The first time I wanted to dig deep into the world of Computer Science was a year ago when I encountered my favourite anime, which showed me how splendid a game could be in the future with advanced computer technologies that the background stories are automatically generated by AI which have independent thinking abilities. Delving deeper into it, CS became more and more charming, particularly those spectacular AI, VR and etc., offering the possibility to break the limit of material world and allow players to enjoy immersive game environment.

Last year, I attended a summer school at University of Oxford, and it was my first time to attended a CS course. Surprisingly, programming attracted me. It was like communicating with a friend who would give me expected responses, which was even more comfortable than interacting with a human. We had several tasks, involving designing websites and implementing an encryption and decryption program. While the tutor only taught us fundamental programming skills like selection statements and loops and I had not learnt programming before, I had to learn coding from some online materials the tutor recommended, from which I gradually developed my self-learning ability.

In order to accomplish the encryption program, I searched online for functions I might need and came up with several plans. At first, I was considering of writing a dictionary. However it was impossible to cover all characters of all languages in the world. As I learnt more, I then knew that all characters are uniquely encoded as numbers using Unicode. Hence, I decided to encode strings into numbers, which can be encrypted with mathematical functions. Meanwhile, I used various functions for characters of different positions in a string to increase the complexity of my encryption. For example, y=x^2 would be used for letters on even positions while those have factor 7 would choose another function. Similarly, the decryption processes used corresponding inverse functions. This project expanded my knowledge of encryption quite a few, and I did realise that cryptography is ubiquitous and indispensable, it is widely used for encryption of websites, accounts and etc.

After our presentations, tutors introduced us about the history of cryptography like enigma in the World War II, which aroused my curiosity to learn more effective encryption methods. After the summer school, I still immersed in the ocean of encryption and learned another two algorithms. One is the XOR encryption, a symmetric encryption algorithm, which is relatively simple, and the other is a widely used algorithm: RSA. I found that the theory of the XOR encryption was easy to understand: each binary digit of the numerical encoding of the plaintext is applied with the key using XOR operation. When the receiver decrypts the cipher, they use the same method with the same key to get the plaintext as the XOR operation is reversible. This is convenient but can also be vulnerable, for example, if the plaintext has sequences of repeated characters. On the other hand, key distribution is crucial to all symmetric encryption method, which also increases the vulnerability of the XOR encryption. The RSA algorithm, however, is a symmetric encryption method and is more robust, because breaking its key requires large number prime factorisation. As this is an NP-hard problem, it is not solvable by any practical algorithm whose time complexity doesn’t grow exponentially. More specifically, when the key is short, a simple algorithm is adequate to break it, whereas with a key of length more than 1024 bits, breaking the key can’t be done within a reasonably short time. Therefore, the RSA encryption’s security is guaranteed unless the P=NP question is solved or a usable quantum computer is invented. I believe this is one of the reasons why it is the most commonly used. In addition, digital signature is also widely used using the RSA algorithm. Meanwhile, it is an asymmetric encryption, which means that it avoids danger in the process of key distribution as private key should be kept secret completely while only public key is published for encryption or signature verification.

I have read a book named Aha Algorithm, which introduces various algorithms based on readily comprehensible daily cases such as sorting algorithms. After finishing reading, I realised that the algorithms are in our life rather than profound concepts I used to consider. Basic events and details that we naturally neglect are arranged systematically and turned into well-regulated approaches to address problems efficiently. For example, the algorithm of calculating the shortest path is fundamental to the navigation function of mapping applications. It encouraged me to explore more theoretical and fundamental aspects behind applications.

In 2019, I participated in Euclid Contest (top 25%) and STEP 1 examinations (grade 1), harvesting quite good results. While I was preparing, I acquired extra mathematical knowledge beyond A-level syllabus and I found some of them were related to CS such as number theory, which is widely used in encryption, and helped me gain better comprehension when learning encryption algorithms. I also attended the BPhO competition and received a silver award, from which I got practice of logical thinking and problem-solving ability for science questions.

Gradually knowing more about complicated theories hidden behind seemingly simple computer operations, I long for comprehensive knowledge from tertiary education and determine to maintain the motivation for CS. I have got a strong desire for being one of game and AI industry staffs who establish and support surreal worlds in games.