CMSC 389T HW5 SOLUTION

Phong Dinh and William Gasarch

Jan 11, 2017

Problem 2

Computing the following using the repeated squaring method.
Part a: $2^{20} \pmod{17}$

Write 20 in binary representation, we get $20 = (10100)_2$.
That means we really want to compute

$$2^{2^4} \times 2^{2^2} \pmod{17}$$

We have

$$\begin{aligned}
2^{2^0} &\equiv 2^1 \equiv 2 \pmod{17} \\
2^{2^1} &\equiv 2^2 \equiv 4 \pmod{17} \\
2^{2^2} &\equiv 2^4 \equiv 16 \pmod{17} \\
2^{2^3} &\equiv \left(2^{2^2}\right)^2 \equiv 16^2 \pmod{17}
\end{aligned}$$

Since we know $16 \equiv -1 \pmod{17}$, thus we have

$$\begin{aligned}
2^{2^3} &\equiv 16^2 \equiv (-1)^2 \equiv 1 \pmod{17} \\
2^{2^4} &\equiv \left(2^{2^3}\right)^2 \equiv 1^2 \equiv 1 \pmod{17}
\end{aligned}$$

Therefore,

$$\begin{aligned}
2^{20} &\equiv \left(2^{2^4}\right) \times \left(2^{2^2}\right) \pmod{17} \\
&\equiv 1 \times 16 \pmod{17} \\
&\equiv 16 \pmod{17}
\end{aligned}$$

We OMIT the solution for the rest of the problems since the technique required to solve other parts are similart to part a.

Problem 3

Alice and Bob are going to do Diffie Helman with $p = 29$ and $g = 2$.
Part a: Assume that Alice picks $a = 10$. What does Alice send Bob?
Alice will send $g^a \pmod{p}$, thus Alice sends

$$2^{10} \pmod{29}$$

Using repeated squaring method, we write $10 = (1010)_2$, then what we really want is

$$2^{2^3} \times 2^{2^1} \pmod{29}$$

$$\begin{aligned} 2^{2^1} &\equiv 2^2 \equiv 4 \pmod{29} \\ 2^{2^2} &\equiv \left(2^{2^1}\right)^2 \equiv 4^2 \equiv 16 \pmod{29} \\ 2^{2^3} &\equiv \left(2^{2^2}\right)^2 \equiv 16^2 \equiv 24 \pmod{29} \end{aligned}$$

Thus, we have

$$g^a \equiv 2^{10} \equiv 4 \times 24 \equiv 96 \equiv 8 \pmod{29}$$

Therefore, Alice wants to send Bob 9.

Part b: Assume that Bob sends $b = 8$. What does Bob send Alice?
Bob wants to send $g^b \pmod{p}$, then Bob wants to send

$$2^8 \pmod{29}$$

From the previous part, we know

$$2^{2^3} \equiv 24 \pmod{29}$$

Thus, Bob wants to send Alice 24.

Part c: What is the shared secret key?
The shared secret key is $g^{ab} \pmod{p}$. From Alice's side, she can compute this by

$$24^{10} \pmod{29}$$

Again, we will use repeated squaring method to compute $24^{10} \pmod{29}$. We will OMIT this step here.

After that, we get

$$24^{10} \equiv 20 \pmod{29}$$

This is our shared secret key.
To confirm that our solution is correct, we can also compute the shared secret key from Bob's side as well. Bob will compute $8^8 \pmod{29}$. By using repeated squaring method (again, we OMIT it here), we get

$$8^8 \equiv 20 \pmod{29}$$

In binary, $20 = (10100)_2$.
<u>Part d</u>: If Alice uses a and Bob uses b then let the shared secret key be $s(a, b)$. Find pairs (a_1, b_1), (a_2, b_2) so that $a_1 \neq a_2$, $b_1 \neq b_2$, and $s(a_1, b_1) = s(a_2, b_2)$.

If you choose any pairs such that $a_1 \neq a_2$, $b_1 \neq b_2$, and $a_1 \times b_1 = a_2 \times b_2$, then $s(a_1, b_1) = s(a_2, b_2)$. I will prove it here.
Let $Q = a_1 b_1 = a_2 b_2$, then we have

$$s(a_1, b_1) \equiv g^{a_1 b_1} \equiv g^Q \pmod p$$
$$s(a_2, b_2) \equiv g^{a_2 b_2} \equiv g^Q \pmod p$$

Therefore,

$$s(a_1, b_1) = s(a_2, b_2)$$

Another acceptable solution is based on Fermat's little theorem (I will OMIT the proof here, take MATH 406 if you are interested).

Theorem 1 *Given p is a prime, and a is an integer that is not divisible by p, then*

$$a^{p-1} \equiv 1 \pmod p$$

In our case, $p = 29$, and $a = g = 2$ is not divisible by 29, then we have

$$2^{28} \equiv 1 \pmod{29}$$

You can choose $a_1 = 28$, and any arbitrary b_1, then

$$s(a_1, b_1) \equiv g^{a_1 b_1} \equiv \left(2^{28}\right)^{b_1} \equiv 1^{b_1} \equiv 1 \pmod{29}$$

Now, if you choose a_2 is a multiple of 28, but not 28 (i.e 56, 84, ...), and arbitrary b_2 that is different from b_1, then we get

$$a_2 = k \times a_1 (k \neq 1)$$

$$g^{a_2 b_2} \equiv g^{k a_1 b_2} \equiv \left(g^{a_1}\right)^{(k b_2)} \equiv 1^{(k b_2)} \equiv 1 \pmod{29}$$

Thus, we see that $s(a_1, b_1) = s(a_2, b_2)$.

Problem 4

Alice and Bob are doing Diffie Helman with prime $p = 6299$ and generator $g = 2$. Alice sends 64. Bob sends 65.
<u>Part a</u>: Find the shared secret key.

We know that p and g are public, and we also know that Alice and Bob are using Diffie Helman key exchange, so we know Alice will send

$$g^a \pmod p$$

In this case, Alice sends

$$2^a \pmod{6299}$$

Since we also know Alice sends 64, that means

$$2^a \equiv 64 \pmod{6299}$$

Clearly, we can see that $a = 6$ is a solution, then we can compute the secret shared key using the message Bob sends to Alice.

$$\text{KEY} = 65^6 \equiv 6177 \pmod{6299}$$

Part b: Give Alice and Bob advice on how they can prevent Eve from using your method, even if $p = 6299$.
We crack this key exchange by looking at the message that Alice and Bob send to each other and see if the message is actually a power of g. Therefore, to prevent this attack, we should tell Alice and Bob to choose a high value of a and b so that the discrete log problem that we need to solve is actually hard.

In practice what people REALLY do is pick a, b between $p/3$ and $2p/3$. (There are reasons why you don't want a or b too large either, like $p-1, p-2$. YOU SHOULD THINK ABOUT WHY USING $p-5$ MIGHT BE BAD.)