Math 111 Contemporary Mathematics
Fall 2015
Lecturer: Dr. Paullin

Name: Key

Cryptography Day 7

---

(1) Find the multiplicative inverse for 5 (mod 12).

units: 1, 5, 7, 11

$5 \cdot 5 = 25 \pmod{12} = 1 \pmod{12}$

$5 \pmod{12}$

(2) Find the multiplicative inverse for 2 (mod 21).

units: 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20

$2 \cdot 11 = 22 \pmod{21} = 1 \pmod{21}$

$11 \pmod{21}$

(3) Does 6(mod 14) have a multiplicative inverse?

$\gcd(6,14) = 2$

$6 \bmod 14$ is not a unit

No

(4) Does 7(mod 15) have a multiplicative inverse?

$\gcd(7,15) = 1$

$7 \pmod{15}$ is a unit

Yes

(5) Encrypt the following word using the times cipher $\star \times \square \pmod{26} = \boxtimes$ given.

(a) DOG, $\star = 7$

	D	O	G
$\square =$	4	15	7
$\star \times 7$	28	105	49
$\boxtimes =$	2	1	23
	B	A	W

BAW

(b) TURTLE, $\star = 11$

	T	U	R	T	L	E
$\square =$	20	21	18	20	12	5
$\star \times 11$	220	231	198	220	132	55
$\boxtimes =$	12	23	16	12	2	3
	L	W	P	L	B	C

LWPLBC

(6) You need to decrypt a message using the times cipher $\star \times \square \pmod{26} = \boxtimes$, where $\star = 3$.

(a) Find $*$.

Since $3 \cdot 9 = 27 = 1 \pmod{26}$ $\quad * = 9$

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

	F	K	P	P	A	O	E
$\boxtimes =$	6	11	16	16	1	15	5
$* \times 9$	54	99	144	144	9	135	45
$\square =$	2	21	14	14	9	5	19
	B	U	N	N	I	E	S