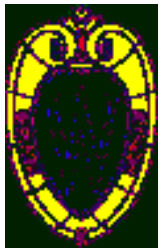


CS/ECE/Math 435
Introduction to Cryptography

Professor Chris DeMarco
Department of Electrical & Computer Engineering
University of Wisconsin-Madison

Spring Semester 2021

Kaltura My Media

canvas.wisc.edu/courses/241717/external_tools/8408

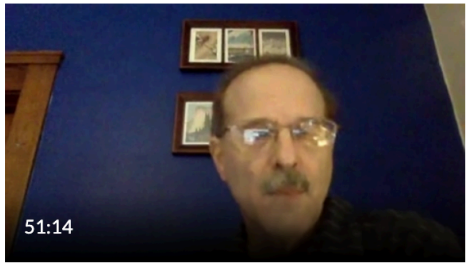
Account
Dashboard
Courses
Calendar
Inbox
History
Commons
Help

Assignments
Discussions
Grades
People
Piazza
Pages
Files
Outcomes
Rubrics
Quizzes
Modules
Collaborations
Chat
BBCollaborate Ultra
Course Summary
Course Syllabus (AEFIS)
Kaltura My Media
Kaltura Gallery
Direct Evidence of

Filters >

All Fields | Creation Date - Descending

Add New | ACTIONS

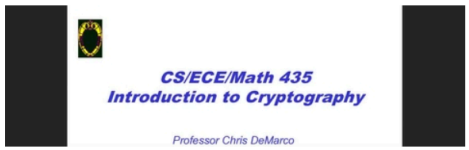


4/26/2021 - CS/ECE/Math 435 Lectures - recording_39

Private

coursemedia-g-83960-241717 | bbcollab

Collaborator • on April 27th, 2021 ▶ 0 💬 0



4/23/2021 - CS/ECE/Math 435 Lectures - recording_38

Practice Final Exam Problems - Set 2

(solutions will be worked as part of lecture/review session)

Long Format 1

Consider the following polynomial on $\mathbb{Z}_2$ (i.e. coefficients in $\mathbb{Z}_2$, argument $x \in \mathbb{Z}_2$):

$$f = x^4 + x^3 + 1$$

You make take as given the fact that f is irreducible

a) Written as polynomials, identify all the elements of the Galois Field associated with f, $GF(2^4)$.

	$GF(2^4)$ elements	Associated binary string
1)	0	0 0 0 0
2)	1	0 0 0 1
3)	X	0 0 1 0
4)	$X+1$	0 0 1 1
5)	X^2	0 1 0 0
6)	X^2+1	0 1 0 1
7)	X^2+X	0 1 1 0
8)	X^2+X+1	0 1 1 1
9)	X^3	1 0 0 0
10)	X^3+1	1 0 0 1
11)	X^3+X	1 0 1 0
12)	X^3+X+1	1 0 1 1
13)	X^3+X^2	1 1 0 0
14)	X^3+X^2+1	1 1 0 1
15)	X^3+X^2+X	1 1 1 0
16)	X^3+X^2+X+1	

In summary: all the possible binary coefficient polynomials, up to degree 3.

6) Compute multiplicative inverse of $x^3 + x^2$ in $GF(2^4)$ with $f = x^4 + x^3 + 1$

Solution (see DeMarco lecture notes # 30)

row #	column q	column d	col x	col y
1	empty	$x^4 + x^3 + 1$	1	0
2	empty	$x^3 + x^2$	0	1
→ 3	x	1	1	x

computation for row 3:

$$x^3 + x^2 \overline{)\; x^4 + x^3 + 1} \quad \text{quotient: } x$$

$$x^4 + x^3$$

$$1 \quad \text{(remainder)}$$

$\Rightarrow q_3 = x$

Algorithm terminates when d entry reaches 1; here that occurs at row 3. By construction, entries in a given row k satisfy: $d_k = f \cdot x_k + a \cdot y_k$; here in row 3:

$$(\#) \quad 1 = \left(x^4 + x^3 + 1\right) \cdot 1 + \left(x^3 + x^2\right) \cdot x$$

In slight abuse of notation, recalling f for $GF(2^4)$ play role analogous to integer N for $\mathbb{Z}_N$, write eqn (#) as

$$\text{mod}\left[\left(x^3 + x^2\right) \cdot x, \left(x^4 + x^3 + 1\right)\right] = 1$$

We conclude that the polynomial X is the multiplicative inverse of $(x^3 + x^2)$ in $GF(2^4)$ with $f = x^4 + x^3 + 1$.

Problem 2 : Cryptanalysis of block size 2 Hill cipher on $\mathbb{Z}_{26}$.

Given ciphertext of 14 characters / $\mathbb{Z}_{26}$ elements :

	block 1		block 2		block 3		block 4		block 5		block 6		block 7	
CIPHER = [	2	7	24	19	2	24	18	12	5	24	3	24	17	14]

a) Partially known corresponding plaintext for first six characters / $\mathbb{Z}_{26}$

0	15	0	11	4	12
↕	↕	↕	↕	↕	↕
A	P	A	L	E	M

(Sample problems as posted to Canvas 4/27 only gave 5 characters - updated here)

a) Objective: Compute $M \in \mathbb{Z}_{26}^{2\times 2}$ of this Hill cipher encryption function

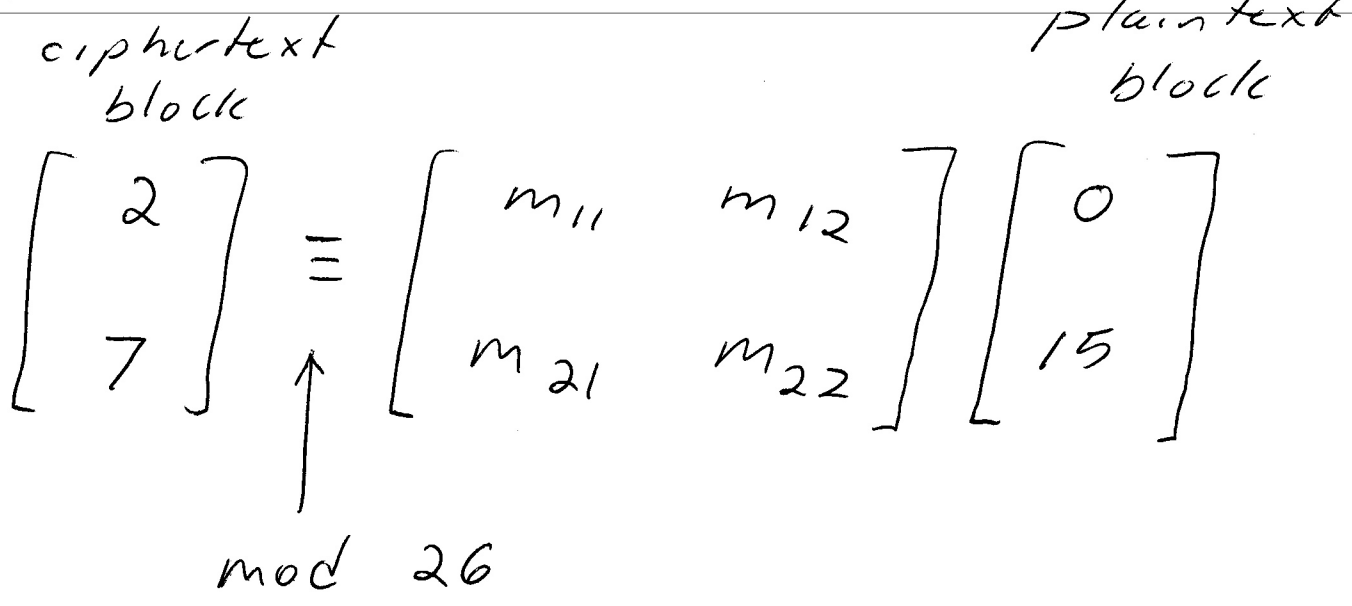
Solution: Each 2-character block of corresponding plaintext/ciphertext yields two linear equations on the four unknowns $m_{11}, m_{12}, m_{21}, m_{22}$.

We'll need four linearly independent equations. And important to note that getting linear independence is in a sense probabilistic, dependent on the particular "sample" of

plaintext/ciphertext. Here that dictates that the first two 2-character blocks of plaintext/ciphertext are not sufficient: we need a third:

So here:

First block:



Second block ciphertext

$$\begin{bmatrix} 24 \\ 19 \end{bmatrix} \equiv \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} \begin{bmatrix} 0 \\ 11 \end{bmatrix} \pmod{26}$$

plaintext

(Note: the repeated appearance of 0 as first entry of plaintext in block 1 and block 2 make these insufficient to solve m_{11}, m_{21})

Third block:

$$\begin{bmatrix} 2 \\ 24 \end{bmatrix} \equiv \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} \begin{bmatrix} 4 \\ 12 \end{bmatrix} \pmod{26}$$

From first block

row 1 $\Rightarrow$ $\text{mod}(15 \cdot m_{12}, 26) = 2$

$\Rightarrow$ $m_{12} = \text{mod}(15^{-1} \cdot 2, 26)$

$\updownarrow$

$= \text{mod}(7 \cdot 2, 26) = 14$

---

row 2 $\Rightarrow$ $\text{mod}(15 \cdot m_{22}, 26) = 7$

$\Rightarrow$ $m_{22} = \text{mod}(15^{-1} \cdot 7, 26)$

$= \text{mod}(49, 26) = 23$

Block 2 gives only redundant, linearly independent information (you can check that it is consistant, yielding same m_{12}, m_{22}).

Block 3:

row 1 : $\mod(4 \cdot m_{11} + 12 \cdot \overset{14}{\overset{\|}{m_{12}}}, 26) = 2$

$\Rightarrow \mod(4 \cdot m_{11}, 26) + \underbrace{\mod(12 \cdot 14, 26)}_{=12} = 2$

$\Rightarrow \mod(4 \cdot m_{11}, 26) = \mod(2-12, 26) = 16$

So $\underline{a}$ choice for m_{11} is $m_{11} = 4$

(but note that $4 \in \mathbb{Z}_{26}^*$, so not unique)

But observe we could also choose $m_{11} = 17$, because $\mod(4 \cdot 17, 26)$ also $= 16$.

For (a), either solution is acceptable. For (b), we'll see which choice produces intelligible plaintext for the rest of the message.

row 2 of block 3 :

$$\begin{matrix} & & 23 \\ & & 11 \\ \mod(& 4 \cdot m_{21} + 12 \cdot m_{22} & , 26) = 24 \end{matrix}$$

$$\Rightarrow \mod(4 \cdot m_{21}, 26) + \underbrace{\mod(12 \cdot 23, 26)}_{16} = 24$$

$$\Rightarrow \mod(4 \cdot m_{21}, 26) = 8 \text{ , so } \boxed{m_{21} = 2} \text{ a solution}$$

Observe $\boxed{m_{21} = 15}$ $\left(\mod(\overbrace{4 \cdot 15}^{60}, 26) = 8\right)$ is also a solution.

So a solution for part (a)

M_1 Hill matrix $= \begin{bmatrix} 4 & 14 \\ 2 & 23 \end{bmatrix}$

But this is not unique.
Alternate solutions consistent with the given plaintext / ciphertext are

$$M_2 = \begin{bmatrix} 17 & 14 \\ 2 & 23 \end{bmatrix}, \quad M_3 = \begin{bmatrix} 4 & 14 \\ 15 & 23 \end{bmatrix}, \quad M_4 = \begin{bmatrix} 17 & 14 \\ 15 & 23 \end{bmatrix}$$

However, preparing for part (b), we do have a well defined test to distinguish an acceptable Hill matrix: it must have a determinant whose value (mod 26) lies in $\mathbb{Z}_{26}^*$.

b) To decrypt the ciphertext, we'll want to compute the decryption function for the Hill cipher; i.e. we'll want M^{-1}. Let's see which of our candidate M_i's is invertible in $\mathbb{Z}_{26}$:

$$\text{mod}(\det(M_1), 26) = \text{mod}(4 \cdot 23 - 2 \cdot 14, 26)$$

$$= 12 \notin \mathbb{Z}_{26}^* \Rightarrow M_1 \text{ not invertible.}$$

$$\text{mod}(\det(M_2), 26) = \text{mod}(17 \cdot 23 - 2 \cdot 14, 26)$$

$$= 25 \in \mathbb{Z}_{26}^* \Rightarrow M_2 \text{ is invertible!}$$

Similarly, $\det(M_3) = 12$ fails,
$\det(M_4) = 25$ passes.

So M_2 and M_4 are our two acceptable candidate Hill ciphers.

Compute M_2^{-1}: inverse$_{\mathbb{Z}_{26}}(\det(M_2))$
$= 25$. So

$$M_2^{-1} \equiv 25 \cdot \begin{bmatrix} 23 & -14 \\ -2 & 17 \end{bmatrix} = \begin{bmatrix} 3 & 14 \\ 2 & 9 \end{bmatrix}$$

$\uparrow$ mod 26

Block 4: $M_2^{-1} \circ \begin{bmatrix} 18 \\ 12 \end{bmatrix} =$

$$\mod\left(\begin{bmatrix} 3 & 14 \\ 2 & 9 \end{bmatrix}\begin{bmatrix} 18 \\ 12 \end{bmatrix}, 26\right) = \begin{bmatrix} 14 \\ 14 \end{bmatrix} \begin{matrix} \leftrightarrow & O \\ \leftrightarrow & O \end{matrix}$$

Block 5:

$$\mod\left(\begin{bmatrix} 3 & 14 \\ 2 & 9 \end{bmatrix}\begin{bmatrix} 5 \\ 24 \end{bmatrix}, 26\right) = \begin{bmatrix} 13 \\ 18 \end{bmatrix} \begin{matrix} \leftrightarrow & N \\ \leftrightarrow & S \end{matrix}$$

Block 6:

$$\mod\left(\begin{bmatrix} 3 & 14 \\ 2 & 9 \end{bmatrix}\begin{bmatrix} 3 \\ 24 \end{bmatrix}, 26\right) = \begin{bmatrix} 7 \\ 14 \end{bmatrix} \begin{matrix} \leftrightarrow & H \\ \leftrightarrow & O \end{matrix}$$

Block 7:

$$\text{mod}\left(\begin{bmatrix} 3 & 14 \\ 2 & 9 \end{bmatrix}\begin{bmatrix} 17 \\ 14 \end{bmatrix}, 26\right) = \begin{matrix} 13 \leftrightarrow N \\ 4 \leftrightarrow E \end{matrix}$$

So candidate Hill matrix M_2 produces plaintext:

APALEMOONSHONE

We'll accept M_2 and this plaintext as correct.

Problem 3 : Diffie-Hellman key exchange with $p = 11$, "candidate" generators (to check as part of problem) $g_1 = 5$, $g_2 = 7$.

Background : Recall that the goal of D-H is to allow two users, A and B, to exchange information in public that allows them to both construct the same key, without that key ever being communicated in public. The exchange is facilitated by network manager who provides p, g.

Solution (a): You are to demonstrate that $g_1 = 5$ is <u>not</u> a generator for $\mathbb{Z}_{11}^*$ (so not suitable for use in D-H with $p = 11$).

Easiest approach: A generator must have the property that for $x, y \in \mathbb{Z}_{11}^*$, $x \neq y$, $\mod(g^x, 11) \neq \mod(g^y, 11)$.

So to prove g is not a generator, sufficient to show $x \neq y$, $x, y \in \mathbb{Z}_{11}^*$ such that $\mod(g^x, 11) = \mod(g^y, 11)$.

Compute:

1) $\mathrm{mod}(5^1, 11) = 5$

2) $\mathrm{mod}(5^2, 11) = 3$

3) $\mathrm{mod}(5^3, 11) = \mathrm{mod}(\mathrm{mod}(5^2, 11) \cdot 5, 11) = 4$

key idea in computing exponentiation in modular case.

4) $\mathrm{mod}(5^4, 11) = \mathrm{mod}(4 \cdot 5, 11) = 9$

5) $\mathrm{mod}(5^5, 11) = \mathrm{mod}(9 \cdot 5, 11) = 1$

6) $\mathrm{mod}(5^6, 11) = \mathrm{mod}(1 \cdot 5, 11) = 5$

7) $\mod(5^7, 11) = \mod(5 \cdot 5, 11) = 3$

$\Rightarrow$ conclude $x = 2$, $y = 7$ yield

Same $g_1^x \equiv g_1^y$ (mod 26), $g_1 = 5$ fails as generator

b) For choice $g_2 = 7$, one may proceed as per (a), and enumerate each $7^x \bmod 26$ for each $x \in \mathbb{Z}_{11}^*$, showing uniqueness of each.

OR, somewhat more efficiently, one may use the theorem provided on your formula sheet (Back notes p. 38-1):

Find each prime divisor of $(p-1) = 10$: these are $q_1 = 2$, $q_2 = 5$.

Then test:

$$\mathrm{mod}\left(g^{(p-1)/q}, p\right) \neq 1$$

Here $\mathrm{mod}\left(7^5, 11\right) = 10 \neq 1$

$\mathrm{mod}\left(7^2, 11\right) = 5 \neq 1$