Archit Agrawal (2020512 13)

CS304: INTRODUCTION TO CRYPTOGRAPHY AND NETWORK SECURITY

Theory Assignment II

Problem 1:

- The DES S-box S_4 is:

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

(a) Given mapping to form row 2 from row 1 is,

$$(y_1, y_2, y_3, y_4) \longrightarrow (y_2, y_1, y_4, y_0) \oplus (0,1,1,0)$$

where y_1, y_2, y_3 and y_4 are bits of entry in row 1.

row 1 entry

$\therefore$ $7 = (0,1,1,1) \longrightarrow (1,0,1,1) \oplus (0,1,1,0) = (1,1,0,1) = 13$

$\therefore$ performing the given transformation on first element of row 1 yields first element of row 2. Similarly, we can prove this for all other elements of row 1.

$13 = (1,1,0,1) \longrightarrow (1,1,1,0) \oplus (0,1,1,0) = (1,0,0,0) = 8$

$14 = (1,1,1,0) \longrightarrow (1,1,0,1) \oplus (0,1,1,0) = (1,0,1,1) = 11$

$3 = (0,0,1,1) \longrightarrow (0,0,1,1) \oplus (0,1,1,0) = (0,1,0,1) = 5$

$0 = (0,0,0,0) \longrightarrow (0,0,0,0) \oplus (0,1,1,0) = (0,1,1,0) = 6$

$6 = (0,1,1,0) \longrightarrow (1,0,0,1) \oplus (0,1,1,0) = (1,1,1,1) = 15$

$9 = (1,0,0,1) \longrightarrow (0,1,1,0) \oplus (0,1,1,0) = (0,0,0,0) = 0$

$10 = (1,0,1,0) \longrightarrow (0,1,0,1) \oplus (0,1,1,0) = (0,0,1,1) = 3$

$1 = (0,0,0,1) \longrightarrow (0,0,1,0) \oplus (0,1,1,0) = (0,1,0,0) = 4$

$2 = (0,0,1,0) \longrightarrow (0,0,0,1) \oplus (0,1,1,0) = (0,1,1,1) = 7$

Archit Agrawal
2020512213

$8 = (1,0,0,0) \rightarrow (0,1,0,0) \oplus (0,1,1,0) = (0,0,1,0) = 2$

$5 = (0,1,0,1) \rightarrow (1,0,1,0) \oplus (0,1,1,0) = (1,1,0,0) = 12$

$11 = (1,0,1,1) \rightarrow (0,1,1,1) \oplus (0,1,1,0) = (0,0,0,1) = 1$

$12 = (1,1,0,0) \rightarrow (1,1,0,0) \oplus (0,1,1,0) = (1,0,1,0) = 10$

$4 = (0,1,0,0) \rightarrow (1,0,0,0) \oplus (0,1,1,0) = (1,1,1,0) = 14$

$15 = (1,1,1,1) \rightarrow (1,1,1,1) \oplus (0,1,1,0) = (1,0,0,1) = 9$

Hence, second row of S_4 can be obtained from first row using the given transformation.

(b) Let us try to find a ~~relation~~ transformation that maps Row 2 to Row 3.

$$(y_1, y_2, y_3, y_4) \rightarrow (t_1, t_2, t_3, t_4) \oplus (0,1,1,0) \rightarrow (x_1, x_2, x_3, x_4)$$

(Row 2) Row 3

Here, t_1, t_2, t_3 and t_4 are Boolean functions on (y_1, y_2, y_3, y_4)

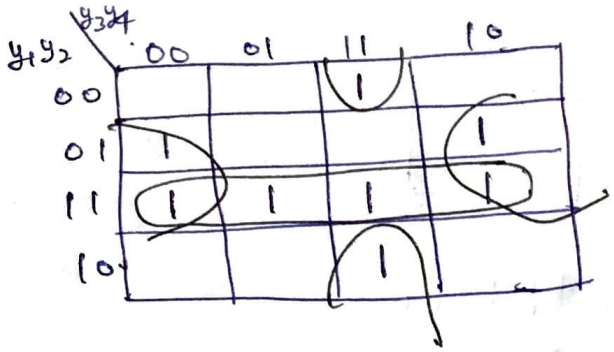
Let's construct the table of mapping of Row 2 to Row 3, i.e. (y_1, y_2, y_3, y_4) to (x_1, x_2, x_3, x_4)

y_1	y_2	y_3	y_4	x_1	x_2	x_3	x_4
0	0	0	0	0	1	1	1
0	0	0	1	0	1	0	1
0	0	1	0	0	0	1	1
0	0	1	1	1	1	0	1
0	1	0	0	1	1	1	1
0	1	0	1	0	0	0	0
0	1	1	0	1	1	0	0
0	1	1	1	0	0	0	1
1	0	0	0	0	1	1	0
1	0	0	1	0	1	0	0
1	0	1	0	0	0	1	0
1	0	1	1	1	0	0	1
1	1	0	0	1	1	1	0
1	1	0	1	1	0	1	0
1	1	1	0	1	0	0	0
1	1	1	1	1	0	1	1

Archit Agrawal
2020512B

Now, using K-map we can find x_1, x_2, x_3 and x_4 as a function of (y_1, y_2, y_3, y_4).

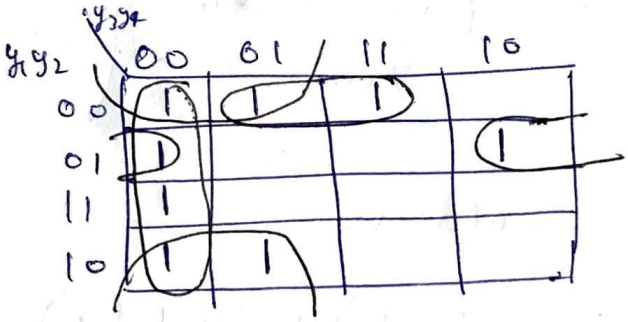
Solving for x_1:



$$x_1 = y_1 y_2 + y_2 \overline{y_4} + \overline{y_2} y_3 y_4$$

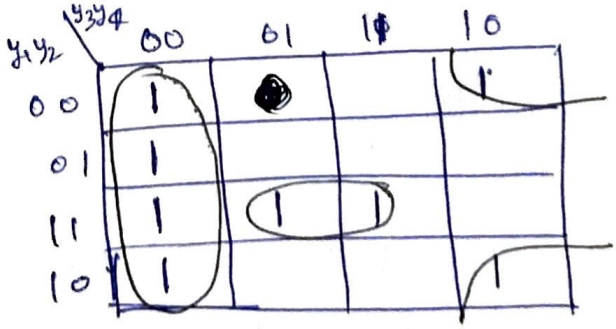
(+ is bitwise OR
. is bitwise AND)

Solving for x_2:



$$x_2 = \overline{y_3}\,\overline{y_4} + \overline{y_2}\,\overline{y_3} + \overline{y_1}\,\overline{y_2}\,y_4 + \overline{y_1}\,y_2\,\overline{y_4}$$

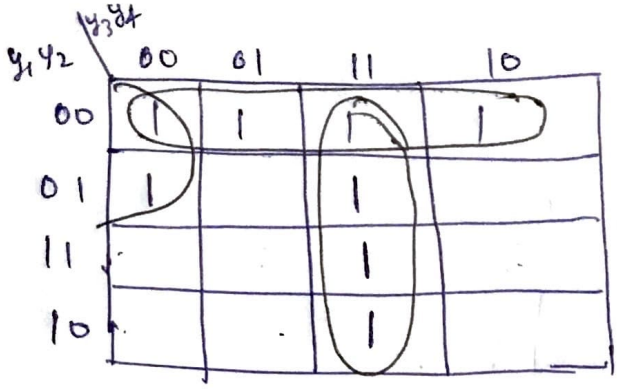
Solving for x_3:



$$x_3 = \overline{y_3}\,\overline{y_4} + y_1 y_2 y_4 + \overline{y_2}\,y_3\,\overline{y_4}$$

Archit Agrawal
2020512 13

Solving for x_4:



$$x_4 = y_3y_4 + \bar{y}_1\bar{y}_2 + \bar{y}_1\bar{y}_3\bar{y}_4$$

Therefore, we have the transformations which maps row 2 to row 3.

$(y_1, y_2, y_3, y_4) \longrightarrow (x_1, x_2, x_3, x_4)$

Row 2 Row 3

(x_i are solved using k-map)

∵ Initially the transformation was:

$$(y_1, y_2, y_3, y_4) \longrightarrow (t_1, t_2, t_3, t_4) \oplus (0, 1, 1, 0) \rightarrow (x_1, x_2, x_3, x_4)$$

$\therefore$ $t_1 \oplus 0 = x_1 \Rightarrow t_1 = x_1$

$t_2 \oplus 1 = x_2 \Rightarrow t_2 = \bar{x}_2$

$t_3 \oplus 1 = x_3 \Rightarrow t_3 = \bar{x}_3$

$t_4 \oplus 0 = x_4 \Rightarrow t_4 = x_4$

$\therefore$ Row 2 can be transformed to row 3 using a similar kind of transformation. Similarly, we can prove that any row can be transformed to any other row.

Archit Agrawal
2020512B

Problem 2 :

Consider the plaintext P divided into n blocks of fixed length. Therefore,

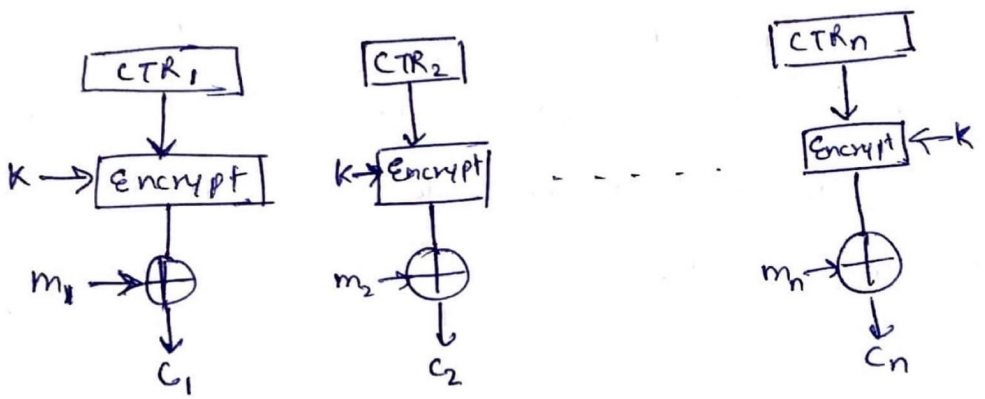
$$P = m_1 || m_2 || m_3 || \cdots || m_n$$

The encryption in Counter (CTR) mode is done as:

$$C_i = Enc(CTR_i, K) \oplus m_i$$

length of CTR_i = length of m_i

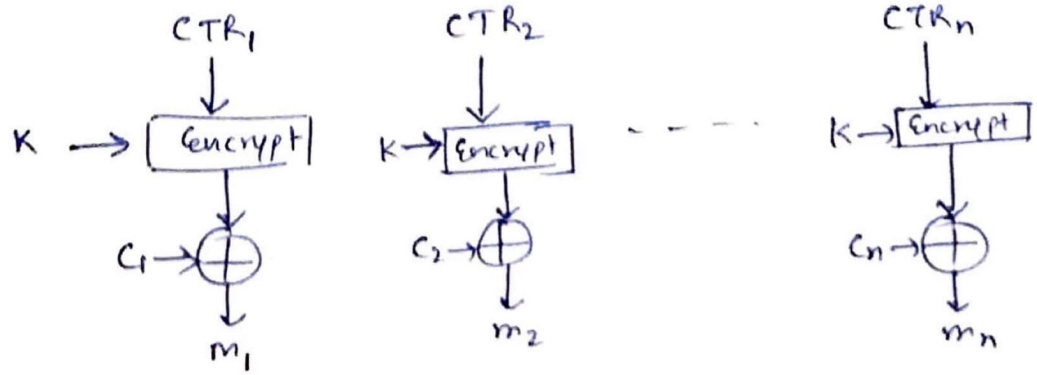
where Enc is a block cipher such as AES and CTR_i is counter used for i^{th} block. The encryption process can be depicted as a flowchart given below. Note $CTR_i \neq CTR_j$



The final ciphertext is $C_1 || C_2 || \cdots || C_n$.

The decryption in Counter mode is done as exactly similar to encryption, but the encrypted counter is xored with ciphertext to get the plaintext.

$$m_i = Enc(CTR_i, K) \oplus C_i$$



Archit Agrawal (2020512 13)

As can be seen in the flowchart that both the encryption and decryption of each block is independent of every other block. It is neither chained as in CBC nor there is any other dependencies between the blocks being processed. Hence, encryption in CTR mode can be parallelized efficiently by processing each block in parallel in different threads (cores) and then ordering the processed blocks in the same order as were there before processing.

Moreover, the keystream, that is, encrypted counter block can be precomputed in advance and stored in memory. This makes the encryption and decryption efficient because there is no need to recompute the keystream for each block.

Problem 3

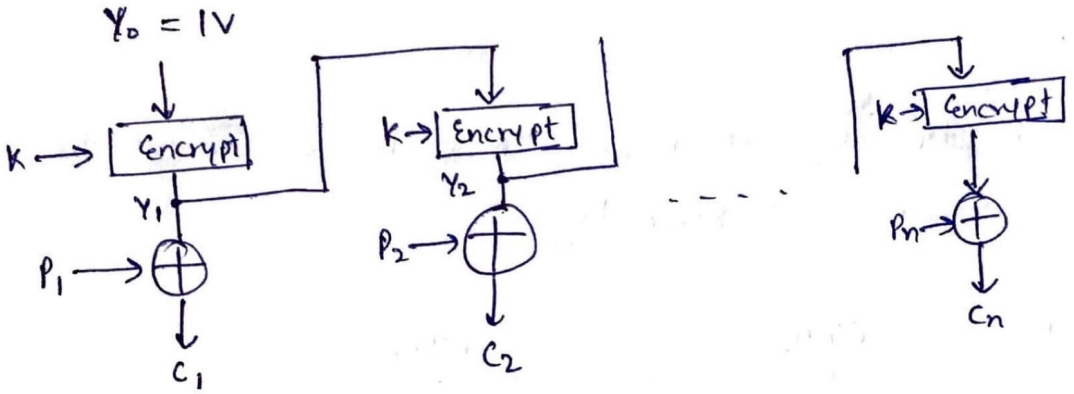
Archit Agrawal
2020512B

The encryption in Output Feedback Mode is done as:

$$Y_0 = IV \text{ and } Y_i = Enc(K, Y_{i-1}) \; \forall \; i \neq 0$$

$$C_i = Y_i \oplus P_i$$

where $P = P_1 || P_2 || \cdots || P_n$ is plaintext, IV is a public parameter and $C = C_1 || C_2 || \cdots || C_n$ is corresponding ciphertext. Encryption in OFB mode can be represented as below. Enc is a block cipher.



Now, we have $X = (x_1, x_2 \cdots, x_n)$ and $X' = (x_1', x_2' \cdots x_n')$ two sequences of n plaintext blocks. These are encrypted in OFB mode using same key and IV. Let's say the corresponding ciphertext are $C = (C_1, C_2 \cdots C_n)$ and $C' = (C_1', C_2' \cdots, C_n')$. Since, Key and IV are same for encrypting both the messages, hence,

$$Y_1 = Enc(K, Y_0 = IV)$$

$\therefore$ Y_1 will be same in both the cases. Similarly,

$$Y_2 = Enc(K, Y_1)$$

$\because$ Y_1 is same and K is same, Y_2 will be same. Similarly, Y_i will be same in both the cases for $0 \leq i \leq n$.

Archit Agrawal
2020051213

$\therefore C = (x_1 \oplus y_1) \,||\, (x_2 \oplus y_2) \,||\, \cdots \,||\, (x_n \oplus Y_n)$

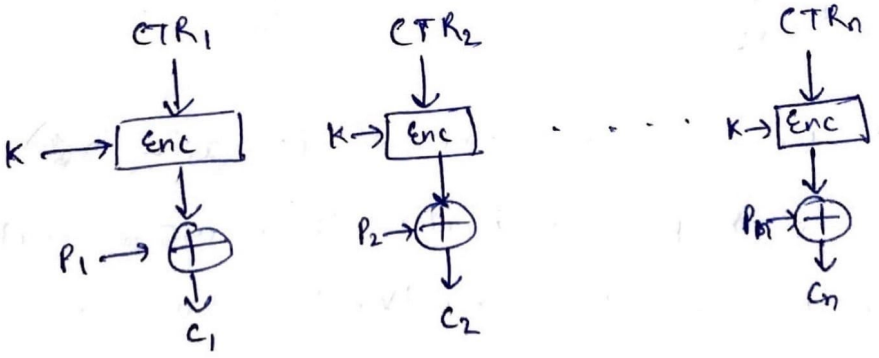
and $C' = (x_1' \oplus Y_1) \,||\, (x_2' \oplus Y_2) \,||\, \cdots \,||\, (x_n' \oplus Y_n)$

$\therefore C \oplus C' = (x_1 \oplus y_1 \oplus x_1' \oplus Y_1) \,||\, (x_2 \oplus Y_2 \oplus x_2' \oplus Y_2) \,||\, \cdots \,||\, (x_n \oplus Y_n \oplus x_n' \oplus Y_n)$

$\Rightarrow C \oplus C' = (x_1 \oplus x_1') \,||\, (x_2 \oplus x_2') \,||\, \cdots \,||\, (x_n \oplus x_n') = X \oplus X'$

Therefore, it is easy to compute $X \oplus X'$, given C and C' if X and X' are encrypted using OFB mode with same key and IV.

Similarly, if ctr is reused in CTR mode to encrypt two different messages and same key.



$Y_i = \text{Enc}(K, CTR_i)$

$C_i = P_i \oplus Y_i$

If same key and CTR_i are used then Y_i will be same.

$\therefore C_{CTR} = (x_1 \oplus Y_1) \,||\, (x_2 \oplus Y_2) \,||\, \cdots \,||\, (x_n \oplus Y_n)$

$C'_{CTR} = (x_1' \oplus Y_1) \,||\, (x_2' \oplus Y_2) \,||\, \cdots \,||\, (x_n' \oplus Y_n)$

$\therefore C_{CTR} \oplus C'_{CTR} = (x_1 \oplus x_1') \,||\, (x_2 \oplus x_2') \,||\, \cdots \,||\, (x_n \oplus x_n')$

$\Rightarrow X \oplus X' = C_{CTR} \oplus C'_{CTR}$

Hence, shown.

Archit Agrawal
2020512 13

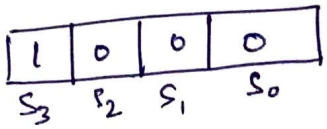
Problem 4

a) Connection Polynomial: x^4+x+1

∴ the linear feedback function is:

$$L(S) = S_0 \oplus S_3$$

∴ the LFSR is (consider right shifting),



$L(S) = S_0 \oplus S_3$

The initial state can be any non-zero state.

To find the period of LFSR, we need to check if $f(x)=(x^4+x+1)$ is primitive. If $f(x)$ is primitive, then period of LFSR is 2^4-1. we will check if all the polynomials of degree less than by the generator x under modulo $f(x)$.

$x^0 = 1$

$x^1 = x$

$x^2 = x^2$

$x^3 = x^3$

$x^4 = (x+1)$

$x^5 = x^2+x$

$x^6 = x^3+x^2$

$x^7 = x^3+x+1$

$x^8 = x^4+x^2+x = x+1+x^2+x = x^2+1$

$x^9 = x^3+x$

$x^{10} = x^2+x+1$

$x^{11} = x^3+x^2+x$

$x^{12} = x^3+x^2+x+1$

$x^{13} = x+1+x^3+x^2+x = x^3+x^2+1$

$x^{14} = x+1+x^3+x = x^3+1$

$x^{15} = x+1+x = 1$

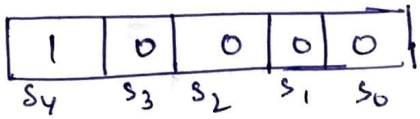
As we can see all the polynomials of degree less than 4 are generated (except polynomial 0). Therefore, $f(x)$ is primitive and period of LFSR is $2^4-1 = 15$.

Arclit Agrawal
2020511213

(b) Connection Polynomial, $f(x) = x^5 + 1$

∵ degree of $f(x)$ is 5, therefore, LFSR is a 5-bit LFSR.

Also, the linear feedback function is $L(S) = S_0$



$$L(S) = S_0$$

Since, the connection polynomial is $f(x) = x^5 + 1$ which is reducible.

$$(x^5+1) = (x+1)(x^4+x^3+x^2+x+1)$$

Therefore, period of LFSR with connection polynomial $f(x)$ is LCM of period of LFSR with connection polynomial $(x+1)$ and period of LFSR with connection polynomial $(x^4+x^3+x^2+x+1)$.

Period of LFSR with connection polynomial $(x+1)$

Clearly, $(x+1)$ is primitive, therefore, period $= 2^1 - 1 = 1$

Period of LFSR with connection polynomial $(x^4+x^3+x^2+x+1)$

We will try to find $\langle x \rangle$ under modulo $(x^4+x^3+x^2+x+1)$ then the size of set, $\phi = |\langle x \rangle|$ = period of LFSR.

$x^0 = 1$
$x^1 = x$
$x^2 = x^2$
$x^3 = x^3$
$x^4 = x^3 + x^2 + x + 1$
$x^5 = x^3 + x^2 + x + 1 + x^3 + x^2 + x = 1$

∴ period of LFSR with connection polynomial $(x^4+x^3+x^2+x+1)$ is 5.

∴ period of LFSR with connection polynomial $f(x) = x^5 + 1$, is

$LCM(1,5) = 5$.

Problem 5

Ardhit Agrawal
20205213

Given, $\lambda : \mathbb{Z}_{105} \longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$,

$$\lambda(x) = (x \bmod 3,\ x \bmod 5,\ x \bmod 7) \quad \text{—— (I)}$$

Let $a_1 \in \mathbb{Z}_3$, $a_2 \in \mathbb{Z}_5$ and $a_3 \in \mathbb{Z}_7$ such that,

$$\lambda(x) = (a_1, a_2, a_3) \quad \text{—— (II)}$$

From (I) and (II), a system of congruences can be constructed,

$$x \equiv a_1 \bmod 3$$
$$x \equiv a_2 \bmod 5$$
$$x \equiv a_3 \bmod 7$$

The inverse of function λ is defined as:

$$\lambda^{-1} : \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \longrightarrow \mathbb{Z}_{105} \text{ such that } \lambda^{-1}(a_1, a_2, a_3) = x$$

We can solve the above system of congruences using Chinese Remainder Theorem, using which we can compute x given a_1, a_2 and a_3 (which will be λ^{-1}). Let's solve the system of congruences.

Clearly $m_1 = 3$, $m_2 = 5$ and $m_3 = 7$ are pairwise co-prime.

Now,

$$M = m_1 \times m_2 \times m_3 = 3 \times 5 \times 7 = 105$$

Let's define $M_i = \frac{M}{m_i}$ where $i \in \{1, 2, 3\}$

$$\therefore M_1 = \frac{105}{3} = 35$$

$$M_2 = \frac{105}{5} = 21$$

$$M_3 = \frac{105}{7} = 15$$

Archit Agrawal
2020511213

Let us define M_i^{-1} where $i \in \{1,2,3\}$ such that $M_i \times M_i^{-1} \equiv 1 \bmod m_i$. M_i^{-1} can be found using Extended Euclidean Algorithm, but here the values are trivial and we can easily ~~solve~~ find M_i^{-1} using trial and error.

The values are:

$$M_1^{-1} = 2, M_2^{-1} = 1, M_3^{-1} = 1$$

Now, according to Chinese Remainder Theorem,

$$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

$$x \equiv (70a_1 + 21a_2 + 15a_3) \bmod 105$$

$\therefore$ $\lambda^{-1} : Z_3 \times Z_5 \times Z_7 \longrightarrow Z_{105}$;

$$\boxed{\lambda^{-1}(a_1, a_2, a_3) \equiv (70a_1 + 21a_2 + 15a_3) \bmod 105}$$

$\therefore$ $$\boxed{\lambda^{-1}(2,2,3) = (140 + 42 + 45) \bmod 105 = 17.}$$

Aarchit Agrawal
2020512 13

(6) The system of congruences given is:

$$x \equiv 12 \mod 25$$
$$x \equiv 9 \mod 26$$
$$x \equiv 23 \mod 27$$

Here, $m_1 = 25$, $m_2 = 26$, and $m_3 = 27$

Also, $a_1 = 12$, $a_2 = 9$ and $a_3 = 23$

First, let's check if m_1, m_2 and m_3 are pairwise coprime or not.

$$m_1 = 25 = 5 \times 5$$
$$m_2 = 26 = 2 \times 13$$
$$m_3 = 27 = 3 \times 3 \times 3$$

Since, m_1, m_2 and m_3 have no same prime factor, therefore, gcd between any two of them is 1. Hence, m_1, m_2 and m_3 are pairwise co-prime. Now,

$$M = m_1 \times m_2 \times m_3$$
$$M = 17550$$

Now, let's compute $M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2}$ and $M_3 = \frac{M}{m_3}$

$$\therefore M_1 = \frac{17550}{25} = 702$$
$$M_2 = \frac{17550}{26} = 675$$
$$M_3 = \frac{17550}{27} = 650$$

Now, we need to compute M_i^{-1} where $i \in \{1, 2, 3\}$ defined as inverse of M_i under modulo m_i. We can do that using Extended Euclidean Algorithm.

Archit Agrawal
2020512 13

Calculating M_1^{-1}

$25 \overline{)\ 702\ (28}$
700
$2 \overline{)\ 25\ (12}$
24
1

Moving in upward direction

$1 = 25 - 1*12$
$1 = 25 - 12(702 - 25*28)$
$1 = 337*25 - 12*702$

$\therefore M_1^{-1} = -12$ or $(-12+25 = 13)$

$\therefore M_1^{-1} = 13$

Calculating M_2^{-1}

$26 \overline{)\ 675\ (25}$
650
$25 \overline{)\ 26\ (1}$
25
1

Moving in upward direction

$1 = 26 - 1*25$
$1 = 26 - (675 - 25*26)$
$1 = 26*26 - 675$

$\therefore M_2^{-1} = -1$ or $(-1+26 = 25)$

$\therefore M_2^{-1} = 25$

Calculating M_3^{-1}

$27 \overline{)\ 650\ (24}$
648
$2 \overline{)\ 27\ (13}$
26
1

Moving in upward direction

$1 = 27 - 2*13$
$1 = 27 - 13*(650 - 24*27)$
$1 = 313*27 - 13*650$

$\therefore M_3^{-1} = -13$ or $(-13+27 = 14)$

$\therefore M_3^{-1} = 14$

Now, x can be calculated as,

$$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

$x = (12 \times 702 \times 13 + 9 \times 675 \times 25 + 23 \times 650 \times 14) \bmod 17550$

$x = (169512 + 151875 + 209300) \bmod 17550$

$x = 470687 \bmod 17550$

$\therefore x = 14387$ Answer

Archit Agrawal
2020571213

Problem 7

Given $n = 18923$, $e = 1261$ and $C = 6127$

Firstly, we need to factorize n into two primes p and q. Clearly, 2 does not divide n, we can start from 3 and keep checking for each prime if it divides n or not. If it divides n, we can say p is that factor and $q = n/p$.

$n \% 3 = 2$
$n \% 5 = 3$
$n \% 7 = 2$
$n \% 11 = 3$
$n \% 13 = 8$
$n \% 17 = 2$
$n \% 19 = 18$
$n \% 23 = 17$
$n \% 29 = 15$
$n \% 31 = 13$

$n \% 37 = 16$
$n \% 41 = 22$
$n \% 43 = 3$
$n \% 47 = 29$
$n \% 53 = 2$
$n \% 59 = 43$
$n \% 61 = 13$
$n \% 67 = 29$
$n \% 71 = 37$
$n \% 73 = 16$

$n \% 79 = 42$
$n \% 83 = 82$
$n \% 89 = 55$
$n \% 97 = 0$
$n \% 101 = 36$
$n \% 103 = 74$
$n \% 107 = 91$
$n \% 109 = 66$
$n \% 113 = 52$
$n \% 127 = 0$

$\because n \% 127 = 0$, $\therefore$ 127 divides 18923

$\therefore n = 18923 = 127 * 149$

Now, we will calculate $\phi(n)$ as,

$$\phi(n) = (p-1)(q-1) = 126 * 148 = 18648$$

Now, since, $e.d \equiv 1 \bmod \phi(n)$, we will find d using Extended Euclidean Algorithm. The division is on the next page.

Archit Agrawal
2020051213

$$
\begin{array}{r|l}
1261 & 18648 \\
 & 17654 \\
\hline
994 & 1261 \\
 & 994 \\
\hline
267 & 994 \\
 & 801 \\
\hline
193 & 267 \\
 & 193 \\
\hline
74 & 193 \\
 & 148 \\
\hline
45 & 74 \\
 & 45 \\
\hline
29 & 45 \\
 & 29 \\
\hline
16 & 29 \\
 & 16 \\
\hline
13 & 16 \\
 & 13 \\
\hline
3 & 13 \\
 & 12 \\
\hline
 & 1
\end{array}
\qquad
\begin{array}{l}
\\
1 \\
\\
1 \\
\\
2 \\
\\
1 \\
\\
1 \\
\\
1 \\
\\
4
\end{array}
$$

Now, moving in reverse direction,

$$1 = 13 - 4*3$$
$$1 = 13 - 4*(16-13)$$
$$1 = 5*13 - 4*16$$
$$1 = 5*(29-16) - 4*16$$
$$1 = 5*29 - 9*16$$
$$1 = 5*29 - 9*(45-29)$$
$$1 = 14*29 - 9*45$$
$$1 = 14*(74-45) - 9*45$$
$$1 = 14*74 - 23*45$$
$$1 = 14*74 - 23*(193-2*74)$$
$$1 = 60*74 - 23*193$$
$$1 = 60*(267-193) - 23*193$$
$$1 = 60*267 - 83*193$$

Archit Agrawal
20205213

$$1 = 60 * 267 - 83 * (994 - 3 * 267)$$

$$1 = 309 * 267 - 83 * 994$$

$$1 = 309 * (1261 - 994) - 83 * 994$$

$$1 = 309 * 1261 - 392 * 994$$

$$1 = 309 * 1261 - 392 * (18648 - 14 * 1261)$$

$$1 = 5797 * 1261 - 392 * 18648$$

$\therefore$ d = Inverse of 1261 under modulo 18648 is 5797.

Now, decryption in RSA is given as,

$$x = c^d \bmod n$$

Using Square and Multiply Algorithm we can compute $c^d \bmod n$ where $c = 6127$ and $d = 5797$ and $n = 18923$.

$c \bmod n = 6127$

$c^2 \bmod n = 15820$

$c^4 \bmod n = 15725$

$c^8 \bmod n = 8784$

$c^{16} \bmod n = 9585$

$c^{32} \bmod n = 1060$

$c^{64} \bmod n = 7143$

$c^{128} \bmod n = 6041$

$c^{256} \bmod n = 10137$

$c^{512} \bmod n = 6879$

$c^{1024} \bmod n = 13141$

$c^{2048} \bmod n = 13506$

$c^{4096} \bmod n = 13239$

Now, $5797 = (1011010100101)_2$

$\therefore x = c^d \bmod n = c^{(4096 + 1024 + 512 + 128 + 32 + 4 + 1)} \bmod n$

$= (13239 * 13141 * 6879 * 6041 * 1060 * 15725 * 6127) \bmod 18923$

$x = 5746$

$\therefore$ the plaintext is $x = 5746$

Problem 8

Archit Agrawal
2020512 13

Given Elliptic curve EL: $y^2 = x^3 + 5x + 3$

We need to find all the points on EL in Z_{13}. A point $(x, y) \in Z_{13}$ iff $1 \leq x, y \leq 12$ and $x, y \in \mathbb{Z}$. A point $(x, y) \in Z_{13}$ will exist on EL iff the left hand side and right hand side are equal under modulo 13, i.e.,

$$y^2 \bmod 13 = (x^3 + 5x + 3) \bmod 13$$

Let us compute these values and store them in tables.

y	$y^2 \bmod 13$
1	1
2	4
3	9
4	3
5	12
6	10
7	10
8	12
9	3
10	9
11	4
12	1

x	$(x^3 + 5x + 3) \bmod 13$
1	9
2	8
3	6
4	9
5	10
6	2
7	4
8	9
9	10
10	0
11	11
12	10

If the second column of both the table is equal then corresponding (x, y) is a point on the curve EL. Therefore, the points on the curve EL are:

$(1,3), (1,10), (4,3), (4,10), (5,6), (5,7), (7,2), (7,11), (8,3), (8,10), (9,6), (9,7), (12,6), (12,7)$

Problem 10

Archit Agrawal
2020511213

Given: $h(x,y) = ax + by \bmod n$

Let us say for inputs (x_1, y_1) and (x_2, y_2) we know the hash value, i.e.

$$h(x_1, y_1) = z_1 \quad \text{(I)}$$
$$h(x_2, y_2) = z_2 \quad \text{(II)}$$

From the definition of hash function,

$$z_1 = h(x_1, y_1) = (ax_1 + by_1) \bmod n$$
$$z_2 = h(x_2, y_2) = (ax_2 + by_2) \bmod n$$

Now, let's compute hash of (kx_1, ky_1),

$$h(kx_1, ky_1) = (akx_1 + bky_1) \bmod n$$
$$h(kx_1, ky_1) = k(ax_1 + by_1) \bmod n$$
$$h(kx_1, ky_1) = (k \cdot z_1) \bmod n$$

Clearly, we can find hash for many inputs of the form (kx_1, ky_1) or (kx_2, ky_2) where $k \in \mathbb{Z}_n$ without actually applying the hash function on these inputs. Also, we can take a linear combination of x_1 and x_2 and same linear combination of y_1 and y_2. for example,

$$h(rx_1 + sx_2, ry_1 + sy_2) = (a(rx_1 + sx_2) + b(ry_1 + sy_2)) \bmod n$$
$$h(rx_1 + sx_2, ry_1 + sy_2) = (r(ax_1 + by_1) + s(ax_2 + by_2)) \bmod n$$
$$h(rx_1 + sx_2 + ry_1 + sy_2) = (r \cdot z_1 + s \cdot z_2) \bmod n$$

Hence, again we computed hash value of input $(rx_1 + sx_2, ry_1 + sy_2)$ without actually applying the hash function on the input given that we know hash value for the inputs (x_1, y_1) and (x_2, y_2).

Problem 11

Archit Agrawal
20205213

Given, $f_{(a,b)}: \mathbb{Z}_p \to \mathbb{Z}_p$ by the rule $f_{a,b}(x) = (ax+b) \bmod p$

Also,

$$f_{a,b}(x) = y \quad \text{and} \quad f_{a,b}(x') = y'$$

$$(ax+b) \bmod p = y \quad \text{and} \quad (ax'+b) \bmod p = y'$$

The above equations can be re-written as:

$$ax + b \equiv y \bmod p \quad \text{---(I)}$$

$$ax' + b \equiv y' \bmod p \quad \text{---(II)}$$

Substracting (I) from (II),

$$a(x' - x) \equiv (y' - y) \bmod p$$

Now, we know, x, y, x', y', p and 'a' is unknown. 'a' can be found by multiplying both sides by inverse of $(x'-x)$ under modulo p on both sides. Inverse of $(x'-x)$ under modulo p exists iff $\gcd(x'-x, p) = 1$

$\because$ p is prime $\Rightarrow \gcd((x'-x), p) = 1$

$\therefore$ $\boxed{a \equiv (y'-y)(x'-x)^{-1} \bmod p}$

Now, b can be found using (I) (or (II)) as:

$$\boxed{b \equiv (y - ax) \bmod p}$$

$\therefore$ It is possible to find a and b $\in \mathbb{Z}_p$ given x, x', y and y'.