1:

Number Theory covers many of the most important topics in mathematics and they are all very deeply and intrinsically connected together.

Starting with divisibility, we say that a nonzero b divides a if a = mb for some m, where a, b and m are integers. A common notation for this is b|a, therefore we say b|a we say that b is divisor of a. a few properties of divisibility are a|1, then a += 1, if a|b and b|a then a+= b.

Euclidean algorithm is one of the basic techniques of number theory. It is a procedure for determining the greatest common divisor of two positive integers. Two integers are relatively prime if their only common positive integer factor is 1. The greatest common divisor of a and b is the largest integer that divides both a and b. We can use the notation gcd(a,b) to mean the greatest common divisor of a and b therefore we also define gcd(0,0)=0. Euclidian algorithm is for easily finding the greatest common divisor of two integers.

Modular arithematic, if an there is an integer a and n is another positive integer, we define a mod n t be the remainder when a is divided by n, then the integer is called the modulus.

$$A = qn + r \quad 0 <= r < n; \quad q=[a/n]$$

Two integers a and b are then said to be congruent modulo n if (a mod n) =(b mod n).

This is written as a = b(mod n). there are properties of congruence such as a=n(mod n) if n|(a-b), a=b(mod n) implies b = a(mod n), a=b(mod n) and b=c(mod n) imply a=c(mod n).

Prime numbers only have divisors of 1 and itself, and they cannot be written as a product of other numbers, they are very central to number theory. Any integer a>1 can be factored ina unique way. This is knonw as the fundamental theorem of arithmetic.

Fermat’s little theorem states the following, that is p is a prime and a is a positive integer not divisible by p then a^p-1 = 1(mod p),

An alternate form of this is a^p = a(mod p). this is veery important in public-key cryptography.

2:

N = pq= 77, then p and q equal 7 and 11

ø(n) = (p-1)(q-1)

ø(n) = (6)(10)

ø(n) = 60

d*13 = 1 mod 60 and d < 60

```
for d in range(60):
    if (d * 13) % 60 == 1:
        print(d)
```

d must be 37

M = C^d mod n

M = 20^37 mod 77

M = 48

3:

i	8	7	6	5	4	3	2	1	0
b_i	1	1	1	0	1	1	0	0	0
c	1	3	7	14	29	59	118	236	472
f	6	216	3321	2006	166	1416	451	1916	3346

6^{472} mod 3415 = 3346

4:

A)

(a) S-box

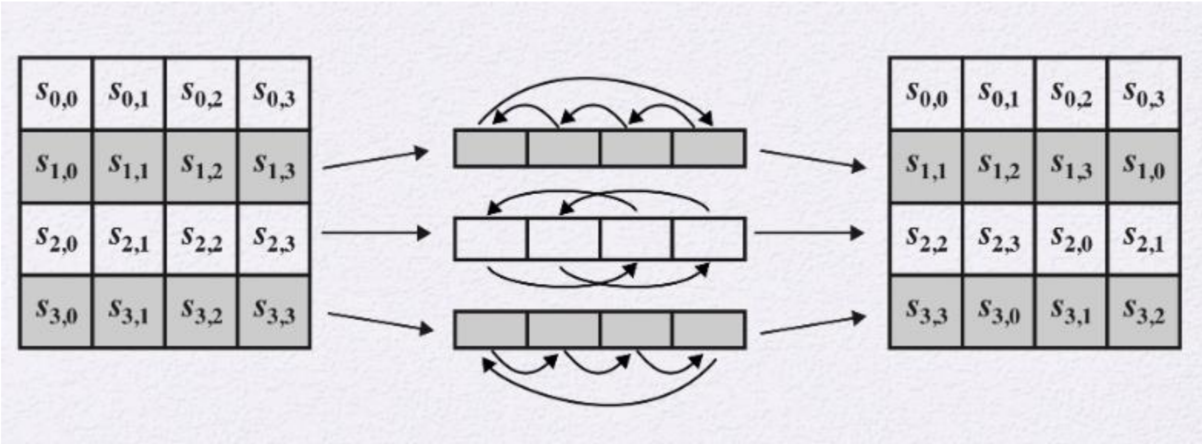
x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

5C	6B	05	F4
7B	72	A2	6D
B4	34	31	12
9A	9B	7F	94

$\rightarrow$

4A	7F	6B	BF
21	40	3A	3C
8D	18	C7	C9
B8	14	D2	22

B)



(a) Shift row transformation

67	A7	78	97
35	99	A6	D9
61	68	68	0F
B1	21	82	FA

67	A7	78	97
99	A6	D9	35
68	0F	61	68
FA	B1	21	82