IERG4130 Assignment 2

LAU Long Ching
SID: 1155127347

16/03/2021

Question 1

The only prime number factors for n=35 is p=7 and q=5.

z = (p − 1)(q − 1) = 24

Since e=5, 5 × d mod 24 = 1

The private key can be (d=29, n=35).

$M = C^d$ mod $n = 11^{29}$ mod 35 = 16.

Question 2

The only prime number factors for n=34163 is p=127 and q=269.

z = (p − 1)(q − 1) = 33768

Since e=5, 5 × d mod 33768 = 1

The private key can be (d=54029, n=34163).

Question 3

(a)

Since we have the prime q=11 and the primitive root α=2,

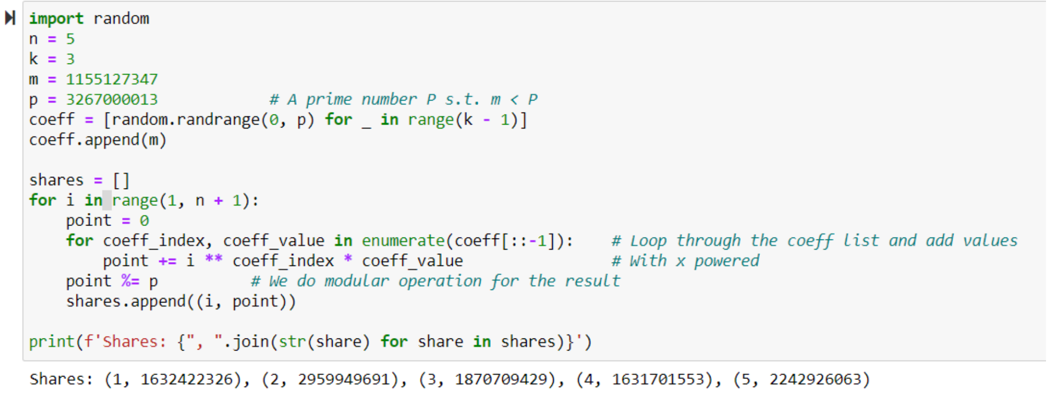
2^x mod 11 = 9

We have Alice's secret key x=6.

(b)

The shared secret key = 3^6 mod 11 = 3.

Question 4



```python
import random
n = 5
k = 3
m = 1155127347
p = 3267000013             # A prime number P s.t. m < P
coeff = [random.randrange(0, p) for _ in range(k - 1)]
coeff.append(m)

shares = []
for i in range(1, n + 1):
    point = 0
    for coeff_index, coeff_value in enumerate(coeff[::-1]):    # Loop through the coeff list and add values
        point += i ** coeff_index * coeff_value                # With x powered
    point %= p          # We do modular operation for the result
    shares.append((i, point))

print(f'Shares: {", ".join(str(share) for share in shares)}')
```

```
Shares: (1, 1632422326), (2, 2959949691), (3, 1870709429), (4, 1631701553), (5, 2242926063)
```

3 pairs of the key (1, 1632422326), (2, 2959949691), (3, 1870709429) would be enough for the decryption.

Please find the .py file attached. The source code can also be found above.

Question 5

(a) (b)

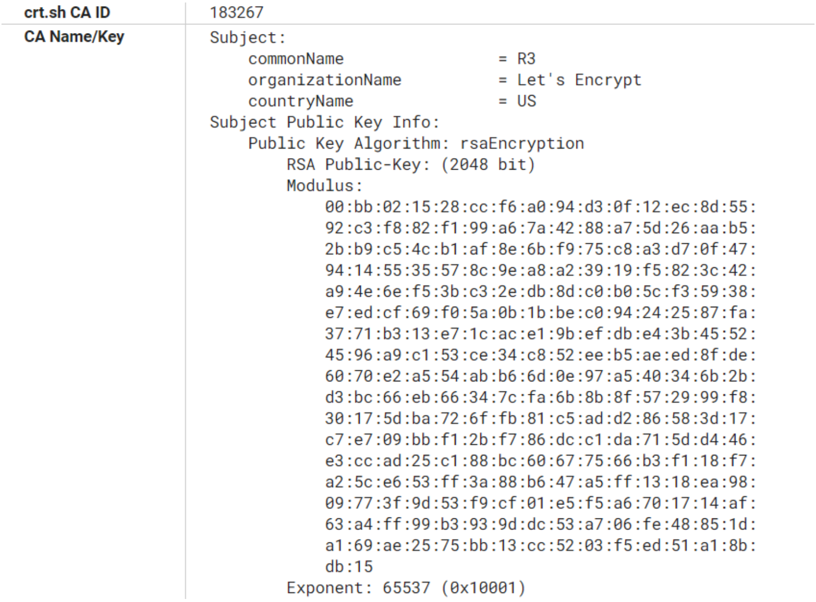
Please refer to attachments.

(c)

The issuer of the certificate is called ”Let’s Encrypt”. It also has a common name ”R3”.

(d)

On crt.sh, we can find the public key of the issuer:

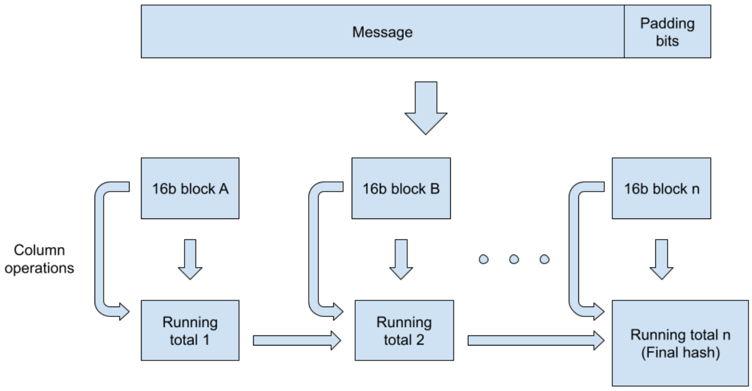


crt.sh CA ID	183267
CA Name/Key	(below)

```
Subject:
    commonName                = R3
    organizationName          = Let's Encrypt
    countryName               = US
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        RSA Public-Key: (2048 bit)
        Modulus:
            00:bb:02:15:28:cc:f6:a0:94:d3:0f:12:ec:8d:55:
            92:c3:f8:82:f1:99:a6:7a:42:88:a7:5d:26:aa:b5:
            2b:b9:c5:4c:b1:af:8e:6b:f9:75:c8:a3:d7:0f:47:
            94:14:55:35:57:8c:9e:a8:a2:39:19:f5:82:3c:42:
            a9:4e:6e:f5:3b:c3:2e:db:8d:c0:b0:5c:f3:59:38:
            e7:ed:cf:69:f0:5a:0b:1b:be:c0:94:24:25:87:fa:
            37:71:b3:13:e7:1c:ac:e1:9b:ef:db:e4:3b:45:52:
            45:96:a9:c1:53:ce:34:c8:52:ee:b5:ae:ed:8f:de:
            60:70:e2:a5:54:ab:b6:6d:0e:97:a5:40:34:6b:2b:
            d3:bc:66:eb:66:34:7c:fa:6b:8b:8f:57:29:99:f8:
            30:17:5d:ba:72:6f:fb:81:c5:ad:d2:86:58:3d:17:
            c7:e7:09:bb:f1:2b:f7:86:dc:c1:da:71:5d:d4:46:
            e3:cc:ad:25:c1:88:bc:60:67:75:66:b3:f1:18:f7:
            a2:5c:e6:53:ff:3a:88:b6:47:a5:ff:13:18:ea:98:
            09:77:3f:9d:53:f9:cf:01:e5:f5:a6:70:17:14:af:
            63:a4:ff:99:b3:93:9d:dc:53:a7:06:fe:48:85:1d:
            a1:69:ae:25:75:bb:13:cc:52:03:f5:ed:51:a1:8b:
            db:15
        Exponent: 65537 (0x10001)
```

Question 6

(a)



(b)

First block:

A	L	I	C
E	T	H	I
N	K	S	T
H	E	A	S

converts to

0	11	8	2
4	19	7	8
13	10	18	19
7	4	0	18

after column operations

4	10	0	18
13	4	8	19
7	11	7	8
0	19	18	2

Running total: $(0,0,0,0) \rightarrow (21,12,8,3) \rightarrow (1,4,15,16)$

Second block:

S	I	G	N
M	E	N	T
I	S	V	E
R	Y	E	A

converts to

18	8	6	13
12	4	13	19
8	18	21	4
17	24	4	0

after column operations

12	18	4	0
8	24	6	4
17	8	13	19
18	4	21	13

Running total: $(1,4,15,16) \rightarrow (20,0,14,9) \rightarrow (2,16,19,13)$

Third block:

S	Y	F	O
R	O	U	R
S	T	U	D
E	N	T	S

converts to

18	24	5	14
17	14	20	17
18	19	20	3
4	13	19	18

after column operations

17	19	19	18
18	13	5	3
4	24	20	17
18	14	20	14

Running total: $(2,16,19,13) \rightarrow (11,6,1,15) \rightarrow (6,19,14,3)$

The hash is GTOD.

(d)

First block:

A	A	A	A
G	A	A	A
N	A	A	A
B	A	A	A

converts to

0	0	0	0
6	0	0	0
13	0	0	0
1	0	0	0

after column operations

6	0	0	0
13	0	0	0
1	0	0	0
0	0	0	0

Running total: $(0,0,0,0) \rightarrow (0,6,13,1) \rightarrow (6,19,14,1)$

Second block:

A	A	A	A
A	B	Z	A
A	A	B	A
A	A	A	A

converts to

0	0	0	0
0	1	25	0
0	0	1	0
0	0	0	0

after column operations

0	0	0	0
0	0	0	0
0	0	25	0
0	1	1	0

Running total: $(6, 19, 14, 1) \to (6, 19, 15, 1) \to (6, 19, 14, 3)$

Third block:

A	A	A	A
A	A	A	A
A	A	A	A
A	A	A	A

converts to

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

after column operations

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

Running total: $(6, 19, 14, 3) \to (6, 19, 14, 3) \to (6, 19, 14, 3)$

The block AAAAGAAANAAABAAAAAAAABZAAABAAAAAAAAAAAAAAAAAAAAA produces the same hash GTOD.