A MONOLITERAL-BILITERAL[-TRILITERAL] CIPHER

Monoliteral-biliteral[-triliteral] cipher

William Friedman mentions a *monoliteral-biliteral cipher* (and a *monoliteral-biliteral-triliteral cipher*) is some NSA training materials, but we were unable to find a description of the cipher. So we will develop our own. The cipher is a prefix-free code that uses letters as the ciphertext symbols.

There must be many ways to define a monoliteral-biliteral cipher, so what follows should not be taken to be definitive. We can fill a Polybius square with an alphabet that has been mixed with a keyword. We then label the rows and columns with nine different letters, leaving one row unlabeled.

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

A plaintext letter is encoded to the row label, if any, followed by the column label. So we can encode a message thus:

```
H  I  D  D  E  N  B Y A  C  O D  E
BI AE BE BE BF CG I H AH AI F BE BF
```

To hide the identities of the code words, remove the spaces:

```
BIAEBEBEBFCGIHAHAIFBEBF
```

One scheme for a monoliteral-biliteral-triliteral cipher is the following. Fill a 3×3×3 cube with a mixed alphabet and label the layers, rows, and columns thus:

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

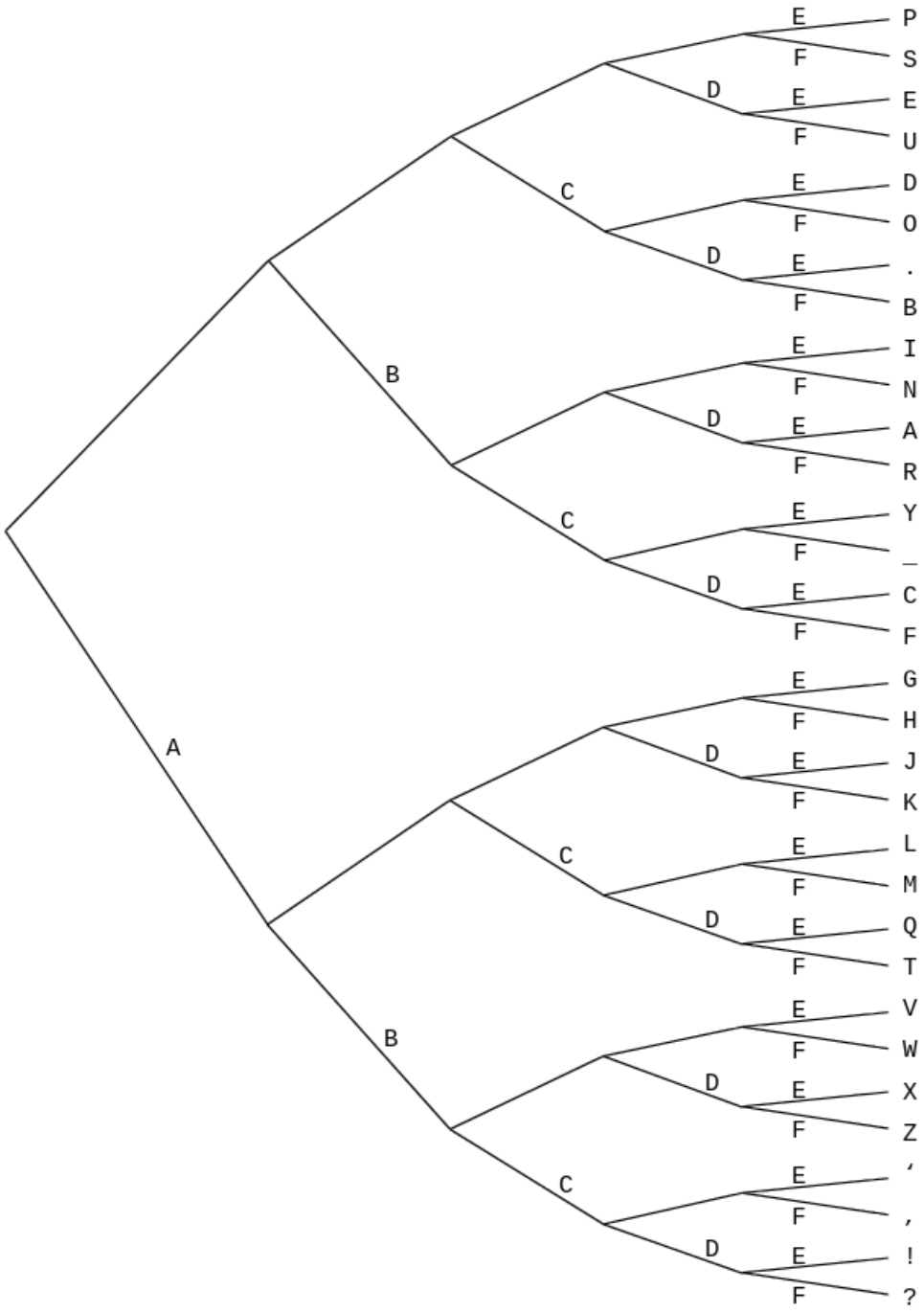
A plaintext character is encoded by a layer label, if any, followed by a row label, if any, followed by a column label. Notice that we include space as a letter.

```
H   I   D  D  E N  _  B  Y _  A  _  C  O  D  E
ACF ACG DE DE F BE DF AE G DF DG DF AF CF DE F
```

Remove the spaces between codewords:

```
ACFACGDEDEFBEDFAEGDFDGDFAFCFDEF
```

This one might be called a “1,2,3,4,5-letter code.”



H I D D E N ? _ B Y _ C O D E S !
AF BE CE CE DE BF ABDEF BDF CDF BCE BCF BCDE CF CE DE F ABCDE

AFBECECEDEBFABDEFBDFCDFBCEBCFBCDECFCEDEFABCDE