Assignment 1

PAGE
DATE

(1) a) $(11^{-1}) \bmod 17$ $\quad T_3 = T_1 - Q \cdot T_2$

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)	17

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

b) $1056^{-1} \bmod 3$

→ Their is no inverse here because 1056, 3 are not coprime, which means their gcd are not equel to 0

(2) a) $3^{301} \bmod 5$

301	7
43	43
1	

$\Rightarrow 301 = 7 \times 43 \quad 3^{301} = 3^{43^7} \Rightarrow (3^{20} * 3^{20} * 3^3)^7$

$3^{20} \bmod 5 = 1$

$3^3 \bmod 5 = 2$

$\Rightarrow 1 * 1 \times 2 \bmod 5 = 2$

$2^7 \bmod 5 = \boxed{3}$

PAGE
DATE

(b) $7^{105} \bmod 143$

105	5
21	3
7	7
1	

$\Rightarrow 7^{105} = 7^{5^{3^7}} \Rightarrow$

$7^5 \bmod 143 = 76$

$76^3 \bmod 143 = 109$

$109^7 \bmod 143$

$= 109^7 = (109^4 \% 143) * (109^2 \% 143) * (109^1 \% 143)$

$= 109^2 \bmod 143 = 12$

$= 109^4 = (109^2)^2 = 12^2 = 144 \bmod 143 = 1$

$= 109 \bmod 143 = 109$

$= 1 * 12 * 109 = 1308 \bmod 143 = \boxed{21}$

(3) gcd (30030, 257)

A	B	Q	R
30030	257	116	218
257	218	1	39
218	39	5	23
39	23	1	16
23	16	1	7
16	7	2	2
7	2	3	1
2	(1)	2	0

gcd is the last B which is (1)

PAGE
DATE

④ $12X = 28 \pmod{233}$

$T_3 = T_1 - Q \cdot T_2$

$x = 28 * 12^{-1} \bmod 233$

A	B	Q	R	T1	T2	T3
233	12	19	5	0	1	-19
12	5	2	2	1	-19	39
5	2	2	1	-19	39	-97
2	1	2	0	39	-97	233

(-97 ← inverse)

$-97 \bmod 233 = 136$

$X = 28 * 136 \bmod 233$

$X = 3808 \bmod 233$

$X = 80$

⑤

Chinese Remainder Theorem

$X \equiv a_1 \bmod m_1$

$X \equiv a_2 \bmod m_2$

$\vdots$

$X \equiv a_n \bmod m_n$

$X \equiv (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_n M_n M_n^{-1}) \bmod M$

Given	Given	To Find	To Find
a_n	m_n	$M_n = M/m_n$	$M_n^{-1} = M_n * M_n^{-1} = 1 \bmod m_n$

PAGE
DATE

(5) $x \equiv 1 \bmod 3$

$x \equiv 2 \bmod 4$

$x \equiv 3 \bmod 5$

G	G	To Find	To Find	To Find
$a_1 = 1$	$m_1 = 3$	$M_1 = 60/3 = 20$	$M_1^{-1} = 20 * 20^{-1} = 1 \% 3 = 2$	60
$a_2 = 2$	$m_2 = 4$	$M_2 = 60/4 = 15$	$M_2^{-1} = 15 * 15^{-1} = 1 \% 4 = 3$	60
$a_3 = 3$	$m_3 = 5$	$M_3 = 60/5 = 12$	$M_3^{-1} = 12 * 12^{-1} = 1 \% 4 = 3$	60

$x = (1 * 20 * 2 + 2 * 15 * 3 + 3 * 12 * 3) \bmod 60$

$x = 238 \bmod 60$

$\boxed{x = 58}$

(6) $(x^5)^{-1} \bmod (x^8 + x^4 + x^3 + x + 1)$ $\quad T_3 = T_1 - Q \cdot T_2$

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	$x^6+x^4+x^3+x$
x^3+x^2+1	1	x^3	0	x^4+x^3+1	$x^5+x^4+x^3+x$	*

x^3

$x^5 \overline{)\, x^8+x^4+x^3+x+1}$ $\quad x^8/x^5 = x^3$

$-(x^8$

$0+x^4+x^3+x+1$

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

x

$x^3+x^2+1 \overline{)\, x^4+x^3+x+1}$ $\quad x^4/x^3 = x$

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

$0+0+0+1$

$x^5/x^4 = x^1$ $\quad x^4/x^4 = 1$

$x+1$

$x^4+x^3+x+1 \overline{)\, x^5}$

$-(x^5+x^4+x^2+x)$

$0+x^4+x^2+x$

$-\ x^4+x^3+x+1$

$0+x^3+x^2+1$

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

$x^3 - x^5 + x^4 + x \bmod$

M. Inv. $\Rightarrow x^5+x^4+x^3+x$

P.T = 32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 b7 34

Key = 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c

(7) AES

=> First Round key: 09 cf 4f 3d

① Rotate => cf 4f 3d 09

② byte sub => 8A 84 EB 01

③ Add Rcon => 8A 84 EB 01 ⊕ 01 000000 => 8B 84 EB 01

④ XOR with key all :-

2B 7E 15 16	28 AE D2 A6	AB F7 15 88	09 cf 4f 3c
⊕ 8B 84 EB 01	= A0 FA FE 17	= 88 58 2C B1	= 23 AF 39 39
A0 FA FE 17	88 58 2C B1	23 AF 39 39	2A 60 76 05

⇓ first round key

=> First Round :

① XOR P.T with original key

$$\begin{pmatrix} 32 & 88 & 31 & e0 \\ 43 & 3A & 31 & 37 \\ f6 & 30 & 98 & B7 \\ A8 & 8D & A2 & 34 \end{pmatrix} \oplus \begin{pmatrix} 2B & 28 & AB & 09 \\ 7E & AE & F7 & CF \\ 15 & D2 & 15 & 4F \\ 16 & A6 & 88 & 3C \end{pmatrix} = \begin{pmatrix} 19 & A0 & 9A & E9 \\ 3D & F8 & C6 & F8 \\ E3 & E2 & 8D & 48 \\ BE & 2B & 2A & 08 \end{pmatrix}$$

② substitute:

$$\begin{pmatrix} D4 & E0 & B8 & 1E \\ 27 & 41 & B4 & 41 \\ 11 & 98 & 5D & 41 \\ AE & F1 & E5 & 30 \end{pmatrix}$$

③ shift Rows

$$\begin{pmatrix} D4 & E0 & B8 & 1E \\ 41 & B4 & 41 & 27 \\ 5D & 41 & 11 & 98 \\ 30 & AE & F1 & E5 \end{pmatrix}$$

④ Mix columns

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

④

$$\begin{pmatrix} 1D & F3 & 48 & 28 \\ 81 & FE & F8 & 06 \\ 7F & 3F & D3 & 26 \\ 1b & 89 & 7A & 4C \end{pmatrix}$$

⑤ Add round key

$$\begin{pmatrix} A0 & 88 & 23 & 2A \\ FA & 58 & AF & 60 \\ FE & 2C & 39 & 76 \\ 17 & B1 & 39 & 05 \end{pmatrix} = \begin{pmatrix} BD & 7B & 6B & 02 \\ 7B & A6 & 57 & 66 \\ 81 & 13 & EA & 50 \\ 0C & 38 & 43 & 49 \end{pmatrix}$$

(8)

PAGE
DATE

$n = 35$

$y^2 = x^3 + 26 \quad a = 0 \quad b = 26$

$P(10, 9)$

$S = \frac{3(10^2) + 0 \% 35}{2(9) \bmod 35} = 20 \cdot 18^{-1} \bmod 35$

A	B	Q	R	T_1	T_2	T_3
35	18	1	17	0	1	-1
18	17	1	1	1	-1	2
17	1	17	0	-1	(2)	-35

$S = 20 - 2 \bmod 35 = 5$

$x_r = 5^2 - 2(10) = 5$

$y_r = 5(10 - 5) - 9) = 16$

$2P = (5, 16)$

$2P + P = (10, 9) + (5, 16)$

$x_Q = 10 \quad y_Q = 9$

$x_P = 5 \quad y_P = 16$

$S = \frac{16 - 9 \% 35}{5 - 10 \% 35} = \frac{7 \% 35}{-5 \% 35} = \frac{7}{30} = 7 \cdot 30^{-1} \bmod 35$

A	B	Q	R	T_1	T_2	T_3
35	30	1	5	0	1	0
30	5	6	0	1	(0)	1

⇒ Their is no multiplicative inverse, as $-5^{-1} \% 35$ doesn't have inverse as $\gcd(35, 5) \neq 1$

So we cannot factor $n = 35$ with P

PAGE
DATE

(9) $X_2 \equiv a^b \bmod P$

Known $\Rightarrow (P, X_2, b)$

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

their is A M.inv b mod $(P-1)$

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

also $X_2 \equiv a^b \bmod P$, the power don't exceed $P-1$

$(X_2)^{b \cdot 1} \equiv (a^b)^{b-1} \bmod P$

$(X_2)^{b-1} \equiv a^{b \cdot b^{-1} \bmod (P-1)} \bmod p$

$X_2^{b-1} \equiv a \bmod p$

$a \equiv X_2^{b-1} \bmod P$