

MIDTERM EXAM
MATH V3025Y Making, Breaking codes
(D. Goldfeld, 3/13/2008)

NAME: _____, e-mail _____

Do all of the following problems. Each problem is worth 5 points. Please NEATLY write out all answers (with explanations) on these sheets.

Problem 1: We use the correspondence $A \rightarrow 0, B \rightarrow 1, C \rightarrow 2, \dots, Z \rightarrow 25$. Let $K = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $0 \leq a, b, c, d < 26$. In the Hill cipher, we encrypt a message (x, y) (where $0 \leq x, y < 26$) to $E((x, y)) = (x, y) \cdot K \pmod{26}$. What is the decryption function $D((x, y))$? Suppose the key is $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$ and the encryption of a plain text message is DELW. What is the plain text message?

Answer:

$$K^{-1} \equiv \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix} \pmod{26} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}.$$

So

$$D((x, y)) = (x, y) \cdot \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \pmod{26}.$$

Now $\text{DELW} = \{3, 4, 11, 22\}$. We first decrypt the first bloc which is $(3, 4)$. Then

$$\begin{aligned} D((3, 4)) &= (3, 4) \cdot \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \pmod{26} \\ &\equiv (113, 98) \pmod{26} \\ &= (9, 20) \\ &= JU \end{aligned}$$

Next, we decrypt the second block $(11, 22)$.

$$\begin{aligned} D((11, 22)) &= (11, 22) \cdot \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \pmod{26} \\ &\equiv (583, 440) \pmod{26} \\ &= (11, 24) \\ &= LY \end{aligned}$$

Therefore, the plaintext message is JULY.

Problem 2: Show that $x^2 + 2x + 2$ is irreducible over \mathbb{F}_3 , the finite field of 3 elements. Consider the finite field of 9 elements consisting of all polynomials in

$$\mathbb{Z}_3[x] \pmod{(x^2 + 2x + 2)}.$$

Compute $(x + 1)^{-1}$ in this field.

Answer:

Let $p(x) = x^2 + 2x + 2$. Then $p(0) = 2$, $p(1) = 2$, $p(2) = 1$. Since $p(x)$ has no roots in \mathbb{F}_3 it must be irreducible in \mathbb{F}_3 .

Let $q(x) = ax + b = (x + 1)^{-1}$. Then

$$(ax + b) \cdot (x + 1) \equiv 1 \pmod{(x^2 + 2x + 2)},$$

which implies

$$ax^2 + (a + b)x + b \equiv 1 \pmod{(x^2 + 2x + 2)}.$$

It follows that

$$ax^2 + (a + b)x + b = \ell \cdot (x^2 + 2x + 2) + 1$$

with $\ell = 0, 1$, or 2 . Consequently

$$a = \ell, \quad a + b = 2\ell, \quad b = 2\ell + 1.$$

There are no solutions to the above unless $\ell = 2$. In this case we have

$$a = 2, \quad b = 2.$$

Consequently:

$$\boxed{(x + 1)^{-1} = 2x + 2.}$$

Problem 3: Consider the RSA encryption algorithm with $N = pq$, the product of two large primes, and e the public key. An attacker (Eve) doesn't know the decryption key but sees the encryption of a message $1 < m < N$. Suppose someone tells Eve that m is divisible by p . Does this information help Eve? Explain.

Answer:

Let $E(m)$ denote the encryption of m with the RSA key e . Then

$$E(m) \equiv m^e \pmod{N}.$$

If Eve knows that $m = pm'$ for some integer m' then this implies that

$$E(m) = p^e m'^e + \ell pq$$

for some integer ℓ . Consequently $p|E(m)$. If q does not divide $E(m)$, then Eve can obtain p by computing the GCD of $E(m)$ and N . This would break RSA in this case.

Problem 4: Describe the El Gamal public key cryptosystem.

Answer:

Fix a large prime p and a primitive root $1 < g < p$.

Alice's public key is the triple: $\{p, g, a \equiv g^x \pmod{p}\}$.

Alice's private key is $1 < x < p$.

To encrypt a message $1 < m < p$, Bob randomly chooses $1 < k < p$ and computes:

$$r \equiv g^k \pmod{p}, \quad s \equiv a^k \cdot m \pmod{p}.$$

He sends the encrypted message: $E(m) = \{r, s\}$, to Alice.

To decrypt the message $E(m)$, Alice computes

$$m \equiv r^{-x} \cdot s \pmod{p}.$$

Problem 5: In the El Gamal signature scheme Alice starts with a prime $p = 563$. Her public key is 168 which is of the form $168 \equiv 2^x \pmod{563}$ and her secret key is x . To compute a digital signature (r_i, s_i) of a message m_i , Alice performs the following steps:

- (1) Alice selects a random k_i with $GCD(k_i, p - 1) = 1$.
- (2) Alice computes $r_i \equiv 2^{k_i} \pmod{p}$.
- (3) Alice computes $s_i \equiv k_i^{-1}(m_i - xr_i) \pmod{p - 1}$.

Alice computes the digital signature $(r_1, s_1) = (73, 449)$ for the message $m_1 = 10$, and later computes the digital signature $(r_2, s_2) = (292, 38)$ for the message $m_2 = 20$. Eve notices that $292 = 4 \times 73$. Show that this implies that $k_2 = k_1 + 2$ making Eve realize she can find k_1 . What is k_1 ?

Hint: $36 \cdot 242 \equiv 1 \pmod{281}$.

Answer:

If $k_2 = k_1 + 2$ then

$$r_1 \equiv 2^{k_1} \pmod{p}, \quad r_2 \equiv 2^{k_1+2} \pmod{p} \equiv 4r_1 \pmod{p}.$$

Using (3), Eve deduces that

$$449k_1 \equiv 10 - xr_1 \pmod{562},$$

which implies:

$$1796k_1 \equiv 40 - 4xr_1 \pmod{562},$$

Further

$$38(k_1 + 2) \equiv 20 - 4xr_1 \pmod{562}.$$

Subtracting the above 2 equations gives

$$1758k_1 - 76 \equiv 20 \pmod{562},$$

which is equivalent to

$$879k_1 \equiv 48 \pmod{281}$$

or

$$36k_1 \equiv 48 \pmod{281}.$$

Using the hint,

$$\boxed{k_1 \equiv 242 \cdot 48 \pmod{281} = 95.}$$

Problem 6: 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

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

Consider the point $(1, 2)$ on the elliptic curve $y^2 = x^3 + 2x + 1$ defined over \mathbb{F}_5 . Compute the value of $3 \cdot (1, 2) = (1, 2) \oplus (1, 2) \oplus (1, 2)$.

Answer:

We first compute $(1, 2) \oplus (1, 2)$. In this case

$$m \equiv (3 + 2) \cdot 4^{-1} \pmod{5} = 0$$

$$x_3 \equiv 0^2 - 1 - 1 \pmod{5} = 3.$$

$$y_3 \equiv 0 \cdot (1 - 4) - 2 \pmod{5} = 3.$$

Consequently

$$\boxed{(1, 2) \oplus (1, 2) = (3, 3).}$$

Next, we compute

$$3 \cdot (1, 2) = (3, 3) \oplus (1, 2).$$

In this case, we have:

$$m \equiv (3 - 2) \cdot (3 - 1)^{-1} \pmod{5} = 3.$$

$$x_3 \equiv 3^2 - 3 - 1 \pmod{5} = 0.$$

$$y_3 \equiv 3 \cdot (3 - 0) - 3 \pmod{5} = 1.$$

Consequently

$$\boxed{3 \cdot (1, 2) = (0, 1).}$$

Problem 7: Find all points (including the point at ∞) that are on the elliptic curve $y^2 = x^3 + x + 2$ over the finite field \mathbb{F}_3 ? Can any of these points have order 3? Can any of these points have order 4?

Answer:

The points on $E(\mathbb{F}_3)$ are

$$\boxed{\infty, (1,1), (1,2), (2,0).}$$

None of these points can have order 3 because the group is of order 4. We know that

$$(2,0) \oplus (2,0) = \infty,$$

so the point $(2,0)$ has order 2. The points $(1,1)$ and $(1,2)$ are not of order 2, so they must have order 4.