# IS53012B/A Computer Security

#### Dr Ida Pu

Room 10, 29 St James Goldsmiths, University of London

2018-19 (since 2007)

i.pu@gold.ac.uk (Goldsmiths)

IS53012B/A Computer Security

2018-19 (since 2007)

Week 4 Workshop Homework Answers

## Answers I

1

	n	2	3	4	5	6	7	8	9	10	11	12	13
r	<del>1</del> – 1	1	2	3	4	5	6	7	8	9	10	11	12
$2^{n-1}$ m	od <i>n</i>	0	1	0	1	2	1	0	4	2	1	8	1
	р	3	5	7	11	13	17	19	23	29	31	37	41
$2^{n-1}$ m	od p	2	4	1	5	6	13	14	3	19	1	13	37

2 Other correct examples are acceptable.

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

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

Perform the following operations using reduction first:

- $= (3+3) \mod 10 = 6$

## Part I

## Homework

i.pu@gold.ac.uk (Goldsmiths)

IS53012B/A Computer Security

2018-19 (since 2007)

Week 4 Workshop Homework Answers

## Answers II

 $\mathbf{6} = (3 \times 4) \mod 10 = 2$ 

 $\mathbf{6} = (3 \times 3) \mod 10 = 9$ 

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	Α	В	C	D	Ε	F	G	Н	- 1	J	K	L	M	N	0
cipher	е	f	g	h	i	j	k	- 1	m	n	0	р	q	r	S
											26				
	Р	Q	R	S	T	U	V	W	X	Υ	Z				
	t	u	V	w	×	y	Z	a	b	С	d				
			- \				- \								

Since cipherchar(i) = plainchar(i + 4), we have

'THE DOG BIT THE MAN' → xli hsk fmx xli qer

→ xlihskfmxxliger

#### Week 4 Workshop Homework Answers

## Answers III

**5** plaintext: 16. 20. index: 15. 13. 21. 5. 18. pad: 20. 0. 9. 17. 16. 22. 18. (index+pad) mod 26: 8. 9. 13. 25. 12. 10. 1. 10. ciphertext: m ciphertext: 25. 12. index: 8. 9. 13. 10. 1. 10. 0. 17. pad: 20. 9. 16. 22. 18. (index-pad+26) mod 26: 3. 15. 13. 16. 21. 20. 5. 18. plaintext: 0 m p

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

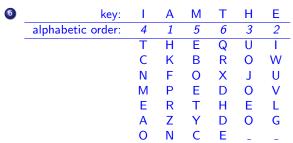
i.pu@gold.ac.uk (Goldsmiths)

IS53012B/A Computer Security

2018-19 (since 2007) 5 / 6

Week 4 Workshop Homework Answers

## Answers IV



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

- **1**  $n = p \times q = 5 \times 7 = 35$ 
  - $r = \varphi(n) = (p-1) \times (q-1) = 24$

  - private key: d = 5
  - **9** public key: (e, n) = (7, 35), where  $n = p \times q$ .

i.pu@gold.ac.uk (Goldsmiths)

IS53012B/A Computer Security

2018-19 (since 2007)

6 / 6