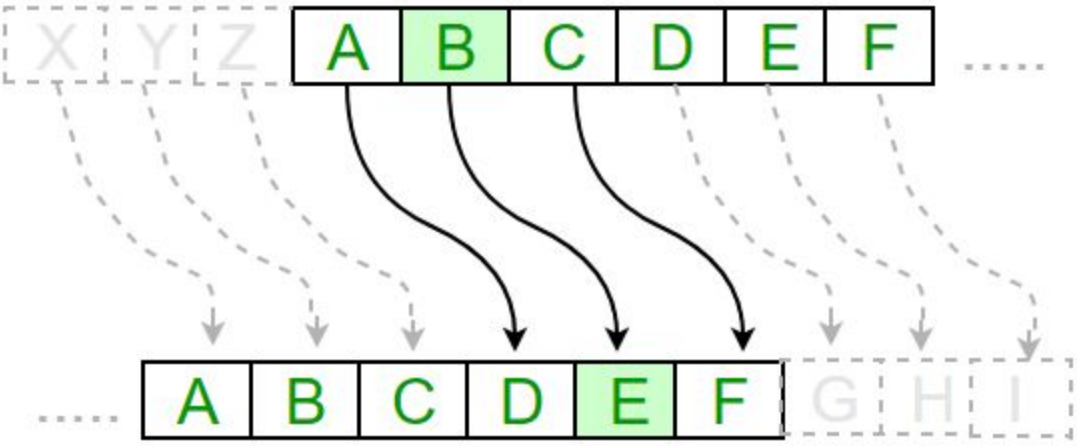
Codebusters Practice Packet

2019-2020

By definition from Google, a cipher is a secret way of writing; a code. This packet will define most of the ciphers required for the regional level (decryption only) as well as provide examples for each of these.

Caesar/Shift Cipher:

Decoding this ciphertext involves the recognition of a shift common to all of the letters in the alphabet. For example, A being D and C being F. This is recognized as a 3 shift.



https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/

1. Decode the following Bill Nye quote with a shift of 10.

XYDRSXQ SC DYY GYXNOBPEV DY LO DBEO, SP SD LO MYXCSCDOXD GSDR DRO VKGC YP XKDEBO.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

U	V	W	X	Y	Z

Aristocrat Cipher:

The aristocrat cipher is the classical substitution style cipher, using a K1 (plaintext alphabet contains a keyword), K2 (cipher alphabet contains a keyword), or a random alphabet (no keyword present in either). All aristocrat ciphers have spaces included. There are four possible aristocrat ciphers you will run into, with a hint (question two), without a hint (question three), with a hint and spelling/grammar errors (question 4), or with spelling/grammar errors and without a hint (question 5).

To decode these ciphers, it is important to be aware of the common occurrence of letters, generally speaking. Typically, the most used letter is E, then T, then A, then O, and so on. The following table expresses these frequencies.

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

https://www.researchgate.net/figure/Relative-Frequency-of-Letters-in-the-English-Language_fig2_325714929

2. Decode the following Bob Ross quote with a K1 alphabet. HINT: PAINT

IYYA FWYHTR. IYYA FV CLFV CJ LFUJ. MJFHVS QB JUJWSCLJWJ — SYH YTIS LFUJ VY IYYA VY BJJ QV.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

U	V	W	X	Y	Z

3. Decode the following The Rock quote.

YS DWAYXS, YS DWRUYB, HRC HXLHBO YS EDS DHYCSOE LZYMSY QR EDS YZZA.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

U	V	W	X	Y	Z

4. Decode the following Will Smith quote with a K1 alphabet. HINT: ALIENS

HOXLU SOWXMDXQ XM DGO AIMD QIAAOL ETDG DI AOBXIQSXDV.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

U	V	W	X	Y	Z

5. Decode the following Gordon Ramsay quote.

LXRW YGHZ RW WJ TPUFCBJJQFP, RL'W SJYJORUI HGCD LJ WBXJJY!

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

U	V	W	X	Y	Z

Patristocrat Cipher:

Patristocrat ciphers are very similar to that of the Aristocrat, but they key difference between the two is the fact that the Patristocrat groups the letters into something that looks like a 5 letter word. Essentially, these spaces in the ciphertext mean nothing in relation to the actual sentence that has been encoded.

There are two different potential Patristocrat ciphertexts that you may have to decode: with a hint (6) and without a hint (7).

6. Decode the following Hailee Steinfeld quote using a K1 alphabet. HINT: STARVING.

GJBRR AZJQS RZEGA EBANR ECAGJ Z'QFEX JQSRY NQXQP ECR.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

U	V	W	X	Y	Z

7. Decode the following Danny DeVito Quote.

MKBCZ' FKGKZ DZCMW HMK'YK WZFEW PYCCN. MKOCS QBTKW ZJFSY FQK'PB YKJNW ZCSFK YPXJO K.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

U	V	W	X	Y	Z

Affine Cipher:

The Affine cipher involves a 4 step process. To explain, every letter of the alphabet can be linked to a number: A is 0, B is 1, C is 2, and so on. So, let's say we had ciphertext that said:

CRAAPO IAVXOB

These letters correspond with the numbers provided:

C	R	R	A	P	O		I	A	V	X	O	B
2	17	17	0	15	14		8	0	21	23	14	1

You can use these numbers with the provided a and b values (THEY WILL ALWAYS BE PROVIDED) to solve the rest of the cipher. For this example, a=3 and b=2.

Ciphertext	C	R	R	A	P	O		I	A	V	X	O	B
y	2	17	17	0	15	14		8	0	21	23	14	1
9(y-2)	0	135	135	-18	117	108		54	-18	171	189	108	-9
9(y-2)mod26	0	5	5	8	13	4		2	8	15	7	4	17
Plaintext	A	F	F	I	N	E		C	I	P	H	E	R

c(y-b) c(y-b)mod26

Now hold on a second, where did that 9 come from??

To decode an affine cipher, you must solve the formula ac=1mod26. Essentially you want to find the value multiplied by your a value that will give you 1 when modified to the 26 scale.

Mod26 means to take whatever numerical value that you have and either add or subtract values until you reach a number from 0-25.

In this case, you multiply 3x9 to get 1mod26, so 9 is your c value.

7. Solve the following Affine cipher with a=5 and b=8.

Ciphertext	I	L	L		W	U		O	C	L	L
y											
Plaintext											

Vigenére Cipher

The Vigenére cipher involves the use of a key and the given table:

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

https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Base.html

Let's say your ciphertext was MMNRAP and the key was KEY.

Find K on the top of the table, and follow down until you see the first letter of the ciphertext, M. When you see M, trace it to the far left column, you should see C. Then, find E on the top of the table and trace down to the second letter, M. Trace this to the left hand column, you will see I. Do this for all of the letters, repeating the key KEY, and you will get plaintext of CIPHER.

8. Decode this Vigénere cipher using key=NICE.

VZQR ZIP HVMV

Baconian Cipher:

The decryption of the baconian cipher involves the use of the following table:

A = aaaaa	I/J = abaaa	R = baaaa
B = aaaab	K = abaab	S = baaab
C = aaaba	L = ababa	T = baaba
D = aaabb	M = ababb	U/V = baabb
E = aabaa	N = abbaa	W = babaa
F = aabab	O = abbab	X = babab
G = aabba	P = abbba	Y = babba
H = aabbb	Q = abbbb	Z = babbb

Typically, this cipher will be given in a mass of as and bs, so you will have to divide the as and bs into groups of 5. For example, aaaaabaaab would be separated into aaaaa baaab, which translates to A S.

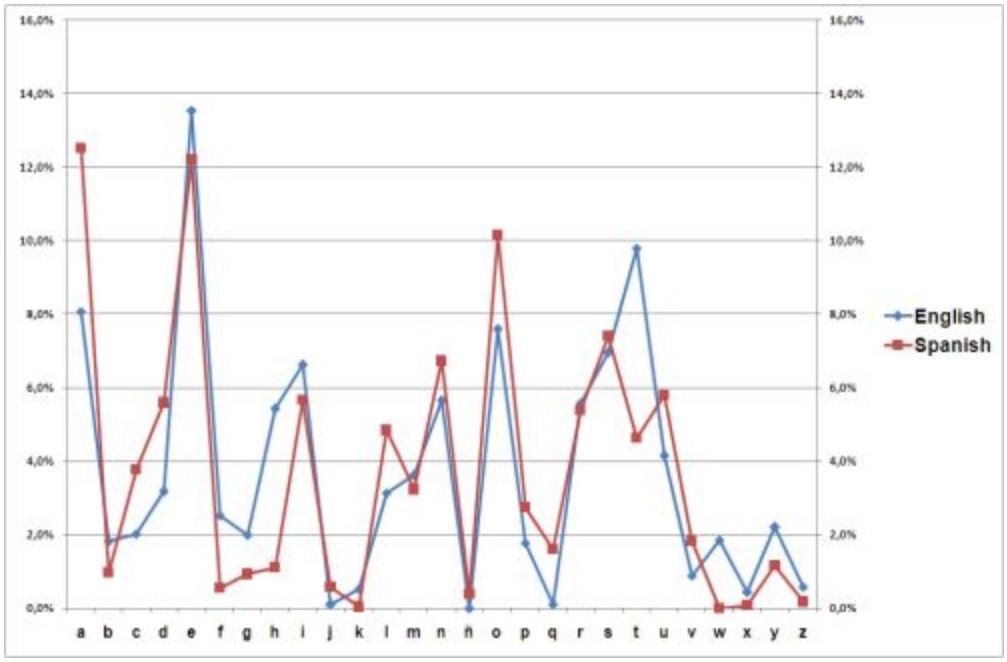
9. Decode the following Baconian cipher.

baabaaabbbaabaaaabaaaabbaaabbaaaabaaaaaaabbabbaabaaaababababaaabaaaaba

aabbaaba

Xenocrypt Cipher:

The Xenocrypt cipher is essentially the aristocrat cipher, but in another language. This is Spanish every time. At the regional level, there are up to one of these allowed, but it is important to understand it. The following links show the most common words in the Spanish language and the alphabet frequencies of the Spanish language:
https://spanishforyourjob.com/commonwords/



https://theblogbyjavier.com/2010/09/21/most-common-letters-in-english-and-spanish-are/

10. Decode this Xenocrypt which is a quote by Sir Isaac Newton in Spanish.

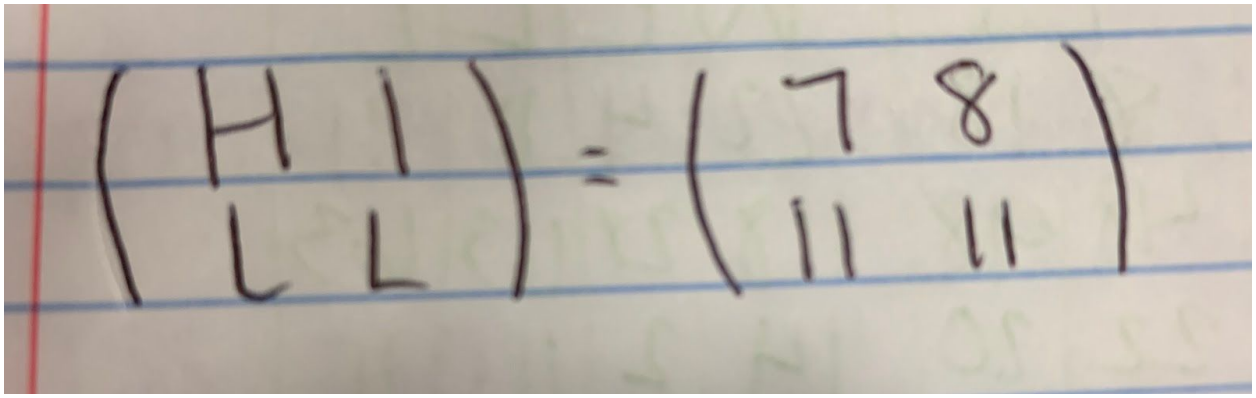
IFNBRI BOPI JLHSRCOFWFLIVN HL UFEN HFI RIP PRJPE HRZNHFSFNI.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

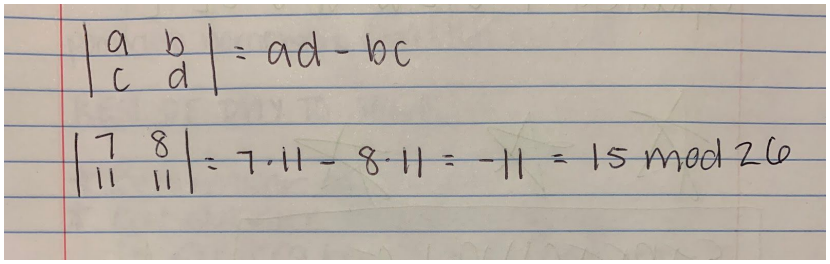
U	V	W	X	Y	Z

Hill Cipher (2x2 Matrix):

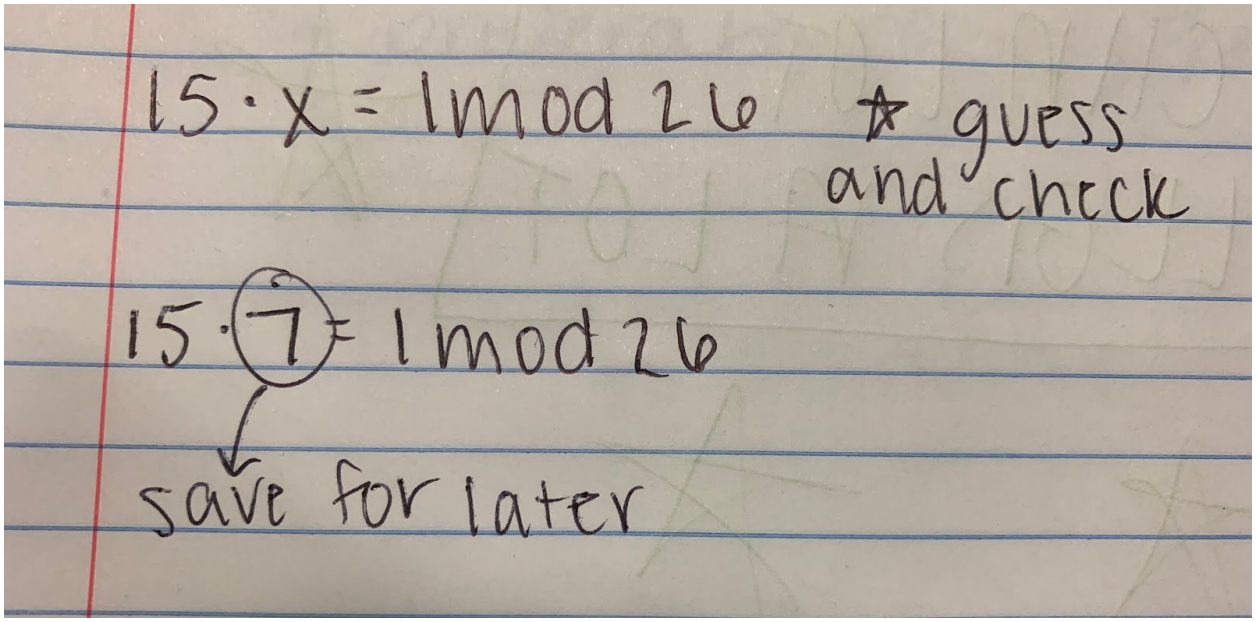
The decryption of a hill cipher involves the use of a key and the ciphertext. For the sake of explaining, say we have a ciphertext SVKUEPWBQI and key HILL. We can divide that key into the following matrix:



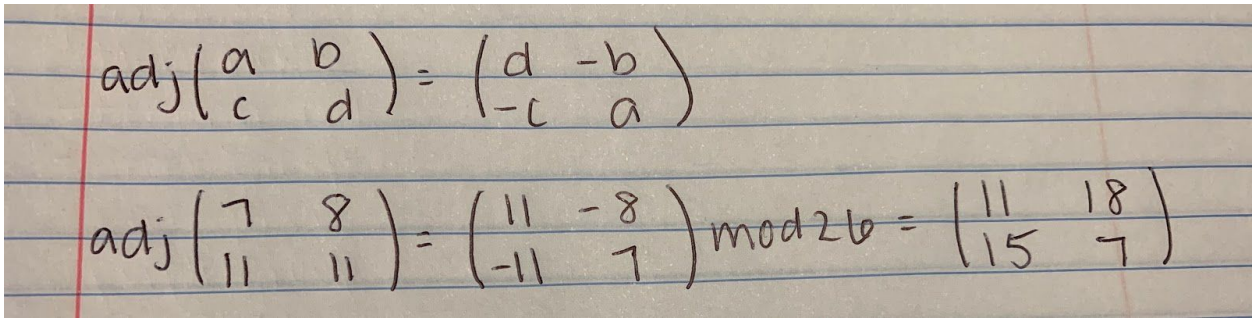
The first step is to find the multiplicative inverse of this determinant, which is done by first finding the determinant:



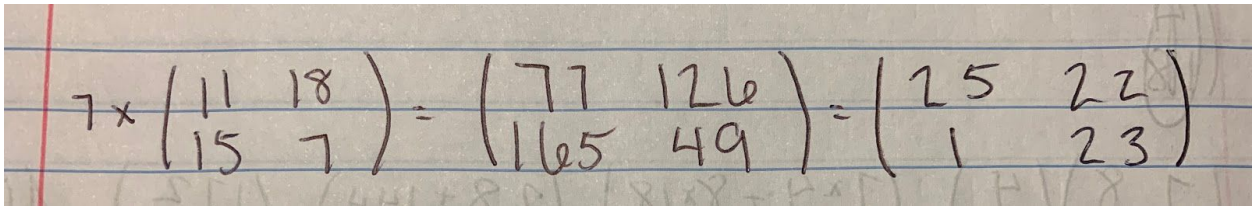
Then, we need to find the inverse of the determinant mod26:



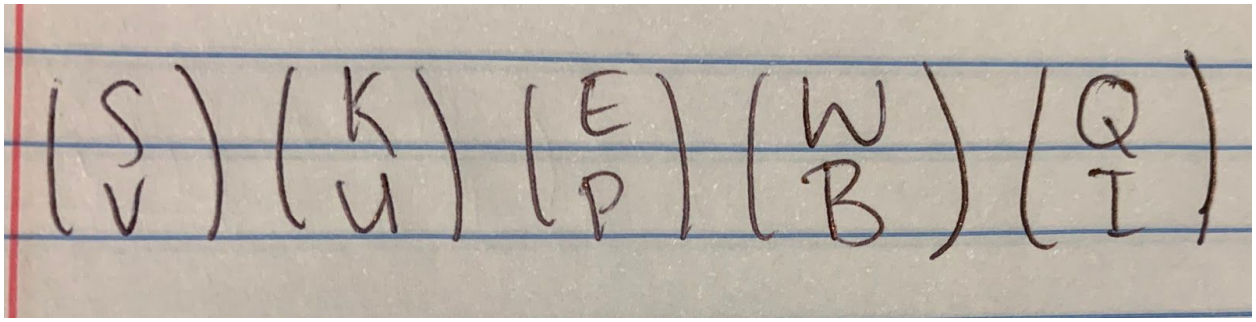
Then, find the adjugate matrix of the original matrix:



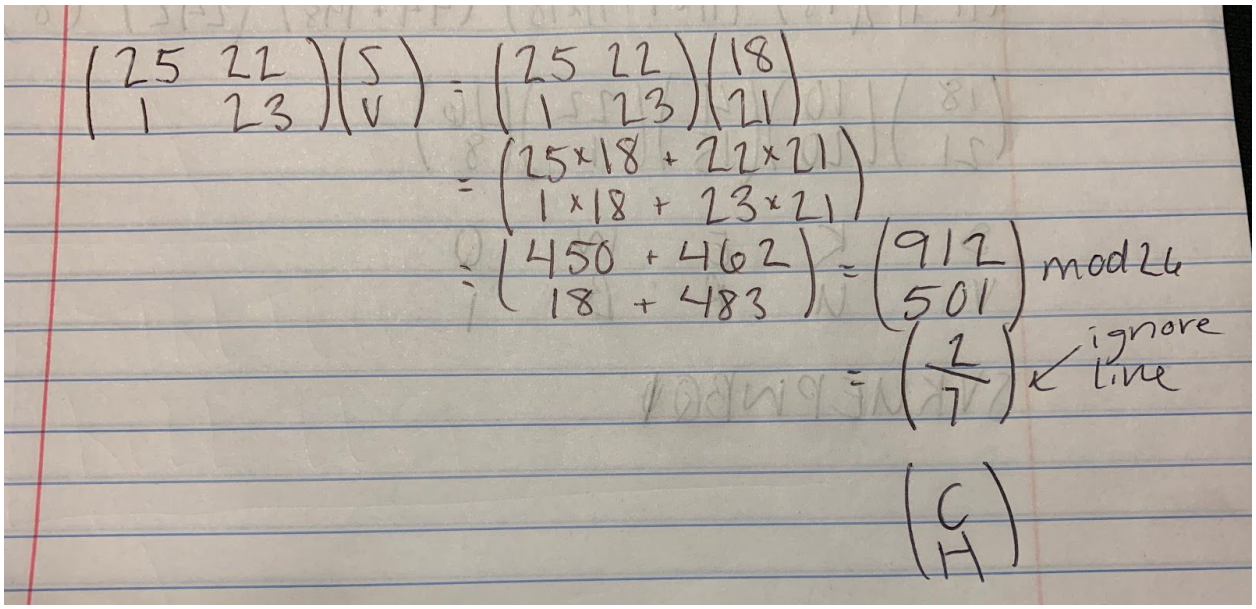
Multiply the adjugate by the numerical value of inverse determinant mod26 (7 in this case) (SOLUTION):



Then, divide the original cipher into a series of matricies:



Multiply the first matrix by the (SOLUTION) matrix:



Then repeat for the rest of the terms, you should get CHOCOLATES.

11. Decode the following Hill cipher using Key= HAIR

HIPXCJWDUD

ANSWER KEY:

1. “Nothing is too wonderful to be true, if it be consistent with the laws of nature.”
2. “Look around. Look at what we have. Beauty is everywhere — you only have to look to see it.”
3. “Be humble, be hungry, and always be the hardest worker in the room.”
4. “Being relistic is the most commen path to mediocrity.”
5. “This lamb is so udnercooked, it’s folowing Mary to school!”
6. “It needs to be said and heard: it’s okay to be who you are.”
7. All is well
8. Iron man dies
9. The egg came first
10. Ningun gran descubrimiento se hizo sin una audaz suposicion.
11. Barbershop