CRYPTOGRAPHY: HOW MATH HELPS MAKE COMMUNICATION SECURE

André Mathurin, Mathematics Teacher – amathurin@bcp.org
Bellarmine College Preparatory (San Jose, CA) – http://webs.bcp.org/sites/amathurin

WHAT IS CRYPTOGRAPHY?

Despite living several thousand miles apart, Bob and Julie want to communicate privately with each other. But if phone lines can be tapped and text messages can be intercepted, how can they ensure the privacy of their communications? Enter **cryptography** – the process of making a message unintelligible to anyone other than the intended parties (i.e. Bob and Julie). For example, Bob sends Julie the following text message:

EN ZNV VBMU SP FP SP GBVBHJ HO LBQDG

Bob and Julie know the meaning, but do you? Probably not, but given enough time and motivation, you (or someone) could figure out what Bob and Julie did to make the message unintelligible. Why is that the case? Because in the process of making a message look "all messed up" there are only two fundamental actions that can happen: **transposition** (scrambling) and **substitution** (replacing).

TRANSPOSITION EXAMPLE: Creating the Appearance of Randomness Using Geometry

Utilizing basic geometry, Bob can create the appearance that the letters of the message have been randomly scrambled when in fact they have scrambled using a clearly defined method (**algorithm**). For example,

ANII UTAM YGAR DTOH WTIN OOWA OOHC

is one of the $367,583,363,006,020,761,599,999$ possible transpositions and it was obtained by creating a 4x7 rectangle using the letters of the original message. And if Julie knows that Bob used a rectangle to scramble the letters, she can use a rectangle to un-scramble the letters. They now have a **cipher system**.

USING KEYS: Going Public with a Cipher System

Suppose Bob accidentally tells someone that he uses rectangles to scramble the messages he sends to Julie. Does that compromise the privacy of his communication with to Julie? To an extent yes, but thanks again to randomness, a reasonable level of security remains because of the large number of possible rectangles that can be constructed ($7!=5,040$) from these letter groupings.

However, privacy will be short-lived if the method for assembling and disassembling their rectangles remains static. So Bob and Julie make their cipher system dynamic by introducing **keys** allowing variation in (1) how the rectangle is created and (2) how the rectangle is assembled/disassembled. For example,

OYOD TOGO UIII THOT WAMN NARC AWAH

represents the same message as before but looks different because the starting point and row ordering (i.e. keys) were changed. Now in addition to sending the text message, Bob must also communicate to Julie the keys he used to generate the transposition so that Julie can *reverse* the transposition. (**inverse function**).

RANDOMNESS: YOUR FRIEND AND FOE

Suppose this time Bob decides to send the same text message to Julie but rather than transpose the order of the letters of the message, he *substitutes* each letter of the message with a different letter. Bob decides to write the letters of the alphabet on small slips of paper and place all of them in a hat, then randomly draws a slip of paper out, one at a time to determine how the substitution will occur. Here is one possible result:

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

Using the chart, Bob would send the text message as

CH YHF JPLE EH AH EH MPJPRR RL BPDZM

While it is possible to “find” the original message by checking all of the possible substitution charts, the time required to do this makes Bob confident his message will remain private for quite awhile. But this random method for replacing the letters of the message makes it impossible for Julie to easily or efficiently *reverse* the substitution unless he also sends Julie the substitution chart!

SUBSTITUTION EXAMPLE: Creating the Appearance of Random Using Algebra

To facilitate this example, let’s pretend that our entire alphabet consists of only 8 letters.

normal alphabet	a	b	c	d	e	f	g	h

1	2	3	4	5	6	7	8

normal alphabet	a	b	c	d	e	f	g	h

1	2	3	4	5	6	7	8

normal alphabet	a	b	c	d	e	f	g	h

1	2	3	4	5	6	7	8