

# 4261 Midterm Practice Problems

Below are a bunch of problems to help you prepare for the midterm. Solutions will become available, but you are encouraged to try to solve these first without any solutions.

The exam will be open note, open book. You'll be allowed a non-programmable calculator.

## 1. Classical Cryptography Problems

- (a) Suppose a key-based Substitution cipher was used with key “johnkerrygeorgebush”. What would the key be if you wanted to use the encryption algorithm to decrypt?
- (b) Suppose a brute force attack on the key used in the Substitution Cipher is considered **successful** when the top 10 most frequent English letters guessed are correct, but that we can't tell at all which cipher alphabet letters match which plain alphabet letters when we have less than 10 correct letters. How many (independent) key guesses does a cryptanalyst need to get a 95% confidence rate of success? At a billion keys per second, how long would it take to obtain this confidence level?
- (c) Supposing that the Hill cryptosystem with key  $\begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix}$  was used to obtain the ciphertext “xa”. What was the original plaintext? (Recall that we convert plaintext blocks to numerical column vectors)
- (d) Let  $p$  be a prime number. Consider the cryptosystem  $(P, C, K, E, D)$  with  $P = C = \mathbb{Z}_p$  and encryption functions of the form  $e_k(x) = x^k \pmod p$ .
  - i. What is the largest possible set  $K$  assuming that every  $k$  should produce a different function  $e_k$ . What is the cardinality  $|K|$  for this biggest set?
  - ii. Give a formula for the decryption function  $d_k$ .
  - iii. Suppose you are given a black box for solving the discrete log problem. Describe how to break the cryptosystem using a chosen plaintext attack.

## 2. Perfect Secrecy

- (a) (From Malkin's Fall 2003 Crypto Course) Consider some variations on the one-time pad, where the message space or the key space may be restricted to correspond to combinations of English letters. In particular, let  $\mathcal{L} = \{A, B, \dots, Z\}$  where each letter is represented in binary, using 5 bits. For example,  $A = 00000, B = 00001, C = 00010, D = 00011, E = 00100$  and so on, up to  $Z = 11001$ .

In the schemes below we assume (as usual) that keys  $k \in K$  are chosen uniformly at random, and encryption and decryption proceed as with the one time pad:  $e_k(x) = x \oplus k, d_k(y) = y \oplus k$ . For each scheme answer the following:

1. What are the sizes of the sets  $P$  and  $K$  (as in the definition of cryptosystems  $(P, C, K, E, D)$ )?

3261 Midterm (continued)

2. For each variation, determine whether the scheme satisfies perfect security, and prove your answer.
  - i. Let  $P = K = \mathcal{L}^5$ . That is, each message and each key consists of a binary representation of 5 letters. For example, we could have a message  $m = HELLO = 00111\ 00100\ 01011\ 01011\ 01110$ , and a key  $k = ZGEMP = 11001\ 00110\ 00100\ 01100\ 01111$ .
  - ii. Let  $P = \mathcal{L}^5$ ,  $K = \{0, 1\}^{25}$ .
  - iii. Let  $P = \{0, 1\}^{25}$ ,  $K = \mathcal{L}^5$ .
- (b) (Another problem from Malkin's Fall 2003 Crypto Course) In this problem you are asked to design two encryption schemes – one completely insecure, and the other perfectly secure – satisfying certain properties. These constructions may seem artificial, but they demonstrate an important point that is relevant also for natural, real life schemes.

For each part, you should define your constructed scheme  $(P, C, K, E, D)$ , and argue intuitively (without formal proof) why this construction satisfies the conditions of the problem.

- i. Give an example of a (bad) private-key encryption scheme, where from seeing the ciphertext Eve can always recover the corresponding plaintext, yet she can gain no information whatsoever about the key.
  - ii. Give an example of a perfectly secure private-key encryption scheme, where from seeing a ciphertext Eve can learn most bits of the key.
3. Block Ciphers

- (a) Suppose that we happened to know that a block cipher on  $N$ -bit blocks was a group in the following sense: Given two keys  $k_1, k_2$  there is a third key  $k_3 = k_1 \circ k_2$  such that encrypting by  $k_1$  then  $k_2$  is equivalent to encrypting by  $k_3$ . In other words,  $e_{k_2} \circ e_{k_1} = e_{k_1 \circ k_2}$ . (DES has been proven to *NOT* satisfy this property). Furthermore, suppose that the structure of the group is well known, and that it is in fact  $\mathbb{Z}_2^N$  (bitstrings of length  $N$  with addition being bitwise XOR). Propose a method for cracking the block-cipher which is much more efficient than searching the entire key space. *HINT*: this is called a **meet in the middle** attack.
- (b) Figure out what the following symbols stand for in my block-cipher lecture:

$$\pi_s, \sigma, \rho, \xi, \kappa$$

Internalize my simplified formulas given there for Substitution Permutation Networks, and Feistel Networks.

4. Number Theory

- (a) Use a cheap calculator to calculate  $1,000,001 \pmod{2341}$ .

3261 Midterm (continued)

- (b) Find integers  $x, y$  such that  $17x + 101y = 1$ .
- (c) Solve the equation  $7d \pmod{30} = 9$  for  $d$ .
- (d) Prove that if  $n|ab$  and  $n$  is relatively prime to  $a$  then  $n|b$ .
- (e) Give an upper bound on the number of multiplications needed to compute  $g^{100}$  inside a group  $G$ .
- (f) Suppose that  $x \in [0, 69]$  satisfies  $x \pmod{7} = 2$  and  $x \pmod{10} = 3$ . Use the Chinese Remainder Theorem to find  $x$ .
- (g) If  $5^{1000}$  is expressed in hexadecimal notation, what is its last digit?
- (h) A Carmichael number is a composite number  $n$  which satisfies Fermat's little theorem in that  $a^n \pmod{n} = a$  for all  $a$ . Prove that  $561 = 3 \cdot 11 \cdot 17$  is a Carmichael number.
- (i) Given  $n|(p-1)$  with  $p$  prime. Formulate and prove a theorem which tells you exactly how many different solutions there are to  $x^n \pmod{p} = 1$ .
- (j) Consider the Discrete-Log Hash function  $h_k$  with key  $k = (p, q, \alpha, \beta) = (51, 103, 5, 6)$ . It has been detected that  $h_k(42) = h_k(214)$ . Use this fact to compute  $\text{Dlog}_5(6)$  and  $\text{Dlog}_6(5) \pmod{103}$ .
- (k) Find all the square roots of  $56 \pmod{143}$ .
- (l) Find the smallest primitive element in  $\mathbb{Z}_{97}^*$ .