SIMPLE ALPHABET CYPHER

MULTIPLE ALPHABET SUBSTITUTION CYPHER

Many encyphering schemes are known to cryptographers. One of the simplest is the cryptogram, a form of single alphabet substitution cypher often found in newspapers and puzzle books. In a single alphabet substitution cypher, each letter of the alphabet stands for a single different letter in the message. Cryptograms are usually easy to solve or "break." Only slightly more complicated is the multiple alphabet substitution cypher, in which a letter can stand for any number of other letters. This encyphering scheme uses a key, a string of characters, which matches up against the original or "clear" text and indicates the relationship of any clear text character in a given position to its corresponding cypher character. The key character determines how far the alphabet is shifted at that point. For example, if A=0, B=1, etc., a key character of A would mean there is no shift in that position - the clear and cypher characters would be the same. A key character of B would mean a shift of one character - A becomes B, B becomes C, ..., Z becomes A. It is not hard to see that encyphering in this scheme is equivalent to addition modulo 26 (assuming only letters are used). Thus a key of SECRET (18,4,2,17,4,19) repeated over and over would encypher "ONE IF BY LAND" (14,13,4,8,5,1,24,11,0,13,3) into "GRGZJUQPCEK" since 18+14=32=6 mod 26=G, 4+13=17=R, 2+4=6=G, etc. To decypher, one merely subtracts the key (again modulo 26) from the cypher text to recover the clear.

Since any character can stand for any other at any point in the message, the multiple alphabet substitution cypher is difficult to break. Indeed, for a key composed of "random" characters with no recognizable or repeated pattern, the cypher is literally impossible to break without access to the key, for a given cypher text could just as easily have come from any clear text.

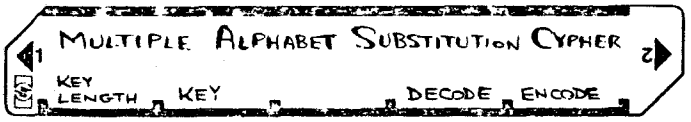
The HP-67/97 program will accept a key of from 3 to 95 characters and encypher or decypher a text five characters at a time. The program keeps track of where it is relative to the start of the key and will automatically repeat the key even if it does not happen to be a multiple of five characters. The user must convert the characters of the key and the clear/cypher texts to/from their numeric equivalents, and supply leading zeroes when necessary.

Example: key = SHAKESPEARE (11 characters)
message = SEAL UP YOUR LIPS AND GIVE NO WORDS BUT MUM; THE BUSINESS ASKETH SILENT SECRECY.
Break the message up into 5-letter blocks. Normally blanks and punctuation are omitted. Convert each letter to its 2-digit equivalent. If the last word does not fill out a 5-character block, add random letters as required. To run, enter number of key characters: 11 A → 5 which indicates the first 5 key characters are to be entered. So enter "SHAKE" in digit form: 1807001004 B → 5 indicating next five, "SPEAR": 1815040017 B → 1 indicating last letter, "E": 04 B → 0. Now the clear blocks are entered:

"SEALU" 1804001120 E → 1011002124 = "KLAVY"
"PYOUR" 1524142017 E → 713182008 = "HNSUI" (note omitted leading zero)
"LIPSA" 1108151800 E → 1500221810 = "PAWSK"
etc. until the last block
"RECYM" 1704022412 E → 919062403 = "JTGYD" (note fill character at end). Complete cypher text is KLAVY HNSUI PAWSK RVVMV VRGDO BHKQY TDYEA HOFMH MNVWK HSUIL WWICI PASOG JTGYD. To decypher, reenter the number of key characters and the key as before, then enter the cypher digits with the D key.
"KLAVY" 1011002124 D → 1804001120 = "SEALU" etc. Can you decypher HPCOM KCSUI MKOEH FQHIC IIUFV OVYXP using the same key?

- Stuart T. Baird (1470)

1. MULTIPLE ALPHABET SUBSTITUTION BY: Stuart T. Baird (1470)
2. CYPHER BY:



STEP	KEY ENTRY	97 KEY CODE
1	LBL A	21 11
	STO A	35 11
	4	04
	+	-55
5	5	05
	/	-24

STEP	KEY ENTRY	KEY CODE
1	1	01
	0	00
	RCL D	36 14
	/	-24
5	STO x i	35 -35 45
	GSB b	23 16 12
	INT	16 34
	STO C	35 13
	5	05
10	x	-35
	RCL A	36 11
	-	-45
	5	05
	X≠Y	-41
15	-	-45
	STO B	35 12
	2	02
	x	-35
	1	01
20	0	00
	X≠Y	-41
	Y^x	31
	STO D	35 14
	2	02
25	6	06
	2	02
	6	06
	2	02
	6	06
30	2	02
	6	06
	2	02
	6	06
	STO A	35 11
35	1	01
	STO I	35 46
	LBL 0	21 00
	RCL I	36 46
	RCL C	36 13
40	X > Y?	16 -34
	GTO 1	22 01
	RCL B	36 12
	RTN	24
	LBL 1	21 01
45	5	05
	RTN	24
	LBL b	21 16 12
	RCL C	36 13
49	STO I	35 46
50	RCL 1	36 01
	RCL D	36 14
	/	-24
	INT	16 34
	STO + i	35 -55 45
55	RTN	24
	LBL c	21 16 13
	RCL 1	36 01
	RCL D	36 14
	/	-24
60	FRAC	16 44
	RCL D	36 14
	x	-35
	STO 1	35 01
	RCL C	36 13
65	STO I	35 46
	RCL D	36 14
	LBL 9	21 09
	STO / i	35 -24 45
	DSZ I	16 25 46
70	GTO 9	22 09
	1	01
	STO I	35 46
	LBL 8	21 08
	EEX	-23
75	1	01
	0	00
	STO x i	35 -35 45
	RCL I	36 46
	RCL C	36 13
80	X = Y?	16 -33
	RTN	24
	ISZ I	16 26 46
	RCL i	36 45
	ENTER	-21
85	INT	16 34
	X≠Y	-41
	FRAC	16 44
	STO i	35 45
	X≠Y	-41
90	DSZ I	16 25 46
	STO + i	35 -55 45
	ISZ I	16 26 46
	GTO 8	22 08
	LBL B	21 12
95	STO i	35 45
	RCL I	36 46
	RCL C	36 13
	X > Y?	16 -34
	GTO 2	22 02
100	EEX	-23
	1	01
	STO I	35 46
	CLX	-51
10	RTN	24
	LBL 2	21 02
	ISZ I	16 26 46
	GTO 0	22 00
	LBL D	21 14
15	RCL A	36 11
	+	-55
	RCL i	36 45
	-	-45
	GTO e	22 16 15
20	LBL E	21 15
	RCL(i)	36 45
	+	-55
	LBL e	21 16 15
	RCL I	36 46
25	STO E	35 15
	R↓	-31
	GSB 7	23 07
	STO 0	35 00
	RCL E	36 15
30	RCL C	36 13
	X ≠ Y?	16 -32
	GTO 3	22 03
	GSB c	23 16 13
	GSB b	23 16 12
35	CLX	-51
	STO E	35 15
	LBL 3	21 03
	RCL E	36 15
	1	01
40	+	-55
	STO I	35 46
	RCL 0	36 00
	RTN	24
	LBL 7	21 07
45	4	04
	STO I	35 46
	R↓	-31
	EEX	-23
49	8	08
50	/	-24
	GSB 5	23 05
	ENTER	-21
	INT	16 34
	STO 0	35 00
55	LBL 4	21 04
	X≠Y	-41
	FRAC	16 44
	EEX	-23
	2	02
60	x	-35
	GSB 5	23 05
	ENTER	-21
	INT	16 34
	EEX	-23
65	2	02
	STO x 0	35 -35 00
	R↓	-31
	STO + 0	35 -55 00
	DSZ I	16 25 46
70	GTO 4	22 04
	RCL 0	36 00
	RTN	24
	LBL 5	21 05
	2	02
75	6	06
	X > Y?	16 -34
	GTO 6	22 06
	-	-45
	RTN	24
80	LBL 6	21 06
	R↓	-31
	RTN	24
85		
90		
95		
100		

STEP	INSTRUCTIONS	INPUT DATA/UNITS	KEYS	OUTPUT DATA/UNITS
1	Enter no. of characters in key	n, $3 \leq n \leq 95$	A	k (see 2.)
2	Enter first k characters (2k digits)	digits	B	k
	of key, each character represented			
	by 2-digit code			
3	Repeat step 2 with next k digits			
	until key exhausted			
4a	ENCODE - Enter first 5 characters	digits	E	cypher
	(10 digits) of clear text			
	repeat 4a until clear message			
	exhausted (next 5, etc.)			
	- or -			
4b	DECODE - Enter first 5 characters	digits	D	clear
	(10 digits) of cypher text			
	repeat 4b until cypher message			
	exhausted (next 5, etc.)			
5	For new message, repeat from step 1			

Best to record card in FIX DSP 0 mode.

Registers all used

0 result	1 key -	2 - -	3 - - -	4 - - -
5 - -	6 - -	7 - -	8 - -	9 - -

0 - -	1 - -	2 - -	3 - - -	4 - - -
5 - -	6 - -	7 - -	8 - -	9 key

A 26..26	B chars last	C no. key bl.	D $10^{2(B)}$	E ctr.	I ctr.

Labels

A init.	B key	C	D decode	E encode
a	b used	c used	d	e used
0 used	1 used	2 used	3 used	4 used
5 used	6 used	7 used	8 used	9 used

00	A	13	N
01	B	14	O
02	C	15	P
03	D	16	Q
04	E	17	R
05	F	18	S
06	G	19	T
07	H	20	U
08	I	21	V
09	J	22	W
10	K	23	X
11	L	24	Y
12	M	25	Z

P/S

around two co