ASSESSMENT 3: PUBLIC-KEY CRYPTOGRAPHY

CAB340: Cryptography

Ash Phillips, n10477659
Due Date: 09/11/22, 11:59 pm

1.0. Number Theory

(a)

Bézout's Identity states there always exists integers *n* and *m* such that:

$$\gcd(p, q) = pm + qn$$

When $\gcd(p, q) = 1$, then $pm + qn = 1$

If $p^{-1}p \equiv 1 \pmod{q}$, then Modular Equivalence gives:

$$p^{-1}p = kq + 1$$
$$p^{-1}p - kq = 1$$
$$p(p^{-1}) + q(-k) = 1$$

With $m = p^{-1}$ and $n = -k$ this becomes:

$$pm + qn = 1$$

So now, with Bézout's Identity, so there always exists integers p^{-1} and $-k$ to satisfy above, if $\gcd(p, q) = 1$ then there exists $p^{-1} \bmod(q)$.

(b)

j	a_j	b_j	q_j	r_j
0	96	35	2	26
1	35	26	1	9
2	26	9	2	8
3	9	8	1	1
4	8	1	8	0

So, gcd(96, 35) = gcd(a_0, b_0) = gcd(a_4, b_4) = gcd(8, 1) = 1
Final value for j = 4.

(c)

	j	a_j	b_j	q_j	m_j	n_j
setting values per step **ii**	3	9	8	1	1	-1
iteration *j* = 2 at step **iv**	2	26	9	2	-1	3
iteration *j* = 1 at step **iv**	1	35	26	1	3	-4
iteration *j* = 0 at step **iv**	0	96	35	2	-4	11

(d)

Here, $m_0 = -4,\ n_0 = 11$

So, Bézout's Identity:

$$x \equiv 96^{-1} mod\ 35 \equiv -4\ mod\ 35 \equiv 31\ mod\ 35 \equiv 31$$

$$y \equiv 35^{-1}\ mod\ 96 \equiv 11\ mod\ 96 \equiv 11$$

2.0. RSA Encryption

(a)

QUT ID = n10477659
So here:

$$e = (10477659 \; mod \; 100) \times 6 + 401$$
$$e = 59 \times 6 + 401$$
$$e = 755$$

(b)

Prime factors product for 755 = 151 × 5

(c)

i.

$$n = p \times q$$
$$n = 2027 \times 2593$$

So, the public key is $n = 5256011$
This key is valid *e* is coprime.

ii.

Then,
$$d = e^{-1} mod \phi(n)$$
$$d = e^{-1} mod\big((p-1)(q-1)\big)$$
$$d = 755^{-1} \; mod\big((2027-1)(2593-1)\big)$$
$$d = 755^{-1} \; mod \; 5251392, \text{ valid as coprime.}$$

iii.

Using the Extended Euclidean algorithm, we can find that:

$$755^{-1} \; (mod \; 5251392) = \; 500795$$

So, private key is $d = 500795$.

(d)

Here:

$$c(\mathrm{m}) = \; \mathrm{m^e mod \; n}$$
$$\mathrm{c(m)} = \; 1024^{755} \mathrm{mod} \; 5256011$$

Using Square-and-Multiply algorithm:
Step 1: Convert the exponent to Binary.
Binary of *e* = 1011110011

Step 2: For the first 1, simply list the number.
Step 3: For each ensuing 0, do square operation.
Step 4: For each ensuring 1, do square and multiply operations.

A python script was used to perform the maths for steps 2-4 to encrypt:

Bit	Operation	Calculation (mod 5256011)
0	SQ	x^2 = 1024^2 = 1048576
1	SQ+MUL	x^2 * x = 1048576^2 * 1024 = 3840142
1	SQ+MUL	x^2 * x = 3840142^2 * 1024 = 1888338

1	SQ+MUL		x^2 * x = 1888338^2 * 1024 = 1374786
1	SQ+MUL		x^2 * x = 1374786^2 * 1024 = 2502307
0	SQ	x^2	= 2502307^2 = 1857839
0	SQ	x^2	= 1857839^2 = 1142342
1	SQ+MUL		x^2 * x = 1142342^2 * 1024 = 3254011
1	SQ+MUL		x^2 * x = 3254011^2 * 1024 = 301448

Therefore, ciphertext is *c* = 3014488

(e)

Chinese Remainder Theorem:

Step 1:

$$d(mod\ p-1) = 500795\ mod\ 2026 = 373$$
$$d(mod\ q-1) = 500795\ mod\ 2592 = 539$$

Step 2:

$$M_p = 3014488^{373}\ mod(2027) = 339^{373}\ mod(2027) = 1363$$
$$M_q = 3014488^{539}\ mod(2593) = 1422^{539}\ mod(2593) = 2361$$

Step 3:

$$M = \left(q \cdot (q^{-1} mod\ p) \cdot M_p + p \cdot (p^{-1} mod\ q) \cdot M_q\right) mod\ pq$$
$$= \left(M_p mod\ p + M_q mod\ q\right) mod\ n$$
$$M = 1363 \times 2593 \times q_1 + 2361 \times 2027 \times q_2\ mod\ 5256011$$

$$q_1 = 2593^{-1}\ mod\ 2027$$
$$= 566^{-1}\ mod\ 2027$$
$$= 727$$
$$q_2 = 2027^{-1}\ mod\ 2593$$
$$= 1663$$

$$M = 1024 \times 2593 \times 727 + 1024 \times 2027 \times 1663\ mod\ 5256011$$
$$= 1930353664 + 3451802624\ mod\ 5256011$$
$$= 5382156288\ mod\ 5256011$$
$$= 1024$$

3.0. Diffie-Hellman Key Agreement

3.1. A (too) simple implementation

(a)

Here:

$j = 659$
$p = 2027$

Using Fermat's Little theorem:

$g^k \equiv 1 \; mod \; p$
$p - 1 = 2026$

Dividers x of 2026 are 2 and 1013.

Finding the smallest g where $g^x \not\equiv 1 \; mod \; p$ for all dividers x starting $g \geq j$:

$659^{1013} \equiv 1 \; mod \; 2027$ $\boldsymbol{fail}$
$660^{1013} \equiv 1 \; mod \; 2027$ $\boldsymbol{fail}$
$661^{1013} \equiv 1 \; mod \; 2027$ $\boldsymbol{fail}$
$662^{1013} \equiv 2026 \; mod \; 2027 \not\equiv 1 \; mod \; 2027$ $\boldsymbol{Pass}$
$662^{2} \equiv 412 \; mod \; 2027 \not\equiv 1 \; mod \; 2027$ $\boldsymbol{Pass}$

As above, 662 passes for all dividers x of $p - 1$, and is therefore a generator.
Using a script, we get:

First 10	$g \geq 659, dividers = 2 \; \& \; 1013, p = 2027$	Is a generator?
1	659	No
2	660	No
3	661	No
4	662	Yes
5	663	No
6	664	Yes
7	665	No
8	666	No
9	667	No
10	668	No

Therefore:

$g = 662$, the smallest generator
$h = 659$, the smallest non-generator

(b)

As above,

$g = 662$, the smallest generator
$h = 659$, the smallest non-generator

(c)

Alice's public key is:

$$\mathrm{x} = (662^{123} \bmod 2027)$$
$$\mathrm{x} = 1492$$

Bob's public key is:

$$\mathrm{y} = (662^{456} \bmod 2027)$$
$$\mathrm{y} = 1781$$

The communications Alice and Bob send to each other are these public numbers:

Alice receives public key $\mathrm{y} = 1781$

And Bob receives public key $\mathrm{x} = 1492$

(d)

We compute Alice and Bob's symmetric keys:

Alice: $k_a = y^a \bmod p$
$= 1781^{123} mod\ 2027$
$= 777$

Bob: $k_b = x^b \bmod p$
$= 1492^{456} mod\ 2027$
$= 777$

Therefore, their session key is 777.

3.2. A passive attack…

(a)

Here:

$$p - 1 = 2026$$
$$order: p = 2$$
$$\frac{p-1}{2} = 1013$$

Using the public keys in 3.1.(c) we get:

$$A_2 = y^{1013} mod\ 2027$$
$$= 1781^{1013} mod\ 2027$$
$$= 1$$

$$B_2 = x^{1013} mod\ 2027$$
$$= 1492^{1013} mod\ 2027$$
$$= 2026$$

(b)

Using $g = 662$:

$$g_2 = g^{1013} mod\ 2027$$
$$= 662^{1013} mod\ 2027$$
$$= 2026$$

Yes. We can see that g_2 is in the form $g^{\frac{p-1}{2}} mod\ p$, which from the theory we know can only be 1 or 2026 (i.e., 1 or -1), so were could then predict g_2 would be $\pm 1\ mod\ 2027$.

(c)

We know $A_2 = 1$ and $B_2 = 2026$ from (a) above, and that $g_2 = 2026$ from (b) above. Now, Alice's secret key modulo 2 is:

$$A_2 = g_2^{a_2} \; mod \; p$$
$$1 \; = 2026^{a_2} \; mod \; 2027$$
$$a_2 = 2$$

And Bob's secret key modul0 2 is:

$$B_2 = g_2^{b_2} \; mod \; p$$
$$2026 \; = 2026^{a_2} \; mod \; 2027$$
$$b_2 = 1$$

(d)

Now, we'll calculate Alice and Bob's public keys:
Alice's public key is:

$$\mathrm{x} = 2026^2 \bmod 2027$$
$$\mathrm{x} = \; 1$$

Bob's public key is:

$$\mathrm{y} = 2026^1 \bmod 2027$$
$$\mathrm{y} = \; 2026$$

Then, we calculate Alice and Bob's symmetric keys:

$$k \; = \; y^{a_2} \; mod \; p$$
$$= 2026^2 mod \; 2027$$
$$= \; 1$$

Therefore, $K_2 = \; 1$

To verify:

$$K_2 = K^p \; mod \; 2027$$
$$= 777^{1013} \; mod \; 2027$$
$$= 1$$

3.3. An active attack…

(a)

Yes. The corresponding public key that BadBob will send to Alice is:

$$\widehat{\mathrm{B}} = \; 2026$$

As, using $\hat{\mathrm{b}} = \frac{\varphi(p)}{2}$:

$$\widehat{\mathrm{B}} = \; \mathrm{x}^{\frac{\varphi(p)}{2}} \bmod \mathrm{p}$$

$$= x^{1013} mod \; 2027$$
$$= 662^{1013} mod \; 2027$$
$$= 2026$$

(b)

Using $p = 2027$ and $g = 662$, redoing the equations above we find:

	Alice key a	BadBob key b	Alice receives $\widehat{B}$	Bob receives A	Session key
1	123	1013	2026	1492	2026
2	124	1013	2026	555	1
3	125	1013	2026	523	2026
4	131	1013	2026	557	2026
5	132	1013	2026	1847	1
6	133	1013	2026	433	2026
7	223	1013	2026	1618	2026
8	224	1013	2026	860	1
9	225	1013	2026	1760	2026
10	226	1013	2026	1622	1

(c)

Above we can see when Alice's key changes, the session key will always be ± 1 mod 2027. This is happening because BadBob chose the same value that was given by $\frac{p-1}{2}$, 1013. This caused Alice to only ever receive the public key $\widehat{B} = 2026$. By using these values to then calculate their session keys the value will only ever be ± 1 mod 2027. This could result in a hazard in the real world as the session key would be easily predictable, creating a vulnerability.

3.4. …And a fix for both!

(a)

Using $h = 659$, Alice's public key is:

$$= 659^{123} \bmod 2027$$
$$= 1207$$

And Bob's public key is:

$$= 659^{456} \bmod 2027$$
$$= 153$$

Alice and Bob then exchange these public numbers and we compute the symmetric keys:

$$k_a = y^a \, mod \, p$$
$$= 153^{123} mod \, 2027$$
$$= 1009$$

$$k_b = x^b \, mod \, p$$
$$= 1207^{456} \, mod \, 2027$$
$$= 1009$$

Therefore, the session key is 1009.

(b)

As seen in 3.2 above, when using a generator on subgroup of order 2 you can only receive the values 1 and 2026. This means that when conducting a passive attack, an attacker only needs to be able to predict the value of the key using 1 and 2026. By instead using a non-generator number, $h = 659$, values other than 1 and 2026 can be used, therefore defeating the first attack.

(c)

In 3.3, by BadBob choosing $\hat{b}$ and therefore forcing the key agreement to misbehave, the same issue occurred; the shared key would only ever be ± 1 mod 2027 due to the generator. To show how using a non-generator will mitigate this attack we will calculate the value again.

By using the same value for $\hat{b} = \frac{\varphi(p)}{2}$ but then using *h* instead of *g* we get:

$$\hat{B} = h^{\frac{\varphi(p)}{2}} \bmod p$$

$$= h^{1013} mod\ 2027$$
$$= 659^{1013} mod\ 2027$$
$$= 1, \text{ instead of the 2026 we found before.}$$

Now, using the *a* and *b* from row one in the table created in 3.3.(b):
We find Alice's new public key:

$$x = 659^{123} \bmod 2027$$
$$x = 1207$$

	Alice key a	BadBob key b	Alice receives $\hat{B}$	Bob receives A	New Session key	Old Session key
1	123	1013	1	1207	1	2026
2	124	1013	1	829	1	1
3	125	1013	1	1048	1	2026
4	131	1013	1	1237	1	2026
5	132	1013	1	329	1	1
6	133	1013	1	1949	1	2026
7	223	1013	1	1583	1	2026
8	224	1013	1	1319	1	1
9	225	1013	1	1665	1	2026
10	226	1013	1	628	1	1

As can be seen by redoing these calculations using *h* and our new $\hat{B}$ the session key will only ever be 1. This means the attack can be easier to mitigate, $\hat{B}$ just needs to be changed.

4.0. Elliptic-Curve Cryptography

4.1. Elliptic-curve arithmetic

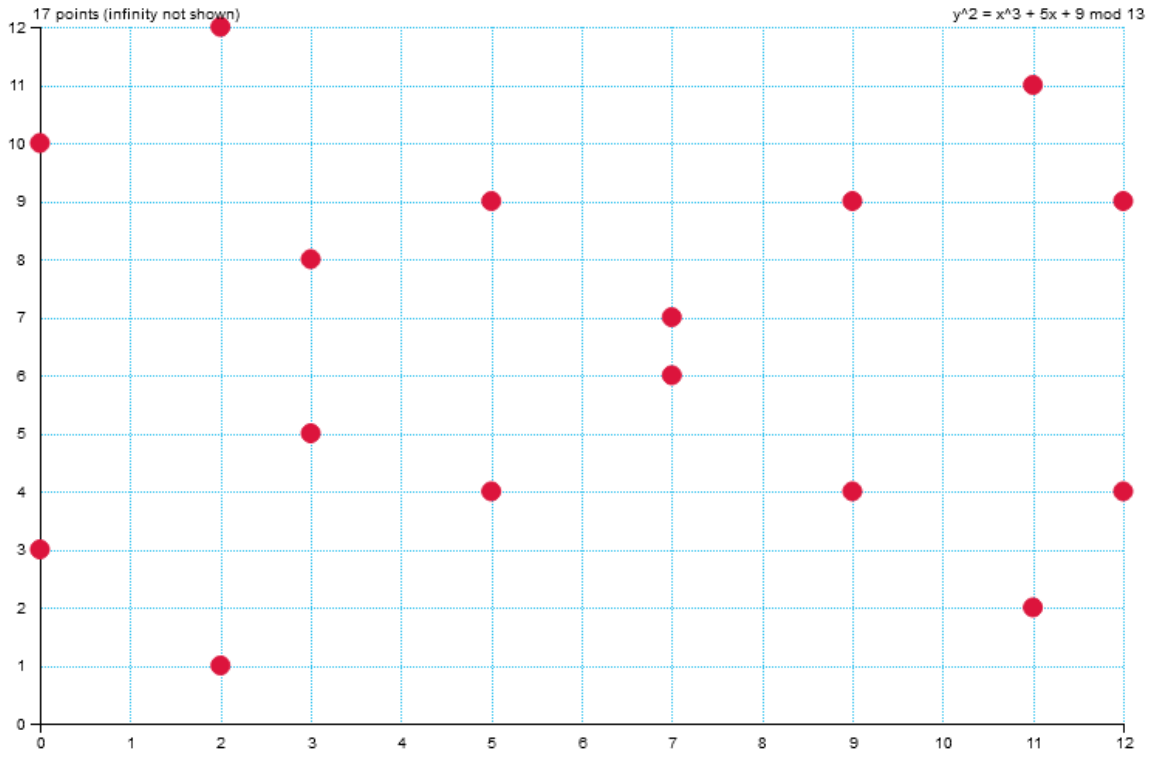
(a)

Using the bash script for the lecture:

$$p = 13\ ;\ a = 5\ ;\ b = 9$$

```
E: y^2 = x^3 + 5 x + 9 (mod 13)
. . # . . . . . . . . . . 12
. . . . . . . . . . . # . 11
# . . . . . . . . . . . . 10
. . . . . # . . . # . . # 9
. . . # . . . . . . . . . 8
. . . . . . . # . . . . . 7
. . . . . . . # . . . . . 6
. . . # . . . . . . . . . 5
. . . . . # . . . # . . # 4
# . . . . . . . . . . . . 3
. . . . . . . . . . . # . 2
. . # . . . . . . . . . . 1
. . . . . . . . . . . . . 0
E= (2,1) (11,2) (0,3) (12,4) (9,4) (5,4) (3,5) (7,6) (7,7) (3,8)
(12,9) (9,9) (5,9) (0,10) (11,11) (2,12) (inf)
#E= 17
```

Plot of this data using excel:



(b)

The order of the curve is 17.
And 17 is prime therefore valid.

(c)

Here, z = 9
So:

$$G = (x_G, y_G) = \textit{smallest value where } y_G \textit{ is equal to } z = (5,9)$$

$$H = (x_H, y_H) = \textit{largest value where } y_H \textit{ is equal to } z + 2 = (11,11)$$

Both points were present in the results for the bash script in (a) and therefore do lie on the curve.

(d)

Finding the slope of the tangent to the curve at G:

$$\begin{aligned} s &= (3{x_G}^2 + a) \cdot (2y_G)^{-1} \mod p \\ &= (3 \cdot 5^2 + 5) \cdot (2 \cdot 9)^{-1} \mod 13 \\ &= (10 + 5) \cdot (2 \cdot 9)^{-1} \mod 13 \\ &= (2) \cdot (5)^{-1} \mod 13 \\ &= (2) \cdot (8) \mod 13 \\ &= 3 \end{aligned}$$

Finding x_R coordinate of the other point where the tangent at P intersects the curve:

$$\begin{aligned} x_R &= s^2 - 2 \cdot x_G \mod p \\ &= 3^2 - 2 \cdot 5 \mod 13 \\ &= 9 - 10 \mod 13 \\ &= 9 - 10 \mod 13 \\ &= -1 \mod 13 \\ &= 12 \mod 13 \\ &= 12 \end{aligned}$$

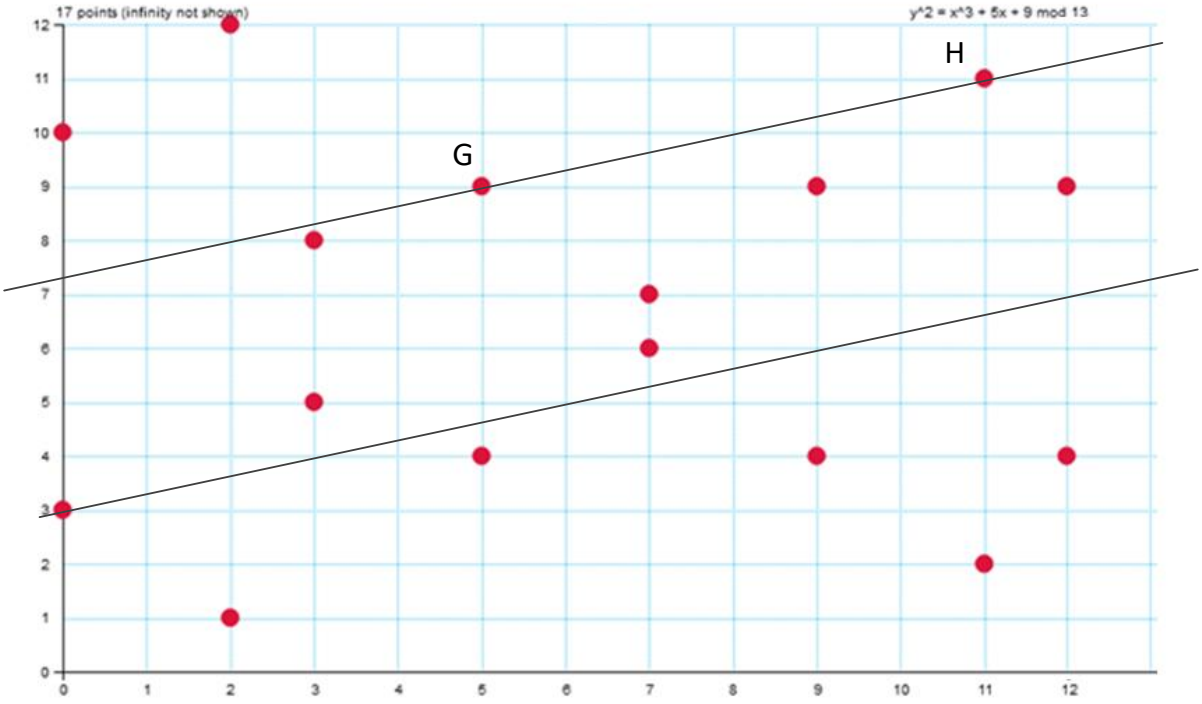
Finding the corresponding y_R coordinate, but with opposite sign for the mirror image:

$$\begin{aligned} y_R &= -y_G + s \cdot (x_G - x_R) \mod p \\ &= -9 + 3 \cdot (5 - 12) \mod 13 \\ &= -9 + 3 \cdot (-7) \mod 13 \\ &= -30 \mod 13 \\ &= 9 \mod 13 \\ &= 9 \end{aligned}$$

Therefore:

$$2\mathrm{G} = (\mathrm{x_R}, \mathrm{y_R}) = (12,9)$$

(e)



The line GH intersects at the 3rd point (0, 3).
We take the mirror image to get G + H = (0, 10).

(f)

To verify the above findings, we first find the slope of the straight line through G and H:

$$\begin{aligned} s &= (y_H - y_G) \cdot (x_H - x_G)^{-1} \mod p \\ &= (11 - 9) \cdot (11 - 5)^{-1} \mod 13 \\ &= (2) \cdot (6)^{-1} \mod 13 \\ &= (2) \cdot (11) \mod 13 \\ &= 9 \end{aligned}$$

We then find the x coordinate of the 3rd point, where the line PQ intersects the curve:

$$\begin{aligned} x_R &= s^2 - x_H - x_G \mod p \\ &= 9^2 - 11 - 5 \mod 13 \\ &= 3 - 11 - 5 \mod 13 \\ &= -13 \mod 13 \\ &= 13 \mod 13 \\ &= 0 \end{aligned}$$

Lastly, we find the corresponding y coordinate, but with the opposite sign for the mirror image:

$$\begin{aligned} y_R &= -y_H + s \cdot (xH - xR) \mod p \\ &= -11 + 9 \cdot (11 - 0) \mod 13 \\ &= -11 + 9 \cdot 11 \mod 13 \\ &= -11 + 8 \mod 13 \end{aligned}$$

$$= -3 \ \ mod\ 13$$
$$= 10 \ \ mod\ 13$$
$$= 10$$

Therefore, we have verified the above findings as here:

$$G + H = (x_R, y_R)$$
$$= (0,10)$$

Which matches the findings in (e).

4.2. Elliptic-curve Diffie-Hellman key agreement

(a)

Starting with the group generator (5,9) and repeatedly adding it to itself produces the subgroup:
(5,9) → (12,9) → (9,4) → (3,8) → (2,12) → (7,6) → (0,3) → (11,2) → (11,11) → (0,10) → (7,7) → (2,1) → (3,5) → (9,9) → (12,4) → (5,4) → ∞

The order of the subgroup for G (number of points including infinity) = 17

A snippet of the working for first 7 points in the above subgroup:

$$y = x^3 + 5x + 9 \bmod 13$$
$$Group\ Generator\ G = (5,9)$$
$$2G = G + G = (5,9) + (5,9) = (12,9)$$
$$3G = G + 2G = (5,9) + (12,9) = (9,4)$$
$$4G = G + 3G = (5,9) + (9,4) = (3,8)$$
$$5G = G + 4G = (5,9) + (3,8) = (2,12)$$
$$6G = 2G + 4G = (12,9) + (3,8) = (7,6)$$
$$7G = G + 6G = (5,9) + (7,6) = (0,3)$$
$$\vdots$$

(b)

If Alice's secret key *a* = 5
Then, the public point *A* she sends to Bob is:

$$P_A = a \cdot G$$
$$= 5 \cdot G$$
$$= (2,12)$$

(c)

If Bob's secret key *b* = 7
Then, the public point *B* he sends to Alice is:

$$P_B = b \cdot G$$
$$= 7 \cdot G$$
$$= (0,3)$$

(d)

First, find the point $7P_A$:

$$P_A = (2,12)$$
$$2P_A = (2,12) + (2,12) = (0,1)$$
$$4P_A = 2P_A + 2P_A = (0,1) + (0,1) = (9,4)$$
$$6P_A = 2P_A + 4P_A = (0,1) + (9,4) = (3,5)$$
$$7P_A = P_A + 6P_A = (2,12) + (3,5) = (5,9)$$

Next, find the point $5P_B$:

$$P_B = (0,3)$$
$$2P_B = (0,3) + (0,3) = (9,9)$$
$$3P_B = P_B + 2P_A = (0,3) + (9,9) = (3,8)$$
$$5P_B = 2P_B + 3P_B = (9,9) + (3,8) = (5,9)$$

Therefore, the shared secret S from Alice's point of view is:

$$S_A = a \cdot P_B = 5 \cdot (0,3) = (5,9)$$

And the shared secret S from Bob's point of view is:

$$S_B = b \cdot P_A = 7 \cdot (2,12) = (5,9)$$

The ECDH protocol works according to the theory in this case as $S_A = S_B$