Editor's note

Hard to believe that this is the Spring issue, after the severely cold weather we have had this entire month. This year, it was February that came in like a lion; let’s hope that it goes out like a lamb.

In this issue there are three Lunch With… events to report upon. With conference travel I’ve missed two; but Gordon Rostoker covered for me, and provided summaries. There is one more event to come for this academic year, on 27 March.

Happily the In Memoriam list is shorter than in December. Finally, for the reprinting of previous Mousing Around articles by Keith Smillie, I’ve chosen two that logically combine, on the general subject of cryptography.

Ruth Gruhn

Notices

Lunch With… event coming on Wednesday 27 March.

Biologist Colleen St. Clair will speak on the subject of adaptation, conflict, and coexistence in urban coyotes.

The event will be held in the Papaschase Room upstairs at the Faculty Club at 12 noon. Please notify Emeritus House by phone or e-mail before noon on Monday 25 March.

Reports

Lunch With … Event of 28 November 2018

The presentation by Gerda de Vries, a Professor of Mathematics and Statistical Sciences, was enthusiastically received by a larger than normal audience of 33. It was devoted to how mathematics could be used to design quilts that were both attractive to the eye and challenged the skill of the quilter.
The speaker explained the mathematical ideas behind the quilts she had designed, and brought along the actual quilts so that the members of the audience could see their complexity close up. She introduced the audience to the concept of tiling – that is, the creation of a surface made of geometrical forms that fitted together with no overlap and no gaps. The geometrical forms ranged from simple squares and triangles to more complex figures originally designed by the famous Dutch graphic artist MC Escher. Of particular interest were quilts that featured optical illusions that gave the impression of three dimensions on a flat surface. The enthusiasm of the speaker in presenting complex ideas of translation and rotation of simple structures left the audience enthralled at a presentation that could have kept their attention for much longer than 45 minutes, plus the many questions that followed.

Gordon Rostoker

Lunch With…. Event of 23 January 2019

On this occasion, the audience was provided an entertaining presentation by Professor Joseph Patrouch, the Director of the Wirth Institute at the University of Alberta. His talk centered in the period at the end of World War I, and how the peace treaties after the cessation of hostilities on the western front led to the creation of many new countries from the wreckage of the Austro-Hungarian Empire. Much of his presentation focused on the battles that took place after November 11, 1918, which was when fighting ceased on the western front. In fact, hostilities continued on other fronts, particularly bordering on the Mediterranean Sea, for some considerable time thereafter. Other fronts that he described included the Italian Front, with Italy initially trying to take over territory to the east (e.g., Albania) so as to control the Adriatic Sea; and the Pacific Front, where the western powers were all trying to control a piece of the Orient. His talk concluded with an interesting description of the internment camps set up in Canada immediately after the start of the Great War. He opined that the British were the first to use internment camps, even setting them up in Great Britain at the start of the war. The British model was used by other countries in order to detain and contain foreign nationals who were deemed to be a threat. The Wirth Institute was able to obtain records of Canadian detainees from documents discovered in Europe (Canada having destroyed their records after the war). In conclusion, Professor Wirth invited anyone who was interested to visit the Wirth Institute and to participate in the Central European Cafes that take place once a month in the Student Lounge in Arts and Convocation Hall.

Gordon Rostoker

Lunch With … Event of 27 February 2019

The speaker at this event was Trevor Schmidt, artistic director of the Northern Lights Theatre Company. Trevor presented an entertaining review of his long and hectic life in the theatrical profession, beginning early as a child performer. With an MFA from the University of Calgary, and experience at the Banff School of Fine Arts, Trevor spent some time in the theatre scene in Toronto; but eventually ended up in Edmonton, with its many theatre companies. He has now been associated with the Northern Lights Theatre Company for 18 years.
The Northern Lights Theatre is well known in Edmonton for its plays featuring controversial themes. This season’s theme is “A Woman’s Body – and her right to control it”. The plots are deliberately provocative, with the objective to challenge the audience to think about their personal views of the issue, with a “talk-back” forum after the show. The Company intends to stay small: to grow “not bigger but better”.

*Ruth Gruhn*

### In Memoriam

<table>
<thead>
<tr>
<th>Name</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Baird</td>
<td>Political Science</td>
</tr>
<tr>
<td>George Ball</td>
<td>Entomology</td>
</tr>
<tr>
<td>Desmond Brown</td>
<td>History</td>
</tr>
<tr>
<td>Gary Horlick</td>
<td>Chemistry</td>
</tr>
<tr>
<td>Ed Leonard</td>
<td>Mathematics</td>
</tr>
<tr>
<td>Roger Morton</td>
<td>Geology</td>
</tr>
<tr>
<td>Peter Olley</td>
<td>Pediatrics</td>
</tr>
<tr>
<td>Tom Pocklington</td>
<td>Political Science</td>
</tr>
<tr>
<td>Fred Zwicker</td>
<td>Zoology</td>
</tr>
</tbody>
</table>

### Mousing Around

*Keith Smillie*

52. *dihzuhpdunvrfubswrorjb*

After our discussion of prime numbers and their importance in Internet transactions, we should make a few remarks on *cryptology*, the science of secret writing. Cryptology includes using a given *key* for encrypting the *plaintext* message into *ciphertext*, and conversely using the key in decrypting the ciphertext into the original plaintext.

One of the earliest historical examples is the cipher used by Julius Caesar, now called the Caesar cipher, in which each letter in a message is replaced by the letter which occurs three letters farther along in the alphabet; i.e., *a* is replaced by *d*, *b* by *e*, …, and *z* by *c*. For example, the plaintext *professorsemeriti*
would give the ciphertext surhvvurvhphulwl, which could be deciphered simply by replacing each letter by the letter occurring three letters previous.

Caesar’s method may be generalized to a shift of an arbitrary number of letters; and, for example, a shift of seven letters in our plaintext example would give wyvmlzzvzitypap. A cipher such as a Caesar cipher in which each letter is replaced by another letter but retains its position in the text is called a substitution cipher.

Another type of cipher is the transposition cipher, in which each letter changes its position in the text but retains its identity. A very simple example is the reversal of each successive triplet of letters so that our plaintext example becomes orpsefrosmesireit.

Substitution ciphers with a single Caesar shift are relatively easy to break with a frequency analysis of the letters in a sufficiently long sample of ciphertext, since the relative frequencies of letters, and also successive pairs of letters, in large samples of English text are known. In the late sixteenth century, the French diplomat Blaise Vigenère developed a method of enciphering which used a number of different Caesar ciphers in a systematic way on the same plaintext. For example, if we wish to encipher our example using four Caesar ciphers represented by the key FRED, we write the plaintext with the key repeated above it as follows:

```
FREDFREDFREDF
professorsemerli
```

Then the first, fifth, ... letters in the plaintext are encoded with a Caesar shift of five, since F is the sixth letter of the alphabet; the second, sixth, ... letters are encoded with a Caesar shift of seventeen, since R is the eighteenth letter, etc. The resulting ciphertext is uisijjwrwjipjimwn. The Vigenère cipher, as it was called, was not immediately adopted; and it was not until the middle of the nineteenth century that a method based on a rather complicated frequency analysis was developed for deciphering it.

Near the close of World War I, American cryptologists used random keys of the same length as the message being enciphered with the Vigenère cipher. Keys of randomly sequenced letters were printed on sheets and assembled in large pads. Since each key was used only once, these pads became known as “onetime pads”; and if used properly, provided an unbreakable cipher.

Cryptographic methods were used extensively in warfare, beginning even earlier than the reign of Julius Caesar. One of the better-known ciphers of World War I was the German ADFGVX cipher introduced in March 1918, a type that combined both substitution and transposition. It is said that the French intelligence officer who broke this cipher on June 2 just in time for the Allies to repulse a German offensive on Paris lost 15 kg in his feverish and successful effort to break the code. The best-known example of World War I cryptanalysis is, of course, the Zimmermann Telegram, an incident in which the British intercepted and deciphered a telegram being sent by the German Foreign Minister, Arthur Zimmermann, to the Mexican president to persuade him to invade the United States.

In the 1920s a German inventor, Arthur Scherbius, developed an electromechanical device somewhat resembling a typewriter in size and appearance for both enciphering and deciphering text. The Enigma, as it was called, was adopted by the German military; and over 30,000 were in use during World War II. The decoding of the Enigma traffic at the Government Code and Cypher School at Bletchley Park, Buckinghamshire, has been said to have shortened the War by three years.

All of the cryptographic methods discussed here have the serious fault that the keys must be known in advance to both sender and receiver. The secure transmission of these keys -- whether used by Julius Caesar in communicating with his legions or Admiral Dönitz with his U-boats -- was a continuing problem for which there was no completely satisfactory solution. However, work in the 1970s and 1980s led to the development of Public Key Encryption, in which messages enciphered with a published key could only be deciphered if the unpublished part of the key were known. This topic, and the role played in it by prime numbers, will be the subject of a later column.
There is a large literature on secret codes and ciphers. In my opinion one of the best books for the general reader is *The Code Book* by Simon Singh (Anchor Books, 1999), which I have read with great pleasure twice and have consulted many times. I can recommend it without reservation both as an excellent introduction to the history of cryptography and also as a superb example of science writing for the general reader. There is a considerable number of works of fiction in which cryptology plays a central role. Some of the best known short stories appear in *Famous Stories of Code and Cipher* edited by Raymond T. Bond (Reprinted by Collier Books, 1965), which gives an excellent brief historical summary of the subject in an Introduction.

56. **Public Key Encryption**

The deciphering of the German Enigma traffic at Bletchley Park mentioned in a previous column marked the first use of the electronic computer in cryptography. The Colossus computer, which was designed and built for this work, and whose existence was kept secret, was the world’s first electronic digital computer. Unfortunately at the end of the War, all models and the blueprints were destroyed by the British government; and the ENIAC designed and built in the United States was considered to be the first programmable electronic computer.

In the 1990s the British painstakingly reconstructed a Colossus from a few wartime photographs and “some fragments of circuit diagrams which some engineers kept quite illegally, as engineers always do”. The machine was first turned at Bletchley Park on June 6, 1996, with HRH the Duke of Kent throwing the switch.

The use of computers in cryptology means that all messages, whether enciphered or not, must be stored internally as binary or base-2 numbers; i.e., as sequences of 0s and 1s. The characters in a message, either plaintext or ciphertext, would be encoded as 7-binary-digit sequences using the American Standard Code for Information Interchange (ASCII). For example, U would be represented by 1010101, O by 1101111, F by 1100110, and A by 1000001; so the plaintext message UofA would be represented by the 28-binary-digit number

$$101011011111001101000001$$.

If this figure were enciphered by a transposition cipher that interchanged successive pairs of digits, then the ciphertext would be the 28-digit binary number

$$0101011101111100111000010$$.

This number could then be transmitted to the recipient, who would have to know the transposition key to decipher it.

In the mid-1970s the Americans adopted a Data Encryption Standard (DES) which has become a world standard. A message is divided into successive 56-binary-digit sequences, and each sequence is subjected to a complicated shuffling process - described by one author as “a bit like kneading a slab of dough” - determined by a key which is itself a 56-digit binary number. This procedure allows a total of roughly 100,000 trillion keys. However sufficient this astronomical number of keys may be, the problem of secure key-exchange still must be addressed.

At about the same time as the DES standard was adopted, scientists at Stanford University developed a method for the secure exchange of keys. The procedure, called the Diffie-Hellman-Merkle key exchange scheme after the three persons who developed it, was first publicly demonstrated at the 1978 National Computer Conference to what has been described as an “astonished audience”. Even though keys still had to be exchanged, this transaction could be done either in person or securely by telephone, postal service, or email.

The problem of key exchange was solved at about the same time by three MIT scientists - Ronald
Rivest, Adi Shamir, and Leonard Adleman - whose procedure became known simply as RSA. The procedure involved the use of an asymmetric key, with one public key for encipherment and a second private key for decipherment, instead of one symmetric key for both encipherment and decipherment. We shall describe the procedure first by a brief analogy, and then with a few remarks about its implementation in which very large prime numbers play a vital role.

Let us suppose that I wish to send a letter to my friend George. I write the letter and put it in a case that can be locked with a padlock. Then I go to the post office - any post office anywhere in the world - where I see a large collection of padlocks, all with people's names on them and without keys. I purchase a George-padlock, use it to lock the case, and send it to George. As George is the only person with a key to a George-padlock, he can retrieve my letter knowing that it has not been read by another person. The padlock may be considered analogous to the public key, and the physical key to the private key.

All we need to say here about the mathematics of RSA is that the main part of any public key, which may be looked up in a directory of public keys, is a very large number which is the product of two primes, whereas the private key is based on the two prime numbers themselves. Given two numbers, however large, it is a relatively simple computation to find their product; but the converse operation of factoring the number into its prime components can be orders of magnitude more difficult. A few years ago it was estimated that a public key of the order of magnitude 10^{308}, not an unreasonably large key for complete security, would require a hundred million personal computers working for a thousand years to break into its two prime factors, which would have about 150 digits each.

But what about these quantum computers we are beginning to hear about, which when developed will allow billions of similar calculations to be done in parallel? They may pose a serious threat to RSA and Internet security. If I ever learn something about the quantum world and the current attempts to build a quantum computer, I'll write a column (or two) on the topic. But don't hold your breath waiting!

Let's hope soon…