ADFGVX

Monday, September 14, 2020 11:36 AM

Confusion and Diffusion

Father of Information Theory - Claude Shannon
Defined a term called "entropy" for language.
If there are patterns in your text, then parts of the text are redundant and probably can be compressed. (Entropy is a measure of spread) For example, the English language has an entropy of only about maybe 2 bits per letter or something like that. (Effective meaning is that someone could come up with a code for a message and reduce the length of the message and still communicate the information…) Modern application of this idea - when you look at zip files, there are almost no patterns. And if you try to zip a zip file, it won't shrink any more!!!

In crypto, a good ciphertext has almost perfect entropy (not distinguishable from complete random bits…)

If you want to hide a message from some one, you can do it in two major ways:

1) Confusion - changing a symbol for another symbol
2) Diffusion - have one character in the plaintext affect a different position character in the ciphertext, potentially several of them.

EVERYTHING WE'VE SEEN SO FAR, COMES UNDER CATEGORY #1.

So, one of the big advancements from Playfair, involved using BOTH #1 and #2, and in fact, almost all modern day ciphers use a healthy dose of both techniques.

One of the most famous examples of something like Playfair that also uses diffusion is the cipher ADFGVX used by the Germans in World War I.

A multistep cipher

Step 1: Secret Key is a 6 x 6 grid with row and column labels ADFGVX.

	A	D	F	G	V	X
A	G	5	R	n0	U	3
D	W	B	F	7	K	D
F	M	V	letO	A	9	Y
G	S	Let I	X	L	H	J
V	6	N	C	P	Q	2
X	E	n1	Z	8	4	T

Plaintext: TODAYIS9142020AMONDAY

T = XX (row label, col label)
O = FF (row lable, col label)
D = DX (row label, col label)
A = FG
Y = FX
I = GD
S = GA
9 = FV
1 = XD
4 = XV
2 = VX
n0 = AG
2 = VX
n0 = AG
A = FG
M = FA
O = FF
N = VD
D = DX
A = FG
Y = FX

Phase 1 cipher: XXFFDXFG…

Phase 2:

There is a secret keyword, "FREEFOOD"

F	R	E	E	F	O	O	D
4	8	2	3	5	6	7	1
X	X	F	F	D	X	F	G
F	X	G	D	G	A	F	V
X	D	X	V	V	X	A	G
V	X	A	G	F	G	F	A
F	F	V	D	D	X	F	G
F	X						

Now, read the columns in the order that they are NUMBERED:

GVGAG (col 1)
FGXAV (col 2)
FDVGD (col 3)
XFXVFF (col 4)
DGVFD (col 5)
XAXGX (col 6)
FFAFF (col 7)
XXDXFX (col 8)

Note: The yellow characters are the effect of the first plaintext character, thus showing diffusion.

Ciphertext:
GVGAGFGXAVFDVGDXFXVFFDGVFDXAXGXFFAFFXXDXFX

Step 2 is essentially a transposition and this performs diffusion…a character's effect on the ciphertext is diffuse and affects different letter positions.

LEAVE AS AN EXERCISE FOR THE CLASS:

Given the square and the key word, decrypt a message that was encrypted using ADFGVX.