IS53012B/A Computer Security

Dr Ida Pu

Room 10, 29 St James
Goldsmiths, University of London

2018-19 (since 2007)

Part I

Homework

Answers I

1.

n	2	3	4	5	6	7	8	9	10	11	12	13
$n-1$	1	2	3	4	5	6	7	8	9	10	11	12
$2^{n-1} \mod n$	0	1	0	1	2	1	0	4	2	1	8	1
p	3	5	7	11	13	17	19	23	29	31	37	41
$2^{n-1} \mod p$	2	4	1	5	6	13	14	3	19	1	13	37

2. Other correct examples are acceptable.

$$(5+3) \mod 5 = [(5 \mod 5) + (3 \mod 5)] \mod 5 = 3$$

$$(6*7) \mod 5 = [(6 \mod 5) * (7 \mod 5)] \mod 5 = 2$$

3. Perform the following operations using reduction first:
   1. $= (3+4) \mod 10 = 7$
   2. $= (3+3) \mod 10 = 6$
   3. $= (4+8) \mod 12 = 0$
   4. $= (7+5) \mod 12 = 0$

Answers II

5. $= (3 \times 4) \mod 10 = 2$
6. $= (3 \times 3) \mod 10 = 9$
7. $= (4 \times 8) \mod 12 = 8$
8. $= (7 \times 5) \mod 12 = 11$

4. For convenience of discussion, we use capital letters for the plain text and lower case for encrypted message.

i	1	2	3	4	5	6	7	8	9	..					
plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
cipher	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
	..										26				
	P	Q	R	S	T	U	V	W	X	Y	Z				
	t	u	v	w	x	y	z	a	b	c	d				

Since $ciphercha r(i) = plainchar(i+4)$, we have
'THE DOG BIT THE MAN' → xli hsk fmx xli qer
→ xlihskfmxxliqer

Answers III

5.

plaintext:	c	o	m	p	u	t	e	r
index:	3.	15.	13.	16.	21.	20.	5.	18.
pad:	5.	20.	0.	9.	17.	16.	22.	18.
(index+pad) mod 26:	8.	9.	13.	25.	12.	10.	1.	10.
ciphertext:	h	i	m	y	l	j	a	j
ciphertext:	h	i	m	y	l	j	a	j
index:	8.	9.	13.	25.	12.	10.	1.	10.
pad:	5.	20.	0.	9.	17.	16.	22.	18.
(index-pad+26) mod 26:	3.	15.	13.	16.	21.	20.	5.	18.
plaintext:	c	o	m	p	u	t	e	r

It is hopeless in practice because the pad is as long as the plaintext.

Answers IV

6.

key:	I	A	M	T	H	E
alphabetic order:	*4*	*1*	*5*	*6*	*3*	*2*
	T	H	E	Q	U	I
	C	K	B	R	O	W
	N	F	O	X	J	U
	M	P	E	D	O	V
	E	R	T	H	E	L
	A	Z	Y	D	O	G
	O	N	C	E	_	_

The plaintext: 'THE QUICK BROWN FOX JUMPED OVER THE LAZY DOG ONCE' by transposition cipher.

7.

1. $n = p \times q = 5 \times 7 = 35$
2. $r = \varphi(n) = (p-1) \times (q-1) = 24$
3. Let $(p \times d) \mod r = 1$, So $d = 5$
4. private key: $d = 5$
5. public key: $(e, n) = (7, 35)$, where $n = p \times q$.