Algorithms: Assignment #2

Tanvi Magdum
magdum.t@northeastern.edu

January 22, 2023

Answers

1 Problem 1 Solution :

1.1 Problem 1a Solution -

$3^{1500} \mod 11$

$3^1 = 3$

$3^2 = 9$

$3^4 = 9^2 = 81 \equiv 4(81 \mod 11 = 4)*$

$3^8 = 4^2 = 16 \equiv 5(16 \mod 11 = 5)*$

$3^{16} = 5^2 = 25 \equiv 3(25 \mod 11 = 3)*$

$3^{32} = 3^2 = 9$

$3^{64} = 9^2 = 81 \equiv 4(81 \mod 11 = 4)*$

$3^{128} = 4^2 = 16 \equiv 5(16 \mod 11 = 5)*$

$3^{256} = 5^2 = 25 \equiv 3(25 \mod 11 = 3)*$

$3^{512} = 3^2 = 9$

$3^{1024} = 9^2 = 81 \equiv 4(81 \mod 11 = 4)*$

$1500 - 1024 = 476$

$476 - 256 = 220$

$220 - 128 = 92$

$92 - 64 = 28$

$28 - 16 = 12$

$12 - 8 = 4$

$4 - 4 = 0$

Now, combine all parts.

$3^{1500} \mod 11 = (3^{1024} \times 3^{256} \times 3^{128} \times 3^{64} \times 3^{16} \times 3^8 \times 3^4) \mod 11$

$3^{1500} \mod 11 = ((3^{1024} \mod 11) \times (3^{256} \mod 11) \times (3^{128} \mod 11) \times (3^{64} \mod 11) \times (3^{16} \mod 11) \times (3^8 \mod 11) \times (3^4 \mod 11)) \mod 11$

$3^{1500} \mod 11 = (4 \times 3 \times 5 \times 4 \times 3 \times 5 \times 4) \mod 11$

$3^{1500} \mod 11 = 14400 \mod 11$

$3^{1500} \mod 11 = 1$

1.2 Problem 1b Solution -

$5^{4358} \mod 10$

$5^1 = 5$

$5^2 = 25 \equiv 5(25 \mod 10 = 5)*$

$5^4 = 5^2 = 25 \equiv 5(25 \mod 10 = 5)*$

$5^8 = 5^2 = 25 \equiv 5(25 \mod 10 = 5)$

$5^{16} = 5^2 = 25 \equiv 5(25 \mod 10 = 5)$

$5^{32} = 5^2 = 25 \equiv 5(25 \mod 10 = 5)$

$5^{64} = 5^2 = 25 \equiv 5(25 \mod 10 = 5)$

$5^{128} = 5^2 = 25 \equiv 5(25 \mod 10 = 5)$

$5^{256} = 5^2 = 25 \equiv 5(25 \mod 10 = 5)*$

$5^{512} = 5^2 = 25 \equiv 5(25 \mod 10 = 5)$

$5^{1024} = 5^2 = 25 \equiv 5(25 \mod 10 = 5)$

$5^{2048} = 5^2 = 25 \equiv 5(25 \mod 10 = 5)$

$5^{4096} = 5^2 = 25 \equiv 5(25 \mod 10 = 5)*$

$4358 - 4096 = 262$

$262 - 256 = 6$

$6 - 4 = 2$

$2 - 2 = 0$

Now, combine all parts.

$5^{4358} \mod 10 = (5^{4096} \times 5^{256} \times 5^4 \times 5^2) \mod 10$

$5^{4358} \mod 10 = ((5^{4096} \mod 10) \times (5^{256} \mod 10) \times (5^4 \mod 10) \times (5^2 \mod 10)) \mod 10$

$5^{4358} \mod 10 = (5 \times 5 \times 5 \times 5) \mod 10$

$5^{4358} \mod 10 = 625 \mod 10$

$5^{4358} \mod 10 = 5$

1.3 Problem 1c Solution -

$6^{22345} \mod 7$

$6^1 = 6*$

$6^2 = 36 \equiv 1(36 \mod 7 = 1)$

$6^4 = 1^2 = 1$

$6^8 = 1^2 = 1*$

$6^{16} = 1^2 = 1$

$6^{32} = 1^2 = 1$

$6^{64} = 1^2 = 1*$

$6^{128} = 1^2 = 1$

$6^{256} = 1^2 = 1*$

$6^{512} = 1^2 = 1*$

$6^{1024} = 1^2 = 1*$

$6^{2048} = 1^2 = 1$

$6^{4096} = 1^2 = 1*$

$6^{8192} = 1^2 = 1$

$6^{16384} = 1^2 = 1*$

$22345 - 16384 = 5961$

$5961 - 4096 = 1865$

$1865 - 1024 = 841$

$841 - 512 = 329$

$329 - 256 = 73$

$73 - 64 = 9$

$9 - 8 = 1$

Now, combine all parts.

$6^{22345} \mod 7 = (6^{16384} \times 6^{4096} \times 6^{1024} \times 6^{512} \times 6^{256} \times 6^{64} \times 6^8 \times 6^1) \mod 7$

$6^{22345} \mod 7 = ((6^{16384} \mod 7) \times (6^{1024} \mod 7) \times (6^{512} \mod 7) \times (6^{256} \mod 7) \times (6^{64} \mod 7) \times (6^8 \mod 7) \times (6^1 \mod 7)) \mod 7$

$6^{22345} \mod 7 = (1 \times 1 \times 1 \times 1 \times 1 \times 1 \times 1 \times 6) \mod 7$

$6^{22345} \mod 7 = 6 \mod 7$

$6^{22345} \mod 7 = 6$

2 Problem 2 Solution :

2.1 Problem 2a Solution -

GCD (648, 124)

Using Euclid's algorithm,

$GCD(648, 124) = GCD(124, 648 \mod 124) = GCD(124, 28)$

$GCD(124, 28) = GCD(28, 124 \mod 68) = GCD(28, 12)$

$GCD(12, 4) = GCD(4, 12 \mod 4) = GCD(4, 0)$

$GCD(4, 0) = 1$

2.2 Problem 2b Solution -

GCD (123456789, 123456788)

Using Euclid's algorithm,

$GCD(123456789, 123456788) = GCD(123456788, 123456789 \mod 123456788) = GCD(123456788, 1)$

$GCD(123456788, 1) = GCD(1, 123456788 \mod 1) = GCD(1, 0)$

$GCD(1, 0) = 1$

2.3 Problem 2c Solution -

GCD $(2^{300} * 3^{200}, 2^{200})$

Using Euclid's algorithm,

$GCD((2^{300} * 3^{200}, 2^{200}) = GCD(2^{200}, 2^{300} * 3^{200} \mod 2^{200}) = GCD(2^{200}, 0)$

$GCD(2^{200}, 0) = 2^{200}$

3 Problem 3 Solution :

Alice and Bob can mutually agree on shared secret numbers on the insecure channel. Both the numbers need to be positive whole numbers. One of them should be prime number p and another generator g, which is primitive root of p and g < p. A primitive root means values of -

$g^1 \mod p$, $g^2 \mod p$, $g^3 \mod p$, ..., $g^{p-1} \mod p$ all must be distinct. Then, Alice has to use her personal key x where x < p. Alice calculates A which can be sent to Bob on insecure channel. Value of A contains the secret key x of Alice -

$A = g^x \mod p$

Now, Alice has to send 'A' to Bob. When Bob receives 'A', he uses his personal key y where y < p and calculates B which can be shared on insecure channel. Bob responds with B to Alice -

$B = g^y \mod p$

Both of them know values of 'g' and 'p'. Alice now knows value of 'B' and Bob knows value of 'A'. The key is generated at both sender and receiver side. So Alice calculates -

$K = B^x \mod p$

and Bob calculates -

$K = A^y \mod p$

Both values of K for Alice and Bob should come equal. Thus, the Diffie-Hellman key is generated and information is transferred successfully without leak.

Let us see an example. Consider the value of p as 11, a prime number and value of g as 2, since $g^n \mod p$ gives distinct values for distinct n, where 0 < n < p.

Suppose, Alice needs to send her secret key x=3. So she calculates A -

$A = g^x \mod p$

$A = 2^3 \mod 11$

$A = 8$

Alice sends A=8 to Bob. Now, Bob uses his secret key y=5. He calculates B -

$B = g^y \mod p$

$B = 2^5 \mod 11$

$B = 10$

Bob responds with B=10 to Alice. Now Alice has her secret key x=3 and number Bob sent B=10. Bob has his secret key y=5 and number Alice sent A=8. So both can calculate a common key K.

Alice calculates K as -

$K = B^x \mod p$

$K = 10^3 \mod 11$

$K = 10$

Bob calculates K as -

$K = A^y \mod p$

$K = 8^5 \mod 11$

$K = 10$

Thus, we can observe that Alice and Bob exchanged their secret information and both came up with a common key K, i.e the Diffie-Hellman key using the the exchanged information. In this way, Alice sent her secret key to Bob over insecure channel without any information leak or external manipulation.

4 Problem 4 Solution :

Please start with the 'README.txt' file first. Please refer to 'Main.java' for source code in Java for Q4. Input format is provided through 'input.txt' file. Screenshots of outputs for 2 sample inputs are provided as output1 and output2.