ADFGVX Cipher

The Germans used the ADFGVX cipher during World War I. Towards the end of the war, in 1918, they added a “V” to it. (Previously, it was the ADFGX ciher.) These notes will only cover this improved version of the cipher, which allows to encrypt the 26 letters as well as the 10 digits.

The secret key for the cipher is a 6 x 6 grid, where each row and column is labeled with the 6 letters in the cipher name: A, D, F, G, V, X. These letters were chosen because they are different from one another in Morse code, so that even if a slight error occurred in transmission, it’s likely that the error would be caught and could be corrected. Inside the table there are 36 slots, the 36 plaintext characters (letters and digits) would randomly be filled in these slots and this made up the key. Here is an example key:

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

To encrypt a message, first substitute each letter/digit with the two letter code corresponding to the row, then column of the location of the letter.

For example, if we were to start encrypting

```
IAM28YEARSOLDNOW
```

We’d have:

I	A	M	2	8	Y	E	A	R	S	O	L	D	N	O	W
FX	AX	XF	FV	FD	GX	DA	AX	FA	VD	AD	XX	VV	AV	AD	DF

This is the first, intermediate step. The next step is to pick another key word (so the secret key is two parts, both a 6 x 6 table AND a key word), and then create a grid with labeled with these letters. Let’s say our keyword is “KNIGHTS”. Then, copy the letters from the intermediate ciphertext above into the grid, row by row:

4	5	3	1	2	7	6
K	**N**	**I**	**G**	**H**	**T**	**S**
F	X	A	X	X	F	F
V	F	D	G	X	D	A
A	X	F	A	V	D	A
D	X	X	V	V	A	V
A	D	D	F			

Now, label the columns by the alphabetical order of the letters in the keyword. If the same letter appears more than once, then label these from left to right (another example will be shown shortly with this case). Then, sort the columns in this order:

1	2	3	4	5	6	7
G	**H**	**I**	**K**	**N**	**S**	**T**
X	X	A	F	X	F	F
G	X	D	V	F	A	D
A	V	F	A	X	A	D
V	V	X	D	X	V	A
F		D	A	D		

Finally, read the ciphertext letters in **COLUMN** first order, top to bottom down each column to get:

XGAVFXXVVADFXDFVADAXFXXDFAAVFDDA

Thus, this cipher is a compound cipher, where there are 2 keys that get applied with 2 different functions in sequence. In some sense, we can model this encryption as follows:

f(plain, key1) = y
g(y, key2) = ciphertext

Thus, the total encryption function looks like g(f(plain, key1), key2).

The first step is effectively a substitution while the second step is a transposition. This mirrors what Claude Shannon, known as the father of Information Theory said, that to obscure information, we have two main methods: confusion and diffusion.

Roughly speaking, confusion is what substitution does, replacing known symbols with different ones. This confuses. Then diffusion is the scientific term which means for the effects of one item to spread through the whole. Thus, in terms of cryptography, this means that the effect of one plaintext letter in a particular position should affect the ciphertext letter(s) **in a different position.**

All good modern ciphers use both confusion and diffusion, and this German cipher is the first example we've seen thus far, of mixing these two techniques. After modern day ciphers are examined, this cipher truly represents a bridge from the very old classical days to the beginning of encryption with computers.

So, the first step substitutes different symbols in place, while the second step moves around the letters quite a bit. Not only that, but both phases are relatively easy to carry out by hand. It's not to hard to see that one could get quite quick at encrypting in this manner by hand once they had some practice.

To decrypt, given the key, reverse the process. First, write down the keyword. Divide the ciphertext length by the keyword length. The ceiling of this value is the # of columns you need. Take the remainder of the division and this tells you how many of the columns are filled completely, unless the result is 0, in which case all columns are completely filled.

Then, start copying down the appropriate number of letters into the appropriate column. In our example, we have 32 ciphertext letters. Note that ceiling (32/7) = 5 and 32%7 = 4. So, the first four columns will have 5 letters and the last three columns will have 4 letters.

In our example, since the first letter alphabetically in the keyword is ‘G’, and ‘G’ is originally in position 4, and 4 ≤ 32%7, we will copy the first five letters of the ciphertext into the column for G:

XGAVFXXVVADFXDFVADAXFXXDFAAVFDDA

4	5	3	1	2	7	6
K	**N**	**I**	**G**	**H**	**T**	**S**
			X			
			G			
			A			
			V			
			F			

Since the second letter alphabetically in the keyword is ‘H’, and this is in position five, we’ll copy the next four letters of the ciphertext into this column:

XGAVFXXVVADFXDFVADAXFXXDFAAVFDDA

4	5	3	1	2	7	6
K	**N**	**I**	**G**	**H**	**T**	**S**
			X	X		
			G	X		
			A	V		
			V	V		
			F			

And so on, until the whole grid is filled:

4	5	3	1	2	7	6
K	**N**	**I**	**G**	**H**	**T**	**S**
F	X	A	X	X	F	F
V	F	D	G	X	D	A
A	X	F	A	V	D	A
D	X	X	V	V	A	V
A	D	D	F			

Then, we read the grid in row order, top to bottom, and left to right within the rows.

FX	AX	XF	FV	FD	GX	DA	AX	FA	VD	AD	XX	VV	AV	AD	DF

Then, finally, we use the 6 x 6 grid as a look up table (this part’s easier) to find each character substitution. When we see “FX”, we just go to row ‘F’ and column ‘X’ and reveal that the corresponding plaintext is the letter ‘I’, and continue in this manner.

Though the cryptanalysis of this cipher is beyond the scope of the class, some things to note are that when the keyword length is even, each column only consisted of letters taken from the top of the square grid or the left of the square. This positional information consisted of “mixed frequencies” of plaintext characters, and was exploited by Georges Paivin who broke the cipher. In order to gather enough information, he needed there to be high traffic, so that many statistical quantities tended to average out.

These notes are based on the following source:

https://en.wikipedia.org/wiki/ADFGVX_cipher