

# 4261 Midterm

## October 25, 2004

This exam is open notes, open book. You may use a non-programmable calculator, but all other electronic devices are prohibited.

Write all answers in the space provided. If you run out of space use the back of the page. If you need scratch paper, ask a TA or the professor. Exam starts at 4:10 and ends at 5:25. Total no. of points is 100. Write your name and email address on the top of any *loose* page.

It is highly recommended that you read the entire exam before proceeding as problems are not written in order of difficulty.

Question:	1	2	3	Total
Points:	40	40	20	100
Score:				

4261 Midterm (continued)

1. Short Answer. Unjustified numerical answers receive no credit.

(a) (8 points) What are the last 2 digits of  $2004^{2004}$  base-10?

(b) (8 points) What is the probability that a random element in  $\mathbb{Z}_{16001}^*$  is primitive? You may assume that 16,001 is prime.

(c) (8 points) How many cube roots does 7 have in  $\mathbb{Z}_{33}^*$  ?

(d) (8 points) How many square roots does 9 have in  $\mathbb{Z}_{561}$  ?

(e) (8 points) It is known that 5 and 13 are primitive in  $\mathbb{Z}_{47}^*$ . The following equation has been discovered:  $5^9 13^{21} \equiv_{47} 5^{13} 13^{29}$ . Find  $\text{Dlog}_{13}(5) \pmod{47}$ .

4261 Midterm (continued)

2. (40 points) Block Ciphers and Perfect Secrecy.

Described below are two block ciphers  $BC_a, BC_b$ . In each case, plaintexts and ciphertexts are 64-bit blocks so  $\mathcal{P} = \mathcal{C} = \mathbb{Z}_2^{64}$ . Keyspace  $\mathcal{K}$  and encryption and decryption functions are defined below. One of the block ciphers satisfies perfect secrecy, while the other does not. Determine whether the given block cipher is perfect<sup>1</sup>. Prove your claim in each case.

- (a) For  $BC_a$  we view each block as describing a 64-bit number so cipherspace/plainspace is identified with  $\mathbb{Z}_{2^{64}}$ . Keys are 64 bits long as well, but we view the first 63 bits as describing a number in  $\mathbb{Z}_{2^{63}}$  and the last bit as a number in  $\mathbb{Z}_2$ ; in other words,  $\mathcal{K} = \mathbb{Z}_{2^{63}} \times \mathbb{Z}_2$ . For a key  $K = (m, n)$  with  $m \in \mathbb{Z}_{2^{63}}, n \in \mathbb{Z}_2$  view  $m, n$  as residing in  $\mathbb{Z}_{2^{64}}$  and define encryption by setting  $e_{(m,n)}(x) = (2m + 1)x - n$ .

- (b)  $BC_b$  is defined as follows:  $\mathcal{K} = \mathbb{Z}_2^{128}$ . Encryption is given by  $e_k(x) = \sigma(x) \oplus k_L \oplus k_R^R$ . Here  $\sigma$  is some fixed 64-bit (one-to-one) substitution,  $k_L$  is the left half of  $k$  (the first 64 bits) and  $k_R^R$  is the reversal of the right half of  $k$ .

---

<sup>1</sup>Here we are only asking if the block cipher is perfect when a single block is transmitted; neither will be perfect if more than one block is transmitted per key.

4261 Midterm (continued)

3. Classical Cryptography. Consider the following generalization of the Hill cipher where instead of only multiplying by a matrix, we also add a vector. In particular,  $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^n$  ( $n$ -dimensional column vectors),  $\mathcal{K} = M_n(26)^* \times \mathbb{Z}_{26}^n$  where each key  $K$  is composed by an invertible matrix and vector, i.e.  $K = (M, v)$  and encryption is defined by  $e_K(x) = Mx + v$ .

(a) (8 points) Suppose we know that the ciphertext is  $y = \begin{pmatrix} 24 \\ 15 \end{pmatrix}$ , and that the key was

$K = \left( \begin{pmatrix} 11 & 4 \\ 1 & 17 \end{pmatrix}, \begin{pmatrix} 5 \\ 9 \end{pmatrix} \right)$ . What is the plaintext  $x$ ? Justify.

(b) (12 points) Explain how to cryptanalyze this cipher using a known plaintext attack.