Advanced Security CA 2

Question One

Number Theory encompasses: Divisibility, Greatest Common Divisor (GCD)/the Euclidean Algorithm, Extended Euclidean Algorithm, Modular Arithmetic among others.

- Divisibility
    - Divisibility is one of the most fundamental concepts in number theory. ... If a divides b, we say “a is a divisor of b”, “b is divisible by a”, “a is a factor of b”, “b is a multiple of a”. The “divisor” a in this definition can be negative but must be nonzero; divisibility by 0 is not defined. The Division Algorithm is that given any positive integer n and any nonnegative integer a, if we divide a by n we get an integer quotient q and an integer remainder r that obey the following relationship:
        - $a = qn + r \qquad 0 \le r < n;\ q = [a/n]$
- The Euclidean Algorithm/Greatest Common Divisor (GCD)
    - The greatest common divisor (GCD) of two nonzero integers a and b is the greatest positive integer d such that d is a divisor of both a and b; that is, there are integers e and f such that a = de and b = df, and d is the largest such integer. The GCD of a and b is generally denoted gcd(a, b). Two integers are relatively prime if their only common positive integer factor is 1.
        - Example
            - 600 = 4 × 136 + 56
            - 136 = 2× 56 + 24
            - 56 = 2× 24 + 8
            - 24 = 3× 8 + 0
            - GCD(600,136) = 8
- Extended Euclidean Algorithm
    - The Extended Euclidean Algorithm is, as you might imagine, an extension of the standard Euclidean Algorithm. The standard version was developed to find the greatest common divisor (GCD) of two numbers. The Extended algorithm adds the capability to find the Bézout coefficients for the two input numbers.
        - Example (273, 399)
        - a = 273, b = 399
          a is not 0
          a_1 = 126 (399 % 273)
          b_1 = a = 273

        - a_1 is not 0
          a_2 = 21 (273 % 126)
          b_2 = a_1 = 126

        - a_2 is not 0
          a_3 = 0 (126 % 21)
          b_3 = a_2 = 21

        - a_3 is 0

> b_3 is 21
> So GCD is 21

- Modular Arithmetic
    - Modular arithmetic, sometimes referred to as modulus arithmetic or clock arithmetic, in its most elementary form, arithmetic done with a count that resets itself to zero every time a certain whole number N greater than one, known as the modulus (mod), has been reached.

It is also used for Chinese Remainder Theorem, RSA Encryption among others.

Question 2

To Decrypt the Plaintext (M) we must first find the prime factors of the integer N (77). To do this 77 must be factorised which in this case is 7x11 since they are 2 distinct prime factors.

Divisors of 77 are 1, 7, 11, 77.

Then d=e−1modφ

D=13-1mod60=37

From there its just regular RSA decryption as all the factors are known which makes the decrypted number 48

Question 3

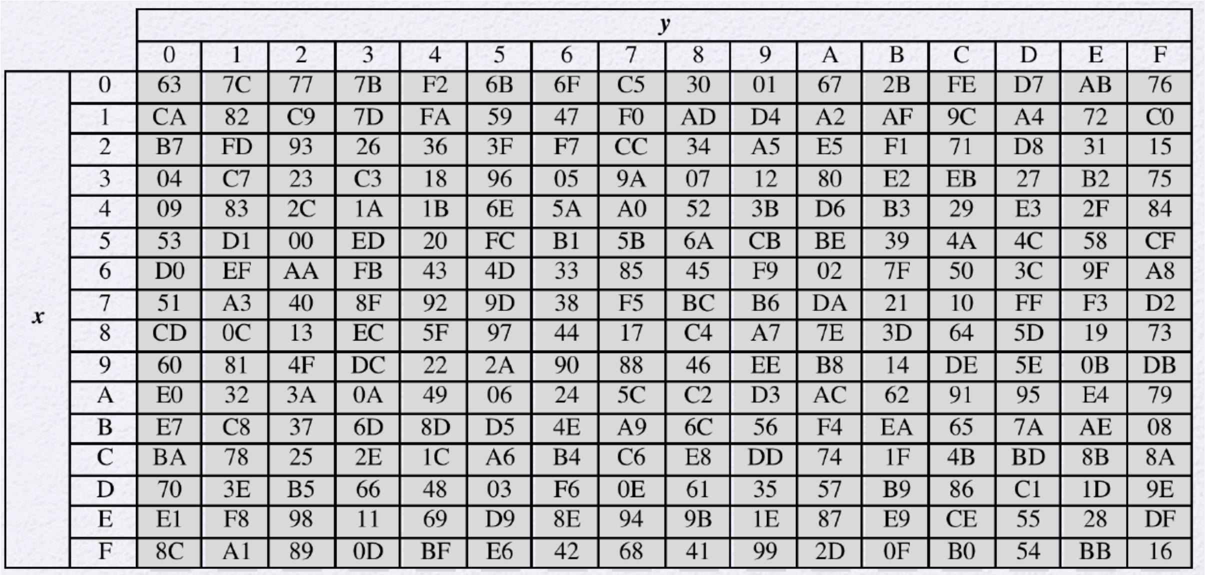
Use Fast Exponentiation Algorithm to determine 6^{472} mod 3415:

1	C1 = $1^2 \cdot 6^1 = 1 \cdot 6 = 6$ mod 3415
1	C2 = $62 \cdot 6^1 = 36 \cdot 6 = 216$ mod 3415
1	C3 = $216^2 \cdot 6^1 = 46656 \cdot 6 = 279936 = 3321$ mod 3415
0	C4 = $3321^2 \cdot 6^0 = 11029041 \cdot 1 = 11029041 = 2006$ mod 3415
1	C5 = $2006^2 \cdot 6^1 = 4024036.6= 24144216 = 166$ mod 3415
1	C6 = $166^2 \cdot 6^1= 27556.6= 165336 = 1416$ mod 3415
0	C7 = $1416^2 \cdot 6^0 = 20050561= 2005056 = 451$ mod 3415
0	C8 = $451^2 \cdot 6^0= 203401 \cdot 1 = 203401 = 1916$ mod 3415
0	C9 = $1916^2 \cdot 6^0= 3671056 \cdot 1 = 3671056 = 3346$ mod 3415

Answer 3346

Question 4

Part A



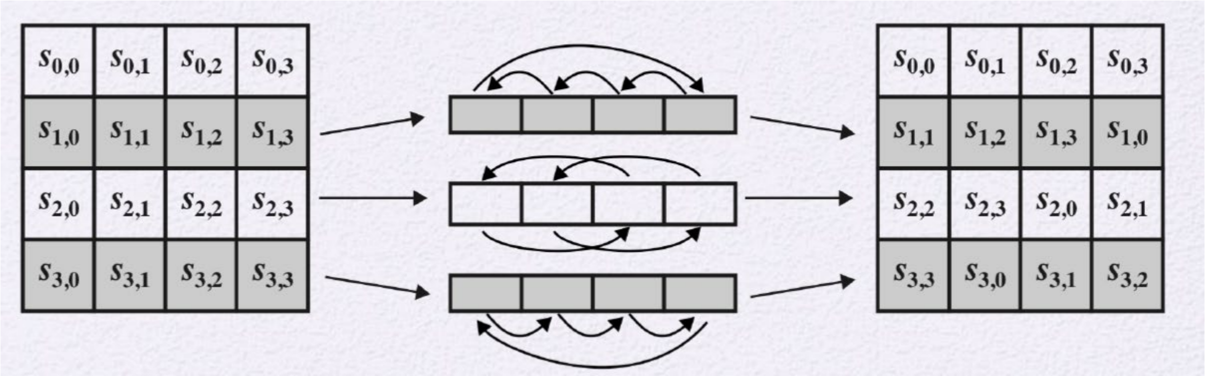
		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	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

→

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

Part B



$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,1}$	$s_{1,2}$	$s_{1,3}$	$s_{1,0}$
$s_{2,2}$	$s_{2,3}$	$s_{2,0}$	$s_{2,1}$
$s_{3,3}$	$s_{3,0}$	$s_{3,1}$	$s_{3,2}$

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	68	61
Fa	B1	21	82