Home Assignment 1

1] a) 11, 17 ⇒ m

A	B	Q	R	T_1	T_2	T_3
17	11	1	6	0	1	-1
11	6	1	5	1	-1	2
6	5	1	1	-1	2	-3
5	1	5	0	2	-3	

$-3 + 17 = \boxed{14}$

b)

A	B	Q	R	T_1	T_2	T_3
1056	3	352	0	0	1	

their gcd $\neq 1$ ⇒ there's no multiplicative inverse

2] a) $3^{301} \bmod 5 \Rightarrow 3^4 = 1 \bmod 5$

$3^{300} \cdot 3^1 = (3^{75})^4 \cdot 3 \rightarrow 3 \bmod 5$

$\cdot (3^4 \bmod 5)^{75}$

$= 1$

$\Rightarrow \boxed{3}$

b) $7^{105} \bmod 143$ $\phi(143) = \phi(13) \times \phi(11)$

$12 \times 10 = 120$

13	143
11	11

$\Rightarrow 7^{120} = 1 \bmod 143$

$7^{10} \times 7^{10} \times 7^{10} \times 7^{10} \times 7^{10} \times 7^{10} \times 7^{10} \times 7^{10} \times 7^{10} \times 7^{10} \times 7^5$

$7^5 \bmod 143 = 76$

$7^{10} \bmod 143 = 56$

$56^5 \bmod 143 = 23$

$23 \times 23 \times 76 = 40204 \bmod 143 = \boxed{21}$

3)

A	B	Q	R	S_1	S_2	S_3	T_1	T_2	T_3
30030	257	116	218	1	0	1	0	1	-116
257	218	1	39	0	1	-1	1	-116	117
218	39	5	23	1	-1	6	-116	117	-701
39	23	1	16	-1	6	-7	117	-701	818
23	16	1	7	6	-7	13	-701	818	-1519
16	7	2	2	-7	13	-33	818	-1519	3856
7	2	3	1	13	-33	112	-1519	3856	-13087
2	1	2	0	-33	112				

$S * A + T * B = C$

$112 \times 30030 + -13087 \times 257 = 1$

4) $12x \equiv 28 \bmod 233$ ÷4

$3x \equiv 7 \bmod 233$

$x = 7/3 \bmod 233$ gd inverse 3 mod 233

A	B	Q	R	T_1	T_2	T_3
233	3	77	2	0	1	-77
3	2	1	1	1	-77	78
2	1	2	0	-77	78	

$x = 78 \times 7 = 546 \bmod 233$ → 80

$X = 80 + 233K$

5) ① $x \equiv 1 \mod 3$ $\quad X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \mod M$

② $x \equiv 2 \mod 4$

③ $x \equiv 3 \mod 5$

Given		required		
$a_1 = 1$	$m_1 = 3$	$M_1 = 20$	$M_1^{-1} = 2$	$M = m_1 \times m_2 \times m_3$
$a_2 = 2$	$m_2 = 4$	$M_2 = 15$	$M_2^{-1} = 3$	$= 3 \times 4 \times 5$
$a_3 = 3$	$m_3 = 5$	$M_3 = 12$	$M_3^{-1} = 3$	$= 60$

$M_1 = \frac{M}{m_1} = \frac{60}{3} = 20$

$M_2 = 60/4 = 15$

$M_2 = 60/5 = 12$

$X = 1 \times 20 \times 2 + 2 \times 15 \times 3 + 3 \times 12 \times 3$

$40 + 90 + 108 \mod 60 = 58$

smallest = 58

next smallest = $58 + 60 = 118$

1	1	1	1	-3	4
1	3	0	-3	4	

5	2	0	1	-2	5
2	1	2	0	-2	5

$X = 140 + 120 + 180$

6] $P(x) = x^8 + x^4 + x^3 + x + 1$

A	B	Q	R	T_1	T_2	T_3
$x^8+x^4+x^3+x+1$	x^5	x^3	x^4+x^3+x+1	0	1	$-x^3$
x^5	x^4+x^3+x+1	$x+1$	x^3+x^2+1	1	x^3	x^4+x^3+1
x^4+x^3+x+1	x^3+x^2+1	x	1	$-x^3$	x^4+x^3+1	
x^3+x^2+1	1	x^3+x^2+1	0			

$x^8+x^4+x^3+x+1$ % x^5 $\quad Q = x^3$

① x^8

$x^4+x^3+x+1 \rightarrow r$

x^5 $\quad Q = x+1$

④ $x^5+x^4+x^2+x$ $\quad 1-(x^3(x^{11}+1))$

x^4+x^2+x $\quad 1-x^7-x^3$

⑤ x^4+x^3+x+1

x^3+x^2+1 $\quad Q = 1$

x^4+x^3+x+1

x^4+x^3+x

1

$-x^3-(x(x^4+x^3+1))$

$x^3-x^5-x^4+x$ %2 $-x^5+x^4+x^3+x+1$

x^8-x^5+1 $\quad$ inverse x^5

8421

odd: 1

even 0

A	10
B	11
C	12
D	13
E	14
F	15

7] key generation:

2b 7e 15 16 | 28 ae d2 a6 | ab f7 15 88 | 09 cf 4f

① cf 4f 3c 09 => 8A 84 EB 01

② 1000 1010

+ 0000 0001

1000 1011 | 1000 0100 | 1110 1011 | 0000 0001

+ 0010 1011 | 0111 1110 | 0001 0101 | 0001 0110

1010 0000 | 1111 1010 | 1111 1110 | 0001 0111

A 0 F A F E 1 7

w(5) = 1010 0000 | 1111 1010 | 1111 1110 | 0001 0111

+ 0010 1000 | 1010 0010 | 1101 0010 | 1010 0110

1000 1000 | 0101 1000 | 0010 1100 | 1011 0001

8 8 5 8 2 C B 1

w(6) = 1000 1000 | 0101 1000 | 0010 1100 | 1011 0001

+ 1010 1011 | 1111 0111 | 0001 0101 | 1000 1000

0010 0011 | 1010 1111 | 0011 1001 | 0011 1001

2 3 A F 3 9 3 9

w(7) 0010 0011 | 1010 1111 | 0011 1001 | 0011 1001

+ 0000 1001 | 1100 1111 | 0100 1111 | 0011 1100

0010 1010 | 0110 0000 | 0111 0110 | 0000 0101

2 A 6 0 7 6 0 5

1st key: A0 FA FE 17 88 58 2C B1 23 AF 39 39

2A 60 76 05

8421

odd 1
even 0

A	10
B	11
C	12
D	13
E	14
F	15

*encryption:

① XOR with key

(+)
0011 | 0010 | 0100 | 0011 | 1111 | 0110 | 1010 | 1000
0010 | 1011 | 0111 | 1110 | 0001 | 0101 | 0001 | 0110
0001 | 1001 | 0011 | 1101 | 1110 | 0011 | 1011 | 1110
1 9 3 D E 3 B E

(+)
1000 | 1000 | 0101 | 1010 | 0011 | 0000 | 1000 | 1101
0010 | 1000 | 1010 | 0010 | 1101 | 0010 | 1010 | 0110
1010 | 0000 | 1111 | 1000 | 1110 | 0010 | 0010 | 1011
A 0 F 8 E 2 2 B

(+)
0011 | 0001 | 0011 | 0001 | 1001 | 1000 | 1010 | 0010
1010 | 1011 | 1111 | 0111 | 0001 | 0101 | 1000 | 1000
1001 | 1010 | 1100 | 0110 | 1000 | 1101 | 0010 | 1010
9 A C 6 8 D 2 A

(+)
1110 | 0000 | 0011 | 0111 | 1011 | 0111 | 0011 | 0100
0000 | 1001 | 1100 | 1111 | 0100 | 1111 | 0011 | 1100
1110 | 1001 | 1111 | 1000 | 1111 | 1000 | 0000 | 1000
E 9 F 8 F 8 0 8

⇒ 19 3D E3 BE | A0 F8 E2 2B | 9A C6 8D 2A | E9 F8 F8 08

② Sub-byte

D427 | 11 AE | E0 41 98 F1 | B8 B4 5D E5 | 1E 41 41 30

③ Shift row

D4 11 5D 30
27 98 E5 1E
11 F1 B8 41
AE E0 B4 41

D4	E0	B8	1E
27	41	B4	41
11	98	5D	41
AE	F1	E5	30

④ Mix Column

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} D4 & E0 & B8 & 1E \\ 41 & B4 & 41 & 27 \\ 5D & 41 & 11 & 98 \\ 30 & AE & F1 & E5 \end{bmatrix}$$

02.D4 : 0000 0010
1101 0100
1101 0110

01.5D : 0000 0001
0101 1101
0101 1100
1101 0110
1000 1010

02.E0 : 0000 0010
1110 0000
1110 0010

01.41 : 0000 0001
0100 0001
0100 0000
1110 0010
1010 0010

03.41 : 0000 0011
0100 0001
0100 0010

01.30 : 0000 0001
0011 0000
0011 0001
0100 0010
0111 0011
1000 1010
1111 1001

03.B4 : 0000 0011
1011 0100
1011 0111

01.AE : 0000 0001
1010 1110
1010 1111
1011 0111
0001 1000
1010 0010
1011 1010

02.B8: 0000 0010
1011 1000
1011 1010

03.41: 0000 0011
0100 0001
0100 0010

01.11: 0000 0001
0001 0001
0001 0000
1011 1010
1010 1010

01F1: 0000 0001
1111 0001
1111 0000
0100 0010
1011 0010
1010 1010
0001 1000

02.1E: 0000 0010
0001 1110
0001 1100

03.27: 0000 0011
0010 0111
0010 0100

01.98: 0000 0001
1001 1000
1001 1001
0001 1100
1000 1101

01.E5: 0000 0001
1110 0101
1110 0100
0010 0100
1100 0000
1000 0101
0100 0101

01.D4: 0000 0001
1101 0100
1101 0101

02.41: 0000 0010
0100 0001
0100 0011

03.5D: 0000 0011
0101 1101
0101 1110
1101 0101
1000 1011

01.30: 0000 0001
0011 0000
0011 0001
0100 0011
0111 0010
1000 1011
1111 1001

01.E0: 0000 0001
1110 0000
1110 0001

02.B4: 0000 0010
1011 0100
1011 0110

03.41: 0000 0011
0100 0001
0100 0010
1110 0001
1010 0011

01.AE: 0000 0001
1010 1110
1010 1111
1011 0110
0001 1001
1010 0011
1011 1010

01.B8: 0000 0001
1011 1000
1011 1001

02.41: 0000 0010
0100 0001
0100 0011

03.11: 0000 0011
0001 0001
0001 0010
1011 1001
1010 1011

01.F1: 0000 0001
1111 0001
1111 0000
0100 0011
1011 0011
1010 1011
0001 1000

01.1E: 0000 0001
0001 1110
0001 1111

02.27: 0000 0010
0010 0111
0010 0101

03.98: 0000 0011
1001 1000
1001 1011
0001 1111
1000 0100

01.E5: 0000 0001
1110 0101
1110 0100
0010 0101
1100 0001
1000 0100
0100 0101

01.D4: 0000 0001
1101 0100
1101 0101

02.5D: 0000 0010
0101 1101
0101 1111
1101 0101
1000 1010

01.E0: 0000 0001
1110 0000
1110 0001

02.41: 0000 0010
0100 0001
0100 0011
1110 0001
1010 0010

01.B8: 0000 0001
1011 1000
1011 1001

02.11: 0000 0010
0001 0001
0001 0011
1011 1001
1010 1010

01.41: 0000 0001
0100 0001
0100 0000

03.30: 0000 0011
0011 0000
0011 0011
0100 0000
0111 0011
1000 1010
1111 1001

01.B4: 0000 0001
1011 0100
1011 0101

03.AE: 0000 0011
1010 1110
1010 1101
1011 0101
0001 1000
1010 0010
1011 1010

01.41: 0000 0001
0100 0001
0100 0000

03.F1: 0000 0011
1111 0001
1111 0010
0100 0000
1011 0010
1010 1010
0001 1000

01.1F: 0100 0001
0001 1110
0001 1111

0298: 0000 0010
1001 1000
1001 1010
0001 1111
1000 0101

03.D4: 0000 0011
1101 0100
1101 0111

01.5D: 0000 0001
0101 1101
0101 1100
1101 0111
1000 1011

03.E0: 0000 0011
1110 0000
1110 0011

01.41: 0000 0001
0100 0001
0100 0000
1110 0011
1010 0011

01.27: 0000 0001
0010 0111
0010 0110

03.E5: 0000 0011
1110 0101
1110 0110
0010 0110
1100 0000
1000 0101
0100 0101

01.41: 0000 0001
0100 0001
0100 0000

02.30: 0000 0010
0011 0000
0011 0010
0100 0000
0111 0010
1000 1011
1111 1001

01.B4: 0000 0001
1011 0100
1011 0101

02.AE: 0000 0010
1010 1110
1010 1100
1011 0101
0001 1001
1010 0011
1011 1010

03.B8: 0000 0011
1011 1000
1011 1011

01.11: 0000 0001
0001 0001
0001 0000
1011 1011
1010 1011

03.1E: 0000 0011
0001 1110
0001 1101

01.98: 0000 0001
1001 1000
1001 1001
0001 1101
1000 0100

01.41 0000 0001
0100 0001
0100 0000

02.F1: 0000 0010
1111 0001
1111 0011
0100 0000
1011 0011
1010 1011
0001 1000

01.27: 0000 0001
0010 0111
0010 0110

02.E5: 0000 0010
1110 0101
1110 0111
0010 0110
1100 0001
1000 0100
0100 0101

4) XOR with round key

1111	1001	1011	1010	0001	1000	0100	0101
1010	0000	1111	1010	1111	1110	0001	0111
0101	1001	0100	0000	1110	0110	0101	0010
5	9	4	0	E	6	5	2

1111	1001	1011	1010	0001	1000	0100	0101
1000	1000	0101	1000	0010	1100	1011	0001
0111	0001	1110	0010	0011	0100	1111	0100
7	1	E	2	3	4	F	4

1111	1001	1011	1010	0001	1000	0100	0101
0010	0011	1010	1111	0011	1001	0011	1001
1101	1010	0001	0101	0010	0001	0111	1100
D	A	1	5	2	1	7	C

1111	1001	1011	1010	0001	1000	0100	0101
0010	1010	0110	0000	0111	0110	0000	0101
1101	0011	1101	1010	0110	1110	0100	0000
D	3	D	A	6	E	4	0

$$\begin{bmatrix} 59 & 71 & DA & D3 \\ 40 & E2 & 15 & DA \\ E6 & 34 & 21 & 6E \\ 52 & F4 & 7C & 40 \end{bmatrix}$$

8] a=0 b=26 m=35 3P=P+2P

2P: x_p:10 x_y:9 $s = 3(10)^2 + 0 \% 35 = 20$

$s = 2(9) = 18$

		Q					
35	18	1	17	0	1	-1	$s = 220 \% 35 = \boxed{5}$
18	17	1	1	1	-1	2	$x_r = 5^2 - 2(10) \% 35 = 5$
17	1	17	0	-1	2		$y_y = 5(10-5) - 9 = \boxed{16}$

3P=P+2P

x_p:10 y_p:9 $x_q = 5$ $y_q = 16$

$s = \frac{9-16}{10-5} = \frac{-7}{5}$ $-5 + 35 = 30$

		Q	R			
35	30	1	5	0	1	-1
30	5	6	0	1	-1	

gcd(7,1) can't factor by 35 nor its factor 3 & 7 so can't do point addition & doubling

$x_1 = \alpha^{a} \bmod p$

9] $x_2 = \alpha^{b} \bmod p$

$\gcd(b, p-1) = 1$

b & p-1 coprime

$b \cdot b^{-1} \equiv 1 \bmod (p-1)$

↳ can be deduced by extended euclidean algorithm

Eliminate power b multiply power b^{-1}

$(x_2)^{b \cdot 1} = \alpha \bmod p$

can reach α as p & x_2 are known

we reach b^{-1} by euclidean