# Answers to Exercises Najeeb Hassan 9988342

## Week 1

### Q1 :

```
Table[Replace[Replace[Replace[x, RotI], RefB], RotIinv], {x, 1, 26, 1}]
```

```
{8, 11, 13, 19, 6, 5, 16, 1, 14, 12, 2, 10, 3, 9, 21, 7, 26, 25, 4, 22, 15, 20, 24, 23, 18, 17}
```

### Q2 :

```
RotI = {1 → 5, 2 → 11, 3 → 13, 4 → 6, 5 → 12, 6 → 7, 7 → 4, 8 → 17,
  9 → 22, 10 → 26, 11 → 14, 12 → 20, 13 → 15, 14 → 23, 15 → 25, 16 → 8, 17 → 24,
  18 → 21, 19 → 19, 20 → 16, 21 → 1, 22 → 9, 23 → 2, 24 → 18, 25 → 3, 26 → 10}
```

```
RotIinv = {5 → 1, 11 → 2, 13 → 3, 6 → 4, 12 → 5, 7 → 6, 4 → 7, 17 → 8,
  22 → 9, 26 → 10, 14 → 11, 20 → 12, 15 → 13, 23 → 14, 25 → 15, 8 → 16, 24 → 17,
  21 → 18, 19 → 19, 16 → 20, 1 → 21, 9 → 22, 2 → 23, 18 → 24, 3 → 25, 10 → 26}
```

```
Table[Replace[Replace[Replace[x, RotI], RefB], RotIinv], {x, 1, 26, 1}]
```

```
{8, 11, 13, 19, 6, 5, 16, 1, 14, 12, 2, 10, 3, 9, 21, 7, 26, 25, 4, 22, 15, 20, 24, 23, 18, 17}
```

### Q3 :

```
EnigmaGuts = {1 → 8, 8 → 1, 2 → 11, 3 → 13, 4 → 19, 5 → 6, 6 → 5, 7 → 16, 8 → 1,
  9 → 14, 10 → 12, 11 → 2, 12 → 10, 13 → 3, 14 → 9, 15 → 21, 16 → 7, 17 → 26,
  18 → 25, 19 → 4, 20 → 22, 21 → 15, 22 → 20, 23 → 24, 24 → 23, 25 → 18 , 26 → 17}
```

### Q4 :

```
Table[ReplaceAll [x, EnigmaGuts] , {x, 1, 26, 1}]
{8, 11, 13, 19, 6, 5, 16, 1, 14, 12, 2, 10, 3, 9, 21, 7, 26, 25, 4, 22, 15, 20, 24, 23, 18, 17}
```

### Q5 :

```
Table [Enigma1 [1, n] , {n, 0, 25, 1} ]
```

```
{8, 10, 11, 16, 2, 26, 10, 20, 6, 3, 18, 25, 17, 22, 7, 18, 10, 8, 12, 3, 21, 25, 2, 26, 20, 18}
```

### Q6 :

```
list1 = Table [Enigma1 [1, n] , {n, 0, 25, 1} ]

list2 = Range[0, 25]
```

```
Enigma1[10, 1]
```

```
MapThread[Enigma1, {list1, {list2}}]
```

{1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1}

# Week 2

## Q1:

```
EnigmaMachine[text_, key_] :=
 MapThread[Enigma1, {text, Table[key + n, {n, 0, Length[text] - 1, 1}]}]
```

## Q2:

```
EnigmaMachine[{1, 2, 3, 4, 5}, 28]
```

{11, 3, 12, 9, 22}

```
EnigmaMachine[EnigmaMachine[{1, 2, 3, 4, 5}, 28], 28]
```

{1, 2, 3, 4, 5}

## Q3:

```
plain = {1, 3, 4, 23, 9, 2, 12, 8}

cypher = {17, 4, 14, 6, 17, 3, 4, 23, 8, 8, 19, 3, 1, 24, 22, 11, 6, 22, 15}

CyFrag = {3, 4, 23, 8, 8, 19, 3, 1}

CribCycle = [3, 4, 23, 8, 1]

crib = {1 → 3, 2 → 4, 3 → 23, 4 → 8, 8 → 1}

CribLocation = 6
```

the number of elements in the crib cycle is 5

## Q4:

```
Cyfrag = {3, 4, 23, 8, 8, 19, 3, 1}
Distance between each member of the crib cycle :
    (1 → 3) = 1
   (2 → 4) = 2
   (3 → 23) = 3
  (4 → 8) = 4
   (8 → 1) = 8
```

### Q5:

```
Bombe[plain_, cyfrag_, k_] :=
 If[Enigma1[plain[[1]], k] == cyfrag[[1]] && cyfrag[[1]] == plain[[2]] &&
   Enigma1[plain[[2]], k + 1] == cyfrag[[2]] && cyfrag[[2]] == plain[[3]] &&
   Enigma1[plain[[3]], k + 2] == cyfrag[[3]] && cyfrag[[3]] == plain [[4]] &&
      Enigma1[plain[[4]], k + 3] == cyfrag[[4]] && cyfrag[[4]] == plain[[8]] &&
      Enigma1[plain[[8]], k + 7] == cyfrag[[8]] && cyfrag[[8]] == plain[[1]],
  {"YES!!!", k}, {"no"}]

Table[Bombe[plain, cyfrag, k], {k, 0, 25, 1}]

{{"no"}, {"no"}, {"no"}, {"no"}, {"no"}, {"no"}, {"no"}, {"no"}, {"no"},
 {"no"}, {"no"}, {"no"}, {"no"}, {"no"}, {"no"}, {"no"}, {"no"}, {"no"},
 {"no"}, {"YES!!!", 19}, {"no"}, {"no"}, {"no"}, {"no"}, {"no"}, {"no"}}
```

The key setting found for the cribbed plaintext by using the Bombe expression is 19.

### Q6:

the Key setting for the whole ciphertext is 14.

### Q7:

3423881921

---

# Week 3

### Q1 :

```
  m = 12345;  a= 11111;  GCD[m,a]
EulerPhi[m]
Mod[a^EulerPhi[m],m]

1

6576

1

m = 123; a = 11; GCD[m, a]
EulerPhi[m]
Mod[a^EulerPhi[m], m]

1

80

1
```

## Q2:

```
ExtendedGCD[7, 17]
Mod[5 * 13, 17]
{1, {5, -2}}
14

[107] := GCD[148×953×050, 179×424×673]
PowerMod[123×456×789, EulerPhi[179×424×673] - 1, 179×424×673]

1
172×609×538

Mod[135×798×642 * 172×609×538, 179×424×673]

21×562×478

Mod[123×456×789 * 21×562×478, 179×424×673]

135×798×642

PowerMod[123×456×789, -1, 179×424×673]

172×609×538

Clear[x];
Solve[ 12 x == 8, {x}, Modulus → 16]

{{x → 2 + 4 C[1]}}

Clear[x];
Solve[ 12 x == 8, {x}, Modulus → 16] /. Table[{C[1] → n}, {n, 0, 4, 1}]

{{{x → 2}}, {{x → 6}}, {{x → 10}}, {{x → 14}}, {{x → 18}}}

x /. Solve[ 12 x == 8, {x}, Modulus → 16]

{2 + 4 C[1]}

x /. Solve[ 13 x == 1, {x}, Modulus → 16]

{5}
```

## Q3:

```
ChineseRemainder[{1, 0, 0}, {11, 13, 17}]
ChineseRemainder[{0, 1, 0}, {11, 13, 17}]
ChineseRemainder[{0, 0, 1}, {11, 13, 17}]
```

```
221
1496
715
```

```
u1 = ChineseRemainder[{1, 0, 0}, {13, 29, 64}]
u2 = ChineseRemainder[{0, 1, 0}, {13, 29, 64}]
u3 = ChineseRemainder[{0, 0, 1}, {13, 29, 64}]
```

7424

13 312

3393

```
ChineseRemainder[{10, 5, 7}, {13, 29, 64}]
```

19 783

```
Mod[10 * u1 + 5 * u2 + 7 * u3, 13 * 29 * 64]
```

19 783

## Q4.

```
<< "FiniteFields`"
```

```
k = 111111
```

111 111

```
Prime[k]
```

1 456 667

```
p = 1456667
```

1 456 667

```
PrimeQ[p]
PowerList[GF[p, 1]][[2]]
```

True

{2}

```
Primitive1 = PowerList[GF[p, 1]][[2]]
```

{2}

```
KeyB = 1500
```

1500

```
KeyA = 2500
```

2500

```
publiccA = PowerMod [Primitive1, KeyA, p]
```

{824 424}

```
publiccB = PowerMod[Primitive1, KeyB, p]
{767 659}

PowerMod[767 659, KeyA, p]
1 058 208

PowerMod[824 424, KeyB, p]
1 058 208
```

## Q5

```
k = 111 111
111 111

Prime[k]
1 456 667

p = 145 667;

a = Primitive1;

 r = RandomInteger[{0, p - 2}]
85 393

u = 123;

R = PowerMod[a, r, p]
{6919}

cB = PowerMod[a, mB, p]
{70 988}

S = Mod[PowerMod[cB, r, p] u, p]
{3313}

mB = 1640;

Mod[S * PowerMod[PowerMod[R, mB, p], -1, p], p]
{123}
```

## Q6

```
p = 145 667;

a = Primitive1;

mA = 2500;

r = RandomInteger[{0, p - 2}]

106 752

u = 123;
```

```
S =.;

R = PowerMod[a, r, p]

106752

u = 123;

S =.;

R = PowerMod[a, r, p]

{27140}

S /. Solve[{r S == u - mA * R}, {S}, Modulus -> p - 1] [[1]]

36463

cA = PowerMod [Primitive1, KeyA, p]

{44974}

R = PowerMod[a, r, p]

{54012}

cA = 2500; R = PowerMod[a, r, p] ; S = 36363;

PowerMod[a, u, p] == Mod[ PowerMod[cA, R, p] * PowerMod[R, S, p], p]

{True}
```

## Q7

```
pB = Prime[1450]
qB = Prime[1500]
nB = pB * qB
phiB = EulerPhi[nB]

12109

12553

152004277

151979616

eB = RandomInteger[{1, nB}];
While[GCD[eB, phiB] ≠ 1, eB = RandomInteger[{1, nB}]];
eB
ExtendedGCD[eB, phiB]

82430045

{1, {-34328395, 18618886}}

dB = -34328395;
Mod[eB * dB, phiB]

1
```

```
nB = 99 052 741; eB = 81 119 923; dB = -34 328 395;
m = 12 345 678;
c = PowerMod[m, eB, nB]
```

```
38 447 790
```

```
PowerMod[c, dB, nB]
```

```
47 918 729
```

```
NumberTheory ' NumberTheoryFunctions '
```

```
NumberTheory′ NumberTheoryFunctions′
```

```
a = ChineseRemainder[{1, 0}, {9733, 10 177}]
b = ChineseRemainder[{0, 1}, {9733, 10 177}]
```

```
45 287 650
```

```
53 765 092
```

```
p = 9733; q = 10 177; d = 16 391 903; c = 38 447 790; c1 = Mod[c, p]
c2 = Mod[c, q]
d1 = Mod[d, p - 1]
d2 = Mod[d, q - 1]
m1 = PowerMod[c1, d1, p]
m2 = PowerMod[c2, d2, q]
```

```
2440
```

```
9261
```

```
3215
```

```
8543
```

```
4237
```

```
9706
```

```
n = 99 052 741; Mod[m1 * a + m2 * b, n]
```

```
52 757 097
```

## Q8

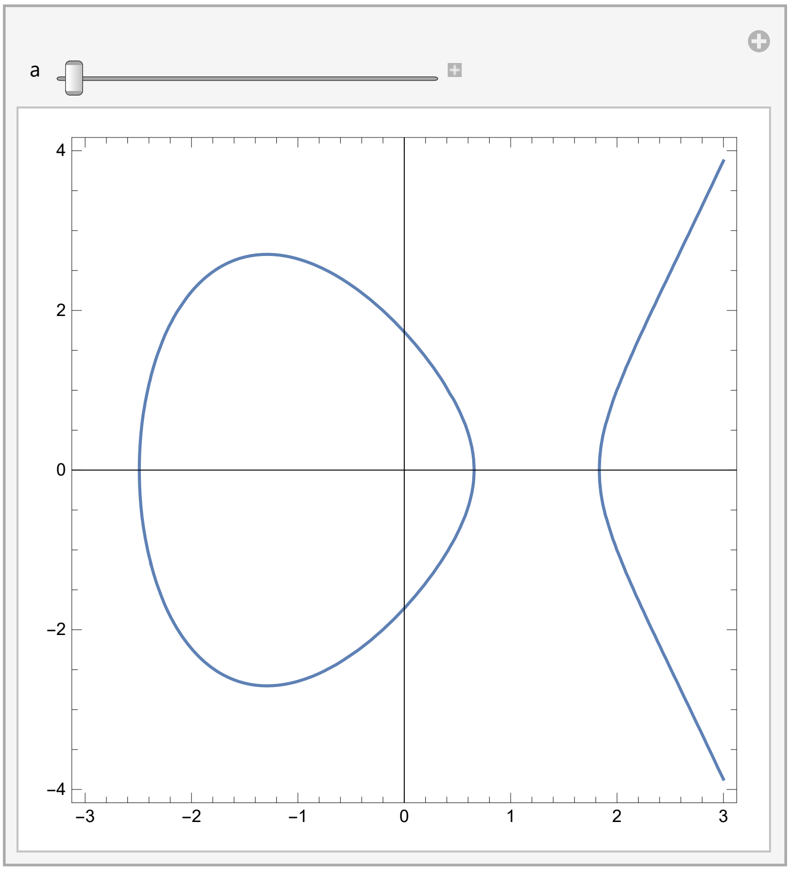
```
m = 11 111 111; c = PowerMod[m, dB, nB]
```

```
90 296 910
```

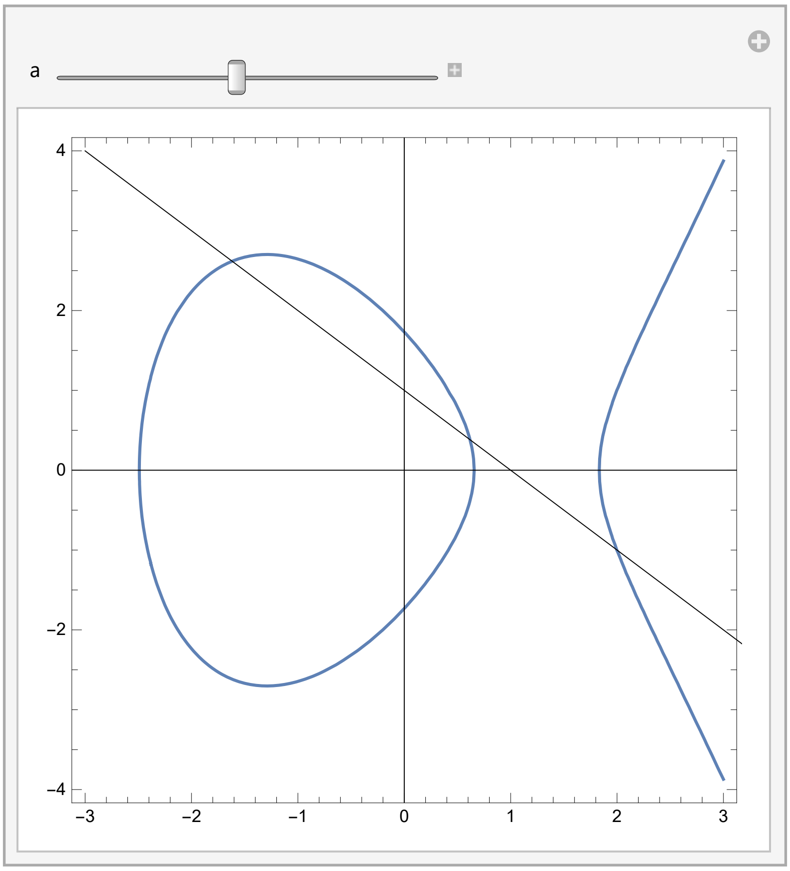
# Week 4

## Q1

```
Manipulate[
 ContourPlot[y^2 == x^3 - 5 x + 3, {x, -3, 3}, {y, -4, 4}, Axes → True], {a, -5, -3}]
```



```
Manipulate[ContourPlot[y^2 == x^3 - 5 x + 3, {x, -3, 3}, {y, -4, 4},
  Axes → True , Epilog → Line[{{-3, 4}, {4, -3}}]], {a, -5, -3}]
```

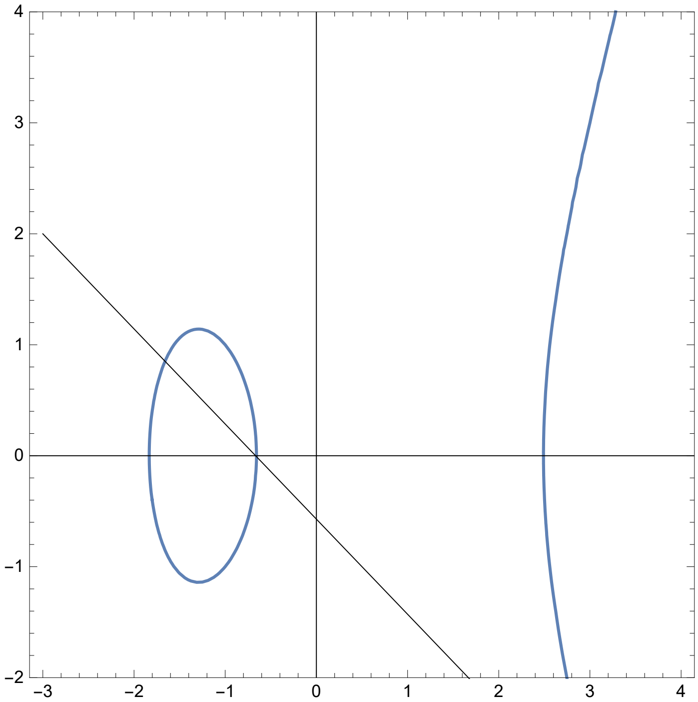


## Q2

The intersection line only crosses over one point once it is on -3.

## Q3

```
ContourPlot[x^3 - 5 x - 3 == y^2, {x, -3, 4}, {y, -2, 4},
 PlotRange → {-4, 4}, Axes → True, Epilog -> Line[ {{-3, 2}, {4, -4}}]]
```




## Q4

```
NSolve[ {y² == x³ - 5 x + 3, y == -x + 1}, {x, y}]
{{x → -1.61803, y → 2.61803}, {x → 2., y → -1.}, {x → 0.618034, y → 0.381966}}
```

## Q5

```
p = 11;

Table[Solve[ {y² == x³ - 5 x + 3, x == u}, {x, y}, Modulus -> p], {u, 0, p - 1}]
{{{x → 0, y → 5}, {x → 0, y → 6}}, {},
 {{x → 2, y → 1}, {x → 2, y → 10}}, {{x → 3, y → 2}, {x → 3, y → 9}},
 {{x → 4, y → 5}, {x → 4, y → 6}}, {{x → 5, y → 2}, {x → 5, y → 9}}, {},
 {{x → 7, y → 5}, {x → 7, y → 6}}, {}, {{x → 9, y → 4}, {x → 9, y → 7}}, {}}
```

## Q6

```
p = 11;
Clear[x];
ec = x^3 - 5 x + 3;
il = 4 x + 1;
Factor[il^2 - ec, Modulus -> p]
```

10 (2 + x) (7 + x) (8 + x)

```
x = Mod[{-2, -7, -8}, p]
y = Mod[4 * x + 1, p]
```

{9, 4, 3}

{4, 6, 2}

```
InterpolatingPolynomial[{{5, 3}, {2, 7}}, 5]
```

3

```
EllipticAdd[p_, a_, b_, c_, P_List, Q_List] :=
 Module[{lam, x3, y3, P3}, Which[P == {O}, R = Q, Q == {O}, R = P, P[[1]] ≠ Q[[1]],
   lam = Mod[(Q[[2]] - P[[2]]) PowerMod[Q[[1]] - P[[1]], -1, p], p];
   x3 = Mod[lam^2 - a - P[[1]] - Q[[1]], p];
   y3 = Mod[-(lam (x3 - P[[1]]) + P[[2]]), p];
   R = {x3, y3}, (P == Q) && (P ≠ {O}),
   lam = Mod[(3 * P[[1]]^2 + 2 a * P[[1]] + b) PowerMod[2 P[[2]], -1, p], p];
   x3 = Mod[lam^2 - a - P[[1]] - Q[[1]], p];
   y3 = Mod[-(lam (x3 - P[[1]]) + P[[2]]), p];
   R = {x3, y3}, (P[[1]] == Q[[1]]) && (P[[2]] ≠ Q[[2]]), R = {O}]; R]
```

```
p = 11; a = 0; b = 6; c = 3; EllipticAdd[p, a, b, c, {5, 3}, {2, 7}]
EllipticAdd[p, a, b, c, {5, 3}, {5, 3}]
EllipticAdd[p, a, b, c, {2, 6}, {2, 7}]
EllipticAdd[p, a, b, c, {5, 7}, {O}]
EllipticAdd[p, a, b, c, {5, 7}, {5, 5}]
EllipticAdd[p, a, b, c, {O}, {2, 7}]
```

{7, 7}

{10, 1}

{O}

{5, 7}

{O}

{2, 7}

## Q7

```
FactorInteger[432]
IntegerDigits[432, 2]
IntegerDigits[432/2, 2]
IntegerDigits[432/3, 2]
```

```
{{2, 4}, {3, 3}}

{1, 1, 0, 1, 1, 0, 0, 0, 0}

{1, 1, 0, 1, 1, 0, 0, 0}

{1, 0, 0, 1, 0, 0, 0, 0}
```

```
p = 863; P =.;
a = 100; b = 10; c = 1;
P[0] = {121, 517};
P[i_] := P[i] = EllipticAdd[p, a, b, c, P[i - 1], P[i - 1]];
Q = EllipticAdd[p, a, b, c,
  EllipticAdd[p, a, b, c, P[8], P[7]],          EllipticAdd[p, a, b, c, P[5], P[4]]]
EllipticAdd[p, a, b, c, EllipticAdd[p, a, b, c, P[7], P[6]],
 EllipticAdd[p, a, b, c, P[4], P[3]]]
EllipticAdd[p, a, b, c, P[7], P[4]]
```

```
{O}

{19, 0}

{341, 175}
```

## Q8

```
QAlice = EllipticAdd[p, a, b, c, P[7], P[1]]
QBob = EllipticAdd[p, a, b, c, P[8], P[5]]
```

```
{162, 663}

{341, 688}
```

## Q9

```
<< FiniteFields`
```

```
z16 = GF[2, 4]
```

```
GF[2, {1, 0, 0, 1, 1}]
```

```
FullForm[%]
```

```
GF[2, List[1, 0, 0, 1, 1]]
```

```
FieldIrreducible[z16, x]
```

```
FieldIrreducible[GF[2, {1, 0, 0, 1, 1}], {9, 4, 3}]
```

```
Characteristic[z16]
```

```
2
```

```
ExtensionDegree[z16]
```
4

```
FieldSize[z16]
```
16

```
dd = z16[{0, 0, 1, 1}]
```
$\{0, 0, 1, 1\}_2$

```
dd + dd
```
0

```
dd - dd
```
0

```
ee = z16[{1, 1, 0, 0}]
```
$\{1, 1, 0, 0\}_2$

```
dd ee
```
$\{1, 0, 1, 1\}_2$

```
dd / ee
```
$\{0, 0, 1, 0\}_2$

```
ee = z15[{1, 1, 0, 0}]
```
z15[{1, 1, 0, 0}]

```
dd
```
$\{0, 0, 1, 1\}_2$

```
dd ee
```
z15[{1, 1, 0, 0}] $\{0, 0, 1, 1\}_2$

```
dd / ee
```
$$\frac{\{0, 0, 1, 1\}_2}{\text{z15}[\{1, 1, 0, 0\}]}$$

## Q10

```
ee = z16[{1, 1, 0, 0}]
```
$\{1, 1, 0, 0\}_2$

```
(dd^n)^3 + ee (dd^n)^2
```
$\{0, 0, 1, 1\}_2^{3n} + \{0, 0, 1, 1\}_2^{2n} \{1, 1, 0, 0\}_2$

```
y^2 + x y
```
{52, 60, 10}

```
x^3 + ee x^2

{{0, 1, 0, 0}_2, 64, {0, 1, 0, 0}_2}

Z2mEllipticAdd[a_, c_, P_List, Q_List] := Module[{lam, x3, y3, P3, R},
  Which[P == {O}, R = Q, Q == {O}, R = P, ToElementCode[P[[1]]] ≠ ToElementCode[Q[[1]]],
   lam = (Q[[2]] + P[[2]]) / (Q[[1]] + P[[1]]);
   x3 = lam^2 + lam + a + P[[1]] + Q[[1]];
   y3 = lam (x3 + P[[1]]) + x3 + P[[2]];
   R = {x3, y3}, ((ToElementCode[P[[1]]] == ToElementCode[Q[[1]]]) && (ToElementCode[
         P[[2]]] == ToElementCode[Q[[2]]])) && (P ≠ {O}), lam = P[[1]] + P[[2]] / P[[1]];
   x3 = lam^2 + lam + a;
   y3 = P[[1]]^2 + (lam + 1) x3;
   R = {x3, y3}, (ToElementCode[P[[1]]] == ToElementCode[Q[[1]]]) &&
    (ToElementCode[P[[2]]] ≠ ToElementCode[Q[[2]]]), R = {O}];
  R]

P =.;
a = ee;
c = 0;
P[0] = {x, y};
P[i_] := P[i] = Z2mEllipticAdd[a, c, P[i - 1], P[i - 1]]
Q = EllipticAdd[p, a, b, c,
  EllipticAdd[p, a, b, c, P[8], P[7]],          EllipticAdd[p, a, b, c, P[5], P[4]]]
EllipticAdd[p, a, b, c, EllipticAdd[p, a, b, c, P[7], P[6]],
 EllipticAdd[p, a, b, c, P[4], P[3]]]
EllipticAdd[p, a, b, c, P[7], P[4]]

{Mod[{1, 1, 0, 0}_2, 863], Mod[-688 - 66 (-341 + Mod[{1, 1, 0, 0}_2, 863]), 863]}
```

# Week 5

```
RandomInteger[1, 40]
{0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1,
 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0}

AliceBasis = Table[RandomInteger[1, 40]]
{0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1,
 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0}

AliceData = Table[RandomInteger[1, 40]]
{1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1,
 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1}

BobBasis = Table[RandomInteger[1, 40]]
{1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0,
 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1}

if[
 AliceData == Bobdata ×
    EqualBases = 1 ×
    else ×
    EqualBases = 0
]

if[0]

if[
 AliceBasis = BobBasis ×
    Bobdata = AliceData ×
    EqualBases
]

if[{1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1,
  1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1}]


Bobdata = Intersection[AliceBasis, BobBasis]
{0, 1}
```