Midterm #2

MATH 481/581 — Cryptography
Monday, April 13, 2026

Please print your name:

No notes, calculators or tools of any kind are permitted. There are 36 points in total. You need to show work to receive full credit.

Good luck!

Problem 1. (4 points) Alice and Bob select $p = 19$ and $g = 10$ for a Diffie–Hellman key exchange. Alice sends 3 to Bob, and Bob sends 12 to Alice. What is their shared secret?

Problem 2. (3 points) Bob's public RSA key is $N = 21$, $e = 5$. Determine Bob's secret private key.

Problem 3. (3 points) Bob's public ElGamal key is $(p, g, h) = (11, 6, 3)$. Determine Bob's secret private key.

Armin Straub
straub@southalabama.edu

Problem 4. (4 points) Consider the (silly) block cipher with 3 bit block size and 3 bit key size such that

$$E_k(b_1b_2b_3) = (b_2b_1b_3) \oplus k.$$

Encrypt $m = (100\ 100\ 111\ldots)_2$ using $k = (110)_2$ and CBC mode ($\mathrm{IV} = (111)_2$).

Problem 5. (3+4 points) Consider the finite field $\mathrm{GF}(2^4)$ constructed using $x^4 + x + 1$.

(a) Multiply x^3 and $x^3 + x^2$ in $\mathrm{GF}(2^4)$.

(b) Determine the inverse of x^3 in $\mathrm{GF}(2^4)$.

Armin Straub
straub@southalabama.edu

Problem 6. (15 points) Fill in the blanks.

(a) Bob's public RSA key is $N=21$, $e=5$. Using that, Alice encrypts $m=2$ to $c=$ ☐.

(b) For his public RSA key, Bob selected $N=55$. The smallest choice for e with $e \geqslant 2$ is ☐.

(c) Bob's public ElGamal key is (p, g, h). To send m to Bob, we encrypt it as

$c=$ ☐. (Indicate if any random choices are involved.)

(d) For his ElGamal key, which of p, g and x must Bob choose randomly? ☐

(e) For a public ElGamal key, Bob selected $p=29$. He has ☐ choices for g.

(f) The computational Diffie–Hellman problem is: given ☐, determine ☐.

(g) DES has a block size of ☐ bits, a key size of ☐ bits and consists of ☐ rounds.

(h) 3DES (with independent DES keys) has a key size of ☐ bits. The effective key size is ☐ bits.

(i) AES-128 has a block size of ☐ bits. AES-256 has a block size of ☐ bits.

(j) Which is the only nonlinear layer of AES? ☐

(k) 6 is a primitive root modulo 13. For which x is 6^x a primitive root modulo 13? ☐

(l) If x has (multiplicative) order 45 modulo m, then x^6 has order ☐.

(m) As part of the Miller–Rabin test, it is computed that $70^{47} \equiv 307$, $70^{94} \equiv 376$, $70^{188} \equiv 1 \pmod{377}$.

What do we conclude? ☐

(n) Up to x, there are roughly ☐ many primes.

(o) The approximate proportion of primes among numbers up to 2^{1024} is ☐. (Simplify!)

(extra scratch paper)