JOHNS HOPKINS
CENTER *for* TALENTED YOUTH

CTY SUMMER PROGRAM FINAL EVALUATION

Student: Nikita Noskov
Course: Cryptology
Site: Carlisle, PA

Date: July 13, 2018
Instructor: Isaac Defrain
Teaching Assistant: Marcus Elia

Congratulations, Nikita, on successfully completing Cryptology. Please see the enclosed course description for more detailed information on the course.

Overall Performance
Your overall performance in this class was excellent. You developed a strong understanding of many of the concepts presented in this course, and you demonstrated this knowledge to your classmates in a clear, thoughtful manner. Your willingness to challenge yourself was refreshing, and your skill in synthesizing complex concepts quickly was impressive.

Content Proficiency
Your desire to learn led to a mastery of much of the content in this class. In addition to the course content, you solved many of the NSA challenge problems. Your care and attention to detail led to impressive results, like when you identified the key length during one of our Vigenère cipher activities. Even when you initially struggled, you worked hard to develop strong skills such as your proficiency with the Hill cipher and the group theory of permutations. The skills you have developed will improve your capacity for formal reasoning and will also help you be a better critical thinker and problem solver.

Reasoning and Problem Solving
Your reasoning and problem-solving skills were impressive. You reasoned out many concepts without having encountered them before. Your conversion to binary and use of bit rearrangement in your group's cryptosystem was genuinely original and even predated our discussion of digital encryption. Your reasoning for the placement of vowels in the ciphertext of a monoalphabetic substitution cipher was also quite insightful. Your skill at learning on your own and communicating your ideas clearly to others will continue to help you in all aspects of your life.

Collaboration and Participation
You were an active participant during all our lessons and discussions. You regularly asked interesting questions, answered questions that I posed, and offered to share your insights with the class. You were always an asset to your group during our decryption challenges. You worked well in your group while creating the SHIFR Cipher and made sure to incorporate everyone's ideas. You eloquently presented an example of encryption with your cipher to the other Cryptology class.

Suggestions and Recommendations
Your exemplary performance demonstrates that you have great potential in the areas of mathematics and computer science. I encourage you to expand your knowledge of topics such as linear algebra, abstract algebra, statistics, number theory, computer programming, and the related fields of physics and engineering, among others, to find what subject most sparks your interest. I am confident you will make great contributions to the realm of mathematics and computer science if you continue in your pursuits.

Nikita, it was a true pleasure having you in the class. Marcus and I wish you the best of luck in the future!

Johns Hopkins Center for Talented Youth
Course Description: Cryptology

Course Code: 18S.CODE.CAR.1B Instructor: ISAAC DEFRAIN

Cryptology was part of the 2018 Center for Talented Youth (CTY) Summer Residential Program held in Carlisle, Pennsylvania. The course met for three weeks, five hours per day, five days per week, and students attended a two-hour homework session five nights per week, supervised by the instructor or teaching assistant. There were at least 100 contact hours with the discipline.

Information is power. Even before the first written word, the need to safeguard information created an ongoing evolutionary battle between codemakers and codebreakers.

Cryptology is the study of secret writing such as codes and ciphers. In this course, students began their journey with an introduction to many early techniques for creating secret writing, such as cipher wheels, the Caesar shift, monoalphabetic substitution, and the Vigenere cipher. They moved on to learn about modern techniques including RSA public key cryptography. Delving deeper into modern techniques, students explored how data transmitted by computer can be secured with digital encryption which ultimately led to a discussion of blockchain technology. Analyzing the vulnerabilities of each encryption system enabled students to attack and decrypt messages using techniques such as frequency analysis and cribbing. Students applied what they learned to build their own cryptosystem and analyze it for vulnerabilities.

The historical context of cryptography and cryptographic devices was provided to further develop understanding of this branch of mathematics. For example, students examined the design and fallibility of the Enigma Machine, one of the most important cryptographic devices in history.

The text used in this course was *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* by Simon Singh.