Midterm 1997
Out: October 24, 1997
Due: October 31, 9pm 1997

Instructions: Submit your answers on these pages. You shouldn’t need extra room (if you do, staple extra sheets to these pages). You should not discuss any of the material with anybody other than the CS007 TA’s and the CS007 professor. If you have a reasonable understanding of the material, these problems should not be difficult. If you are having difficulty, it may be because you are making a problem more difficult than it really is. Good luck!

1. Sign your name to the following statement:

   During the period the midterm was in progress, I did not discuss course material anybody but the CS007 TA’s and instructor. I neither gave help to nor received help from any other student, including looking at other’s work or showing mine.

2. (8 Points) Compute the following. Give the answer in standard form. That is, your answer should be between 0 and one less than the modulus.

   (a) $16 + 2 \pmod{8}$

   (b) $57 \cdot 73 \pmod{17}$

   (c) $3 \cdot (87 - 5) \pmod{7}$

   (d) $(-5) - (-11) \pmod{10}$
3. **(12 Points)** Fill in the following table of mod-17 inverses, then calculate the following mod 17.

<table>
<thead>
<tr>
<th>$x$</th>
<th>$x^{-1}$ (mod 17)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
</tr>
</tbody>
</table>

(a) $2/7$

(b) $3/5$

(c) $8/5$

(d) $-(3/4)$

(e) $-(9/2)$

4. **(9 Points)** For each modulus $m$ given below, circle the numbers **not** relatively prime to $m$, and then tell us the value of the phi function for $m$.

(a) $m = 25$

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

$\phi(25) =$?

(b) $m = 26$

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

$\phi(26) =$?
(c) \( m = 101 \)
\[
\begin{align*}
0 & 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 \ldots 97 98 99 100 101 \\
\phi(101) = ?
\end{align*}
\]

5. **(12 Points)**

(a) Roughly how many digits does the number \( b \) have? Give a formula.

(b) Suppose the number \( c \) has \( n \) digits and the number \( d \) has \( m \) digits. For each of the following, give a formula in terms of \( m \) and \( n \).

   i. Roughly how many digits does \( 10000 \cdot c \) have?

   ii. Roughly how many digits does \( c + d \) have?

   iii. Roughly how many digits does \( c \cdot d \) have?

   iv. Roughly how many digits does \( c \cdot d^2 \) have?

(c) Say you have five different numbers, each having about \( k \) digits. Roughly how many clock ticks does DigiComp require to multiply all these numbers together? Give a formula in terms of \( k \). Show your work.

6. **(12 Points)** Abbot and Costello work for the NSO, evaluating the security of cryptosystems. They receive the following table as a proposal for an encryption function.
Abbott says

“This system has the following property: For each key, a plaintext chosen randomly according to the uniform distribution (over all possible plaintexts) encrypts to a ciphertext chosen randomly according to the uniform distribution (over all possible ciphertexts).”

Therefore the system achieves perfect secrecy.”

Costello responds

“Abbott, you’re wrong. The system does achieve perfect secrecy but not for the reason you give. In fact, I can rearrange the ciphertexts in the table so as to give an encryption function that has the property you cite but that does not achieve any kind of secrecy!”

Costello is correct.

(a) Show how to rearrange the ciphertexts in the table so as to get an encryption function that has the property Abbott cites but obviously does not achieve secrecy.

(b) Why does the originally proposed encryption achieve perfect secrecy? Explain by referring specifically to the table.

7. (15 Points) Each night at 2:00 am, the Boston Globe sends its text for the next morning’s paper over the phone lines to the printing presses. The text consists of 50,000 symbols, each represented by a number from 0 to 29. Thus the text is represented by a sequence of
50,000 numbers. For security, the Globe encrypts this sequence using a one-time pad. Each
cyphertext number is the mod 30 sum of the corresponding plaintext and key numbers.
The Providence Journal has heard rumors that the Globe will publish a story on the real
reason the Patriots won’t move to Rhode Island. The Journal wants to get the story so as
not to get scooped by the Globe. They hire Eve, renowned for her eavesdropping skills, to
intercept the Globe’s cyphertext as it makes its way to the printing presses. Eve is to intercept
the cyphertext and send it by modem to the Journal’s Department of Sneaky Stunts.
Eve takes the job but has no desire to crawl down sewers and up telephone poles. She therefore
hatches a scheme to trick the Journal by making up a fake cyphertext to send to them. That
way, she can stay warm and comfortable at home.
She knows from previous issues of the Globe that the distribution of symbols is as follows.

```
<table>
<thead>
<tr>
<th>Symbol</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0.012345</td>
</tr>
<tr>
<td>B</td>
<td>0.012345</td>
</tr>
<tr>
<td>C</td>
<td>0.012345</td>
</tr>
</tbody>
</table>
```

She comes up with the following distribution of numbers.

```
<table>
<thead>
<tr>
<th>Number</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.012345</td>
</tr>
<tr>
<td>1</td>
<td>0.012345</td>
</tr>
<tr>
<td>2</td>
<td>0.012345</td>
</tr>
</tbody>
</table>
```

She generates a sequence of 50,000 numbers, each chosen according to the above distribution,
and sends this sequence to the Journal.

(a) Why does the Journal realize she has tried to fool them? Explain precisely and specifically.

(b) How could Eve have successfully fooled the Journal? Explain precisely and specifically.

8. (15 Points) Alice plans to send Bob a message accompanied by a MAC. (The method for generating the MAC is the one we discussed in class; also described in the text.) They have previously agreed on a uniformly random secret key for use with the MAC. The message will be sent in plaintext. The set of possible messages is 0, 1, ..., 12 and the set of possible values of the MAC is also 0, 1, ..., 12. Calculation of the MAC value is done modulo 13.

Eve plans to intercept the message and MAC, and send her own (fake) message, namely 12. She must also pick a fake MAC to accompany this message; her hope is to fool Bob into accepting the fake message as really being from Alice. She therefore needs to know the probability distribution for the MAC that should accompany the message 12 (i.e. if Alice were to send the message 12, what is the distribution of the MAC that would accompany that message?) Eve knows that the key for the MAC was chosen randomly and uniformly.

In each of the following scenarios, help Eve by sketching the distribution of the value of the MAC that should accompany her fake message.

(a) Eve must choose her fake MAC before seeing either the true message or the true MAC. Give the distribution of the MAC that would accompany the message 12.
(b) Eve has intercepted the true message, 1, and the accompanying MAC, 2. Given what Eve now knows, sketch the distribution of the MAC that would accompany the message 12.

(c) Alice started to send the message 1 and the MAC 2, but changed her mind about the message and instead sent the message 2 and the MAC 4. Eve intercepted all this information. Given what Eve now knows, sketch the distribution of the MAC that would
accompany the message 12.

probability

<p>| | | | | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

MAC to accompany message 12

9. (6 Points) Rosencrantz and Guildenstern and you are working for the NSO. The three of you are studying an encryption method. The plaintext is a twenty-digit number, and so is the key. The cyphertext is the mod-$10^{20}$ sum of the plaintext and the key. The group is debating how to select the key in order to achieve the greatest level of secrecy, because they know that the cryptosystem will be used in a highly critical mission: encryption of the 10-letter secret ingredient in a new special, “Hamlette Surprise”, to be served at the Ratty.

Rosencrantz: “Naturally, the key should be chosen at random so that it is unpredictable to eavesdroppers. However, we should ensure that the key is not zero; if the key were zero, the cyphertext would be identical to the plaintext, and the eavesdropper would notice. Therefore, I propose that the key should be chosen uniformly among $1, 2, \ldots, 9999999999999999$.”

Guildenstern: “I agree that the key should be chosen at random. However, we should ensure that the key is not 111111111111111. After all, since every potential eavesdropper knows that this number is the chef’s favorite number, the first thing the eavesdropper would do would be to try decrypt with this key—if it were indeed the key used, the eavesdropper would notice that the result was an ingredient. I therefore propose that the key should be chosen uniformly among $0, 1, 2, \ldots, 1111111111111110, 1111111111111111, \ldots, 9999999999999999, 99999999999999999999999999999999$. That is, the key can be any twenty-digit number except 1111111111111111.”
(Fill in your response, addressing the proposals of your colleagues. What do you recommend?)

10. (16 Points) Arnold has come up with a new proposal for a highly secure one-way function. The security parameter $k$ is the number of digits of the modulus. We won’t tell you precisely how the function is defined (it’s classified), but we can tell you how long computations take (as a function of $k$). Let $A(x)$ denote the proposed one-way function.

**Forward direction:** Given input $x$, to calculate $A(x)$ takes $2 \cdot k^6$ ticks.

**Backward direction:** Given input $y$, to calculate a pre-image of $y$ under $A$ takes $10 \cdot k^{10}$ ticks.

What do you think of the proposed one-way function, based on what you know? Is it secure enough to recommend for use in financial transactions on the Internet?

11. (12 Points) Consider the following encryption function:

- **Plainspace:** 0, 1, 2, 3, 4
- **Keyspace:** 0, 1, 2, 3, 4
- **Cypherspace:** 0, 1, 2, 3, 4

$$f(plain, key) = plain^3 + key^2 \mod 5$$

(a) For each possible key $k$, the corresponding projection of the encryption function, $Encrypt_{key=k}$, is a function whose domain is the set of plaintexts and whose codomain is the set of cyphertexts. Sketch each of these projection functions below.
(b) Is the function uniquely decryptable?

(c) Is the encryption function uniquely de-keyable?

(d) Does the encryption method achieve perfect secrecy? If so, explain why; if not, suggest a function with the same keyspace, plaintext, and cyphertext that does.

12. (8 Points) Prof. Klein wants to provide the CS007 safe’s combination to the TA’s using secret-sharing. The combination is known to be an eight-digit number. Prof. Klein chooses mod-10^8 numbers \( p, q, r, s, t \) so that they obey the following equations.

\[
\begin{align*}
    p + q &\equiv \text{the safe’s combination} \pmod{10^8} \\
    r + s + t &\equiv q \pmod{10^8} \\
    r + q &\equiv \text{the safe’s combination} \pmod{10^8}
\end{align*}
\]

(Obviously, Prof. Klein has inhaled a bit too much chalk dust and has gotten a little confused about secret sharing.) He provides \( p \) to Kevin I., \( q \) to Kevin S., \( r \) to Sandy, \( s \) to Sheryl, and, still confused, \( t \) to Kevin I.

For each group of TA’s given below, say whether or not the group can collectively figure out the combination.

(a) Sandy and Sheryl and Kevin S.

(b) Kevin I. alone

(c) Sandy and Kevin I.
(d) Sheryl and Kevin S.

(e) Sandy and Kevin S.