EXAM #1A
MATH V3025 Making, Breaking Codes
(D. Goldfeld, 10/3/2017)

NAME: ______________________________________, E-mail ________________________

Do all of the following problems. Each problem is worth 10 points. Only a simple basic non-graphing calculator is allowed. Please NEATLY write out all answers (with explanations) on these sheets.

Problem 1: We use the correspondence $A \to 0,\ B \to 1,\ C \to 2,\ \ldots,\ Z \to 25$. Let $K = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ where $0 \le a, b, c, d < 26$. In the Hill cipher, we encrypt a message (x, y) (where $0 \le x, y < 26$) to

$$\mathcal{E}((x, y)) = (x, y) \cdot K \ \big(\text{mod} 26\big).$$

What is the decryption function $\mathcal{D}((x, y))$? Suppose the key is $K = \left(\begin{smallmatrix} 2 & 9 \\ 5 & 7 \end{smallmatrix}\right)$ and the encryption of a plain text message is {2, 15} = {C, P}. What is the plain text message?

Answer:

Problem 2:

(a) Alice and Bob are using RSA in a network. Alice's RSA modulus is $n_{\mathrm{A}} = 2059$, and Bob's is $n_{\mathrm{B}} = 1633$. Suppose that n_{A} and n_{B} are each a product of two primes and $\gcd(n_{\mathrm{A}}, n_{\mathrm{B}}) > 1$. Find the factorization of n_{A} and n_{B} using the Euclidean algorithm.

Show all work. Just producing an answer without any computations gets zero points.

Answer:

(b) Suppose Alice's public encryption key is e_{A}. Find an integer $1 < r$ such that Alice's decryption key d_{A} can be written in the form

$$d_{\mathrm{A}} \equiv e_{\mathrm{A}}^{-1} \pmod{r}.$$

Answer:

Problem 3: Find a solution $1 \leq x \leq 105$ for the system of congruences:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ 2x &\equiv 3 \pmod 5 \\ x &\equiv 5 \pmod 7 \end{aligned}$$

Show all work. Just producing an answer without any computations gets zero points.

Answer:

Problem 4:

(a) Fix an integer $n > 1$. Let $S_n := \{a_1, a_2, \ldots, a_{\phi(n)}\}$, where the a_i are distinct and coprime to n. Sketch a proof of the fact that for every integer $1 \leq y < n$ with $\mathrm{GCD}(y, n) = 1$ the set

$$y \cdot S_n \pmod{n} \;:=\; \Big\{a_1 y \pmod{n},\ a_2 y \pmod{n},\ \ \ldots,\ \ a_{\phi(n)} y \pmod{n}\Big\}$$

is just a reordering of S_n.

Answer:

(b) Use the above to prove Euler's extension of Fermat's Little Theorem.

Answer:

Problem 5: Briefly describe the El Gamal encryption algorithm. You must state the public information, the secret decryption key, and the algorithm for encrypting and decrypting messages.

Answer:

Problem 6: Find an integer $x > 1$ such that

$$3^{2x} \equiv 1 \pmod{1225}.$$

Explain your reasoning. Just producing an answer without any explanation gets zero points.

Answer: