Homework 09

Physics II

Due Friday,June 7, 2024

College of the Atlantic. Spring 2024

There is one part to this assignment.

Part 1: WeBWorK. There is no WeBWorK this week.
Part 2: Not WeBWorK. Here are some non-WeBWorK problems this week.

- If you want, you can do these problems in pairs and hand in only one write-up.
- "Hand in" the problem on google classroom. You can take a picture of your work, or type up your work, or scan your work.

1. Encrypt the following message `WATCH OUT FOR THE BEES`. Use the word `BOHR` as a repeating key.

2. Decrypt the following message `ULWOWZZ EWILK HGZB`. The message was encoded using the description for course ES 3018 *Herpetology*.

3. Evaluate the Euler totient function $\phi(N)$ for the following values of N:

   (a) $N = 15$
   (b) $N = 16$
   (c) $N = 17$

   There's no need to include a lengthy write-up, but please show your work.

4. Beowulf uses RSA with $(e = 5, n = 14)$ and sends you the encrypted message `5 8 6`. Decrypt this message, one numeral at a time, using $(d = 11, n = 14)$

5. (You will likely need to use wolframalpha to help you with these computations.) Suppose Anastajia and Beowulf are using an RSA public-key encryption to send a message from Beowulf to Ana. Suppose Ana chooses $p = 97$ and $p_2 = 89$.

   (a) What number n will Beowulf and Ana use as the modulus for their calculations?
   (b) Which of the following are possible choices that Ana could use for the public encryption exponent e?
      i. 89
      ii. 91
      iii. 100
      iv. 101
   (c) Suppose Ana chooses $e = 17$. Show that the choice of $d = 497$ satisfies the criteria for d.
   (d) Suppose that Beowulf wishes to send the message $m = 1001$ to Ana. (The message is the single number 1001, not four digits sent separately.) What would Beowulf get for the encrypted message?
   (e) How would Ana decrypt this message? Try it and see? Does she successfully recover Beowulf's original message?

6. **Optional**. The following message was encoded[1] using a simple substitution scheme. I.e., each letter is encoded as some other letter. Decode the message.

```
R yldre svzex zj r grik fw kyv nyfcv, trccvu sp lj "Lezmvijv", r
grik czdzkvu ze kzdv reu jgrtv. Yv vogvizvetvj yzdjvcw, yzj
kyflxykj reu wvvczexj rj jfdvkyzex jvgrirkvu wifd kyv ivjk |
r bzeu fw fgkztrc uvcljzfe fw yzj tfejtzfljevjj. Kyzj uvcljzfe
zj r bzeu fw gizjfe wfi lj, ivjkiztkzex lj kf fli gvijferc
uvjzivj reu kf rwwvtkzfe wfi r wvn gvijfej evrivjk kf lj.
Fli krjb dljk sv kf wivv flijvcmvj wifd kyzj gizjfe sp nzuvezex
fli tzitcv fw tfdgrjjzfe kf vdsirtv rcc czmzex tivrklivj reu
kyv nyfcv fw erkliv ze zkj svrlkp. Efsfup zj rscv kf rtyzvmv
kyzj tfdgcvkvcp, slk kyv jkizmzex wfi jlty rtyzvmvdvek zj ze
zkjvcw r grik fw kyv czsvirkzfe reu r wfleurkzfe wfi zeevi
jvtlizkp.
```

7. **Optional:** Euler's theorem states that:

$$a^{\phi(N)} = 1 \mod N\,, \tag{1}$$

for any integer N for for any a that is co-prime to N. RSA encryption works because it is possible to find integers e, d, and N such that

$$(m^e)^d = m \mod N\,. \tag{2}$$

In the above equation e is the encryption exponent, d is the decryption exponent, N is the modulus, and m is the message.

Recall that the RSA recipe for finding e, d, and M is as follows:

(a) Choose two prime number p and q.

(b) The modulus N is given by $N = pq$.

(c) Calculate $\phi(N)$. Note that this is fast, since $\phi(pq) = (p-1)(q-1)$, if p and q are both prime.

(d) Choose e such that

  i. $1 < e < \phi(N)$,
  ii. e is co-prime with N and $\phi(N)$.

(e) Choose d such that $de \mod \phi(N) = 1$.

Use Euler's theorem to show that if e, d, and N are chosen as described above, then it follows that Eq. (2) is true.

8. **Optional**. The Vigenère square—the square sorta crossword puzzle lookin thing—is actually an table for addition with letters, where the letters "wrap around". The mathematical term for this would be arithmetic modulo 26. One would refer to the letters as the set $\mathbb{Z}_{26}$, which is a set with arithmetic modulo 26.

[1] I wrote this problem ten years ago. I have no idea what the correct answer is, but I recall being told by a student two years ago who cracked this code that the statement is kinda weird and philosophical.

(a) Write out the addition and multiplication tables for $\mathbb{Z}_5$. (For example, the elements of $\mathbb{Z}_5$ are $\{0, 1, 2, 3, 4\}$, $2 + 4 = 1$, and $2 \times 4 = 3$

(b) Write out the addition and multiplication tables for $\mathbb{Z}_6$.

(c) Note that there is a difference between the multiplcation tables for $\mathbb{Z}_5$ and $\mathbb{Z}_6$. For $\mathbb{Z}_5$, each element appears once and only once in each row (except for the frist row), whereas this is not the case for $\mathbb{Z}_6$. Why do you think this is the case? What is different about $\mathbb{Z}_5$ and $\mathbb{Z}_6$? Make a conjecture about what must be true about n so that in the multiplication table for $\mathbb{Z}_n$ each number appears once and only once in each row except for the top row.

(d) The next three problems lead you through a proof of the conjecture you might have formulated above. These problems are from Susan Loepp and William K. Wooters, *Protecting Information: Fomr Classical Error Correction to Quantum Cryptography*, Cambridge University Press, 2006.

   i. Let $a \in \mathbb{Z}_n$. Show that a and n are relatively prime (the only common demonimator of both a and n is 1) if and only if there exists an element $b \in \mathbb{Z}N$ such that $ab = 1$.

   ii. Let $a \in \mathbb{Z}_n$. Show that a and n are relatively prime if and only if a's row in the multiplication table of $\mathbb{Z}_n$ contains every element of $\mathbb{Z}_n$.

   iii. Show that n is a prime number if and only if in the multiplication table for $\mathbb{Z}_n$, except for the first row, all elements of $\mathbb{Z}_n$ appear in each row.

   The symbol "$\in$" is read "is in", or "is an element of". The statement $a \in \mathbb{Z}_n$ means that a is an element of or belongs to $\mathbb{Z}_n$. For example, $4 \in \mathbb{Z}_6$, but $7 \notin \mathbb{Z}_6$.