

(3 points) Name:

SOLUTIONS

1. (5 points) Give all possible solutions of the linear congruence $3x \equiv 6 \pmod{15}$.

The $\gcd(3, 15) = 3$ does divide 6, so there are 3 different solutions mod 15. By looking at it, we know $x=2$ works, so $x \equiv 2 \pmod{15}$ is one solution mod 15. We add $\frac{15}{3} = 5$ to get the others.

Solutions: $x \equiv 2 \pmod{15}$, $x \equiv 7 \pmod{15}$, $x \equiv 12 \pmod{15}$

2. (9 points) Fill in the following table with the cipher alphabet for a columnar substitution cipher with keyword NO COPYING. Show your work!

A	B	C	D	E	F	G	H	I	J	K	L	M
N	A	K	U	O	B	L	V	C	D	M	W	P

NOCPYIG
ABDEFHJ
KLMORST
UVWXZ

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	Q	X	Y	F	R	Z	I	H	S	G	J	T

3. Give the keyword for the Vigenere Cipher which would:

- (a) (4 points) Encrypt CLOCK as UFBPI.

2	11	14	2	19
C	L	O	C	K
+				
20	6	15	15	8
U	F	B	P	I

I solve Plain + Key = Crypto for Key

- (b) (4 points) Decrypt UFEGB as TOWER

U	F	E	G	B
-				
T	O	W	E	R

Key = Crypto - Plain

20	-	19	=	1	(mod 26)	→	B
5	-	14	=	-9	=	17	(mod 26) → R
4	-	22	=	-18	=	8	(mod 26) → I
6	-	4	=	2	(mod 26)	→	C
2	-	17	=	-15	=	11	(mod 26) → K

20	-	2	=	18	(mod 26)	→	S
5	-	11	=	-6	=	20	(mod 26) → U
14	-	14	=	0	=	13	(mod 26) → N
15	-	2	=	13	(mod 26)	→	N
8	-	10	=	-2	=	24	(mod 26) → Y

BRICK