Introduction to Cryptography: Assignment 8

Group number 57

Elwin Tamminga s1013846

Lucas van der Laan s1047485

1

(a) Yes, because 1061 is only divisible by 1 or itself.

(b) The order of a is always 1061, because $ord(a) = 1061/\gcd(1061, a)$, but $\gcd(1061, a)$ is always 1 because 1061 is a prime number.

(c) We can calculate that $2^{1060} \mod 1061 = 1$, which we can factorize it as $(2^{530})^2 \equiv 1060^2 \mod 1061 = 1$. We can also factorize it as $(2^2)^{530} \equiv 4^{530} \mod 1061 = 1$. In general, we can say that any number that can be multiplied with another number to get 1060 is a multiplicative order, because we can rewrite it such that $2^{x*y} \mod 1061 = 1$.

So the order of g can be any number that is a divisor for 1060.

The list of numbers are the divisors of 1060: $[1, 2, 4, 5, 10, 20, 53, 106, 212, 265, 530, 1060]$.

(d) We are looking for an x in the list of divisors of 1060 that satisfies $112^x \mod 1061$, to do this we use square-and-multiply:

$$
\begin{aligned}
&t = g & g &= 112, & p &= 1061 \\
&t = g^2 = t \cdot t & g^2 &= 873 & &= 112 \cdot 112 \\
&t = g^4 = t \cdot t & g^4 &= 331 & &= 873 \cdot 873 \\
&t = g^5 = t \cdot g & g^5 &= 998 & &= 331 \cdot 112 \\
&t = g^{10} = t \cdot t & g^{10} &= 786 & &= 998 \cdot 998 \\
&t = g^{20} = t \cdot t & g^{20} &= 294 & &= 786 \cdot 786 \\
&t = g^{53} = g^{20} \cdot g^{20} \cdot g^{10} \cdot g^2 \cdot g & g^{53} &= 1 & &= 294 \cdot 294 \cdot 786 \cdot 873 \cdot 112
\end{aligned}
$$

(e) The order of 112 is 53. So we can do $38481 \mod 53 = 3$, which maps to $112^3 \mod 1061 = \mathbf{164} = 112^{38481} \mod 1061$

2

(a)

$$
\begin{aligned}
6^0 &\equiv 1 \\
6^1 &\equiv 6 \\
6^2 &\equiv 13 \\
6^3 &\equiv 9 \\
6^4 &\equiv 8 \\
6^5 &\equiv 2 \\
6^6 &\equiv 12 \\
6^7 &\equiv 3 \\
6^8 &\equiv 18 \\
6^9 &\equiv 16 \\
6^{10} &\equiv 4 \\
6^{11} &\equiv 1
\end{aligned}
$$

So the elements that are in the list: $[1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18]$

(b) 11, because there are 11 elements in the cyclic subgroup generated by the generator <6>.

(c) 4, because $6 \cdot 4 \equiv 1$ (mod 23).

(d) 7, because we found in (a) that $6^7 \equiv 3$.