".

Dari proses enkripsi di atas, tidak sulit bagi Anda untuk mempelajari proses dekripsinya.

Soal Latihan Sandi ADFGVX

1) Enkrip "kirim 150 pasukan" menggunakan kunci substitusi dan transposisi seperti pada contoh di atas.

Jawab:

Tabel Substitusi:

1 2 3 4 5 4 5 1 3 2
k u n c i c i k n u

Ciphertekst:

.....

.....

2) Enkrip nama Anda (maks. 15 huruf) menggunakan kunci substitusi "19agustus2008" dan kunci transposisi "bulan".

Jawab:

Kunci yang digunakan adalah "19agust208".

A D F G V X

A						
D						
F						
G						
V						
X						

Tabel Substitusi:

Tabel Transposisi:

...
...

Pesan Asli :

.....

.....

3) Dekrip “DAADDD FGAFAF GFDFGF GGGGGG
GFGVDA GDXXGF” menggunakan kunci
substitusi “when2go93” dan kunci transposisi
“thekey”.

Jawab:

Tabel Transposisi:

... ..
... ..

	A	D	F	G	V	X
A						
D						
F						
G						
V						
X						

Tabel Substitusi :

Pesan Asli :

.....

.....

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.