Cryptanalysis of the SIGABA

Thesis Defense Handout (2 sides)

Michael Lee

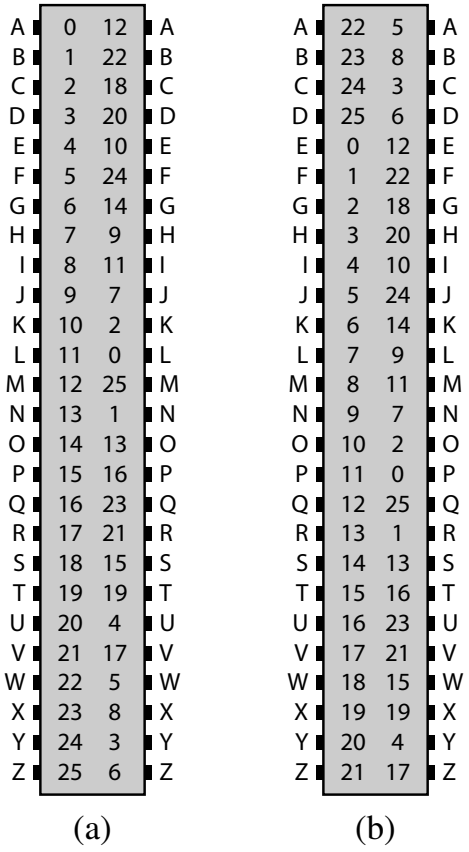

Figure 1: Generic rotor. (a) This is a rotor in its unshifted position. (b) The same rotor rotated through four positions.

i :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
x_i :	Z	M	U	L	T	I	P	U	R	P	O	S	E	Z						
y_i :	F	V	I	K	M	M	V	O	R	U	S	A	V	B	Z	G	K	D	U	E

i :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
x_i :		Z	M	U	L	T	I	P	U	R	P	O	S	E	Z					
y_i :	F	V	I	K	M	M	V	O	R	U	S	A	V	B	Z	G	K	D	U	E

i :	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212
x_i :			Z	M	U	L	T	I	P	U	R	P	O	S	E	Z		
y_i :	Y	M	I	L	F	A	S	Y	J	D	N	E	I	Y	Q	I	F	Y
A_i :			16	16	17	18	19	19	20	21	21	22	23	24	25	26		
B_i :			9	9	9	10	11	12	12	13	13	14	15	16	17	18		
C_i :			13	14	14	15	16	17	17	17	18	19	20	21	22	22		

Table 1: Cribbing a ciphertext encrypted with three rotors at positions 0, 1, and 197.

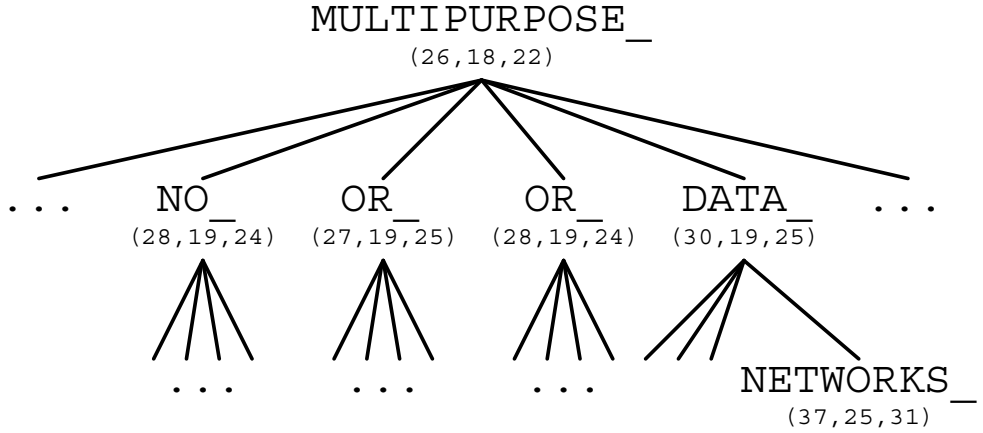

Figure 2: Extending the crib for three rotors. Rotor positions are represented by an ordered triple (A_i, B_i, C_i) below each word.