CMSC 389 Final. VERSION α

1. This is a closed book exam, though ONE sheet of notes is allowed. **You may not use a Calculator**. If you have a question during the exam, please raise your hand.
2. There are 5 problems which add up to 100 points. The exam is 1 hours 30 minutes.
3. In order to be eligible for as much partial credit as possible, show all of your work for each problem, **write legibly**, and **clearly indicate** your answers. Credit **cannot** be given for illegible answers.
4. After the last page there is paper for scratch work.
5. Please write out the following statement: "*I pledge on my honor that I will not give or receive any unauthorized assistance on this examination.*"

6. Fill in the following:

NAME :
SIGNATURE :
SID :

SCORES ON PROBLEMS (FOR OUR USE)

Prob 1:
Prob 2:
Prob 3:
Prob 4:
Prob 5:
TOTAL

1. (20 points) No explanations required.

   (a) Daleks use an alphabet on 200 letters. How many affine ciphers can they use?

   (b) What is $2^{10,000} \pmod{14}$?

   (c) Alice and Bob use Diffie-Helman with $p = 11$, $g = 2$. Alice picks $a = 5$ and Bob picks $b = 5$ (not a typo- they picked the same numbers). What is their shared secret key?

   (d) Alice and Bob use the 1-time pad. The key is 00000000. Alice wants to send 0011. What does she send?

SOLUTION TO PROBLEM 1

Part a:

We need to compute how many numbers that are relatively prime with 200. We know that $200 = 2^3 \times 5^2$, so

$$\phi(200) = \phi(2^3) \times \phi(5^2) = (2^3 - 2^2) \times (5^2 - 5^1) = 4 \times 20 = 80$$

NOTE that in homework, we have already proved that given p and q are two primes, then

$$\phi(p^a q^b) = (p^a - p^{a-1})(q^b - q^{b-1})$$

Part b:

We first want to compute $\phi(14)$. Since we know $14 = 2 \times 7$, we have

$$\phi(14) = \phi(2) \times \phi(7) = 1 \times 6 = 6$$

It is known that

$$\forall n, \forall\ a\ \texttt{such that}\ 0 \leq a \leq (n-1), a^{\phi(n)} \equiv 1 \pmod{n}$$

Therefore

$$2^6 \equiv 1 \pmod{14}$$

In addition,

$$10000 = 1666 \times 6 + 4$$

Thus, we have

$$2^{10000} \equiv 2^{1666 \times 6 + 4} \equiv \left(2^6\right)^{1666} \times 2^4 \equiv 1^{1666} \times 16 \equiv 16 \equiv 2 \pmod{14}$$

Part c:

Alice will send $g^a \pmod{p}$ to Bob, so she will actually send

$$2^5 \equiv 32 \equiv 10 \pmod{11}$$

Bob will compute the shared secret key by computing

$$10^5 \equiv (-1)^5 \equiv (-1) \equiv 10 \pmod{11}$$

Therefore, the shared secret key is 10.

Part c:

We need to perform an $\oplus$ now. Alice will send $0011 \oplus 00000000$, which is equal to 0011 itself.

2. (20 points) For each statement below state if it is TRUE or FALSE. EXPLAIN your answer and be COHERENT, CLEAR, and CONCISE. Someone who has NOT taken this course but UNDERSTANDS the basic concepts should be able to understand the answers (some such person might grade this question.)

   (a) Eve knows that Alice and Bob are using the Vig cipher and the key word is a short sentence in English. Given a very long text that is coded by the Vig cipher Eve can find the length of the keyword.

   (b) If Alice and Bob use a Vig cipher where the keyword is generated randomly and is as long as the text, then that cipher is UNCRACKABLE.

   (c) Assume the Vorlons use a 27 letter alphabet. There is an

   $$s \in \{1, \ldots, 26\}$$

   (NOTE- shifting by 0 NOT allowed) such that if they use a shift cipher with shift s then the code and decode table will be the same.

SOLUTION TO PROBLEM 2

Part a: THE ANSWER IS TRUE.

We can still perform an attack on this Vigenere cipher by finding possible key lengths (by looking at repeated sequence of letters), and then compute the key. Since the key length is short, it is possible for Eve to actually compute the key length first, and then she can also compute the actual key after that.

Part b: THE ANSWER IS TRUE.

As long as the keyword is generated randomly and have the same length with the text, then this is similar to one-time pad. We mentioned that one-time pad is UNCRACKABLE because the message will look random to Eve. Similarly, we can conclude that this Vigenere cipher is UNCRACKABLE.

Part c: THE ANSWER IS FALSE.

Let $f(x) = x + s \pmod{27}$, $s \neq 0$ be the coding function for this shift cipher.

Let $g(x) = x - s \pmod{27}$, $s \neq 0$ be the decoding function for this shift cipher.

Since we want the code and decode table to be the same, then

$$f(x) = g(x) \Leftrightarrow x + s \equiv x - s \pmod{27} \Leftrightarrow 2s = 0 \pmod{27}$$

We will leave this to you to prove that there is no such $s \in \{1, \ldots, 26\}$ such that $2s \equiv 0 \pmod{27}$. Therefore, this statement is FALSE.

3. (10 points) For the scenario below discuss if Eve can, with todays technology and mathematics, crack the code.

   Alice and Bob are using Diffie-Helman. They use large values of p, g. They happen to pick a, b s.t. $1 \leq a \leq \log p$ and $p/3 \leq b \leq 2p/3$, and Eve knows this.

   SOLUTION TO PROBLEM 3
   YES SHE CAN CRACK IT. Eve will see g^a go from Alice to Bob and from Bob to Alice. Eve KNOWS that $1 \leq a \leq \log p$ so she can try ALL $g^0, g^1, \ldots, g^{\log p}$ which is only $\log p$ possibilities. Hence she can find a. Once she has a, and she also knows g^b, she knows the $(g^b)^a = g^{ab}$ which is the shared secret string.

4. (ADDED - THIS WAS NOT ON LAST YEARS FINAL BUT YOU WANTED A VERIF SS PROBLEM.)

Zelda wants to do VERIFIABLE Secret Sharing with A_1, A_2, A_3, A_4 so that if 2 of them get together they can find out the secret but any 1 cannot. She uses the mod field p where p is large. But alas, A_4 has a computer that can solve Discrete Log problems mod p. Alice gives out the shares and the appropriate powers of g. For each of the following statements state TRUE or FALSE and EXPLAIN your answer.

(a) A_4 learn the secret.

(b) A_4 learn A_1's share.

(c) A_4 give a false value of $f(4)$ and have the other players not realize this.

SOLUTION

Recall that Zelda will

- Pick random a_1.
- Form $f(x) = a_1x + s$.
- Give A_1 $f(1)$, A_2 $f(2)$, A_3 $f(3)$, and A_4 $f(4)$.
- Give EVERYONE g^{a_1}, g^s.

a) YES. Since A_4 has g^s and can compute Discrete Log, he can get s.

b) YES. Since A_4 has g^s and g^{a_1} and can compute Discrete Log, he can get a_1 and s. Hence he can compute $f(1)$ and learn A_1's share.

c) NO. The Verifiable part of Verifiable Secret Sharing still works. Assume that A_4 gives a value $f(4)' \neq f(4)$. We show he gets caught. EVERYONE has g^{a_1} and g^s, so EVERYONE can compute $(g^{a_1})^4 \times g^s = g^{4a_1+s} = g^{f(4)}$. Once A_4 reveals his (false) value $f(4)'$, EVERYONE will compute $g^{f(4)'}$ and they will find out its NOT $g^{f(4)}$.