MATH 178 Homework #4

Tamir Enkhjargal

April 2019

SmC

2.

Plaintext	Encode	$C \equiv 7(P) + 11(\text{mod}26)$	Ciphertext
T	19	14	O
R	17	0	A
A	0	11	L
N	13	24	Y
S	18	7	H
F	5	20	U
E	4	13	N
R	17	0	A
F	5	20	U
U	20	21	V
N	13	24	Y
D	3	6	G
S	18	7	H

Ciphertext: `OALYHUNAUVYGH`

3.

(i) O=14→G=6, K=10→E=4

$$C \equiv aP + b(\text{mod}26) \tag{1}$$
$$6 \equiv a * 14 + b(\text{mod}26) \tag{2}$$
$$4 \equiv a * 10 + b(\text{mod}26) \tag{3}$$
$$2 \equiv 4 * a(\text{mod}26) \tag{4}$$
$$2 * a \equiv 1(\text{mod}13) \tag{5}$$
$$a = 7 \tag{6}$$
$$6 \equiv 7 * 14 + b(\text{mod}26) \tag{7}$$
$$b \equiv 6 - 7 * 14(\text{mod}26) \tag{8}$$
$$b = 12 \tag{9}$$

The enciphering key (a,b) is (7,12). Therefore the deciphering key (a',b') is (15,12), where $15 = \text{a}^{-1}$

(ii) Deciphering the message: `POSTPONE YOUR VISIT OK`

(iii) Using the key (a,b) = (7,12). Enciphering the message: `AGSO IGGZ GE`

4.

The size of all key pairs is equal to $\varphi(38)*38 = \varphi(2^2*19)*38 = \varphi(2^2)\varphi(19)*38 = 2*18*38 = 1368$ total keypairs.

5.

S- $= 512 \rightarrow$ NG $= 357$
-T $= 721 \rightarrow$ KX $= 293$

$$C \equiv aP + b(\text{mod}729) \tag{1}$$
$$293 \equiv a*721 + b(\text{mod}729) \tag{2}$$
$$357 \equiv a*512 + b(\text{mod}729) \tag{3}$$
$$-64 \equiv a*209(\text{mod}729) \tag{4}$$
$$a*209 \equiv 665(\text{mod}729) \tag{5}$$
$$a \equiv 665*293(\text{mod}729) \tag{6}$$
$$a = 202 \tag{7}$$
$$a' = 646 \tag{8}$$
$$293 \equiv 202*721 + b(\text{mod}729) \tag{9}$$
$$b \equiv 293 - 202*721(\text{mod}729) \tag{10}$$
$$b = 451 \tag{11}$$

Ciphertext	Decode	$P \equiv 646*C + 451(\text{mod}729)$	Plaintext
TC	19*27+2=515	717	-P
UG	20*27+6=546	331	MH
AR	0*27+17=17	498	SM
XK	23*27+10=631	566	U-
OK	14*27+10=388	323	L-