Math 111 Contemporary Mathematics
Fall 2015
Lecturer: Dr. Paullin

Name: Key

Cryptography Day 10
Cryptography Review Day

Modular Arithmetic

(1) Simplify 16 (mod 7)

$\boxed{2 \pmod 7}$

(2) Simplify 12154 (mod 11)

$\boxed{10 \pmod{11}}$

(3) If $13^4 \pmod{11} = 5$, what is $13^8 \pmod{11}$?

$8 = 4 + 4$

$13^8 = 13^4 \cdot 13^4 \pmod{11} = 5 \cdot 5 \pmod{11} = 25 \bmod 11 = \boxed{3 \pmod{11}}$

(4) If $17^3 \pmod 9 = 8$, what is $17^{10} \pmod 9$?

$10 = 3 + 3 + 3 + 1$

$17^{10} = 17^3 \cdot 17^3 \cdot 17^3 \cdot 17^1 \pmod 9 = 8 \cdot 8 \cdot 8 \cdot 17 \pmod 9 = \boxed{1 \pmod 9}$

(5) Find the additive inverse for 10 (mod 31).

$\overline{10} \pmod{31} = (31 - 10) \bmod 31 = \boxed{21 \pmod{31}}$

(6) Find the additive inverse for 64 (mod 14).

$\overline{64} \pmod{14} = \overline{8} \pmod{14} = (14 - 8) \bmod 14 = \boxed{6 \pmod{14}}$

(7) Simplify -17(mod 33)

$-17 = \overline{17} \pmod{33} = (33 - 17) \bmod 33 = \boxed{16 \pmod{33}}$

(8) Simplify -135 (mod 21)

$-135 = \overline{135} \pmod{21} = \overline{9} \pmod{21} = (21 - 9) \bmod 21 = \boxed{12 \pmod{21}}$

(9) Find b such that b $\cdot$ 12(mod 18)=0.

$\boxed{b = 3}$ since $3 \cdot 12 = 36 \pmod{18} = 0$

although $b \in \{3, 6, 9, 12, 15\}$ is also acceptable

(10) List the factors of 30.

30: $\boxed{1, 2, 3, 5, 6, 10, 15, 30}$

(11) Find the gcd(22,64).

22: 1, 2, 11, 22

64: 1, 2, 4, 8, 16, 32, 64

$\boxed{\gcd(22, 64) = 2}$

(12) Find the gcd(91,5).

91: 1, 7, 13, 91

5: 1, 5

$\boxed{\gcd(91, 5) = 1}$

(13) Find the multiplicative inverse for 4 (mod 25).

$\underline{?} \times 4 \pmod{25} = 1$

$\boxed{19 \pmod{25}}$

(14) Does 3(mod 21) have a multiplicative inverse?

gcd(3,21) = 3 $\boxed{\text{No}}$

(15) Does 9(mod 16) have a multiplicative inverse?

gcd(9,16) = 1 $\boxed{\text{Yes}}$

Codes and Cryptography

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

(16) A Ceasar Cipher is a special case of the Shift Cipher. What is Δ for a Ceasar Cipher?

$\boxed{\Delta = 3}$

(17) Using a Shift Cipher with $\Delta = 5$, encrypt the word PUMPKIN.

P U M P K I N

Δ +5

□=16 21 13 16 11 9 14

⊠=21 26 18 21 16 14 19

$\boxed{\text{U Z R U P N S}}$

(18) Using a Shift Cipher with $\Delta = 3$, Find ∇ and decrypt the word VFDUHFURZ.

$\Delta + \nabla = 26$

$3 + \nabla = 26$

$\boxed{\nabla = 23}$

V F D U H F U R Z

⊠ : 22 6 4 21 8 6 21 18 26

∇+23 □ = 45=19 29=3 27=1 44=18 31=5 29=3 44=18 41=15 49=23

$\boxed{\text{S C A R E C R O W}}$

(19) A Vigenère Cipher is being used with the following shifts:
$\Delta_1 = 8, \Delta_2 = 1, \Delta_3 = 18, \Delta_4 = 22, \Delta_5 = 5, \Delta_6 = 19, \Delta_7 = 20$
What Keyword is being used for this Vigenère Cipher?

8 1 18 22 5 19 20

$\boxed{\text{H A R V E S T}}$

(20) Use the Keyword CANDY to encrypt the word COSTUME using a Vigenère Cipher.

C A N D Y

Δ= 3 1 14 4 25

C O S T U M E

□= 3 15 19 20 21 13 5

Δ 3 1 14 4 25 3 1

⊠ = 6 16 33=7 24 46=20 16 6

$\boxed{\text{FPGXTPF}}$

(21) Use the Keyword FALL to decrypt the word GVFGSO using a Vigenère Cipher.

F A L L

Δ= 6 1 12 12

∇= 20 25 14 14

G V F G S O

⊠= 7 22 6 7 19 15

∇= 20 25 14 14 20 25

□ = 27=1 47=21 20 21 39=13 40=14

$\boxed{\text{A U T U M N}}$

(22) Use the times cipher with $\star = 3$ to encrypt the word FOOTBALL.

	F	O	O	T	B	A	L	L
$\square =$	6	15	15	20	2	1	12	12
$\star \times 3$ $\boxtimes =$	18	45=19	45=19	60=8	6	3	36=10	36=10
	R	S	S	H	F	C	J	J

(23) You need to decrypt a message using the times cipher $\star \times \square$ (mod 26)=$\boxtimes$, where $\star = 5$.

(a) Find $*$.

$\star = 5$

$*$ is the mult. inverse of $\star$

$\underline{?} \times 5 \pmod{26} = 1$

$21 \times 5 = 105 \pmod{26} = 1$

$\boxed{* = 21}$

(b) Use $*$ to decrypt the word HYEFYQ.

	H	Y	E	F	Y	Q
$\boxtimes =$	8	25	5	6	25	17
$* \cdot 21$ $\square =$	168 = 12	525 = 5	105 = 1	126 = 22	525 = 5	357 = 19
	L	E	A	V	E	S

(24) RSA Cipher

(a) If we pick our primes p=11 and q=7, find **n** and **m**.

$n = p \cdot q = 11 \cdot 7 = \boxed{77 = n}$

$m = (p-1)(q-1) = 10 \cdot 6 = \boxed{60 = m}$

(b) List 3 good values for e(mod m).

e is a unit (mod 60)

$e \in \boxed{\{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59\}}$

(c) List 3 bad values for e(mod m).

e is not a unit

$e \in \boxed{\{2,3,4,5,6,8,9,10,12,14,15,16,18,20,21,22,24,25,26,27,28,30,32,33,34,35,36,38,39,40,42,44,45,46,48,50,51,52,54,55,56,57,58\}}$

(d) Encrypt the word SQUIRREL using the RSA Cipher if **n=77** and **e=7**.

	S	Q	U	I	R	R	E	L
$\square =$	19	17	21	9	18	18	5	12
$\square^7 \pmod{77} = \boxtimes =$	68	52	21	37	39	39	47	12

(e) If **e=7**, find the decryption exponent **d**.

d = mult. inverse of e(mod m) $\underline{?} \times 7 \pmod{60} = 1$

$43 \cdot 7 \pmod{60} = 301 \pmod{60} = 1$

$\boxed{d = 43}$

(f) Decrypt the message 58 37 47 back to the English Alphabet using our RSA Cipher. It might be helpful to know that:
58^{14}(mod 77)=4
37^{21}(mod 77)=15
47^{21}(mod 77)=69

$\boxed{\text{PIE}}$

$\longrightarrow$

$\boxtimes = 58$

$\boxtimes^{43} \pmod{77}$ $\qquad 43 = 14 + 14 + 14 + 1$

$$\square = 58^{43} = 58^{14} \cdot 58^{14} \cdot 58^{14} \cdot 58^{1} \pmod{77}$$
$$= 4 \cdot 4 \cdot 4 \cdot 58 \pmod{77}$$
$$= 3712 \pmod{77}$$
$$= 16$$

$\boxtimes = 37$

$\boxtimes^{43} \pmod{77}$ $\qquad 43 = 21 + 21 + 1$

$$\square = 37^{43} = 37^{21} \cdot 37^{21} \cdot 37^{1} \pmod{77}$$
$$= 15 \cdot 15 \cdot 37 \pmod{77}$$
$$= 8325 \pmod{77}$$
$$= 9$$

$\boxtimes = 47$

$\boxtimes^{43} \pmod{77}$ $\qquad 43 = 21 + 21 + 1$

$$\square = 47^{43} = 47^{21} \cdot 47^{21} \cdot 47^{1} \pmod{77}$$
$$= 69 \cdot 69 \cdot 47 \pmod{77}$$
$$= 223767 \pmod{77}$$
$$= 5$$

$\square = $ 16 9 5

$\boxed{\text{P} \quad \text{I} \quad \text{E}}$