Cryptology and Combinatorics

Thomas Lenell

December 9, 2015

1 History

Cryptology originated possibly as early as 1900 BC with the Egyptians who would write their hieroglyphics in non-standard forms to hide their meaning. Over time, cryptography evolved through many forms. In the Caesar Cypher, the value of every letter is shifted by three, e.g. a becomes d, b becomes e, etc. In Greece, messages would be written on a long strip of paper wrapped around a stick, the idea being that unless you had a stick of the same size, you couldn't properly decode the letter. Other countries would use different languages or code words. In some cases a message would be coded by reading a book, and writing down the page number, line number, and number of characters in from the side of the page where the letter being encoded is located. Among the most famous examples of cryptography is the enigma machine created by the Germans for military use in World War II. It had a series of five plates linked to the keyboard. In each message, only three of the plates were used. These plates were selected by higher commands on a rotating schedule, so in order to decipher the message, you'd have to know what date the message was written and have access to the orders stating which plates were to be used.

At first, when computers were introduced to the cryptography world, they were used for counting, to show possible numbers of combinations, in many cases, just showing how secure a message is. From there, the possibilities began to be seen. Instead of having to compute all the possible solutions to an encrypted system, a computer could make the calculations and spit out the possible outcomes using whatever method you designated. When computers began to be encrypted, other computers were used to do brute-force attacks to punch all possible codes into the first computer until it was unlocked. Thanks to advances in technology, that kind of encryption breaking is nearly pointless as there are an unlimited number of possible encryption keys.

An encryption key is the data packet that a computer generates to transmit with encrypted data to tell the computer on the receiving end of a transmission how to decrypt that message. To make things even more difficult on would be hackers, more than just the 26 characters of our alphabet are utilized in encryption. Every symbol on your keyboard, the ten numbers, and other symbols (varying based on encryption system) are also used. Then, to go the extra mile, a security program could also include characters from other languages. Modern encryption protocols take not only one of the previously mentioned methods for encryption, but multiple, and will cycle through them in order to make code-breaking as difficult as possible. Within cryptology, is a field known as Combinatorial Cryptology which focuses on Combinatorics as a method for encrypting data.

The particular method I found that drew my attention is the cubical combinatorics method. This method takes an approach that is both fun and simple to explain. All that it takes to understand it is an idea of how a rubics cube works

2 Example

Now, suppose you have a message to send with a total of 54 or fewer characters. Lay your message over a rubik's cube so that each character is on a separate block, and if you have fewer characters, the blank characters will have some other character to represent that it is blank.

Now scramble that cube. In order to decode your message, the solver would have to solve the cube and know where you started, plus how you filled in the cube. Otherwise, all they have is a jumble of characters in blocks of 9. Now let's look at this in terms a computer would see. First, it's looking a series of matrices containing the characters you input. Second, in place of a color, it sees a hexadecimal number which represents a color. From there, the computer can easily sort the data, no matter how jumbled, into the separate faces. But past that, it needs additional information. The only pieces which have to be in a specific location are the corners and center bricks. Everything else can float freely. Without knowing the order of the faces, and the way in which the bricks in each face were filled, the computer can only give you a series of possibilities, which would be in the trillions.

In our cube, there are 8 corners pieces, and 12 edge pieces. This gives us 8! ways to arrange the cornes. Seven of these can be oriented independently with each one depending on orientation of the previous corners in the list so we have 3^7 possibilities. For the edges, we have 12!/2 ways to arrange them. With an odd number of permuatations, using the same logic as above, 11 of the twelve edge pieces can be arranged dependent only on the order and arrangement of their predecessors. There are therefore 2 to the 11th ways to arrange them. When we put everything together, there are $8! * 3^7 * 12!/2$ * 2 to the 11th possible arrangements of the above message. This is roughly 43 quintillion possibilities.

Now imagine you had a significantly larger cube. Possibly 10x10x10. The number of possible combinations increases factorially. In order to properly decrypt a message encrypted in this way, you would need the same information, the face order (which face you start with and the order you progress from face to face), arrangement order (how you fill in each face), and the color values (hexi-decimal code assigning each block a color corresponding to a specific face). Without all of this, your computer will be listing possible combinations for years with no way to tell what the proper interpretation of the original message is.

References