

# Bacon's Bilateral Cipher

Math 135, January 25

In 1623, Francis Bacon created a cipher system using the techniques of substitution and *steganography* - the art of writing hidden messages in such a way that no one apart from the sender and receiver know of its existence. We describe his system using binary notation (rather than the a-b notation he used).

**Binary representation of the Roman alphabet:** We give a table which translates each letter of the alphabet to 5 bit binary words.

Table 1: Binary alphabet

A	B	C	D	E	F	G	H	I
00000	00001	00010	00011	00100	00101	00110	00111	01000
J	K	L	M	N	O	P	Q	R
01001	01010	01011	01100	01101	01110	01111	10000	10001
S	T	U	V	W	X	Y	Z	
10010	10011	10100	10101	10110	10111	11000	11001	

**Variation of Font:** Fix the rule that if a letter has a 0 above it remains in normal font while a letter with a 1 above it will be in boldface. (Note: Bacon used a much more subtle difference in font. see Barr pg. 14).

**Encryption:** Now assume you want to encipher the 23 letter plain text:

BACON TAUGHT ME HOW TO THINK

1. Choose any block of text (call it the message text) which is at least 5 (the number of binary bits in our alphabet) times the length of the message:

$$23 \times 5 = 115.$$

We will choose the text of the Wikipedia entry for Phrenology:

*"Phrenology is a theory which claims to be able to determine character, personality traits, and criminality on the basis of the shape of the head."*

2. Rewrite the message text in blocks of five letters

Phren ology isath eoryw hichc laims tobea bleto  
deter minec harac ter,pe rsona lityt raitS, andcr  
imina lityo ntheb asiso fthes hapeo ftheh ead.

3. Translate our plaintext into binary code using table 1 so that

BACON TAUGHT ME HOW TO THINK

becomes

00001 00000 00010 01110 01101 10011 00000 10100  
00110 00111 10011 01100 00100 00111 01110 10110  
10011 01110 10011 00111 01000 01101 01010.

4. Now place each binary block over the corresponding block of message text.

00001 00000 00010 01110 01101 10011 00000 10100  
Phren ology isath eoryw hichc laims tobea bleto  
00110 00111 10011 01100 00100 00111 01110 10110  
deter minec harac ter,pe rsona lityt raitS, andcr  
10011 01110 10011 00111 01000 01101 01010.  
imina lityo ntheb asiso fthes hapeo ftheh ead.

Recalling our variation of font rule...0 is normal, 1 is boldface we then get

Phren**o**logy is a **t**heory which **c**laims to be **a**ble to dete **r**mine **c**haracter, personality  
**t**raits, and **c**riminality **o**n the **b**asis of the **s**hape of the **h**ead.