Messages from Modern Inventors to the Next Generation

4. *Cryptographic Technology that Support the Internet Community* – Dr. Mitsuru Matsui, Mitsubishi Electric Corporation

In today's society with information technology (IT) such as the Internet, mobile phones, and electronic money, "cryptographic technology" is a necessity. The encryption of data enables people to exchange information they want to keep secret. Dr. Matsui has been conducting research on cryptography at Mitsubishi Electric Corporation. He broke a code that was said to be "impossible to break" in the United States. He is one of the leading cryptographers in Japan and developed a new type of cryptography which is now used in mobile phones etc.

What inspired you to become an inventor/a researcher?

Twenty years ago, when I first started doing research on cryptography, we didn't have the Internet or mobile phones so most people associated cryptography with spy movies or mysteries. In fact, I didn't know anything about cryptographic technology until I started working at the company. One day, on hearing the news that a cryptographer abroad had announced an incredible code-breaking method, I read his scientific paper for the fun of it. This led me to start studying cryptography. Breaking a code is similar to putting together a gigantic jigsaw puzzle. When one patiently tries to put together the puzzle by trial and error using the information provided, one begins to see parts of the picture and gradually the whole picture is revealed. Cryptography must have fit my personality, and I became captivated by the research, which I initially conducted by reproducing the work of others. My research evolved little by little into an original method "linear cryptanalysis (a code breaking method with a small amount of calculation, by creating a similar calculation of the block cipher using simpler calculation formulas)," and using this method, I was the first person in the world to succeed in an experiment that broke the encryption standard of the United States at that time (DES).

What kinds of challenges have you faced as an inventor, and how have you overcome those challenges?

My next research project was to create a new code that would benefit the general public. Breaking a code is enjoyable because it is like solving a puzzle, but when it comes to creating your own code, it is a different story. A code that everyone will use has to be small and speedy, but if the code is too simple, it may easily be broken. I had a hard time creating a code that was difficult to break and very easy to use, but finally, the issue was resolved with the idea of “recursive structure” (in which small parts are used over and over again to assemble the whole thing) and the subsequent development of a block cipher named MISTY. My experience in breaking codes was very useful in designing MISTY. Since breaking a code requires a technology for conducting an attack (spear) and designing a code requires a technology for defending against an attack (shield), I believe that I was able to create a better shield from carrying out research on spears.

What gives you joy as an inventor/a researcher?

It was important that MISTY became an international standard* so that many people would use MISTY. There are a number of organizations that establish various standards in the world. We made efforts to have MISTY adopted as the international encryption standard for a new type of mobile phone (i.e., third generation (3G) mobile phones). Conferences on the standardization of mobile phone technology at that time were mainly held in Europe, so I went there to have discussions with the local cryptographers and jointly created an encryption standard based on MISTY. The close ties that I developed with the cryptographers around the world through these activities have been a valuable asset. MISTY technology is now used in mobile phones throughout the world and plays an active role in protecting people’s privacy. It is somewhat unfortunate that cryptographic technology cannot be seen and thereby be more widely known, but I feel great pleasure as a researcher now that MISTY is used by many people in a tangible form as an international standard.

*International standard: For example, the shape and size of batteries are fixed so they can be used for any product. This is because manufacturers have agreed on a fixed shape and size (standard). Establishing a global “standard” in order to make products user-friendly and expedite production for manufacturers is called “international standardization.”

One of the computers used for breaking the US Data Encryption Standard (summer of 1993

LSI used for the first MISTY developed (one of the ICs)

What message would you like to give to future inventors?

From my experience, when you get stuck while trying to solve a difficult problem or issue, I think it is often effective to completely move away from the problem for a while. Once when I was trying to break a code, I ran up against a brick wall and gave up on cryptanalysis in order to try something completely different. But later, when I happened to recall the problem, I realized that what I had assumed to be incorrect was actually correct. This was my first conceptualization of “linear cryptanalysis.” I feel that this kind of thing happens all the time. It is often said that a researcher needs to be tenacious and assiduous, but I think that not being too enthusiastic and having the flexibility to change one’s ideas and perspectives is actually important for a researcher.