

# Week 3 worksheet

① a.)  $a = 754, b = 512$

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

$$\begin{array}{r} & 242 \\ 1 & \end{array}$$
$$754 = 512m_2 + r_2$$

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

$$\begin{array}{r} & 28 \\ 2 & \end{array}$$
$$512 = 242m_3 + r_3$$

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

$$\begin{array}{r} & 18 \\ 8 & \end{array}$$
$$242 = 28m_4 + r_4$$

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

$$28 = 18 m_5 + r_5$$

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

$$18 = 10 m_6 + r_6$$

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

$$10 = 8 m_7 + r_7$$

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

$$8 = 2 m_8 + r_8$$

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

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

b.)

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

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

$$2 = 10 - 18 + 10$$

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

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

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

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

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

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

$$2 = 26.512 - 55(242)$$

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

$$2 = 81(512) - 55(754)$$

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

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

$$x \equiv 2 \pmod{11}$$

Use Euclid's corollary to

find that:

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

$$m = 17$$

$$n = 11$$

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

$$a = 5$$

$$b = 2$$

Plug into

$$x = bcm + adn \pmod{mn}$$



$$x = 2 \cdot 2 \cdot 17 + 5 \cdot -3 \cdot 11 \pmod{17 \cdot 11}$$

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

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

or alternatively,

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

(2.)

a.)

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

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

$$4^3 \pmod{5} \equiv 4 \pmod{5}$$

Correct!

~~X~~

✓

It has generated 4 twice

which means it won't generate

any values in the group and

$\therefore$  is not a generator

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

$$2^1 \Rightarrow 2$$

$$2^2 \Rightarrow 4$$

$$2^3 \Rightarrow 8$$

$$2^4 \Rightarrow 5$$

$$2^5 \Rightarrow 10$$

$$2^6 \Rightarrow 9$$

$$2^7 \Rightarrow 7$$

$$2^8 \Rightarrow 3$$

$$2^9 \Rightarrow 6$$

$$2^{16} = 1 \quad \boxed{ } \quad \checkmark$$

$\therefore 2$  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:

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

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

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

$$1 = 11m + 2n$$

Using equations above:

$$1 = 11 - 5 \cdot 2$$

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

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

Yes but your numbers should remain consistently in the world of mod 11

is 6 mod 11  


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

$$\equiv 4 \checkmark$$

10693

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

has order 10.

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

$$g^{h+10n} = g^h \cdot g^{10n} \equiv g^h \cdot 1^n \equiv g^h \pmod{11}$$

$\therefore$  any integer in the form

$h+10n$  produces the same

The working out is good but you should explicitly mention fermat's little theorem (FLT)

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

$$10 = 2 \cdot 5$$

So we can find  $h \pmod{2}$

and  $h \pmod{5}$  and use  
these to get  $h \pmod{10}$

$$2^{5h} \equiv 7^5 \pmod{11} \text{ - only depends on } h \pmod{2}$$

$$7^5 \pmod{11} \equiv 10$$

$$\text{so } 2^{5h} \equiv 10 \pmod{11} \text{ so}$$

$$h \equiv 1 \pmod{2}$$

$$2^{2h} \equiv 7^2 \pmod{11} \equiv 5$$

$$\text{so } h \equiv 2 \pmod{5}$$

Using Euclid:

$$1 = 1 \cdot 5 - 2 \cdot 2$$

$$\begin{array}{r} b \\ | \\ 1 & & m & a & d & n \\ | & | & | & | & | \end{array}$$

$$x \equiv 2 \cdot -2 \cdot 2 + 1 \cdot 1 \cdot 5$$

$$\begin{aligned} a &\equiv 1 \\ m &\equiv 2 \\ b &\equiv 2 \\ n &\equiv 5 \\ c &\equiv -2 \\ d &\equiv 1 \end{aligned}$$

$$\equiv 7 \pmod{10}$$



$$\equiv h \pmod{10}$$

③ a.) Let  $m = 7$



b) Let  $h \equiv 3$

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



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



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

m ss

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

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

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

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

Using brute force we find

$$a = 4$$

$$9.) \quad c = 6$$

make sure you say that they are the numbers mod 11!

$$ss = 4$$

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

$$6 \quad \checkmark \quad \text{as } 4 \times 3 \equiv 1 \pmod{11}$$

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

h.) When p is large, an adversary's brute force attack would take much longer, as they would have to try

$1, \dots, p$  until the run into the right answer. This is

the Discrete Logarithm Problem.