CS/ECE/MATH 435 FINAL, FALL 2009

Nigel Boston

For full credit you must explain your reasoning (except in question 1). Answer the questions in any order.

1. (4 points) Are the following statements true or false? No justification is needed for your answers to this question.

(a) Elliptic curve cryptography uses a form of Diffie-Hellman key exchange.

(b) Hill ciphers acting on blocks of length two have perfect secrecy.

(c) A cryptographic hash function must be a 1-1 function, i.e. send different inputs to different outputs.

(d) In $\mathbf{Z}_N$, where N is a product of two distinct odd primes, there are exactly two square roots of 1.

2. (9 points) (a) Give (explicitly) an example of a *Feistel cipher*.

(b) Give an overview of the main components of DES (the Data Encryption Standard) or of AES (the Advanced Encryption Standard). Do one or or the other, not both. Indicate at least two security features in the design.

(c) When DES was compromised, why did they turn to triple DES instead of just double DES? Explain carefully why encrypting twice with different DES keys does not yield as much security as one might hope.

3. (9 points) (a) Define *affine cipher*. Make sure you give the formal definition showing that these form a cryptosystem. Is it polyalphabetic?

(b) You intercept the message RPIID ISUWD OYGRP IGUGR IS, which has been encrypted by an affine cipher. What does frequency analysis suggest?

(c) Recall that the most common digrams in English are TH and HE. Find the decryption and encryption functions for the cipher. Decipher the message.

4. (9 points) (a) Describe in detail the RSA cryptosystem.

(b) An RSA cryptosystem has public key $N = 55$ and $e = 3$. Letters are converted to numbers by $A \mapsto 2, B \mapsto 3, ..., Z \mapsto 27$. Encrypt the message CIA.

(c) Find the private key. Decrypt the message $8, 9, 51$.

(d) Suppose an RSA cryptosystem with modulus N having 2048 bits is used but with the same method of converting letters to numbers. Suppose that by frequency analysis we guess that numbers n_1, n_2, n_3, n_4 stand for A, C, I, and O respectively. How does knowing n_1, n_2, n_3, n_4 tell us information about the modulus N?

5. (9 points) (a) Define *Vigenere cipher*. Explain why a linear feedback shift register (LFSR) produces a Vigenere cipher.

(b) A linear feedback shift register with 4 cells produces the bit stream 100010100. Find the explicit rule that it is using to generate the next bit. What is its period?

(c) Suppose that letters are converted to binary strings of length 5 by $A \mapsto 00000, B \mapsto 00001, C \mapsto 00010, ..., Z \mapsto 11001$. Using the above bit stream as the key, encrypt the message BYE.

(d) Describe Kasiski analysis. Could Kasiski analysis be used to decrypt a long enough English message encrypted as in (c)?