# Week 3 worksheet

① a) $a = 754$, $b = 512$

$r_0 = 754$, $r_1 = 512$, $i = 2$

$754 = 512 m_2 + r_2$ (1, 242)

$m_2 = 1$, $r_2 = 242$, $i = 3$

$512 = 242 m_3 + r_3$ (2, 28)

$m_3 = 2$, $r_3 = 28$, $i = 4$

$242 = 28 m_4 + r_4$ (8, 18)

$m_4 = 8$ $r_4 = 18$, $i = 5$

$$28 = 18 \overset{1}{m_5} + \overset{10}{r_5}$$

$$m_5 = 1, \quad r_5 = 10, \quad i = 6$$

$$18 = 10 \overset{1}{m_6} + \overset{8}{r_6}$$

$$m_6 = 1, \quad r_6 = 8, \quad i = 7$$

$$10 = 8 \overset{1}{m_7} + \overset{2}{r_7}$$

$$m_7 = 1, \quad r_7 = 2, \quad i = 8$$

$$8 = 2 m_8 + r_8$$

$$m_8 = 4, \quad r_8 = 0$$

return $r_7 = \underline{\underline{2}}$

b.)

$$2 = 10 - 1(8)$$

$$2 = 10 - 1(18 - 1(10))$$

$$2 = 10 - 18 + 10$$

$$2 = 2(10) - 18$$

$$2 = 2(28 - (18)) - 18$$

$$2 = 2 \cdot 28 - 3(18)$$

$$2 = 2 \cdot 28 - 3(242 - 8(28))$$

$$2 = 26(28) - 3 \cdot 242$$

$$2 = 26(512 - 2(242)) - 3 \cdot 242$$

$$2 = 26 \cdot 512 - 55(242)$$

$$2 = 26 \cdot 512 - 55(754 - 512)$$

$$2 = \underbrace{81}_{w}(512) - \underbrace{55}_{q}(754)$$

5

$$a = -55, \quad b = 81$$

c.) $x \equiv 5 \pmod{17}$

$x \equiv 2 \pmod{11}$

Use Euclid's corollary to find that:

$$1 = 2 \cdot 17 - 3 \cdot 11$$

$m = 17$ $\quad$ $n = 11$

$c = 2$ $\quad a = -3$

$a = 5$ $\quad b = 2$

Plug into

$$x = bcm + adn \mod (mn)$$

$$\downarrow$$

$$x = 2 \cdot 2 \cdot 17 + 5 \cdot -3 \cdot 11 \mod (17 \cdot 11)$$

$$x = 68 - 165 \pmod{187}$$

$$x = -97 \pmod{187}$$

or alternatively,

$$x = 90 \pmod{187}$$

2. a.)

$4^1 \pmod 5 \equiv 4 \pmod 5$

$4^2 \pmod 5 \equiv 1 \pmod 5$

$4^3 \pmod 5 \equiv 4 \pmod 5$ ✗

It has generated 4 twice which means it won't generate all values in the group and ∴ is not a generator

b.) $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

$2^1 \Rightarrow 2$

$2^2 \Rightarrow 4$

$2^3 \Rightarrow 8$

$2^4 \Rightarrow 5$

$2^5 \Rightarrow 10$

$2^6 \Rightarrow 9$

$2^7 \Rightarrow 7$

$2^8 \Rightarrow 3$

$2^9 \Rightarrow 6$

$$2^{10} \equiv 1$$

$\therefore$ 2 is a generator as it generates all values of of the set.

c.) Inverse of $2 \pmod{11}$

First, use Euclid's algo to find the equations:

$$11 = 2(5) + 1$$

$$2 = 1(2) + 0$$

Now we need $m, n$ s.t.

$1 = 11m + 2n$

Using equations above:

$1 = 11 - 5 \cdot 2$

$\therefore \quad m = 1, \quad n = -5$

$-5 \pmod{11} = 6$ so inverse is $\underline{6}$

d) $7^6 \pmod{11}$

$\equiv 4$

$10 \mathbb{Z}$

e.) The group $\mathbb{Z}/11\mathbb{Z}^*$ has order 10.

Hellman's pubic key is $g^h \pmod{11}$

$g^{h+10n} \equiv g^h \cdot g^{10n} \equiv g^h \cdot 1^n \equiv$

$g^h \pmod{11}$

$\therefore$ any integer in the form $h+10n$ produces the same

public key as h.

f.) $2^h \equiv 7 \pmod{11}$

Is it something to do with setting $m = 5$ and $n = 2$?

$g = 2 \pmod{11}$

I'm not sure can I see the answer?

(3.) a.) Let $m = 7$

b) Let $h = 3$

$$2^3 \pmod{11} = 8$$

c.) $$5^3 \pmod{11} = 4$$

d.) $c = 7 \cdot 4 \pmod{11} = 6$

e.) If m was 0 then c would also always be zero, regardless of the shared secret.

It is also not in the set $(\mathbb{Z}/11\mathbb{Z})$

f.) $5 = 2^{a} \pmod{11}$

| a | $2^a \pmod{11}$ |
|---|---|
| 1 | 2 |
| 2 | 4 |
| 3 | 8 |
| 4 | 5 |

Using brute force we find

$a = 4$.

g.) $c = 6$

$$ss = 4$$

$$ss^{-1} \equiv 3$$

as $4 \times 3 \equiv 1 \pmod{11}$

$$c \cdot ss^{-1} \equiv 7 \pmod{11}$$

h.) When $p$ is large, an adversary's brute force attack would take much longer, as they would have to try $1, \ldots, p$ until the run into the right answer. This is

the Discrete Logarithm Problem.