Math 351 Homework 5

Due Monday, October 31 at 5pm

Solutions should be written LaTeX or Markdown and converted to a PDF. You are encouraged to work with others on the assignment, but you should write up your own solutions independently. This means no copy pasting. You should reference all of your sources, including your collaborators.

(1) Compute the last two digits of 3^{45}.

(2) Prove that there is no primitive root modulo 2^n for any $n \geq 3$.

(3) Find the integer a such that $0 \leq a < 113$ and

$$102^{70} + 1 \equiv a^{37} \pmod{113}.$$

(4) Using the RSA public key $(n, e) = (441484567519, 238402465195)$, encrypt the current year.

(5) Suppose Michael creates an RSA cryptosystem with a very large modulus n for which the factorization of n cannot be found in a reasonable amount of time. Suppose that Nikita sends messages to Michael by representing each alphabetic character as an integer between 0 and 26 (`A` corresponds to 1, `B` to 2, etc., and a space ␣ to 0), then encrypts each number *separately* using Michael's RSA cryptosystem. Is this method secure? Explain your answer.