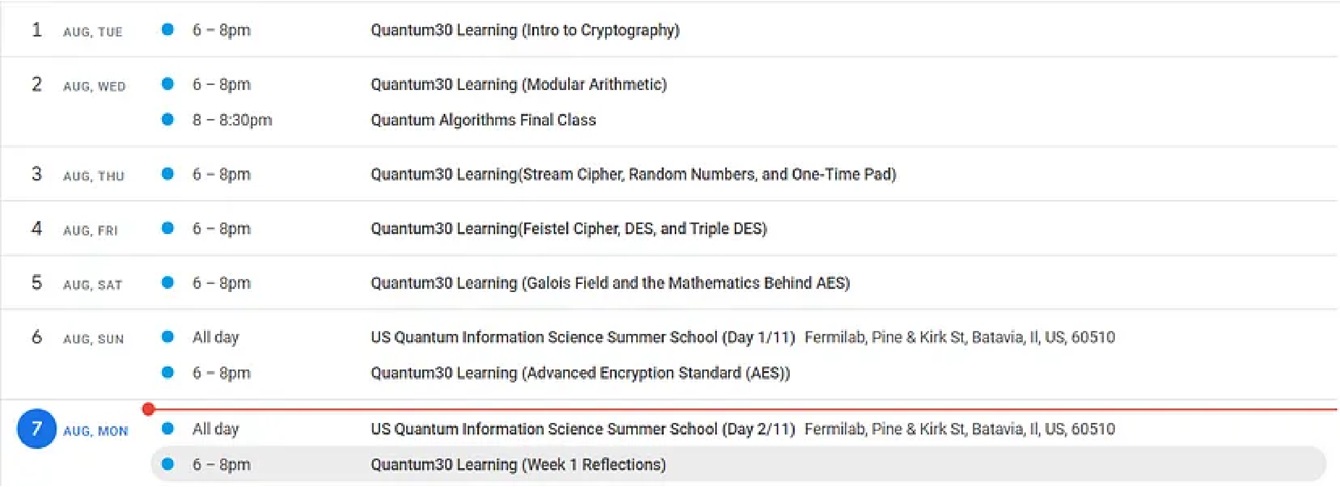
Week 1 Reflections: A Journey into the Fascinating World of Cryptography

WOMANIUM GLOBAL ONLINE QUANTUM MEDIA PROJECT #Quantum30 Challenge Day 7

Introduction:

As the first week of our exciting journey into the realm of cryptography completes, it’s time to reflect on the whirlwind of knowledge we’ve absorbed. This week has been nothing short of enlightening, as we delved into the fundamental concepts and techniques that underpin the art and science of securing information. From the very basics of cryptography to the intricacies of advanced encryption algorithms, each day has been a step forward in understanding the magic behind safeguarding our digital world.



1	AUG, TUE	6 – 8pm	Quantum30 Learning (Intro to Cryptography)	
2	AUG, WED	6 – 8pm	Quantum30 Learning (Modular Arithmetic)	
		8 – 8:30pm	Quantum Algorithms Final Class	
3	AUG, THU	6 – 8pm	Quantum30 Learning(Stream Cipher, Random Numbers, and One-Time Pad)	
4	AUG, FRI	6 – 8pm	Quantum30 Learning(Feistel Cipher, DES, and Triple DES)	
5	AUG, SAT	6 – 8pm	Quantum30 Learning (Galois Field and the Mathematics Behind AES)	
6	AUG, SUN	All day	US Quantum Information Science Summer School (Day 1/11)	Fermilab, Pine & Kirk St, Batavia, Il, US, 60510
		6 – 8pm	Quantum30 Learning (Advanced Encryption Standard (AES))	
7	AUG, MON	All day	US Quantum Information Science Summer School (Day 2/11)	Fermilab, Pine & Kirk St, Batavia, Il, US, 60510
		6 – 8pm	Quantum30 Learning (Week 1 Reflections)	

Week 1 Reflections

Day 1: Introduction to Cryptography

Our journey began with a comprehensive *introduction to cryptography*, laying the groundwork for the weeks ahead. We explored the historical context, the importance of encryption, and the various types of cryptography. The concepts of *plaintext, ciphertext, encryption, and decryption* were demystified, providing us with a solid foundation to build upon.

Day 2: Modular Arithmetic

Day two introduced us to the intriguing world of M*odular Arithmetic* — a crucial tool in modern cryptography. We learned how to perform arithmetic operations within a finite set of numbers, and how this concept plays a pivotal role in the creation of cryptographic algorithms. Modular arithmetic not only challenged our mathematical thinking but also opened our eyes to the creativity required in designing secure encryption schemes.

Day 3: Stream Cipher, Random Numbers, and One-Time Pad

This day we have expanded our horizons with an exploration of *Stream Ciphers* and the significance of *Random Numbers* in cryptography. The concept of a *One-Time Pad*, a theoretically unbreakable encryption scheme when used correctly, left us in awe of its simplicity and effectiveness. We understood the delicate balance between security and practicality in implementing these techniques.

Day 4: Feistel Cipher, DES, and Triple DES

The fourth day saw us dive deeper into block ciphers, with a focus on the *Feistel Cipher* structure. The *Data Encryption Standard (DES)* and its successor, *Triple DES*, showcased how cryptographic algorithms evolve to meet the growing challenges of security. We uncovered the architecture behind these algorithms and their contributions to modern encryption protocols.

Day 5: Galois Field and the Mathematics Behind AES

Our exploration of mathematics continued on day five as we ventured into *Galois Fields*. We discovered their role in constructing complex algebraic structures that power modern encryption techniques. This mathematical foundation served as a bridge to understanding the *Advanced Encryption Standard (AES)*, a cornerstone of modern cryptography. The intricate mathematics behind AES left us in awe of the brilliant minds that crafted these algorithms.

Day 6: Advanced Encryption Standard (AES)

The final day of the week was dedicated entirely to *AES*, one of the most widely used and respected encryption standards in the world. We delved into its mechanics, from key expansion to the various transformation rounds, witnessing how its combination of substitution, permutation, and mixing provides unparalleled security. Understanding AES marked a significant milestone in our journey, showcasing the culmination of mathematical concepts and practical implementation.

. . .

Looking Ahead:

As we bid adieu to our first week, it's evident that the road ahead is filled with more discoveries and challenges. Cryptography, as we have learned, is a multifaceted discipline that requires a deep understanding of mathematics, logic, and creativity. With topics like public-key cryptography, digital signatures, and cryptographic protocols still awaiting us in the coming weeks, our anticipation grows to uncover the secrets of secure communication in the digital age.

In Conclusion:

Week 1 of our cryptography expedition has been an exhilarating journey, one that has laid a strong foundation for the weeks to come. From the ancient art of concealing messages to the cutting-edge algorithms that safeguard our online interactions, we've explored the depths of cryptography's history and its mathematical underpinnings. As we move forward, we carry with us the knowledge and insights gained during this initial phase, excited to unravel the mysteries of cryptographic techniques yet to be unveiled.

. . .

I have been exploring Cryptography since the start of this month and throughout this month I will gain in-depth knowledge of this field. Your suggestion will be really helpful for my future endeavor.

This is a part of **WOMANIUM GLOBAL ONLINE QUANTUM MEDIA PROJECT**. This project will help me to dive into the cryptographic world(From Classical to Quantum Approach). From onwards I shall share my learning log with others who are curious about this particular and promising field.

I want to take a moment to express my gratitude to **Marlou Slot** and **Dr. Manjula Gandhi** for this initiative and encouragement and sincere thanks to **Moses Sam Paul Johnraj** for providing the 30-day schedule.

Written by Murshed SK

Physics Undergrad | Quantum Information Science and Computation Enthusiast | Passionate about Quantum Machine Learning | <Womanium | Quantum> Scholar