Codebusters Event Meeting Two

Affine, Vigenere, and Hill

Math Ciphers

Affine, Vigenere, and Hill are all math ciphers; here's how to deal with those:

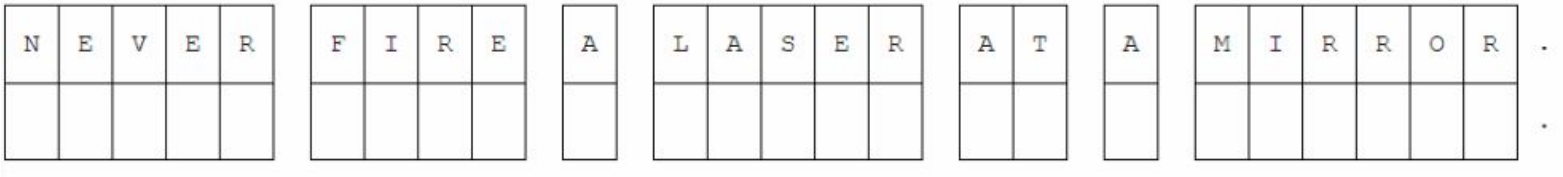
- For all math ciphers, letters **A-Z will be represented by numbers 0-25**.
  - Example: A is represented by zero, B by one, C by two, etc.
  - All of these conversions will be on your reference sheet. However, it's more time efficient to just memorize all the conversions yourself; with practice, it'll become effortless.
- Another **important thing to get fast at is mod 26**. Basically, you'll divide big numbers by 26, and your answer is whatever the remainder is; this is less than 26 and can be converted to a letter.
  - You could also keep subtracting 26 until you get a number less than 26.
  - Example: 265 (mod 26) = remainder of 265 ÷ 26 = 5 = letter F.
  - Here's a **handy-dandy Quizlet** for letter-to-number conversions and multiples of 26, which will help with mod 26: https://quizlet.com/_9djqss?x=1jqt&i=1hf66q.
- You **will be allowed calculators** on all Codebusters tests, but it's probably most time efficient to do mental math whenever possible, especially for Vigenere.

Affine

Uses y = ax + b to encode messages and uses the inverse of y = ax + b to decode messages. x is the number corresponding to the letter you're encoding; a and b are given.

Encoding Affine

5) **[100 points]** Encode this sage advice from Larry Niven using the Affine Cipher with ***a*=7** and ***b*=6**.



1. **Convert the letter** you're encoding to a number.
    a. N is thirteen, E is four, V is twenty-one, R is seventeen, etc.
2. **Find the encryption function** by plugging given a and b values into y = ax + b.
    a. Our encryption function for this question is y = 7x + 6.
3. **Plug all the numbers you're encoding into your function** as x; solve for y.
    a. For N, we would plug in thirteen; y = 7x + 6 = 7(13) + 6 = 97.
4. If your answer for y is larger than 26, **make sure to mod 26**.
    a. 97 ÷ 26 = 3 remainder 19 OR 97 - (26 × 3) = 97 - 78 = 19.
5. Convert the mod 26 answers **back to letters** to get your final answer.
    a. Nineteen converts back to T; all N's in this quote will encode to T.

Inverse

When using modulus, instead of dividing, we multiply by a multiplicative inverse. Multiplying a number by its multiplicative inverse then mod 26 equals one.

1	3	5	7	9	11	15	17	19	21	23	25
1	9	21	15	3	19	7	23	11	5	17	25

Decoding Affine

5) **[100 points]** Solve this quote by Seymoure Cray about what tools he used to design the Cray I supercomputer which has been encoded using the Affine Cipher where ***a*=7** and ***b*=7**.

I	J	U	V	L	G	D

H	U	C

P	R	H	C	W	L	G	G	J

I	H	C	D

1. **Rearrange** y = 7x + 7 (mod 26) in terms of x.
    a. Subtract seven on both sides to get 7x = y - 7 (mod 26).
    b. Now, instead of dividing by seven, multiply by seven's multiplicative inverse of 15 on both sides of the equation to get x = 15y - 105 (mod 26).
    c. Mod 26 to get x = 15y - 1 OR x = 15y + 25 as your function's inverse.
2. Now that you have your function of x = 15y - 1, you can **plug and chug to solve**!
    a. I corresponds to the number eight.
    b. x = 15y - 1 = 15(8) - 1 = 120 - 1 = 119.
    c. 119 (mod 26) = 15 = the letter P.
    d. Rinse and repeat! Keep in mind that you don't need to solve every letter.

The Less Math Strategy

5) **[100 points]** Solve this quote by Seymoure Cray about what tools he used to design the Cray I supercomputer which has been encoded using the Affine Cipher where ***a*=7** and ***b*=7**.

I	J	U	V	L	G	D		H	U	C		P	R	H	C	W	L	G	G	J		I	H	C	D

A	B	C	D	E	F	G	H
Z	O	D	S	H	W		

1. Once again, we know our function is **x = 15y + 25**.
2. Since A corresponds to number zero, the decoded version of A must just be whatever your b value is; in this case, **twenty-five or letter Z**.
3. Now just keep adding your a value to determine what the next letters decode to.
    a. In this case we add our a value of fifteen to Z or twenty-five to get forty; mod 26 to get fourteen or **letter O**.

Vigenere

Start with plaintext and repeatedly add a given keyword to encode. To decode, start with the ciphertext and repeatedly subtract the given keyword.

Encoding Vigenere

7) **[0 points]** Encode this quote by A. A. Milne using a keyword of LAZY.

P	E	O	P	L	E		S	A	Y		N	O	T	H	I	N	G		I	S		I	M	P	O	S	S	I	B	L	E	,		B	U	T		I
																																		,						

D	O		N	O	T	H	I	N	G		E	V	E	R	Y		D	A	Y	.
																				.

Encoding Vigenere

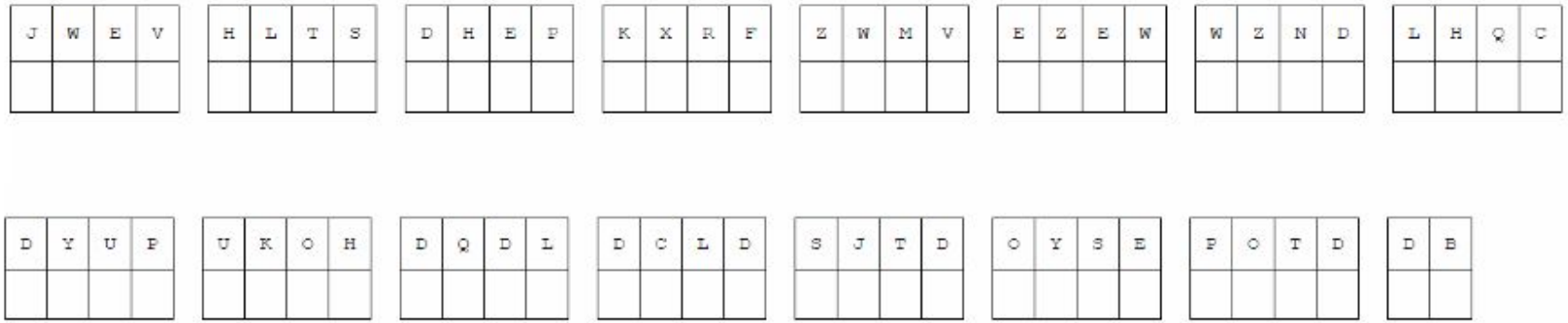
P	E	O	P	L	E
L	A	Z	Y	L	A
11	0	25	24	11	0

S	A	Y
Z	Y	L
25	24	11

1. Convert the **plaintext** to numbers.
    a. P is fifteen, E is four, O is fourteen, etc.
2. Convert the **keyword** to numbers as well.
    a. LAZY becomes eleven, zero, twenty-five, and twenty-four.
3. **Write the keyword repeatedly** under each letter/number of the plaintext.
    a. L corresponds to P, A to E, Z to O, etc.
4. **Add the two** corresponding numbers, then mod 26 to convert back to letters.
    a. P = 15 plus L = 11 equals 26, etc.
    b. 26 (mod 26) = 0 = the letter A.

Decoding Vigenere

4) **[120 points]** The following quote by Chuck Palahniuk has been encoded with the Vigenère Cipher using a keyword of **LIKED**. What does it say?



(Literally the same process except you **subtract the keyword's numbers** instead of adding them...let's try this one together!)

Answer

“You realize that our mistrust of the future makes it hard to give up the past.” (Charles Palahniuk)

Hill

To encode, multiply the plaintext in matrix form by a 2 × 2 key. To decode, multiply plaintext letter matrices by the inverse matrix of the key.

How To Matrix

$$AB = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix}$$

1. This is a **matrix**! It's a rectangular array of numbers in rows and columns. Matrices have a wide variety of applications in algebra, physics, engineering, etc.
2. To multiply matrices, we find the **dot product** of every pair of row and column.
    a. A dot product is when we multiply matching members then sum them up.
    b. We need to find the dot product of the first row in the first matrix with the first column in the second matrix, then with the second column, etc.

$$A = \begin{bmatrix} 3 & 4 \\ 5 & 6 \end{bmatrix} \text{ and } B = \begin{bmatrix} -1 & 0 \\ 4 & 7 \end{bmatrix} \qquad AB = \begin{bmatrix} 3(-1)+4(4) & 3(0)+4(7) \\ 5(-1)+6(4) & 5(0)+6(7) \end{bmatrix} = \begin{bmatrix} 13 & 28 \\ 19 & 42 \end{bmatrix}$$

Encoding Hill

[75 Points] Using a key of **TURN** encode the string **JUXTAPOSING** using the **Hill** Cipher with a 26 character alphabet. e.g.

$$\begin{pmatrix} T & U \\ R & N \end{pmatrix} \equiv \begin{pmatrix} 19 & 20 \\ 17 & 13 \end{pmatrix}$$

*** They don't always give you the matrix so make sure you know how to create it

J	U	X	T	A	P	O	S	I	N	G	

← If there are an odd # of letters, use Z to make the plaintext even

1. Group the plaintext into **2 × 1 matrices**. Use Z as a filler if you have an odd number.
   a. Our first letter matrix would be [J, U] vertically, then [X, T], etc. until [G, Z].
2. Multiply each letter matrix by the **key matrix**.
3. Mod 26 and convert the numbers back to letters to get your **ciphertext**.
   a.

Multiply by the key

19 20	x	9	=	19 * 9 + 20 * 20	=	571	mod 26 =	25 (Z)
17 13	x	20		17 * 9 + 13 * 20		413		23 (X)

Inverse Matrix

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = (ad - bc)$$

Adjugate of a 2 x 2 Matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

1. Like with Affine, we can't divide matrices; we must **multiply by the inverse**.
2. First, find the **adjugate matrix** of the given key by switching terms a and d and using the opposites of terms b and c.
3. Next, find the matrix's **determinant** using the formula (ad - bc).
4. Multiply the **multiplicative inverse** of the determinate by the adjugate matrix.
    a. When multiplying a matrix by one number, simply distribute.

Decoding Hill

24) **[200 points]** Decode this quote by Nelson Mandela which has been encoded using a Hill Cipher with a keyword of **HINT**. Reme

$$\begin{pmatrix} H & I \\ N & T \end{pmatrix} \equiv \begin{pmatrix} 7 & 8 \\ 13 & 19 \end{pmatrix}$$

$$\begin{vmatrix} E \\ A \end{vmatrix} = \begin{vmatrix} 4 \\ 0 \end{vmatrix}$$

E	A	C	X	D	L	O	A	X	K	M	W	V	T	B	H	A	E	Y	Q	R	U

1. Find the **inverse of the key** by multiplying the adjugate matrix by the multiplicative inverse of the determinant.
2. Multiply the resulting matrix by each of the **letter matrices**.
   a.

Adjugate Matrix	Determinant	Multiply Multiplicative Inverse of the Determinant and the Adjugate Matrix	Multiply by letter matrices
$\begin{vmatrix} 7 & 8 \\ 13 & 19 \end{vmatrix} \rightarrow \begin{vmatrix} 19 & -8 \\ -13 & 7 \end{vmatrix}$	a*d - b*c 7 * 19 - 8 * 13 mod 26 = 3 Multiplicative Inverse 3 * **9** mod 26 = 1	$\begin{vmatrix} 19 & -8 \\ -13 & 7 \end{vmatrix} * 9 \mod 26 = \begin{vmatrix} 15 & 6 \\ 13 & 11 \end{vmatrix}$	$\begin{vmatrix} 15 & 6 \\ 13 & 11 \end{vmatrix} * \begin{vmatrix} 4 \\ 0 \end{vmatrix} = \begin{vmatrix} 15*4 + 6*0 \\ 13*4 + 11*0 \end{vmatrix} = \begin{vmatrix} 60 \\ 52 \end{vmatrix} = \begin{vmatrix} I \\ A \end{vmatrix}$ $\begin{vmatrix} 15 & 6 \\ 13 & 11 \end{vmatrix} * \begin{vmatrix} 2 \\ 23 \end{vmatrix} = \begin{vmatrix} 15*2 + 6*23 \\ 13*2 + 11*23 \end{vmatrix} = \begin{vmatrix} 168 \\ 279 \end{vmatrix} = \begin{vmatrix} M \\ T \end{vmatrix}$

Quick Quiz

Make sure to finish this by our next meeting!

Thanks

Any questions, comments, concerns?

michelle.li44@masonohioschools.com
or Michelle Li on Slack

CREDITS: This presentation template was created by **Slidesgo,** including icons by **Flaticon** and infographics & images by **Freepik**.