MATC16 Cryptography and Coding Theory
Gábor Pete
University of Toronto Scarborough

Midterm Test (Feb 24, 2009)

YOUR NAME:

DO NOT OPEN THIS BOOKLET UNTIL INSTRUCTED TO DO SO.

INSTRUCTIONS:

There are 6 numbered pages in this exam. Make sure that, at the start of the exam, this booklet has all its pages. Write your name on each of the odd sides.

Try to answer all questions, indicating all the steps you are making. Show your work. However, verbal explanations shouldn't be lengthy.

You have 110 minutes, that's a lot of time, but not infinite.

The maximum possible score is 50 points.

Calculators are permitted, but the extended Euclidean algorithm and the matrix inversion formula have to be written out, if they are needed in a problem.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

q	r	s	t	u	v	w	x	y	z
16	17	18	19	20	21	22	23	24	25

Problem 1. (5×2 **points)**

(a) What is a public key cryptosystem?

(b) What is a private (symmetric) key cryptosystem?

(c) What is a substitution cipher?

(d) Define the non-repudiation requirement for a cryptosystem. Explain why standard symmetric key systems fail to satisfy it.

(e) What is a one-time pad?

Problem 2. (3×3 **points**)

(a) In the Vigenère cryptosystem, if Alice first encrypts a plaintext with the keyword ALICE, then encrypts the resulting ciphertext with the keyword BOB, is that safer than encrypting only with ALICE?

(b) How does a known plaintext attack work against Vigenère?

(c) Summarize in two or three sentences how a ciphertext only attack works against Vigenère.

Problem 3. (8+3 points)

(a) The plaintext *fool* is encrypted with a 2×2 Hill cipher, resulting in the ciphertext *WISE*. What is the encryption matrix? **(b)** Is it wise to use this matrix for encryption?

Problem 4. (7 points)

Assume that the 9-round Simplified DES, using the key K, encrypts the plaintext P into the ciphertext C. Show that, with the key $K \oplus 11\cdots1$, it encrypts the plaintext $P \oplus 11\cdots1$ into the ciphertext $C \oplus 11\cdots1$. (As usual, $\oplus$ means bitwise addition mod 2. And a hint: you don't need to know the expansion function and the S-boxes.)

Problem 5. (2+2+4 points)

(a) Define Euler's ϕ function.

(b) State the Euler-Fermat theorem.

(c) Compute $1201^{1201} \pmod{707}$.

Problem 6. (5 points)

The encryption exponents $e = 1$ and $e = 2$ should not be used in RSA. Why?