TMA4155 — Mid-term

Kristian Gjøsteen

October 18, 2006

NOTE! This test is intended to give me and you information about what you know and don't know. *This test does not affect your grades in any way what-so-ever.* Therefore you should not write your name or student number or any identifying information on the answer sheet.

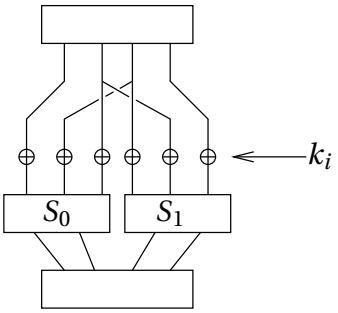
1. The encryption of `MORGENSOL` under the Cæsar cipher with key 3 is:

a. `PRUJHRVRO` **b.** `PRUJHQVRO` **c.** `NPSHFOTPM` **d.** `PRUJHOTPM` **e.** `PRUJHQVR`

2. Which of the following ciphertexts can be encryptions of `YPPERLIG` under a substitution cipher:

a. `XYZÆØÅAB` **b.** `ABBAWINS` **c.** `ABRAKADA` **d.** `XYYGIESE` **e.** `XYYGIEST`

3. Given a Feistel-round with 8 bit block length, a round function given by the diagram



and S-box tables:

	000	001	010	011	100	101	110	111
S_0	00	01	00	01	10	11	10	11
S_1	10	00	11	10	11	00	01	01

When the input block is 0000 0000 and the round key is 111 111, what is the output block?

a. 0000 1101 **b.** 0000 1011 **c.** 0000 0000 **d.** 1101 0000 **e.** 1011 0000

4. The RSA encryption of 1234 under the public key $(2743484263429355401, 3)$ is:

a. 12340000 **b.** 18790809 **c.** 8756543 **d.** 726376 **e.** 1879080904

5. The RSA decryption exponent when $n = 713 = 23 \cdot 31$ and $e = 7$ is

a. 232 **b.** 283 **c.** 180 **d.** 70 **e.** 700

6. 7^{43} is congruent modulo 41 with which of the following numbers:

a. 343 **b.** 7 **c.** 49 **d.** 8 **e.** 15

7. Which of the following numbers are congruent to 2 modulo 3, 4 modulo 5 and 7 modulo 8?

a. 7 **b.** 1 **c.** -1 **d.** -119 **e.** 119

8. There is a number congruent to 2 modulo 5 and 3 modulo 7 between which two numbers:

a. 7 and 13 **b.** 14 and 20 **c.** 21 and 27 **d.** 28 and 34 **e.** 35 and 41

Answers

NOTE! Do not write your name or student number on this sheet.

Mark your answers in the following table (some questions may have more than one correct answer).

	a	b	c	d	e
1		•			
2					•
3	•				
4					•
5		•			
6	•				•
7			•		•
8		•			

If you have any comments (such as constructive criticism, criticism, complaints) regarding the classes, please write in the below box: