

## MCS 210 - Writing Assignment 5

1. This is a reading comprehension writing assignment that will evolve as we read and discuss the book titled "The Code Book" by Simon Singh. I strongly suggest you answer questions as soon as you complete the chapters indicated for each question, rather than waiting to finish the book.
  2. Answer the questions in the next page after reading the corresponding book chapters. Your answers must be written in your own words; do not copy from the book. Answers should be clear and organized, not overly verbose but not too simplistic either.
  3. Create an Overleaf project named MCS210\_WA5
  4. When you have finished writing your revised responses, download your project from Overleaf as a .zip file and submit via Moodle.
- 

### Questions for Chapters 3 and 4:

1. How did the invention of the radio change cryptology?
2. What are the strengths of a one-time pad cipher? Why are they not frequently used?
3. Explain how the enigma cipher works.
4. What is a Turing machine?
5. What impact did cryptology have on World War 2?

### Questions for Chapter 5 and 6:

6. How did the method described in ch 5 fundamentally differ from other methods employed at the time?
7. How did programmable computers change cryptology?
8. Why is key distribution important? Why is it challenging?
9. What is special about RSA?

### Questions for Chapter 7:

10. This book was written in 1999. Based on the writing in this chapter, what has changed with technology since then?
11. Why is cryptology particularly important for the internet?