Math 233: Cryptography

Midterm Exam

March 26, 2018

NAME (please print legibly): _____

Your University ID Number: _____

- **Calculators are allowed for doing arithmetic, not for looking up information. Computers, ipads, etc. are not allowed. The exam is closed book. You may bring one sheet of notes (you can write on both sides).**
- **Show your work and justify your answers. You may not receive full credit for a correct answer if insufficient work is shown or insufficient justification is given.**

- Honor pledge: "I affirm that I have not used, given nor received unauthorized aid during this examination."

  Signature:

QUESTION	VALUE	SCORE
1	10	
2	10	
3	30	
4	25	
5	15	
6	10	
TOTAL	100	

1. (10 points)

1. Find the greatest common divisor of 271 and 843 $d = \gcd(271, 843)$ and find numbers x and y which satisfy the Bezout identity $d = 271x + 843y$ Answers:
   d =
   x =
   y =

   Solution:

$$843 = 3 \cdot 271 + 30 \tag{1}$$
$$271 = 9 \cdot 30 + 1 \tag{2}$$

   Hence $d = 1$ and unraveling we get:

   $d = 1 = 271 - 30 \cdot 9 = 271 - (843 - 3 \cdot 271) \cdot 9 = 271(1 + 27) - 843 \cdot 9$

   from which we get $d = 271 \cdot 28 - 843 \cdot 9$

   so $x = 28$ and $y = -9$. □

2. Solve for z: $271z = 2 \pmod{843}$

   Answer:
   $z =$

   Solution:

   From the Bezout equation we see that $271^{-1} \equiv 28 \pmod{843}$ hence $28 \cdot 271z \equiv z \equiv 28 \cdot 2 \equiv 56 \pmod{843}$ □

2. (10 points) We add 3 punctuation marks to the usual English alphabet and create ciphers using the encoding:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	,	.	?
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

1. An affine-like cipher given by $c \equiv \alpha x + \beta \pmod{29}$ (where c is the ciphertext and x is plaintext) encrypts the plaintext `cab` as `MCH`. Which other three letter combinations encode as `MCH`? Explain your reasoning.

   Solution:

   Because 29 is prime every number less than 29 except 0 has an inverse $\pmod{29}$. We can't have $\alpha \equiv 0$ because in that case the function will would be constant and all outputs would consist of a single letter which is not the case here.

   Every other value of α and every value of β has an inverse so that x can be solved uniquely in terms of y. This means that one and only one three letter combination can produce the characters `MCH`.

   □

2. What are the values for α and β in the encoding above?

   Solution:

   Since a corresponds to 0 we have that $y = \alpha \cdot 0 + \beta = 2$ which corresponds to c. Hence $\beta = 2$.

   Since b which corresponds to 1 is mapped to `H` which corresponds to 7 $\alpha = 5$.

   The equation is $y = 5x + 2 \pmod{29}$. □

3. (30 points)

(a) Does $x^2 \equiv 6 \pmod{13}$ have a solution? (Note: $13 \equiv 1 \pmod 4$)

Solution:

The basic test is that $a^{(p-1)/2} \equiv -1 \pmod p$ means that a is not a square and that if it is equivalent to 1 then it is a square. (Except of course if $p|a$ in which case a to any power is equivalent to 0.) Since $a^{p-1} \equiv 1 \pmod 1$ for any $a \not\equiv 0 \pmod p$ we see that $(x^2)^{(p-1)/2} \equiv -1$ is not possible for non-zero x so a cannot be a square in that case. The converse is harder and can be checked by representing a as a primitive root to some power.

In this case $a = 6$ and $66 \equiv 36^3 \equiv 10^3 \equiv 1000 \equiv 12 \equiv -1 \pmod{13}$ so 6 is not a square and this equation has no solution. □

(b) Is 3 a primitive root mod 13? Explain your answer.

Solution:

3 is not a primitive root since $3^1 \equiv 3, 3^2 \equiv 9, 3^3 = 27 \equiv 1 \pmod{13}$ $\phi(13) = 12$ so 3^i does not map on to all of the numbers co prime to 13 and it's order is 3 not 12.

2 is a primitive root of 13 and its powers are: $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 3, 2^5 \equiv 6, 2^6 \equiv 12 \equiv -1 \pmod{13}$. This is enough to see that the order of 2 must be 12 and therefore 2 is a primitive root. For completeness, however:

$2^7 \equiv 11, 2^8 \equiv 9, 2^9 \equiv 5, 2^{10} \equiv 10, 2^{11} \equiv 7, 2^{12} \equiv 1 \pmod{13}$

This also illustrates why 6 is not a square since it is 2 to a odd power. □

(c) Does 19 have a square root mod 65? If so, how many does it have and what are they? Note that 65 factors as $65 = 5 \cdot 13$.

Solution:

We need to use the Chinese remainder theorem and solve the related equations:

$x^2 \equiv 19 \equiv -1 \equiv 4 \pmod 5$ and

$x^2 \equiv 19 \equiv 6 \mod 13$

Since the second equation has no solutions 19 is not a square $\pmod{65}$.

□

(d) Does 35 have a square root mod 65? If so, how many does it have and what are they?

Solution:

This time the relevant equations are:

$x^2 \equiv 35 \equiv 0 \pmod 5$ and

$x^2 \equiv 9 \mod 13$

The first equation has only one solution 0, while the second has solutions ± 3.

Since $1 = \gcd(5, 13) = 13 \cdot 2 - 5 \cdot 5$ we can combine the solutions 0 and 3 to get $0 \cdot 13 \cdot 2 + 3(-5) \cdot 5 = -75 \equiv -10 \pmod{65}$ which satisfies both equations $\pmod 5$ and $\pmod{13}$ as does 10. So $(\pm 10)^2 = 35 \pmod{65}$ are the two solutions.

□

4. (25 points)

(a) How many numbers less than 40 have inverses (mod 40).

Solution:

The number of integers less than 40 with $\gcd(k, 40) = 1$ is by definition $\phi(40)$. $40 = 8 \cdot 5$. So $\phi(40) = 8 \cdot 5(1 - \frac{1}{2})(1 - \frac{1}{5}) = 4 \cdot 4 = 16$.

The integers are $1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39$

□

(b) How many numbers less than 41 have inverses (mod 41).

Solution:

This is easier: $\phi(p) = p - 1$ so in this case $\phi(41) = 40$. Many more inverses in this case.

□

(c) True or false and explain: $a^{\phi(24)} \equiv 1 \pmod{24}$ for all positive integers a that are not divisible by 24.

Solution:

24 is not prime so this is suspicious. Euler's theorem says that the identity is true if $\gcd(a, 24) = 1$ but there are many integers a which 24 does not divide that have common factors with 24. $a = 2$ for example. First calculate $\phi(24) = 2 \cdot 8(1 - \frac{1}{2}) = 8$.

If the identity were true we would also have some other equations as a consequence of the Chinese remainder theorem:

$a^8 \equiv 1 \pmod 3$ and

$a^8 \equiv 1 \pmod 8$

We already see that $2^3 \equiv 0 \pmod 8$ so the second equation can't hold.

Just to be sure, we consider $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 16, 2^5 \equiv 32 \equiv 8, 2^6 \equiv 16, 2^7 \equiv 32 \equiv 8, 2^8 \equiv 16 \not\equiv 1$

The equality does not hold for all a less than 24.

□

(d) Find a positive integer x less than 13 such that $5^{242} \equiv x \pmod{13}$.

Solution:

In this case $\phi(13) = 12$ and $242 = 12 \cdot 20 + 2$ hence $5^{242} = 5^{12 \cdot 20 + 2} \equiv 1^{20} 5^2 \equiv 25 \equiv -1 \equiv 12 \pmod{13}$

□

5. (15 points)

(a) Using an *affine cipher*, double encryption is equivalent to just a single encryption. Suppose Alice encrypts once using the affine function $3x + 4 \pmod{26}$, then a second time using the affine function $7x + 12 \pmod{26}$. This is equivalent to a single encryption of the form $x \mapsto \alpha x + \beta \pmod{26}$ for which integers α and β (each between 0 and 25)?

Solution:

This is just composition of functions:

$y = 7(3x + 4) + 12 \equiv 21x + 40 \equiv 21x + 14 \pmod{26}$

□

6. (10 points) We define a function f that takes a 3-bit input and yields a 2-bit output as follows: $f(a_1a_2a_3) = a_1a_2 \oplus a_31$, so that for example $f(100) = 10 \oplus 01 = 11$, and $f(111) = 11 \oplus 11 = 00$. (You can consider $\oplus$ to be either XOR or addition on the field $GF(2^n)$ they are equivalent.)

(a) What is $f(011)$?

Solution:

$f(011) = 01 \oplus 11 = 10$ □

(b) Show that f is not linear. In other words, find two 3-bit inputs A and B such that $f(A \oplus B) \neq f(A) \oplus f(B)$.

Solution:

$f(111) = 00$, $f(100) = 11$,

$f(111 \oplus 100) = f(011) = 10 \neq f(111) \oplus f(100) = 11$ □