YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 467b: Cryptography and Computer Security | Handout #12
Professor M. J. Fischer | February 24, 2005

Midterm Examination

Instructions:

This is a closed book examination. *Answer any 6 of the following 7 questions*. Write the numbers of the six questions that you want graded on the cover of your bluebook. All questions count equally. You have 75 minutes. Remember to write your name on your bluebook and to justify your answers. Good Luck!

Problem 1: Caeser cipher

(a) Describe the Caeser Cipher.

(b) What is the size of the key space?

(c) Describe what it means for a cipher to be information-theoretically secure.

(d) Under what conditions is the Caeser Cipher information-theoretically secure?

(e) Describe at least two ways of breaking a Caeser cipher on an English-language message.

Problem 2: Feistel network

Consider a block cipher using 8-bit blocks that is based on the basic DES architecture (Feistel network) with two rounds and no initial or final permutation. The scrambling function for round i is $f_i(x, K) = (2i \cdot K)^x \bmod 15$, for $i = 1, 2$, where the key K is a member of $\mathbf{Z}_{15}$.

If $K = 7$ and the ciphertext is 00111111, what is the plaintext? Draw the picture of the Feistel Cipher network to help you, and show your intermediate results.

Problem 3: Message authentication code

(a) What is a Message Authentication Code (MAC)?

(b) Describe how you would design a way to compute a MAC using the block cipher of problem 2 above.

Problem 4: Chinese remainder theorem

Let $n = 13 \times 9 = 117$.

(a) Find a number $x \in \mathbf{Z}_n$ such that: $\begin{cases} x \equiv 6 \pmod{13} \\ x \equiv 3 \pmod{9}. \end{cases}$

(b) Explain why the number x you found in part (a) is unique in $\mathbf{Z}_n$.

(over)

Problem 5: Euler's theorem

(a) Calculate $\phi(77)$ and $\phi(\phi(77))$.

(b) Find a positive integer $x < 101$ such that $10^{5^{101}} \equiv 10^{5^x} \pmod{77}$.

Problem 6: Discrete logarithm

(a) Find a primitive root of 17. Justify your answer.

(b) Find $\log_b 5 \pmod{17}$, where b is the primitive root you found in part (a).

Problem 7: Simple block cipher

Alice and Bob have designed a very simple block cipher with the following encryption protocol:

1. The message is a binary string. It is padded at the right-most end with 0's so that it's length is divisible by 8.
2. The padded message is split into blocks of 8 bits each.
3. A further block of 8 bits is appended at the right-most end which contains the length of the original message, in bits. (It is assumed that messages are of length less than 2^8 so that the length will fit into an 8-bit block)
4. Alice and Bob agree on a symmetric key of 8 bits.
5. Starting with the left-most message block:
   i. The key is XORed with the message block to obtain the ciphertext block.
   ii. The message block and the key are then added together (using ordinary binary integer addition) and the 8 most significant bits form the key for the next block.

Step 5 is repeated until all of the message blocks have been encrypted. For example, the message

$$11010011 \;\; 11001101 \;\; 10001010 \;\; 1101$$

is padded with 4 zeros and length byte 00011100 to become

$$11010011 \;\; 11001101 \;\; 10001010 \;\; 11010000 \;\; 00011100$$

Using the key 01100110, the message is encrypted to produce the following ciphertext:

$$10110101 \;\; 01010001 \;\; 00111110 \;\; 01001111 \;\; 10101011.$$

Questions:

(a) Write the corresponding decryption protocol and demonstrate it by decrypting the ciphertext

$$11001100 \;\; 01111000 \;\; 11101100 \;\; 10010010$$

using the same key 01100110.

(b) Discuss the security of Alice and Bob's symmetric key cryptosystem.

(end of exam)