YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 467a: Cryptography and Computer Security *Handout #11*
Professor M. J. Fischer *October 13, 2005*

Midterm Examination

Instructions:

This is a closed book examination. *Answer any 5 of the following 6 questions.* Write the numbers of the **five** 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: Hill cipher

Eve captures Bob's Hill cipher machine, which uses a 2-by-2 matrix $M \bmod 26$. She tries a chosen plaintext attack. She finds that the plaintext ba encrypts to HC and the plaintext zz encrypts to GT. What is the matrix M?

Problem 2: Information-theoretic security

(a) Consider the cryptosystem with $\mathcal{M} = \{a, b\}$ and $\mathcal{C} = \mathcal{K} = \{0, 1, 2\}$. The encryption function is given by $E_k(m) = (m + k) \bmod 3$. Is this system information-theoretically secure? Explain.

(b) Suppose now $\mathcal{M} = \{a, b\}$, $\mathcal{C} = \{0, 1\}$, and $\mathcal{K} = \{0, 1, 2\}$. Does there exist an information-theoretically secure encryption function on these sets? Explain.

Problem 3: Feistel network

Happy Hacker was asked to implement a Feistel network, but he couldn't quite remember how stage i worked, so he wrote down the equations:

$$\begin{aligned} L_{i+1} &= R_i \\ R_{i+1} &= f(L_i \oplus R_i, K_i). \end{aligned}$$

However, Happy was having trouble figuring how to decrypt messages encoded in this way.

(a) Show why Happy couldn't come up with a general decryption algorithm by exhibiting a particular function f_1 which makes it impossible to recover (L_i, R_i) from (L_{i+1}, R_{i+1}) when f_1 is used for f in Happy's scheme.

(b) Would have decryption been possible using your function f_1 of part (a) if Happy had gotten the Feistel network correct in the first place? Explain.

(c) Happy finally noticed that he could decrypt if he chose f to be

$$f_2(X, K) = X \oplus K.$$

Explain how to decrypt in this case.

(d) What can you say about the security of the system using Happy's function f_2 from part (c)?

(over)

Problem 4: Chaining modes

Let $E_k(m)$, $D_k(c)$ be a block cipher. Fischer Spiffy Mixer mode (FSM) encrypts a sequence of message blocks $m_1, m_2, \ldots$ by the sequence of ciphertext blocks $c_1, c_2, \ldots$ using the following method:

$$c_i = m_{i-1} \oplus E_k(m_i \oplus c_{i-1})$$

m_0 and c_0 are fixed (public) initialization vectors.

(a) Describe how to decrypt.

(b) Suppose ciphertext block c_3 is damaged in transit. Which plaintext blocks become undecipherable as a result? Explain.

Problem 5: RSA decryption exponent

Bob chooses an RSA modulus $n = 13 \times 7 = 91$.

(a) He wants an easily-remembered encryption exponent, so he wants to use either $e = 10$ (the number of decimal digits) or $e = 26$ (the size of the English alphabet). However, one of these will not work. Which one won't work and why?

(b) Since Bob didn't study for his crypto midterm, he couldn't answer part (a). To play it safe, he decided to stick to primes, so he choose $e = 17$. Find the corresponding decryption exponent d and show how you derived it.

Problem 6: An attack on RSA

Bob received an RSA-encoded message c from Alice. He decrypted it using the fast modular exponentiation algorithm described in class and reproduced here:

```
/* computes m^e mod n iteratively */
int modexp( int m, int e, int n)
{
  int r = 1;
  while ( e > 0 ) {
    if ( (e&1) == 1 ) r = r*m % n;
    e /= 2;
    m = m*m % n;
  }
  return r;
}
```

Nasty manages to break into Bob's machine and to get a snapshot of the stack frame of Bob's process while it was in the middle of decrypting c. In this way, Nasty learns the values of the variables `r`, `e`, `m`, `n` as they were at some instant in time during the execution of `modexp`.

(a) Explain why `modexp` is relevant to Bob's task of decrypting c.

(b) Explain how Nasty can use the values he has captured to decrypt c.

(c) Alice sends Bob another RSA-encoded message c'. Can Nasty also decrypt it with the information already at hand? Why or why not?

(end of exam)