

Nicole Barker

CyberPDX 2016

Lesson Plan

Cryptology in an Algebra 2 Classroom

LESSON OBJECTIVES:

- link coding to exponential growth functions and geometric sequences
- compute decimal values of hexadecimal characters
- decrypt a message given in hexadecimal
- use simple substitution cipher
- decode the punchline to a joke using the Vigenere cipher

LESSON:

- 1) Warm up puzzle (see attached)
Students will be given a baggie of puzzle pieces that complete missing terms in sequences, or match explicit formulas to given sequences.
- 2) Introduce binary system comparing it to a simple geometric sequence (1, 2, 4, 8, 16, ...)
explicit formula gives $t(n) = 1(2)^{n-1}$
- 3) Show examples of how to convert to binary system.
- 4) Continue the talk of exponential growth, and introduce the hexadecimal system.
- 5) Show examples of how to convert to hexadecimal.
- 6) Have students decode a message in hexadecimal to decimal.
- 7) Students will write a short message to be decoded by a partner using either binary or hexadecimal.
- 8) Introduce substitution cipher and provide examples.
- 9) Show students how to use a key to decrypt a message given using the Vigenere cipher.
- 10) Exit ticket: To find the punchline to this joke, "What is a chickens least favorite day?"
Decrypt using a simple substitution cipher:

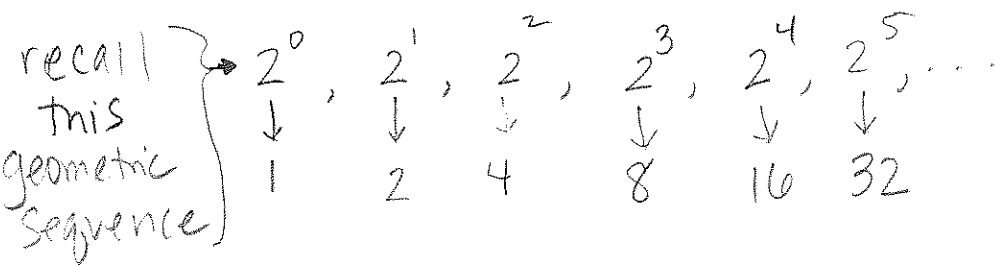
cyp tpd cf hpufhp gw wgutf (the key to decode is sicko)

Using the Vigenere cipher, and the key 'sicko' the punchline is:

XZKNOQ (Friday)

Examples:

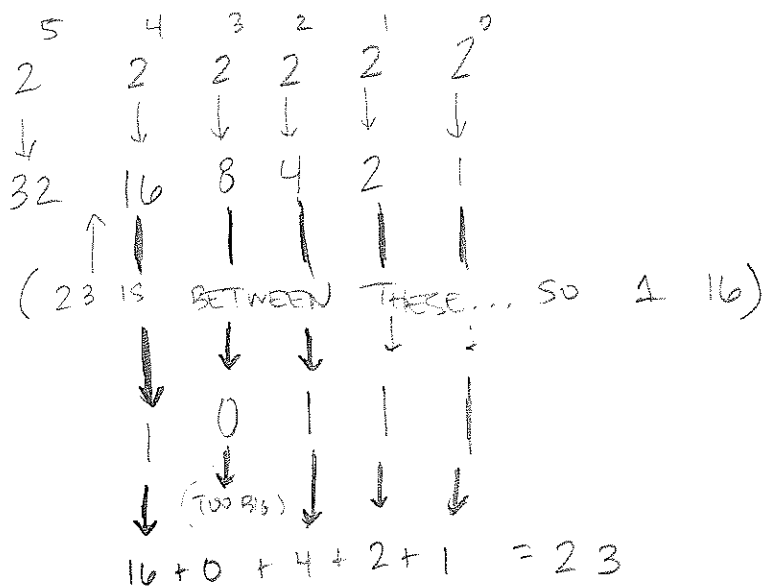
Converting to binary-



so, how would we convert 23 to binary?

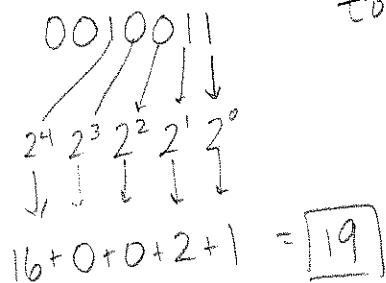
reverse the order of the sequence

$$\begin{array}{r} 23 \\ -16 \\ \hline 7 \end{array}$$



How about converting

to decimal?

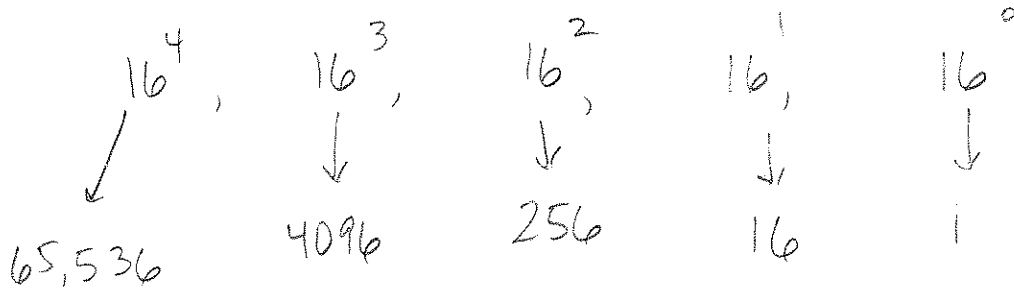


Try converting 10011 to decimal.....

Examples:

Converting to hexadecimal-

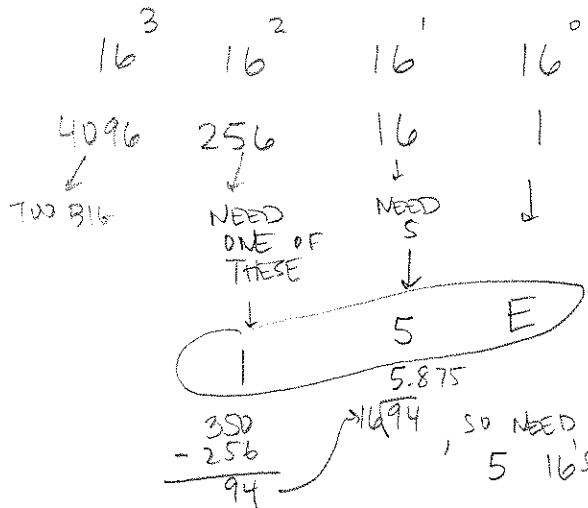
Very similar to binary, only the base is now 16...



since we have 10 digits in base 10, 16 are needed...

						10	11	12	13	14	15				
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

ex: Let's convert 350 into hexadecimal. 6 additional digits...



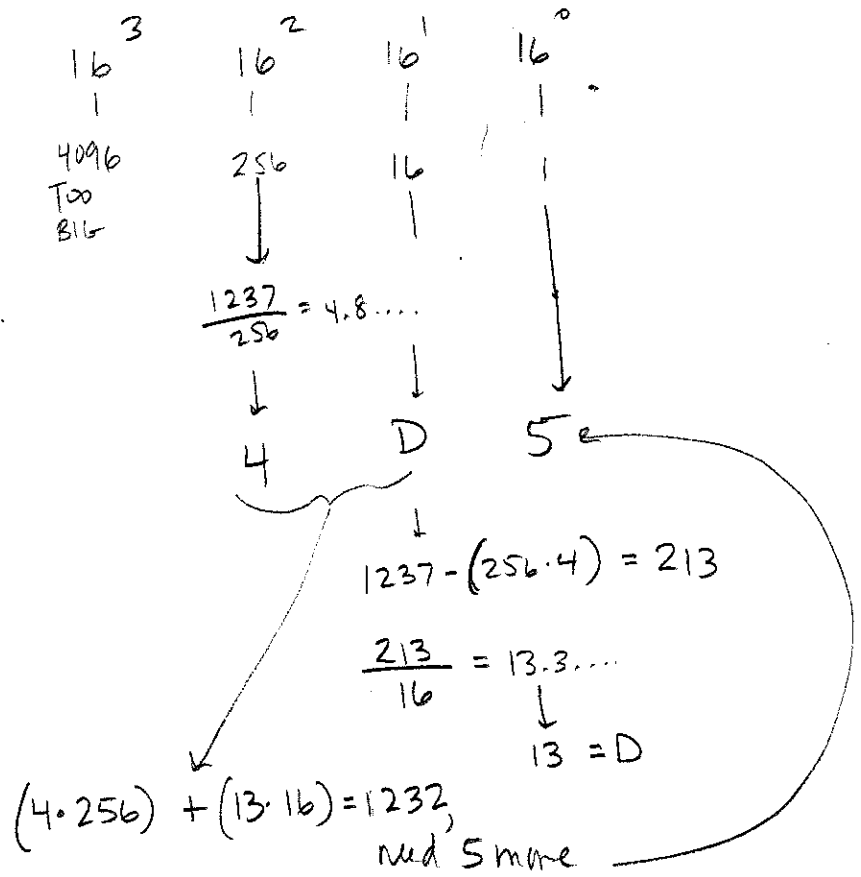
$$\begin{array}{r}
 350 \\
 - 256 \\
 \hline
 94
 \end{array}$$

$$\begin{array}{r}
 350 \\
 - 336 \\
 \hline
 14 = E
 \end{array}$$

So 350 = 15E

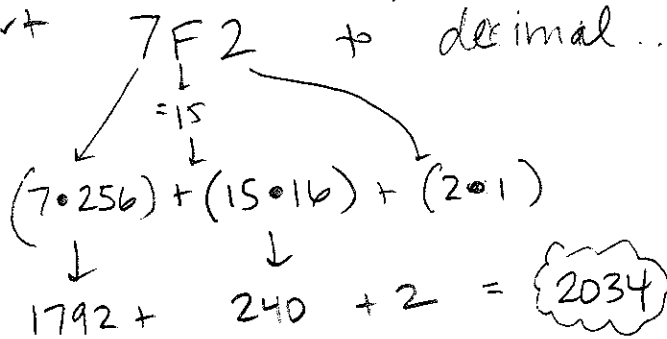


ex: convert 1237 to hexi....



SO $1237 = 4D5$ in hexi

ex: convert 7F2 to decimal...



Examples:

Using a simple substitution cipher-

EACH LETTER IS MATCHED TO A NEW LETTER...
(COULD BE UP BY ONE) TOTAL JUMBLE, ETC.)

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

SO

" I	LOVE	" YOU "	WOULD BE ...
↓	↓↓↓↓	↓↓↓	
" C	ZBLJ	PBY "	

- LOOK FOR HIGH FREQUENCY LETTERS
(SUCH AS... ?? ASK KIDS TO GENERATE A LIST)
- ONE LETTER WORDS "I" "A"
- "THE"

Examples:

Using the Vigenere cipher-

NEED A KEY ...

EX: THE KEY TO DECODE IS "TIGER"

T - L - S

I - O - A

G - T - N

E - X - T

R - R - A

T - V - C

I - T - L

G - G - A

E - Y - U

R - J - S

DECODE: LOTXRVTGYJ

TRY TO DECODE (USING TIGER AS THE KEY...)

UIXOVK

	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