This homework is due on **May 4, 9am ET**.

You are welcome to work with others, however you must explicitly list all collaborators and materials that you used. You must write up your own solution and your own code to every problem. See Georgetown University Honor System. When in doubt, ask the instructor what is allowed.

Problem 1 (Error correcting codes)**.** Use results from Lecture 19 (on Error Correcting Codes) to design an algorithm for the following game. I choose a number from 1 to 16. You can ask yes-no questions, and I'll lie on all or all but one question. Design an algorithm that finds my number using as few questions as possible. (For the full score, prove that there is an algorithm that always asks at most 7 questions.)

Problem 2 (Substitution ciphers)**.** In the class we saw that even though subsitution ciphers have reasonably long keys, they are not secure. Decode the following ciphertext encrypted by a substitution cipher.

> S ilqa l ocaln jilj pxa olh jisr xljspx esmm csra tb lxo msqa ptj jia jcta nalxsxu py sjr wcaao: Ea ipmo jiara jctjir jp fa ramy-aqsoaxj, jilj lmm nax lca wcaljao adtlm. S ilqa l ocaln jilj pxa olh px jia cao ismmr py Uapcusl, jia rpxr py ypcnac rmlqar lxo jia rpxr py ypcnac rmlqa pexacr esmm fa lfma jp rsj opex jpuajiac lj jia jlfma py fcpjiacippo. S ilqa l ocaln jilj pxa olh aqax jia rjlja py Nsrrsrrsbbs, l rjlja reamjacsxu esji jia ialj py sxvtrjswa, reamjacsxu esji jia ialj py pbbcarrspx esmm fa jclxrypcnao sxjp lx plrsr py ycaaopn lxo vtrjswa. S ilqa l ocaln jilj nh yptc msjjma wismocax esmm pxa olh msqa sx l xljspx eiaca jiah esmm xpj fa vtouao fh jia wpmpc py jiasc rksx ftj fh jia wpxjaxj py jiasc wilclwjac. S ilqa l ocaln jpolh.

Feel free to use tools that count frequency of characters in the ciphertext, letter/digram frequency tables (e.g., here), common sense, or implement any tools in your favorite programming language. Name the author of this text, and explain how you arrived at the solution.

Problem 3 (Breaking RSA)**.** Implement four attacks from Lecture 23 on the Textbook RSA to solve the following puzzle: https://colab.research.google.com/drive/1E-6MCkqlY-BEb5VpqChC33WalOQ1Neb6?usp=sharing