(25) 1. Complete these tables of addition and multiplication mod 6.

| + | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | | | | 3 | 4 | |
| 1 | | | | 4 | 5 | |
| 2 | | | | 5 | 0 | |
| 3 | | | | 0 | 1 | |
| 4 | | | | 1 | 2 | |
| 5 | | | | 2 | 3 | |

**Addition**

| × | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | | 0 | 0 | | | |
| 1 | | | 2 | 3 | | |
| 2 | | | | 0 | 2 | |
| 3 | | | | | 0 | 3 |
| 4 | | | | | | 2 |
| 5 | | | | | | |

**Multiplication**

Find all solutions of $4x + 1 = 3 \bmod 6$. Briefly explain your answer.

| $n =$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $2^n =$ | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 | 512 | 1024 |

**Powers of 2**

(20) 2. a) What is 29 in binary? Briefly explain your answer.

b) Compute $8^{29} \bmod 13$. Briefly explain your answer.

(15) 3. `Maple` reports that $\left(48^{456}\right)^{789} \bmod 57$ is 39. What then is the value of $\left(48^{789}\right)^{456} \bmod 57$? Briefly explain your answer. No computation should be necessary for this problem.

(20) 4. a) Define **prime number**.

b) Exactly one of the numbers below is prime. Explain why the others are not.

i) 80000 70000 30002

ii) 80000 20000 30007

iii) 90000 70000 40007

(24) 5. Suppose messages in a language are strings of the letters **A**, **B**, **C**, and **D**. So one message might be **AACDB**. The spy memorizes a phrase, such as **B**ald **D**ucks **A**re **C**ute

and uses it to substitute letters: $\begin{cases} \mathbf{A} \to \mathbf{B} & \underline{\text{B}}\text{ald} \\ \mathbf{B} \to \mathbf{D} & \underline{\text{D}}\text{ucks} \\ \mathbf{C} \to \mathbf{A} & \underline{\text{A}}\text{re} \\ \mathbf{D} \to \mathbf{C} & \underline{\text{C}}\text{ute} \end{cases}$.

The message **AACDB** then becomes **BBACD**.

a) Identify the encryption key, the plaintext, and the ciphertext in this system.

b) If **CCBDD** is an encrypted message using this system with the phrase given, what was the original message?

c) Make up another key for the same system, and use it to encrypt the message **BDBAB**. Please be sure to tell me your key!

d) Could your answer to the previous question (an encryption of the message **BDBAB**) possibly have been **CADBC**? Why or why not?

(20) 6. A committee of 3 people wishes to share a secret so that any majority of the committee (at least 2 of them) must agree to have access to the secret, which is the number **17**. Describe explicitly one way that this can be done.

(15) 7. a) Define **one-time pad**.

b) Write the xor of the bitstrings

```
        00011  10101  11010
and                          .
        10101  11100  00110
```

Answer:

```
        _____  _____  _____
```

(30) 8. Write a paragraph or two explaining why an encryption standard might be useful.

**Comments**

Write clearly and logically; support your assertions.

You may care to explain: first, why have *any* encryption scheme available – what purpose does it serve? Second, why might a widely known standard be good?

(30) 9. Write a paragraph or two explaining real world uses of hash functions and digital signatures. Try to give at least one example where a mistake or weakness in the system used could have serious real-world consequences.

**Comments**

Write clearly and logically; support your assertions.

You should certainly try to explain in a non-technical manner what hash functions and digital signatures are. Also indicate how each might be used, and then discuss the consequences of "a mistake or weakness".

# Final Exam
# Math 103, section 99

May 4, 2000

(1) NAME ______________________________________

**Do all problems, in any order.**
**You may use any notes, books, or calculators on this exam.**

| Problem Number | Possible Points | Points Earned: |
|---|---|---|
| 1 | 25 | |
| 2 | 20 | |
| 3 | 15 | |
| 4 | 20 | |
| 5 | 24 | |
| 6 | 20 | |
| 7 | 15 | |
| 8 | 30 | |
| 9 | 30 | |
| Total Points Earned: | | |