ICTS-RRI Math Circle, Saturday 25th March 2023

Sam

March 21, 2023

If you remember, we started a few sessions ago by making a multiplication table for days of the week. This was modular arithmetic. As you now definitely appreciate, modular arithmetic is not just an idle curiosity, but has real applications in cryptography. In this final session, we will wind up our exploration of cryptography and move on to other things.

We owe modular arithmetic in its present form to Carl Friedrich Gauss the "Prince of Mathematicians". Gauss is said to have claimed that "Mathematics is the queen of sciences and number theory is the queen of mathematics. She often condescends to render service to astronomy and other natural sciences, but in all relations, she is entitled to the first rank." Even Gauss did not anticipate the services that the queen would render to cryptography. This Saturday we will explore a simplified version of cryptography that is in current use and peek a little into the future.

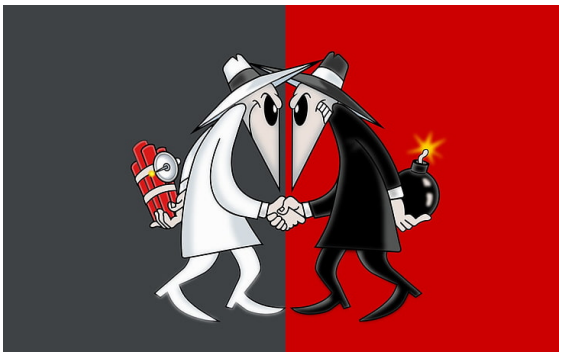

Figure 1: Two spies crossing and double-crossing each other

Before you come to the session, solve the following riddle. As two spies cross, they speak in numbers. Can you figure out what they said?

SPY1:4 423 2 27325-46. 8439 5669 843 2633.
SPY2: 9436 927 8447?
SPY1: 937837329. 93 4283 86 438 688.
SPY2: (434,434! 93?). 968 2468 4646' 6694373 28339!

At the end of this note you will find a write-up on how we learn to solve problems. This is a condensation of some ideas due to the mathematician George Polya. Read through this as a preparation for the session on Saturday. Also please bring along some loose sheets of paper, pencils or pens, a calculator (phone calculator will do), and a ruler.

First Activity: Here are some questions for you:
1. In the code used by the two spies above, what was different from the ciphers we have considered?
2. Fermat's Little Theorem: Last time we played with numbers and arrived at the statement of Fermat's Little Theorem: For p prime

$$a^p = a \text{ modulo } p \tag{1}$$

What can we say when p is replaced by n, which is not necessarily a prime. Let us take the simplest cases $n = 4, 6, 8, 9, 10$ and look for patterns. You have a lot of practice working out powers of numbers mod$n$. For each n make a table of $a^c \text{mod} n$ for varying a and c. Can you find any patterns?

Tea break: 11:15

Second Activity Codes: We saw last time that substitution ciphers were susceptible to frequency analysis. We then looked at running key ciphers. These too are vulnerable. In Vernam Ciphers (one time pads), we use a random key and these are, in theory, uncrackable. (Scrambling the message with garbage just gives you back garbage.) But the problem here is sharing the key. The enemy may intercept the key and read your message. We need to find ways around this.
Public key cryptography (PKC): has one key for encryption which is made public. Decryption requires a private key. In the Ciphers we looked at so far, given the encryption process, it was easy to invert it to find the decryption process. With PKC, this is no longer true. It is like locking yourself out of a room or car. You cannot get back in. If you encrypt a message using PKC and forget it (say after six months), even you will not know how to decrypt your own message. We will play a game of encryption and decryption using PKC.

Finally, we will discuss methods of distributing keys securely using quantum physics.

How to Solve it? by George Polya

This writeup explains in simple language Polya's method for solving problems.

All of us are faced with problems in everyday life and we use a number of tricks to solve them. For instance, you come home from school and find the front door locked and nobody home. What do you do? Think hard. Is there a friendly neighbour? Could there be a window open? Would they have left the key in a hiding place? Can I reach them on the phone? As we get older we get better and better at solving life's problems. We learn from past experience and develop a bag of tricks.

The same is true for problems in mathematics or physics. Many of us use these tricks without being aware that we are using them. For those of you who are learning to solve problems, it is useful to make these rules explicit. This is what George Polya, a Hungarian Mathematician did in a book called "How to solve it?". What follows is a simplified and condensed version of Polya's ideas.

The process is divided into four steps: consciously go through these steps. As you get more experienced, you will use this method without even thinking about it.

1. *Understand the Problem:* It goes without saying that in order to solve a problem we have to understand it. Here are questions that you ask yourself in order to do this:

   - What form will the answer take? Is it a number, a length? Or is it a logical argument? A proof? An algorithm? A strategy?
   - What is the data that is given to me? Scan the statement of the problem to isolate the data.
   - What are the conditions of the problem? For instance, the answer may have to be a whole number. Or, in a logical proof, the statement may apply only to polygons.

2. *Planning an attack on the Problem:* Ask yourself these questions:

   - Have I seen a related problem before? A problem with a similar unknown?
   - How is the data related to the unknown? Is there too little data? Too much data?
   - Can I simplify the problem by considering a special case? an extreme case?
   - Can I simplify the problem by making it more general?
   - Can I give up a condition? Eg. give up the condition that the answer has to be a whole number and solve it with real numbers.
   - In some problems (a maze for example), it is advantageous to work backwards: start from the end, assuming we have reached our goal. Would this work in our problem?
   - Are there obvious symmetries in the problem?

3. *Solve* In this step, we implement the plan devised in the last section. This may involve calculation or developing the logical steps of a proof. It may be that the first attempt does not succeed. If so we go back to the planning stage and refine it.

4. *Review* This step is important for you to develop problem solving skills for the future. Don't regard a solved problem as dead. You can learn a lot from problems you have already solved and use this knowledge in the future. Ask yourself

   - is there a way to check the solution?
   - Can the solution be generalised?
   - Can I use the solution to devise new problems?

   The next time you are faced with a problem, (even a simple one) try to go through these steps and learn from them. With practice you will find your skills improving. Good luck!