FINAL EXAM-A
MATH V3025 Making, Breaking Codes
(D. Goldfeld, 12/21/2017)

NAME: ________________________________, E-mail ________________________

Do all of the following problems. Each problem is worth 7 points. Only a simple basic non-graphing calculator is allowed. Please NEATLY write out all answers (with explanations) on these sheets.

Problem 1: Let $n = 299797 = pq$ be a product of two primes p, q. Suppose you know that

$$2122^2 - 77^2 \equiv 0 \pmod{n}.$$

Find p and q. <u>You must use the Euclidean algorithm to solve this problem.</u> Show all work. Just producing an answer gets zero points.

Answer:

Problem 2:

(a) *(3 points)* Show that if $\mathrm{GCD}(e, 24) = 1$, then $e^2 \equiv 1 \pmod{24}$.

(b) *(4 points)* Show that if $n = 35$ is used as an encryption modulus for RSA then the encryption exponent e is always the same as the decryption exponent d.

Answer:

Problem 3:

(a) *(2 points)* Explain why the polynomial $x^2 + x + 2$ is irreducible over $\mathbb{F}_3$, the finite field of 3 elements.

Answer:

(b) *(5 points)* Using the polynomial $x^2 + x + 2$ compute the square of every element in the finite field of 9 elements.

Answer:

Problem 4: Explain the Pollard $p-1$ attack on RSA.

Answer:

Problem 5: Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over a finite field $\mathbb{F}_p$ where p is a prime. The addition law on E is given by $(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3)$ where $x_3 = m^2 - x_1 - x_2,\ y_3 = m(x_1 - x_3) - y_1$. Here

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } (x_1 y_1) \neq (x_2, y_2) \\ \frac{3x_1^2 + a}{2y_1} & \text{if } (x_1 y_1) = (x_2, y_2). \end{cases}$$

(a) *(3 points)* Find all points on the elliptic curve $E : y^2 = x^3 - x + 6$ over $\mathbb{F}_7$.

Answer:

(b) *(4 points)* Suppose Alice and Bob want to use $E : y^2 = x^3 - x + 6$ over $\mathbb{F}_7$ for elliptic curve Diffie-Hellman key exchange, with $P = (3, 4)$. If Alice chooses a secret multiplier $n_A = 2$ and Bob chooses multiplier $n_B = 3$, what is the key they agree on?

Answer:

Problem 6: Let p be a 200 digit prime and let g be a primitive root (mod p). Assume that Alice chooses a secret number $1 < a < p$ and Bob chooses a secret number $1 < b < p$.

(a): *(3 points)* Explain the Diffie-Hellman key agreement protocol using p, g, a, b as above.

(b): *(4 points)* Assume that p is such that 13 divides $p - 1$. Explain why $a = \frac{p-1}{13}$ would be a bad choice for Alice.

Hint: *Pohlig-Hellman attack.*

Problem 7:

(a) *(2 points)* Define the Hamming distance between 2 codewords in a binary code C and the Hamming distance $d(C)$ of the binary code C.

Answer:

(c) *(5 points)* Show that if $d(C) = 2s + 1$ (for some integer s) then the binary code C can correct up to s errors.

Problem 8: Consider the [5,2] linear code (over $\mathbb{F}_2$) determined by the generating matrix $G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$.

(a) *(4 points)* Determine all cosets (list the elements of each coset) and their syndromes.

Answer:

(b) *(1 point)* How many errors can this code correct? (Explain briefly).

Answer:

(c) *(2 points)* Assume that 11110 is received in a transmission. Show that 11110 is not a valid code word. Correct it using syndrome decoding.

Answer:

Problem 9: For a certain binary linear code, the following 6-bit sequences are all valid code words: $c_1 = 110011$, $c_2 = 011110$, $c_3 = 100110$, and $c_4 = 111000$.

(a) *(5 points)* List the minimum number of all valid codewords for this linear code and find a generator matrix G for the code.

Answer:

(b) *(2 points)* For the generator matrix G of part (a), write down the corresponding parity check matrix for this code.

Answer:

Problem 10:

(a) *(2 point)* Define a cyclic $[n, k]$ binary code.

Answer:

(b) *(5 points)* Let $g(x) = 1 + x^2 + x^3 \in \mathbb{F}_2[x]$ which divides $x^7 - 1$. Find all the codewords in the cyclic $[7, 4]$ binary code generated by $g(x)$.

Answer: