

 Mathematics Department	<h2 style="text-align: center;">Profile of the Month</h2> <h3 style="text-align: center;">LT Karen Bliss</h3>
Chauvenet Hall Editor: Prof. S. Garcia	
Phone: 410-2936728 www.usna.edu/MathDept/	

LT Karen Bliss graduated from University of Missouri-Rolla, a small engineering school, in 1998 with a degree in Applied Math and continued her education at North Carolina State, earning a Master of Science in Applied Math in 2000.

She joined the Navy while in grad school (perhaps to spite her brother, Major Michael Bliss, US Army). Her first assignment with the Navy was at Naval Nuclear Power Training Command, Charleston, SC. She taught the enlisted math curriculum before moving on to teaching Mechanical and Electrical Theory for Machinist Mates. “The transition from teaching math to teaching the mechanics of operating a reactor was a little bumpy here and there, but I credit my math background for making it as smooth as it was. Every topic—from how a relief valve works to how an electrical generator works-- somehow relates back to an equation,” says Bliss. “I also depended heavily on critical thinking and logic, painfully learned during that first proof-writing class that all math majors dread.” LT Bliss was then appointed Director of the Mathematics Division at Nuclear Field ‘A’ School. She served in that position for one year before reporting to the Naval Academy in August 2004. She has taught Calculus I, II, and III and Differential Equations.



In addition to teaching, LT Bliss enjoys participating in local races. She has been running for about 6 years and does a couple of 10-milers and half-marathons each year. This August she branched out and did a triathlon. “I’m pretty slow, but I always make it to the finish line,” says Bliss. “And I still haven’t actually come in last at a race...yet. But I’ll be at the Marine Corps Marathon in 2007, so keep an eye out for me at the end!”

	<h1 style="text-align: center;">Math News</h1>	Mathematics Department Volume 6, Issue 1 Oct 19, 2006
---	--	--

What is Cryptology?

By Prof. George Nakos. Cryptology is the art and science of secret communication. It is used in the military, diplomacy, national security, protection of electronic monetary transactions, prevention of destruction of computer data, etc.

Cryptology is divided into **cryptography** which analyzes methods of encrypting messages, and **cryptanalysis** which analyzes methods of decrypting encrypted messages. A method of encrypting and decrypting messages is called a **cipher**.

A message before it gets encrypted is called **plaintext**. An encrypted message is called **ciphertext**. A **key** is a set of secret rules used to encrypt, or decrypt a message. Here are some ciphers.

1. The **Shift Cipher**, encrypts by shifting letters of the alphabet to the right by a certain amount and wrapping around. The encryption key is the amount by which the letters were shifted. The shifting by three letters is called **Caesar’s Cipher** and is attributed to Julius Caesar. So, in this cipher ‘a’ goes to ‘d’, ‘b’ goes to ‘e’,..., ‘x’ goes to ‘a’, ‘y’ goes to ‘b’, and ‘z’ goes to ‘c’.

For example, the plaintext:

an apple a day keeps the doctor away

encrypted by Caesar’s Cipher becomes

DQDSSOHDGDBNHHSVWKHGRFWRUDZDB

Can you decrypt the following that was encrypted by some **Shift Cipher** of unknown key?

RCCK YRKX CZKK VIJZ JEFK XFCU

Do you think that the Shift Cipher is secure?

2. The **Permutation Cipher** encrypts by permuting the letters of plaintext. This is also known as *anagramming*. For example, cipher text HKNTSA came from the plaintext ‘thanks’ by applying the permutation

1 2 3 4 5 6
2 5 4 1 6 3

This permutation is the encryption key in this case. To decrypt we need to apply the inverse permutation to the ciphertext. If the key permutation is unknown then we need to try out all possible permutations of six letters. The number of permutations of six letters is $6! = 720$. This is large to try by hand. You may think that a computer could do this fast, but if your short message had only 20 letters, then it would take $20! = 2,432,902,008,176,640,000$ tries. The number of keys here is huge. Is this the perfect cipher, due to the large number of permutations we need to try? This is far from true. For example, to decrypt HKNTSA, we may use frequencies of digrams in the English language. It is known that digrams ‘TH’, ‘CK’, and ‘AN’ are the most common, so we may try all permutations of TH, AN, K, S, (only $4! = 24$). However, the answer is already obvious. Can you decrypt the message KTICH by using digram frequencies?



What is Cryptology? (Cont.)

3. The **Substitution Cipher** encrypts by substituting letters of the alphabet for other letters. In other words, we permute the alphabet instead of permuting the plaintext around as we did with the Permutation Cipher. For example, using the substitution (which is the encryption key)

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

the message

you are kidding

encrypts as

WXD IAC PTUUTKM

To decrypt apply the inverse permutation of the alphabet. If the substitution is unknown the decryption is quite a bit harder.

How do we decrypt a message if the substitution key is not known? We start by using the single letter frequencies of the English alphabet. For example, it is known that 'e' is the most frequent letter. It appears in long English texts at the rate of about 12.3%, 't' is the next most frequent at the rate of about 8.8%, 'a' is almost as frequent as 't' at the rate of 8.2%. Next, comes 'o' at rate 7.7%, etc. So if long enough ciphertext is available and, say, that the letter 'k' appears at the highest rate (perhaps close to 12%), then chances are that 'k' was the encryption of 'e'. If the next most frequent letter is 'q', then chances are that this would be encryption of either 't' or 'a', or even 'o'. Continuing and trying out the possible most frequent letters one can most likely decrypt the message.

The above ciphers are very old and they are not secure. Today they are only used for entertainment. However, compositions of substitution ciphers and permutation ciphers are at the core of some of the most secure modern ciphers.

The concept of what we mean by a 'secure cipher' was first put on firm mathematical foundation by Claude Shannon in the late 1940s. In 1949, Shannon published a paper entitled 'Communication theory of Secrecy Systems' in the Bell systems Technical Journal. This paper had great impact in the scientific study of cryptography.

The ciphers described above are all symmetric. This means that knowing the encryption key is equivalent to knowing the decryption key. For example, in the Shift Cipher, if encryption is done by shifting by 4 places to the right, then decryption is done by shifting by 4 places to the left. Also in a substitution cipher if the encryption key is a given permutation of the alphabet, then decryption is done by using the inverse permutation.

In 1976 Diffie and Hillman came up with the idea of an **asymmetric** cryptographic scheme, where knowing the encryption key does not necessarily yield the decryption key. In fact, the encryption key is made public, so that anyone can encrypt a message and send it to the person who posted the encryption key. However, only that person can decrypt the encrypted message. This is called **public key cryptography** and it is a thriving area of cryptography.

If you think you might like cryptography check out some nice books and a good starter website. If you still like it take a course!



What is Cryptology? (Cont.)

References

'Cryptography Theory and Practice', text by Douglas Stinson

'An Introduction to Cryptography', text by Richard Mollin

'Handbook of Applied Cryptography', text by A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone

Starting Website

<http://en.wikipedia.org/wiki/Cryptography>

Some **history** of Cryptology can be found at:

<http://www.resonancepub.com/homecrypto.htm>

MIDN **Alexander Charles George** was the academy junior representing the United States - and the Naval Academy - at the squash world championships that took place last month in Budapest, Hungary. MIDN George, is a member of the Under-23 National Team and is ranked No. 5 in the nation in that category. MIDN George is an applied math major who is also in the Rhodes Junior Scholarship program. **The editor of this Math News publication is very proud not only to have MIDN George as her advisee but also have him as her student in the SM365 class this semester.

For Baseball Lovers:

What is the maximum number of walks possible in 1 inning of baseball for 1 team if Casey is at bat 3 times and makes all 3 outs?

Hint: Assume Casey walks each time and forgets to touch home plate (and is therefore called out)



Question of the Month

If amoebas double the volume every minute and it takes 40 minutes to fill a jar, how long does it take to fill half the jar?

E-mail your answer to Prof. Garcia smg@usna.edu. Among those with the right answer, a randomly chosen midshipman will get to choose between a fantastic math water bottle or a cool koozie.

The symbol used on the head of Math News is one of the Platonic Solids. Ref. <http://mathworld.wolfram.com/PlatonicSolid.html>.