This exam contains

- this cover (page 1),
- four pages of problems (pages 2-5), and
- one blank page (after page 5).

You have 60 minutes. No notes, calculator, computer, etc. are allowed.

Feel free to ask clarification questions during the exam. If you feel that there is a mistake in how a question is posed, then certainly ask for clarification.

Always show your work or otherwise explain your answer. A correct answer with no supporting argument may not earn much credit.

Good luck.

1. After the $(7, 4)$ Hamming code, what is the next Hamming code, in order of increasing size? Do not write the E, D, and C matrices, but give their sizes, and list the crucial algebraic relationships that must hold among them, for the Hamming code to work.

2. After that Hamming code, what is the next one? Again give the sizes of E, D, and C, and list the crucial relationships among them.

3. I'm setting up a starter RSA key set for my daughter, as a gift for her first birthday. I've chosen $p = 23$, $q = 29$, and $e = 15$. Is this e suitable? If not, why not? If so, then what's d?

You're scheduling a singles badminton tournament. Let's call the players $p_1, p_2, \ldots, p_n$. They will play *round-robin*, meaning that every possible matchup between players will happen exactly once. At the end of the tournament, you'll produce a *summary*, that lists the result of each game. The order of the games within the summary, and the order of the players within each game in the summary, are not meaningful.

4. How many summaries are possible, if a summary does not include the scores?

5. How many summaries are possible, if a summary does include the scores? (A badminton game is played to 21 points. For simplicity, assume that it is possible to win by 1 point.)

6. Recall that the 4-bit doubling code is an error-correcting code that encodes any 4-bit message into an 8-bit codeword by simply repeating the 4-bit message. For example, 0111 encodes to 01110111. Assume that there is a 1% chance of error on each of the 8 bits in transmission, and that these probabilities are independent. I send you a message using this code, and you receive a valid codeword. What is the probability that no error occurred in the transmission of the message? Simplify your answer.