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 35 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?

Solution. If Alice's secret is y and Bob's secret is x, then $10^y \equiv 3$ and $10^x \equiv 12 \pmod{19}$.

We compute $10^2, 10^3, \dots$ until we find either 3 or 12:

$10^2 \equiv 5$, $10^3 \equiv 50 \equiv 12 \pmod{19}$.

Hence, Bob's secret is $x=3$. The shared secret is $g^{xy} = (10^y)^x = 3^3 \equiv 8 \pmod{19}$.

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

Solution. $N = 3 \cdot 7$, so that $\phi(N) = 2 \cdot 6 = 12$.

The private key is $d = e^{-1} = 5^{-1} = 5 \pmod{12}$.

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

Solution. We need to solve $6^x \equiv 3 \pmod{11}$. This yields $x=2$.

(Since we haven't learned a better method (no "good" method is known!), we try $x=2,3,4,\dots$ until we find the right one.)

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 ($\mathrm{IV} = (111)_2$).

Solution. $m = m_1m_2m_3\ldots$ with $m_1 = m_2 = 100$ and $m_3 = 111$.

$c_0 = 111$

$c_1 = E_k(m_1 \oplus c_0) = E_k(100 \oplus 111) = E_k(011) = 101 \oplus 110 = 011$

$c_2 = E_k(m_2 \oplus c_1) = E_k(100 \oplus 011) = E_k(111) = 111 \oplus 110 = 001$

$c_3 = E_k(m_3 \oplus c_2) = E_k(111 \oplus 001) = E_k(110) = 110 \oplus 110 = 000$

Hence, the ciphertext is $c = c_0c_1c_2c_3\ldots = (111\ 011\ 001\ 000\ \ldots)$.

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 $\mathrm{GF}(2^4)$.

Solution.

(a) $x^3(x^3 + x^2) = x^6 + x^5 = x^3 + x^2$ in $\mathrm{GF}(2^4)$ where in the final step we perform long division to find that $x^6 + x^5$ divided by $x^4 + x + 1$ is $x^2 + x$ with remainder $x^3 + x$ (this is reduced modulo 2; without reducing modulo 2, the remainder is $-x^3 - 2x^2 - x$).

(b) We use the extended Euclidean algorithm, and always reduce modulo 2:

$$\begin{aligned} \boxed{x^4+x+1} &\equiv x \cdot \boxed{x^3} + (x+1) \\ \boxed{x^3} &\equiv (x^2+x+1) \cdot \boxed{x+1} + 1 \end{aligned}$$

Backtracking through this, we find that Bézout's identity takes the form

$$\begin{aligned} 1 &\equiv \boxed{x^3} + (x^2+x+1) \cdot \boxed{x+1} \equiv \boxed{x^3} + (x^2+x+1)\left(\boxed{x^4+x+1} + x \cdot \boxed{x^3}\right) \\ &\equiv (x^3+x^2+x+1)\boxed{x^3} + (x^2+x+1)\boxed{x^4+x+1} \end{aligned}$$

Hence, $(x^3)^{-1} = x^3 + x^2 + x + 1$ 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 $\boxed{}$ many primes.

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

Solution.

(a) $c = m^e = 2^5 = 32 \equiv 11 \pmod{21}$

(b) Since $\phi(55) = 40$, the smallest choice for e (we need $\gcd(e, 40) = 1$) with $e \geqslant 2$ is 3.

(c) Bob's public ElGamal key is (p, g, h). To send m to Bob, we encrypt it as $c = (g^y, h^y m)$ (all modulo p), where y was randomly chosen.

(d) x must be chosen randomly.

(e) He has $\phi(\phi(29)) = \phi(28) = \phi(2^2)\phi(7) = (2^2 - 2^1) \cdot 6 = 12$ choices for g.

(f) The CDH problem is the following: given $g, g^x, g^y \pmod{p}$, find $g^{xy} \pmod{p}$.

(g) DES has a block size of 64 bits, a key size of 56 bits and consists of 16 rounds.

(h) 3DES (with independent DES keys) has a key size of $3 \cdot 56 = 168$ bits. The effective key size is 112 bits (because of the meet-in-the-middle attack).

(i) AES-128 and AES-256 both have a block size of 128 bits.

(j) The nonlinear layer of AES is ByteSub.

(k) 6^x a primitive root modulo 13 if and only if $\gcd(x, 12) = 1$. These x (modulo 12) are $1, 5, 7, 11$. (The total number is $\phi(\phi(13)) = \phi(12) = \phi(4)\phi(3) = (4-2)(3-1) = 4$.)

(l) If x has (multiplicative) order 45 modulo m, then x^6 has order $45 / \gcd(6, 45) = 15$.

(m) Since $70^{94} \equiv 376 \equiv -1 \pmod{377}$, we conclude that 377 is likely prime.

(However, $377 = 13 \cdot 29$ is not a prime which means that 70 is a strong liar.)

(n) Up to x, there are roughly $x / \ln(x)$ many primes.

(o) By the prime number theorem, there are roughly $2^{1024}/\ln(2^{1024})$ primes up to 2^{1024}. Hence, the proportion of primes among numbers up to 2^{1024} is roughly $\frac{2^{1024}/\ln(2^{1024})}{2^{1024}} = \frac{1}{\ln(2^{1024})} = \frac{1}{1024 \cdot \ln(2)}$.

Comment. $\frac{1}{1024 \cdot \ln(2)} \approx \frac{1}{709.8}$. This means that, roughly, 1 in 710 numbers with 1024 bits is a prime.

(extra scratch paper)