Loads of Codes – Cryptography Activities for the Classroom

Paul Kelley
Anoka High School
Anoka, Minnesota

In the next 90 minutes,
we'll look at cryptosystems:

Caesar cipher
St. Cyr cipher

Tie-ins with algebra

Frequency distribution

Vigenere cipher

Cryptosystem – an algorithm (or series of algorithms) needed to implement encryption and decryption.

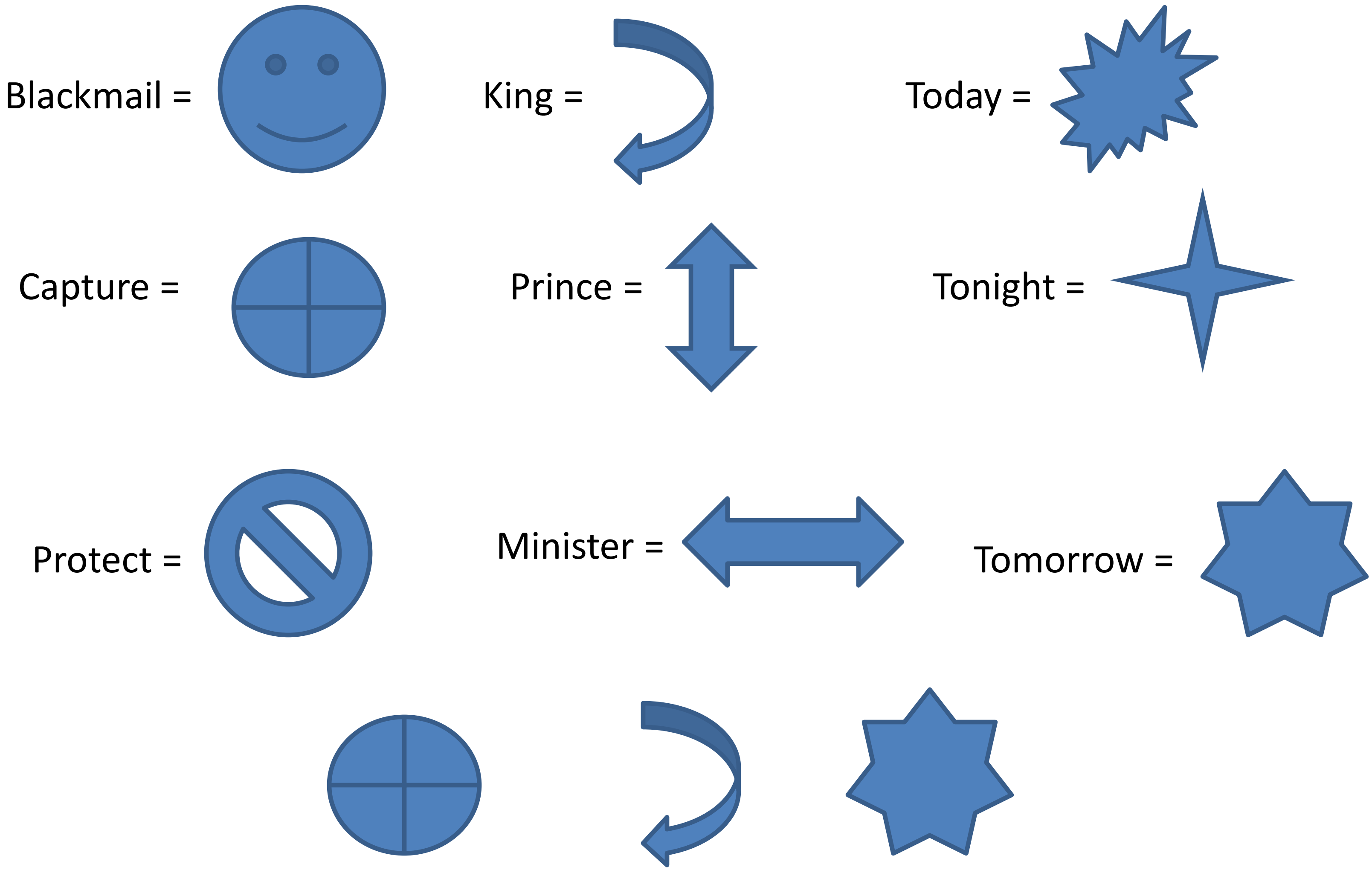
For our purposes, the words encrypt and encipher will be used interchangeably, as will decrypt and decipher.

The idea behind all this is that you want some message to get somewhere in a secure fashion, without being intercepted by "the bad guys."

Code – a substitution at the level of words or phrases

Cipher – a substitution at the level of letters or symbols

However, I think “Loads of Codes” sounds much cooler than “Loads of Ciphers.”



Capture King Tomorrow

Plaintext: the letter before encryption

Ciphertext: the letter after encryption

Rail Fence Cipher – an example of a “transposition cipher,” one which doesn’t change any letters when enciphered.

Example: Encipher “DO NOT DELAY IN ESCAPING,” using a rail fence cipher.

You would send:

DNTEAIECPN OODLYNSAIG

Null cipher – not the entire message is meaningful.

My aunt is not supposed to read every epistle tonight.

BXMT SSESSBW POE ILTWQS
RIA QBTNMAAD OPMNIKQT
RMI MNDLJ ALNN BRIGH
PIG ORHD LLTYQ

BXMT SSESSBW POE ILTWQS

RIA QBTNMAAD OPMNIKQT

RMI MNDLJ ALNN BRIGH

PIG ORHD LLTYQ

Anagram – use the letters of one word, phrase or sentence to form a different one.

Example: “Meet behind the castle”

becomes “These belched a mitten.”

Substitution cipher –
one in which the letters
change during encryption.

The oldest known is the Caesar cipher, in which letters are shifted three places in the alphabet.

Now is a good time to look at the envelopes, and a good time to explain the packets.

Encipher these messages using a Caesar cipher:

1. ABBI IS INCREDIBLY AWESOME.

   DEEL LV LQFUHGLEOB DZHVRPH

2. I LOVE COLLEGE ALGEBRA.

   L ORYH FROOHJH DOJHEUD

3. WE ARE THE ANOKA FAMILY.

   ZH DUH WKH DQRND IDPLOB

4. WINTER IS SUPER COLD.

   ZLQWHU LV VXSHU FROG

5. SENIORS ROCK MY SOCKS.

   VHQLRUV URFN PB VRFNV

Decipher these messages using a Caesar cipher:

1. FDFLH FDUUROO HQMRBV PDWK

   CACIE CARROLL ENJOYS MATH

2. VXEZDB VDQGZLFKHV DUH WDVWB

   SUBWAY SANDWICHES ARE TASTY

3. PLQQHVRWD JRSKHUV

   MINNESOTA GOPHERS

4. FKRFRODWH PDNHV WKH ZRUOG JR URXQG

   CHOCOLATE MAKES THE WORLD GO ROUND

5. IXCCB VZHDWHUV NHHS BRX ZDUP

   FUZZY SWEATERS KEEP YOU WARM

St. Cyr slide –
similar to a Caesar shift,
but the shift could be
any number of letters.

Encipher these messages using a St. Cyr slide:

1. HAPPY HOLIDAYS EVERYBODY (‘k’)

   RKZZI RYVSNKIC OFOBILYNI

2. TIM LIKES TO JUMP ROPE (‘h’)

   APT SPRLZ AV QBTW YVWL

3. I LOVE CIS DONUT FRIDAYS (‘d’)

   L ORYH FLV GRQXW IULGDBV

4. THE DOG FETCHED A BALL (‘y’)

   RFC BME DCRAFCCB Y ZYJJ

5. SPONGEBOB IS YELLOW (‘u’)

   MJIHAYVIV CM SYFFIQ

Decipher these messages using a St. Cyr cipher:

1. GNWYMIFD HFPJ NX IJQNHNTZX (‘f’)

BIRTHDAY CAKE IS DELICIOUS

2. IQDJQ’I SECYDW JE JEMD (‘q’)

SANTA’S COMING TO TOWN

3. XLVP XLYJ XPXZCTPD (‘l’)

MAKE MANY MEMORIES

4. PCDZP SPCRT ITPB ZXRZH WXVW (‘p’)

ANOKA DANCE TEAM KICKS HIGH

5. OZSL’K LZW ESYAU OGJV? (‘s’)

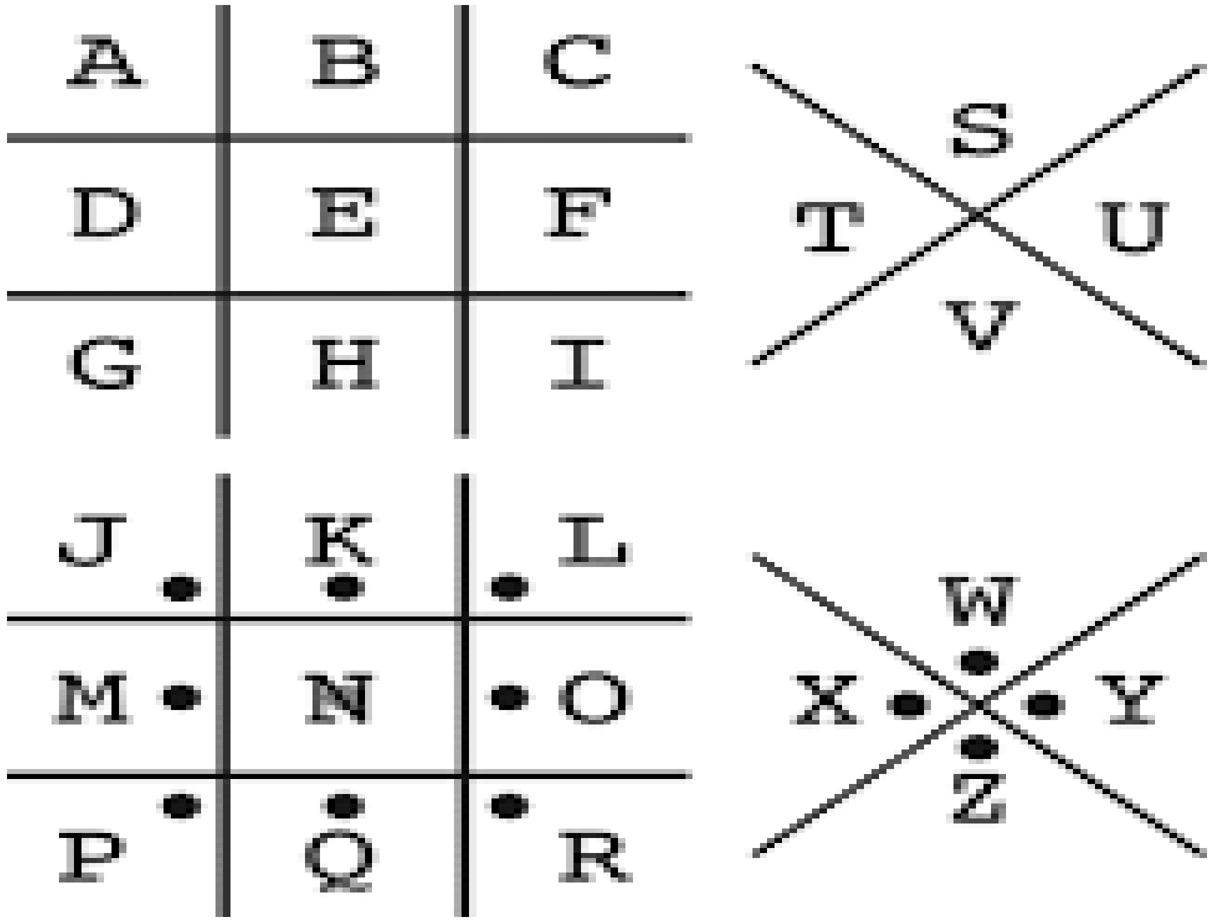
WHAT’S THE MAGIC WORD?

Use a St. Cyr cipher to encipher a message (no more than 20 characters).

Give it to your partner to decipher.
DO NOT tell your partner
the method you used.

How would a high school student approach this?

The Pigpen Cipher

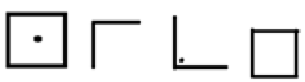


Encipher these messages using a Pigpen cipher:

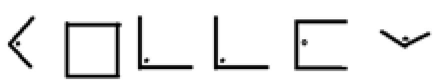
1. MISSISSIPPI

2. RUM

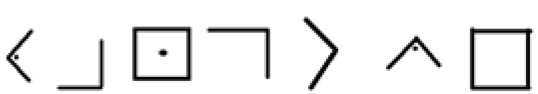
3. NILE



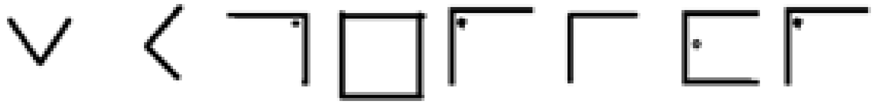
4. YELLOW



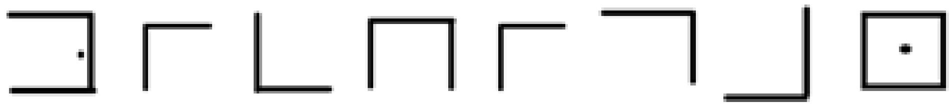
5. YANGTZE



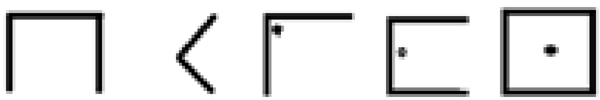
Decipher these messages using a Pigpen cipher:

1. 

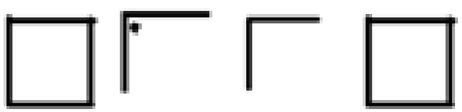
Superior

2. 

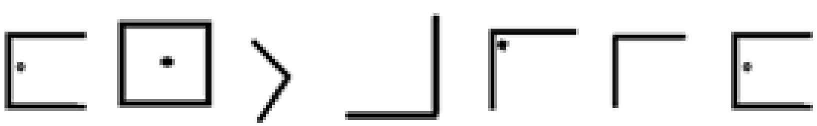
Michigan

3. 

Huron

4. 

Erie

5. 

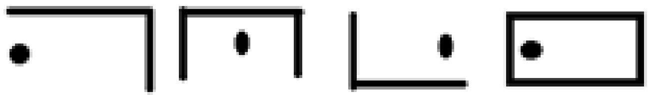
Ontario

Rosicrucian Cipher

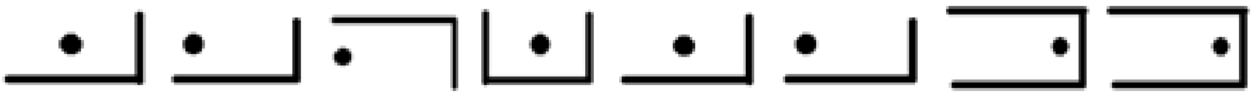
A B C	D E F	G H I
J K L	M N O	P Q R
S T U	V W X	Y Z

Encipher these messages using a Rosicrucian cipher:

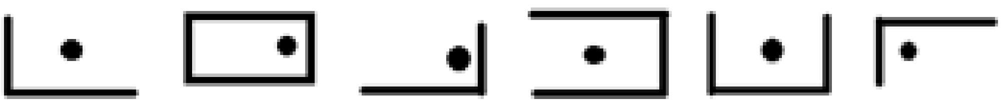
1. SWIM



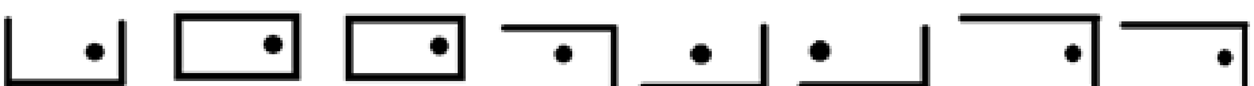
2. BASEBALL



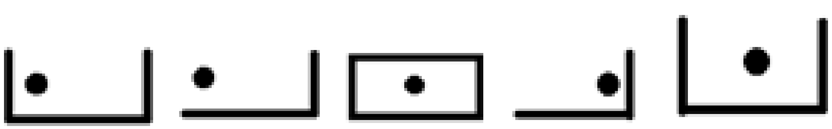
3. HOCKEY



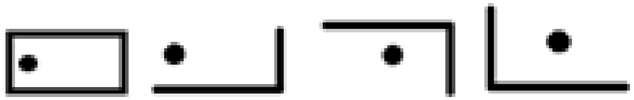
4. FOOTBALL



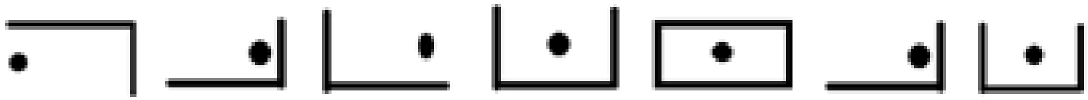
5. DANCE



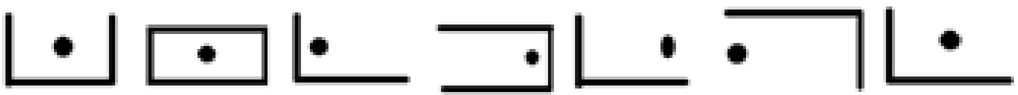
Decipher these messages using a Rosicrucian cipher:

1. 

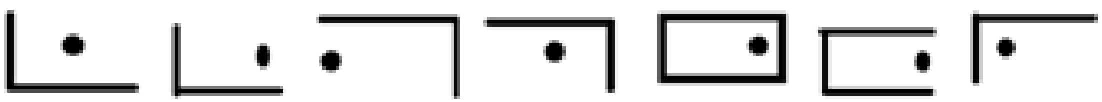
MATH

2. 

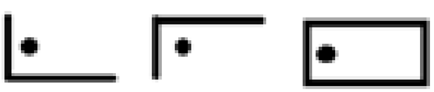
SCIENCE

3. 

ENGLISH

4. 

HISTORY

5. 

GYM

$c = p + 4$

c = the number of the ciphertext letter in our alphabet

p = the number of the plaintext letter in our alphabet

Plaintext

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Ciphertext, using c = p + 4

A	B	C	D	E	F	G	H	I	J	L	K	M
5	6	7	8	9	10	11	12	13	14	15	16	17

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
18	19	20	21	22	23	24	25	26	27	28	29	30

What coding process reverses the alphabet? That is, what is the equation that codes A as Z, B as Y, C as X, etc?

$c = 27 - p$

Is this a shift cipher? Why or why not?

No. In a shift cipher, each letter is moved the same number of places.

Explore $c = 3p + 1$.

(In this case, you'll be using the numbers 1-26.)

How would you encipher the letter "e"?
How about the letter "t"?

How would you decipher the letter "v"?
How about the letter "r"?

This is an approximation of the distribution of the letters in the English language, given a random sample of 1,000 characters.

A	73	J	2	S	63
B	9	K	3	T	93
C	30	L	35	U	27
D	44	M	25	V	13
E	130	N	78	W	16
F	28	O	74	X	5
G	16	P	27	Y	19
H	35	Q	3	Z	1
I	74	R	77		

In your packet, turn to the page on which is written “Name ___________” at the top, and has

A – 73
B – 9
C – 30
etc.

about halfway down the page.

Key	H	A	N	D	H	A	N	D	H
Plain	M	E	E	T	A	T	T	H	E
Cipher	T	E	R	W	H	T	G	K	L

Key	A	N	D	H	A	N	D	H	A
Plain	C	O	R	N	E	R	A	T	M
Cipher	C	B	U	U	E	E	D	A	M

Key	N	D	H	A	N	D	H
Plain	I	D	N	I	G	H	T
Cipher	V	G	U	I	T	K	A

PLAINTEXT

KEY LETTER

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Implement tasks that promote reasoning and problem solving **Teacher and student actions**	
What are *teachers* doing?	**What are *students* doing?**
Motivating students' learning of mathematics through opportunities for exploring and solving problems that build on and extend their current mathematical understanding. Selecting tasks that provide multiple entry points through the use of varied tools and representations. Posing tasks on a regular basis that require a high level of cognitive demand. Supporting students in exploring tasks without taking over student thinking. Encouraging students to use varied approaches and strategies to make sense of and solve tasks.	Persevering in exploring and reasoning through tasks. Taking responsibility for making sense of tasks by drawing on and making connections with their prior understanding and ideas. Using tools and representations as needed to support their thinking and problem solving. Accepting and expecting that their classmates will use a variety of solution approaches and that they will discuss and justify their strategies to one another.

Support productive struggle in learning mathematics Teacher and student actions	
What are *teachers* doing?	**What are *students* doing?**
Anticipating what students might struggle with during a lesson and being prepared to support them productively through the struggle. Giving students time to struggle with tasks, and asking questions that scaffold students' thinking without stepping in to do the work for them. Helping students realize that confusion and errors are a natural part of learning, by facilitating discussions on mistakes, misconceptions, and struggles. Praising students for their efforts in making sense of mathematical ideas and perseverance in reasoning through problems.	Struggling at times with mathematics tasks but knowing that breakthroughs often emerge from confusion and struggle. Asking questions that are related to the sources of their struggles and will help them make progress in understanding and solving tasks. Persevering in solving problems and realizing that is acceptable to say, "I don't know how to proceed here," but it is not acceptable to give up. Helping one another without telling their classmates what the answer is or how to solve the problem.

Pose purposeful questions Teacher and student actions	
What are *teachers* doing?	**What are *students* doing?**
Advancing student understanding by asking questions that build on, but do not take over or funnel, student thinking. Making certain to ask questions that go beyond gathering information to probing thinking and requiring explanation and justification. Asking intentional questions that make the mathematics more visible and accessible for student examination and discussion. Allowing sufficient wait time so that more students can formulate and offer responses.	Expecting to be asked to explain, clarify, and elaborate on their thinking. Thinking carefully about how to present their responses to questions clearly, without rushing to respond quickly. Reflecting on and justifying their reasoning, not simply providing answers. Listening to, commenting on, and questioning the contributions of their classmates.

Expectations for students	Teacher actions to support students	Classroom-based indicators of success
Most tasks that promote reasoning and problem solving take time to solve, and frustration may occur, but perseverance in the face of initial difficulty is important.	Use tasks that promote reasoning and problem solving; explicitly encourage students to persevere; find ways to support students without removing all the challenges in a task.	Students are engaged in the tasks and do not give up. The teacher supports students when they are "stuck" but does so in a way that keeps the thinking and reasoning at a high level.
Correct solutions are important, but so is being able to explain and discuss how one thought about and solved particular tasks.	Ask students to explain and justify how they solved a task. Value the quality of the explanation as much as the final solution.	Students explain how they solved a task and provide mathematical justifications for their reasoning.
Everyone has a responsibility and an obligation to make sense of mathematics by asking questions of peers and the teacher when he or she does not understand.	Give students the opportunity to discuss and determine the validity and appropriateness of strategies and solutions.	Students question and critique the reasoning of their peers and reflect on their own understanding.

Expectations for students	Teacher actions to support students	Classroom-based indicators of success
Diagrams, sketches, and hands-on materials are important tools to use in making sense of tasks.	Give students access to tools that will support their thinking processes.	Students are able to use tools to solve tasks that they cannot solve without them.
Communicating about one's thinking during a task makes it possible for others to help that person make progress on the task.	Ask students to explain their thinking and pose questions that are based on students' reasoning, rather than on the way that the teacher is thinking about the task.	Students explain their thinking about a task to their peers and the teacher. The teacher asks probing questions based on the students' thinking.

Anoka.k12.mn.us/ahskelley

Conference Resources and Handouts

Cryptography