METODE KRIPTOGRAFI
PRODUCT CIPHER

ADFGVX PRODUCT CIPHER

Product cipher merupakan metode yang menggabung 2 metode kriptografi yang berbeda. Salah satu contoh dari metode ini adalah *ADFGVX Product Cipher. ADFGVX Product Cipher* merupakan suatu metode untuk menciptakan fungsi enkripsi kompleks dengan cara menggabungkan beberapa operasi enkripsi dasar sederhana yang saling melengkapi sehingga keduanya melibatkan operasi bolak-balik yang berulang. Operasi dasarnya termasuk subtitusi dan transposisi yang yang dikombinasikan secara bersama-sama. Salah satu produk cipher yang dikembangkan adalah *ADFGVX Product Cipher* [7].

ADFGVX Product Cipher pertama kali digunakan oleh angkatan darat Jerman selama perang dunia pertama. *ADFGVX Product Cipher* dinamakan sejak hanya huruf ADFGVX digunakan. Sistem ini sangat terkenal karena menggunakan 6 subtitusi tabel matriks untuk mengenkripsi 26 huruf besar dan 10 angka untuk menjadi pasangan dari simbol A, D, F, G, V, dan X. *ADFGVX Product Cipher* dikembangkan karena memiliki sandi morse yang jelas. Huruf A, D, F, G, V, X dipilih karena memiliki perbedaan didalam kode-kode sandi morse yang jelas. *ADFGVX Product Cipher* merupakan gabungan dua atau lebih dari metode kriptografi diantaranya adalah subtitusi dan transposisi. *ADFGVX Product Cipher* menggunakan indeks kolom dan baris yang lebih dikenal dengan matriks, dan terdapat enam kolom dan enam baris yang merupakan perpaduan dari huruf ADFGVX [7].

Algoritma kriptografi *ADFGVX Product Cipher* menggunakan subtitusi tabel matriks untuk memetakan setiap huruf *plaintext* menjadi sepasang huruf yang dihasilkan dari kombinasi tabel matriks indeks baris dan kolom. Algoritma ini juga menggunakan kunci

block transposisi untuk membagi huruf menjadi sepasang ke atas kemudian, *ciphertext* ditulis di dalam *block* dan dikirimkan [7].

Tabel subtitusi dari *ADFGVX Product Cipher* digambarkan sebagai berikut :

Tabel 1. Tabel *ADFGVX Product Cipher* [7]

	A	**D**	**F**	**G**	**V**	**X**
A	K	Z	W	R	1	F
D	9	B	6	C	L	5
F	Q	7	J	P	G	X
G	E	V	Y	3	A	N
V	8	O	D	H	0	2
X	U	4	I	S	T	M

1. Enkripsi

   Untuk lebih jelas tentang proses enkripsi algoritma *ADFGVX Product Cipher* maka berikut ini akan diberikan penerapan dari algoritma *ADFGVX Product Cipher*.

   Plain text : PRODUCTCIPHERS

   Key : DEUTSCH

   a. Subtitusi tabel *ADFGVX product cipher* untuk memetakan setiap huruf *plain text* menjadi sepasang huruf yang menggunakan indeks baris dan kolom dari tabel matriks *ADFGVX product cipher*.

Tabel 2. Tabel *ADFGVX Product Cipher* [7]

	A	**D**	**F**	**G**	**V**	**X**
A	K	Z	W	R	1	F
D	9	B	6	C	L	5

F	Q	7	J	P	G	X
G	E	V	Y	3	A	N
V	8	O	D	H	0	2
X	U	4	I	S	T	M

Tabel tersebut akan menghasilkan sebagai berikut : FG(FG = P) AG(AG=R) VD(VD=O) VF(VF=D) XA(XA = U) DG(DG=C) XV(XV=T) DG(DG=C) XF(XF=I) FG(FG=P) VG(VG=H) GA(GA=E) AG(AG=R) XG(XG=S).

Intermediate Text : FG AG VD VF XA DG XV DG XF FG VG GA AG XG

b. Gunakan kunci *Block Columnar* untuk membagi huruf *intermediate text* menjadi *cipher text.*

Key : DEUTSCH

Keyed Block Columnar Transposition Matrix :

Tabel 3. *Keyed Block Columnlar Transposition Matrix* [7]

D	**E**	**U**	**T**	**S**	**C**	**H**
2	3	7	6	5	1	4
F	G	A	G	V	D	V
F	X	A	D	G	X	V
D	G	X	F	F	G	V
G	G	A	A	G	X	G

Cipher text yang dihasilkan dari *plaintext* PRODUCT CIPHER dengan *key* DEUTSCH adalah DXGX FFDG GXGG VVVG VGFG GDFA AAXA.

2. Dekripsi

Proses dekripsi dari *ADFGVX Product Cipher* merupakan kebalikan dari proses enkripsi. Proses dekripsi dimulai dengan cara mentransposisikan *cipher text* ke dalam *keyed block columnar transposition matrix*, selanjutnya dihasilkan *intermediate text* yang kemudian disubtitusikan ke dalam tabel *ADFGVX Product Cipher* (Tabel 3) yang akan menghasilkan *plain text*.

Untuk lebih jelas tentang proses dekripsi algoritma *ADFGVX Product Cipher* maka berikut ini akan diberikan penerapan dari algoritma *ADFGVX Product Cipher*.

Cipher text : AFFA AXAX FDV AGVX GVGF XVG

Key : APOLLO

a. Transposisikan *Cipher text* ke dalam *Keyed Block Columnar Transposition Matrix* untuk menghasilkan *intermediate text.*

Key : APOLLO

Keyed Block Columnlar Transposition Matrix :

Tabel 4. *Keyed Block Columnar Transposition Matrix* [7]

A	**P**	**O**	**L**	**L**	**O**
1	4	2	5	6	3
A	A	A	G	X	F
F	G	X	V	V	D
F	V	A	G	G	V
A	X	X	F		

Intermediate Text yang dihasilkan dari *plain text* AFFA AXAX FDV AGVX GVGF XVG dengan *key* APOLLO adalah AA AG XF FG XV VD FV AG GV AX XF.

b. Subtitusi *intermediate text* ke dalam tabel *ADFGVX Product Cipher* untuk memetakan setiap pasang huruf *intermediate text* menjadi *plain text*.

Tabel 5. Tabel *ADFGVX Product Cipher* [7]

	A	**D**	**F**	**G**	**V**	**X**
A	K	Z	W	R	1	F
D	9	B	6	C	L	5
F	Q	7	J	P	G	X
G	E	V	Y	3	A	N
V	8	O	D	H	0	2
X	U	4	I	S	T	M

Subtitusi ke dalam tabel tersebut akan menghasilkan sebagai berikut : AA(AA=K) AG(AG=R) XF(XF=I) FG(FG=P) XV(XV=T) VD(VD=O) FV(FV=G) AG(AG=R) GV(GV=A) AX(AX=F) XF(XF=I).

Plain text : KRIPTOGRAFI

Referensi :

[7] Http://williamstallings.com/Extras/Security-Notes/lectures/classical.html.