Cryptography problem sheet

1. You are going to send a message to Bob via classical Diffie–Hellmann key exchange.

   (a) Fix $g = 35$ as a generator of $(\mathbb{Z}/3593\mathbb{Z})^*$. Choose your private secret key to be $sk_A = 16$.

   Compute your public key, $g^{sk_A} \mod 3593$.

   (b) You receive the public key 639 from Bob. Compute your and Bob's common secret key.

   (c) Use the common secret key to encrypt the secret message

   "Where_are_you?"

   Use the following alphabet to pad the individual letters:

_	A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

O	P	Q	R	S	T	U	V	W	X	Y	Z	.	?	’
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

@	a	b	c	d	e	f	g	h	i	j	k	l	m	n
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44

o	p	q	r	s	t	u	v	w	x	y	z	!	/
45	46	47	48	49	50	51	52	53	54	55	56	57	58

   (d) Cut the message into blocks of two letters and make use of the following padding scheme:
   1st letter goes to: (number of 1st letter in alphabet)*59,
   2nd letter goes to: (number of 2nd letter in alphabet),
   then sum up these two numbers.

   Example: "HI" goes to $8 * 59 + 9 = 481$.

   (e) Use the common secret key to encrypt the secret message, by multiplying it to every message unit. The modulus to 3593 then gets

converted into a block over the alphabet, by writing the modulus as $x * 59^2 + y * 59 + z$. Then the ciphertext for the message unit is (Alphabet entry of x)(Alphabet entry of y)(Alphabet entry of z).

Example: Padding 3600.

$z := 3600 \mod 59 \equiv 1 \mod 59$

$y := (3600 - z)/59 = 3599/59 = 61 \equiv 2 \mod 59$

$x := (61 - y)/59 = 59/59 \equiv 1 \mod 59.$

So, $3600 = x * 59^2 + y * 59 + z = 1 * 59^2 + 2 * 59 + 1.$

The ciphertext for the encoded message unit 3600 is hence "ABA".

(f) Generate your decryption key, the multiplicative inverse of the common secret key, and decipher Bob's answer,

_XK_FM_Ra_M/_WW_?._EM_'C_Ey_gv_d/_go_CL_vc_uk_gv_Sl_UQ _wp_XT_D@_eL_BN___