2021511192
Archit Verma

DOMS | Page No. | Date / /

Question - 1

The S-Box 4 is:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	07	13	14	03	00	6	09	10	1	02	08	05	11	12	04	15
1	13	08	11	05	06	15	00	03	04	07	02	12	01	10	14	09
2	10	06	09	00	12	11	07	13	15	01	03	14	05	02	08	04
3	03	15	00	06	10	01	13	08	09	04	05	11	12	07	02	14

a) Here given mapping is :-

~~$(y_1, y_2, y_3, y_4) \rightarrow (y_2, y_1, y_4, y_3) \oplus (0,1,1,0)$~~

Lets map all entries of row one (after converting to binary)

$7 = (0,1,1,1) \rightarrow (1,0,1,1) \oplus (0,1,1,0) = (1,1,0,1) = 13$
$13 = (1,1,0,1) \rightarrow (1,1,0,1) \oplus (0,1,1,0) = (1,0,1,1) = 11$
$3 = (0,0,1,1) \rightarrow (0,0,1,1) \oplus (0,1,1,0) = (0,1,0,1) = 5$
$0 = (0,0,0,0) \rightarrow (0,0,0,0) \oplus (0,1,1,0) = (0,1,1,0) = 6$
$6 = (0,1,1,0) \rightarrow (1,0,0,0) \oplus (0,1,1,0) = (1,1,1,1) = 15$
$9 = (1,0,0,1) \rightarrow (0,1,1,0) \oplus (0,1,1,0) = (0,0,0,0) = 0$
$10 = (1,0,1,0) \rightarrow (0,1,0,1) \oplus (0,1,1,0) = (0,0,1,1) = 3.$
$4 = (0,0,0,1) \rightarrow (0,0,1,0) \oplus (0,1,1,0) = (0,1,0,0) = 4$
$2 = (0,0,1,0) \rightarrow (0,0,0,1) \oplus (0,1,1,0) = (0,1,1,1) = 7$
$8 = (1,0,0,0) \rightarrow (0,1,0,0) \oplus (0,1,1,0) = (0,0,1,0) = 2$
$5 = (0,1,0,1) \rightarrow (1,0,1,0) \oplus (0,1,1,0) = (1,1,0,0) = 12$
$11 = (1,0,1,1) \rightarrow (0,1,1,1) \oplus (0,1,1,0) = (0,0,0,1) = 1$
$12 = (1,1,0,0) \rightarrow (1,1,0,0) \oplus (0,1,1,0) = (1,0,1,0) = 10$
$4 = (0,1,0,0) \rightarrow (1,0,0,0) \oplus (0,1,1,0) = (1,1,1,0) = 14$
$15 = (1,1,1,1) \rightarrow (1,1,1,1) \oplus (0,1,1,0) = (1,0,0,1) = 9$

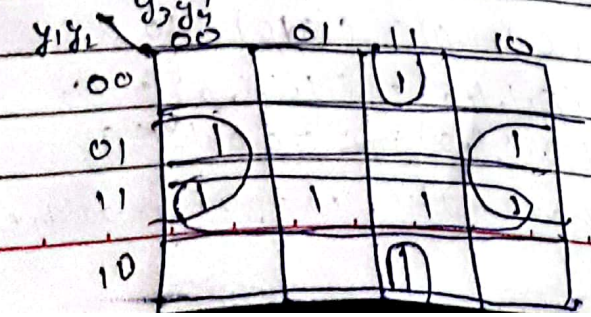
We can clearly see that the output matches with row 2.

2021511312
Mrchit Verma.

We can find the transformation by observing the change of bits. This can be done using the concept of K-map. Performing permutation and then seeing which bit to xor to get result can make it too much computational so we will simply do K-map. First prepare the table for corresponding transformations:-

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

Now for x_1

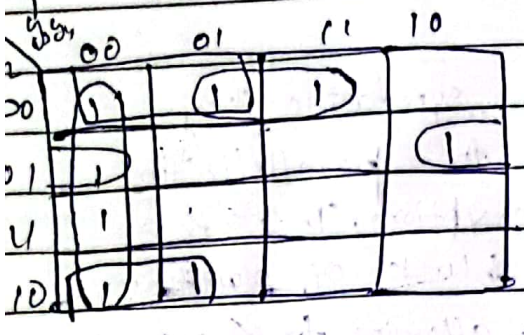


$y_1y_2 + \bar{y}_2\bar{y}_3y_4 + y_2\bar{y}_4$

where + is OR operation.

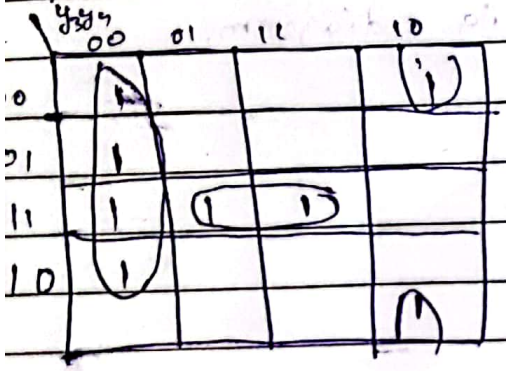
2021511912
Archit verma

for x_2.



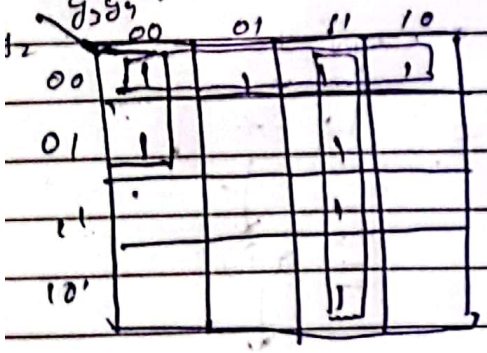
$\bar{y}_3\bar{y}_4 + \bar{y}_1\bar{y}_2y_4 + \bar{y}_1y_2\bar{y}_4 + \bar{y}_2\bar{y}_3$

for x_3 we had



$x_3 = \bar{y}_3\bar{y}_4 + y_1y_2y_4 + \bar{y}_2y_3\bar{y}_4$

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 can have a transition that maps from row2 to row3.

We supposed transition as

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

but	$t_1 \oplus 0 = t_1$	$t_3 \oplus 1 = \bar{t}_3$	$\Rightarrow t_1 = x_1$, $t_2 = \bar{x}_2$, $t_3 = \bar{x}_3$, $t_4 = x_4$
	$t_2 \oplus 1 = \bar{t}_2$	$t_4 \oplus 1 = \bar{t}_4$	

2021511192
Archit Verma

DOMS Page No.
Date / /

Question: 2

The CTR operation for symmetric-key cryptography is well-suited for parallelization both for encryption & decryption. This is because CTR treats each block of plaintext or ciphertext independently, allowing for concurrent processing of multiple blocks simultaneously.

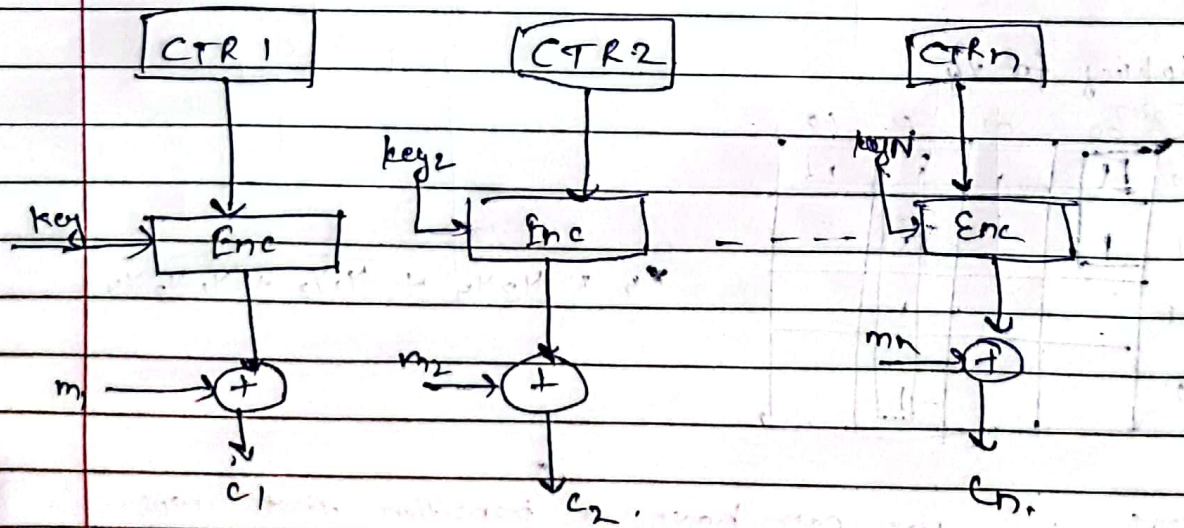
Let us understand thing via diagram.

let $P = m_1 || m_2 - - || m_n$

Now encryption is done as.

$C_i = Enc(Ctr, K) \oplus m_i$.

Below is a flow chart.

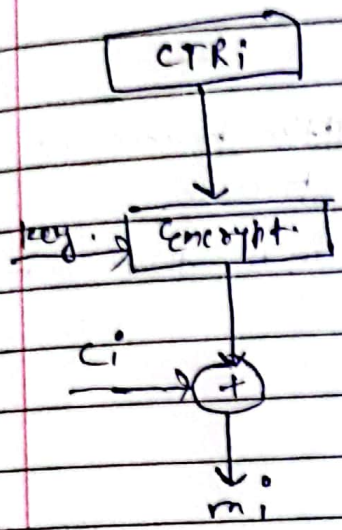


final cipher text = $C_1 || C_2 - - || C_n$.

The decryption also follows same process. The structure of a CTR block for decryption is as

$m_i = dec(CTR, k) \oplus C_i$

2021511132
Archit Verma



note, we will again use encrypt as we are taking XOR so algorithm should follow same step.

so doing for n blocks we had

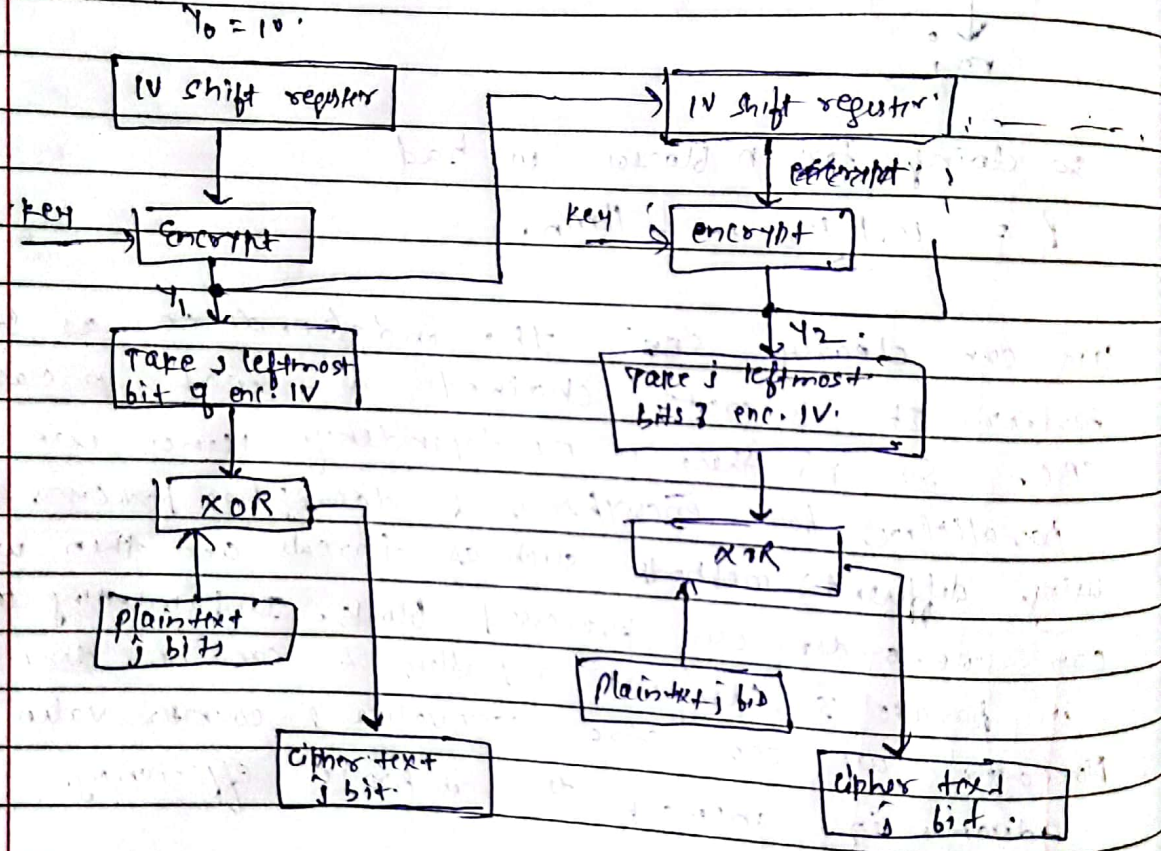
$P = m_1 || m_2 \cdots || m_n$

We can clearly see the independence as stated earlier. It is not chained as was in case of CBC. So no there is no dependency. Hence we can parallelize both encryption & decryption process by using different methods such as threads and then we can re-order our processed block. Implementing counter in parallel is also not a problem & can be done easily. Moreover we can store key value & counter value in advance in memory to improve efficiency.

2021SI1192
Archit Verma

Question 1-3

In OFB, the output of the IV encryption process is fed into the next stage of encryption process.
In this mode data is encrypted in units that are smaller than a defined block size.
OFB works with j bits at a time.



The encryption in output feedback is done as

$Y_0 = IV$

$Y_i = Enc(K, Y_{i-1}) \quad \forall i \neq 0$

Now given

$X = (X_1 \ldots X_n)$

$X' = (X_1' \ldots X_n')$

are two sequence of plaintext block. These are encrypted in plaintext OFB mode using same key

2021SIIS2
Archit Verma

DOMS Page No. Date / /

let
$C = (C_1 \dots C_n)$
$C' = (C_1' \dots C_n')$
be corresponding ciphertext. since key & IV are same
So

Now
$Y_1 = Enc(K, Y_0 = IV)$.
as key and IV are same so Y_1 will also be same for both cases.

$Y_2 = Enc(K, Y_1)$
same goes for Y_2
So we can check this for all $Y_i \; \forall \; 0 \le i \le n$.

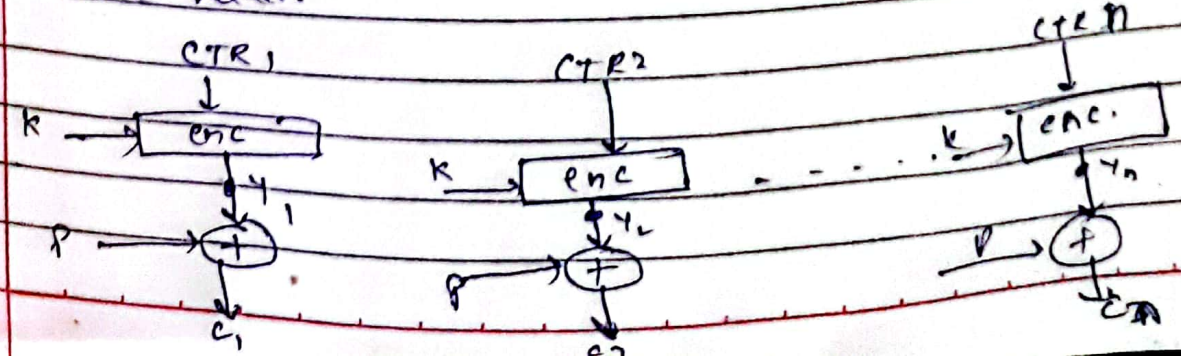
Now,

$C = (X_1 \oplus Y_1 \,||\, X_2 \oplus Y_2 \dots X_n \oplus Y_n)$
$C' = (X_1' \oplus Y_1 \,||\, X_2' \oplus Y_2 \dots X_n' \oplus Y_n)$

when we do
$C \oplus C'$ we get,

$C \oplus C' = (X_1 \oplus X_1' \,||\, X_2 \oplus X_2' \dots X_n \oplus X_n')$
So it is easy to compute $X \oplus X'$ given C & C'.
if we use same key & IV.

Now, In CTR
if same key is used & CTR is reused here.
we have.



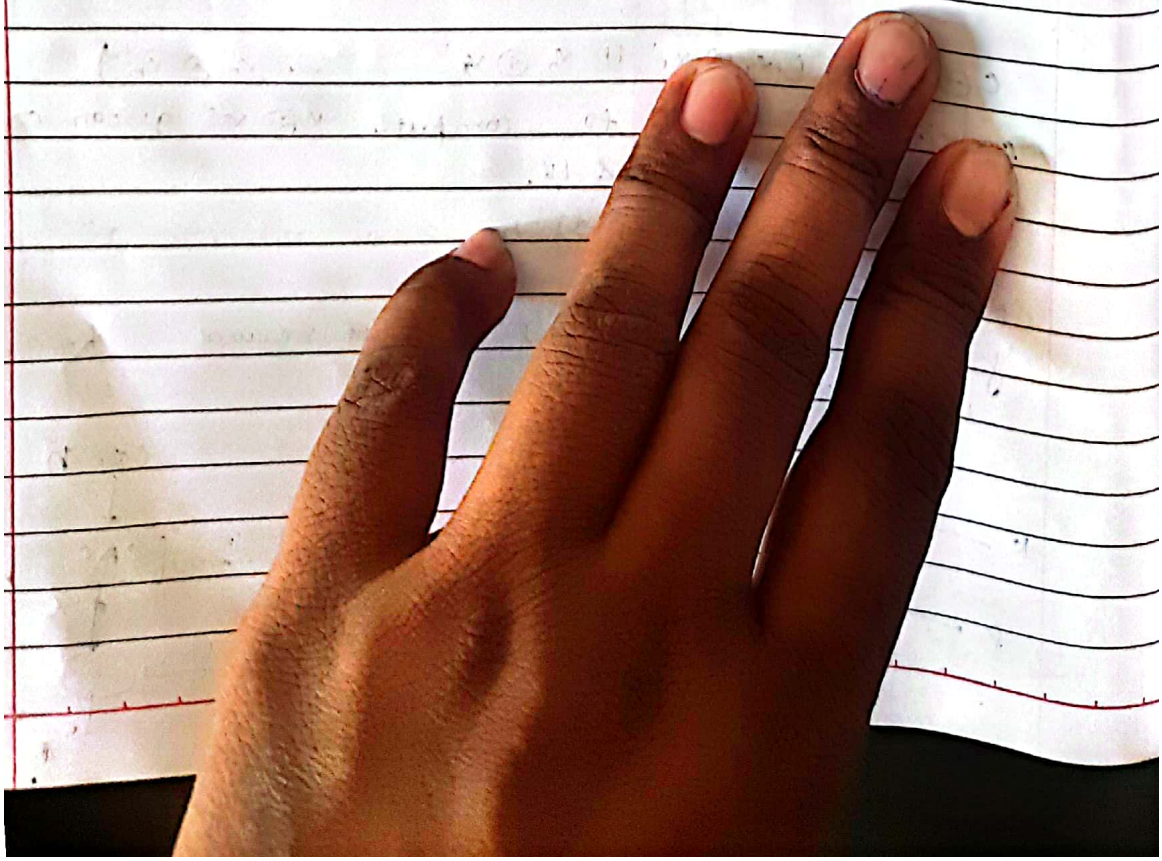
2021511192
Archit Verma

So here again our y_i will be same $\forall x_i, x_i'$ of ith

$$C = (x_1 \oplus y_1) \| (x_2 \oplus y_2) \cdots \| (x_n \oplus y_n).$$
$$C' = (x_1' \oplus y_1) \| (x_2' \oplus y_2) \cdots \| (x_n' \oplus y_n).$$

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

$$\boxed{C \oplus C' = x \oplus x'}$$

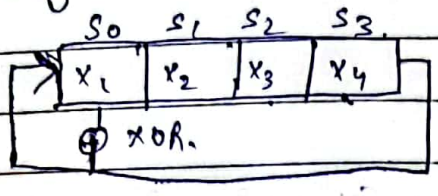


2021511192
Archit Verma

DOMS | Page No.
Date / /

Problem:- 4

a) The given connection polynomial is x^4+x+1



$L = S_0 \oplus S_3$.

So our linear feedback function is $S_0 \oplus S_3$.

We can initialize with any non-zero state.
Here to find period, first let's check if the polynomial is primitive or not. If it is so primitive then LFSR has 2^4-1 period.

We can check it by checking if we get all polynomial of degree less than 4 under modulo operation, we need to not we don't want 0 polynomial. by x^4+x+1. We will check for the period.

$x^0 = 1$
$x^1 = x$
$x^2 = x^2$
$x^3 = x^3$
$x^4 = x+1$
$x^5 = x^2+x$
$x^6 = x^3+x^2$
$x^7 = x^4+x^3 = x^3+x+1$
$x^8 = x^4+x^2+x = x^2+x+x+1 = x^2+1$
$x^9 = x^3+x$
$x^{10} = x^4+x^2 = x^2+x+1$
$x^{11} = x^3+x^2+x$
$x^{12} = x^4+x^3+x^2 = x^3+x^2+x+1$
$x^{13} = x^3+x^2+1$
$x^{14} = x^3+1$
$x^{15} = 1$
Stop 16 rounds

Now we can see that all polynomial except zero polynomial had been generated. So this is irreducible and primitive polynomial. So period is 2^4-1
$= 15$

2021151192
Archit Verma

(b) Connection polynomial
x^5+1
here for $x=1$
$x^5+1 = 1+1 = 0$
So $x+1$ is root of this.
So it is reducible
we can write $x^5+1 = (x+1)(x^4+x^3+x^2+x+1)$

Now the period of LFSR is LCM of both.

Here for $x+1$
$x+1$ is clearly a primitive polynomial.
so period here is
$P = 2^1 - 1 = 1$.

Let again do modulo operation until we get repeat for $x^4+x^3+x^2+x+1$

$x^0 = 1$
$x^1 = x$
$x^2 = x^2$
$x^3 = x^3$
$x^4 = x^3+x^2+x+1$
$x^5 = x^4+x^3x^2+x^2$
$= x^3+x^2+x+1+x^3+x^2+x$
$= 1$
Stop (Galois round)

So period here is 5

So Period of LFSR = LCM(5,1) = 5

2021511192
Archit Verma

DOMS | Page No.
Date / /

Question:- 5

Given

$\lambda : Z_{105} \to Z_3 \times Z_5 \times Z_7$ defined as

$\lambda(x) = (x \bmod 3, x \bmod 5, x \bmod 7)$.

find explicit formula for λ^{-1}.

Let,

$a_1 \in Z_3, a_2 \in Z_5, a_3 \in Z_7$

$\lambda(x) = (a_1, a_2, a_3)$.

Now we can write.

$x \equiv a_1 \bmod 3$

$x \equiv a_2 \bmod 5$

$x \equiv a_3 \bmod 7$

We know that CRT (Chinese remainder theorem) can be used to solve a set of different congruent eqn. We can use the same here.

We can write x as

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

Here $m_1 = 3$

$m_2 = 5$

$m_3 = 7$

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

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$ $\quad M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$

$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$

Now their multiplicative inverses are

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

2021511132
Archit Verma

Now

$X = (a_1 H_1 H^{-1} * a_2 H_2 H_2^{-1} * a_3 H_3 H_3^{-1}) \bmod M$

$X = (700_1 + 210_2 + 150_3) \bmod 105$

So $I^{-1}(2,2,3) = (70 \times 2 + 21 \times 2 + 15 \times 45) \bmod 105$

$= (140 + 42 + 45) \bmod 105$

$= 17$

$I^{-1}(2,2,3) = 17$

2021 [illegible]52
Archit Verma

DOMS Page No. Date / /

Question - 6

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

Again we will solve via CRT

$m_1 = 25$
$m_2 = 26$
$m_3 = 27$
} → relatively prime so we can pursue.

$M = 25 \times 26 \times 27$
$= 17550$

$M_1 = \frac{17550}{25} = 702$

$M_2 = \frac{17550}{26} = 675$

$M_3 = \frac{17550}{27} = 650$

Calculating $M_1^{-1}, M_2^{-1}, M_3^{-1}$

$M_1^{-1} = 13$
$M_2^{-1} = 25$
$M_3^{-1} = 14$

Now

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1})$
$= (12 \times 702 \times 13 + 9 \times 675 \times 25 + 23 \times 650 \times 14) \bmod 17550$

$= 470687 \bmod 17550$

$= \boxed{14387}$

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

$1 = 25 - 2 \times 12$
$1 = 25 - 2(702 - 25 \times 28)$
$1 = 337 \times 25 - 12 \times 702$

$M_1^{-1} = -12 = 13.$

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

$1 = 26 - 1 \times 25$
$1 = 26 - 1 \times (675 - 25 \times 26)$
$1 = 26 \times 26 - 675$

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

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

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

$M_3^{-1} = -13$
$= 14.$

2021511192
Archit Verma

Question:- 7

n = 18923
e = 1261
c = 6127

We know that
n = p x q where p & q are prime
So we need to factorize our n as product of two prime numbers.

Now we will try to find p & q.
let's find 1st prime number.

n%3 ≠ 0	n%29 ≠ 0	n%61 ≠ 0	n%97 ≠ 0
n%5 ≠ 0	n%31 ≠ 0	n%67 ≠ 0	n%103 ≠ 0
n%7 ≠ 0	n%37 ≠ 0	n%71 ≠ 0	n%107 ≠ 0
n%11 ≠ 0	n%41 ≠ 0	n%73 ≠ 0	n%109 ≠ 0
n%13 ≠ 0	n%43 ≠ 0	n%79 ≠ 0	n%113 ≠ 0
n%17 ≠ 0	n%47 ≠ 0	n%83 ≠ 0	n%127 = 0
n%19 ≠ 0	n%53 ≠ 0	n%89 ≠ 0	
n%23 ≠ 0	n%59 ≠ 0	n%69 ≠ 0	

So our first prime number is 127

another is

$\frac{18923}{127} = 149.$

Now calculate Euclid totient

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

2021F1192
Archit Verma

Now we know that

$e \cdot d \equiv 1 \bmod \phi(n)$

$1261 \overline{)18648} \; (14$
1261
6038
5044
$994 \overline{)1261} \; (1$
994
$267 \overline{)994} \; (3$
801
$193 \overline{)267} \; (1$
193
$74 \overline{)193} \; (2$
148
$45 \overline{)74} \; (1$
45
$29 \overline{)45} \; (1$
29
$16 \overline{)29} \; (1$
16
$13 \overline{)16} \; (1$
13
$3 \overline{)13} \; (4$
12
1

$1 = 13 - 4 \times 3$

$1 = 13 - 4 \times (16 - 13)$

$1 = 5 \times 13 - 4 \times 16$

$1 = 5(29 - 16) - 4 \times 16$

$1 = 5 \times 29 - 9 \times 16$

$1 = 5 \times 29 - 9 \times (45 - 29)$

$1 = 14 \times 29 - 9 \times 45$

$1 = 14 \times (74 - 45) - 9 \times 45$

$1 = 14 \times 74 - 23 \times 45$

$1 = 14 \times 74 - 23(193 - 2 \times 74)$

$1 = 60 \times 74 - 23 \times 193$

$1 = 60 \times (267 - 193) - 23 \times 193$

$1 = 60 \times 267 - 83 \times 193$

$1 = 60 \times 267 - 83 (994 - 3 \times 267)$

3754012g. 2502 72,400
1983.
2021571192 Archit Verma

$1 = 309 \times 267 - 83 \times 994$

$1 = 309 \times (1261 - 994) - 83 \times 994$

$1 = 309 \times 1261 - 392 (18648 - 14 \times 1261)$

$1 = 5797 \times 1261 - 392 \times 18648.$

So d i's 5797

Now

$x = c^d \bmod n.$

we can not directly compute c^d on pen paper. So we will use square and multiply method for this.

here

5797 can be written as sum of powers of 2.

$5797 = 4096 + 1024 + 512 + 128 + 32 + 4 + 1.$

$c = 6127$, $n = 18923.$

Now,

$c \bmod n = 6127$	$c^{128} \bmod n = 6041$
$c^2 \bmod n = 15820$	$c^{256} \bmod n = 10137$
$c^4 \bmod n = 15725$	$c^{512} \bmod n = 6879$
$c^8 \bmod n = 8784$	$c^{1024} \bmod n = 13141$
$c^{16} \bmod n = 9585$	$c^{2048} \bmod n = 13502$
$c^{32} \bmod n = 1060$	$c^{4096} \bmod n = 13239$
$c^{64} \bmod n = 7143$	

$x = c^d \bmod n$

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

$= 5746 =$ plain text

2021111382
Archit Verma

DOMS Page No.
Date / /

Question- 8 :-

Given elliptical curve :-

$y^2 = x^3 + 5x + 3$

$a = 5$

$b = 3.$

We need to find all points on curve in Z_{13}.

x and y needs to be integers. So.

y^2 can have following value.

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

Now we will look into eqn $y^2 = x^3 + 5x + 3$. Then we will look is it possible value of y^2 and then we will make all possible pairs.

2021511192
Archit Verma

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

So all the possible point 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), (12,1), (12,7)

2021571132
Archit Verma

Question:-9

The SPN encryption from ex. 4.1 in Stinson's book is used but the S-Box π_S is replaced by a function π_T that is not a permutation.
This mean π_T is not surjective, i.e. there are some output that cannot be achieved from any input.
The attacker will exploit the fact that the last round of SPN encryption involves the non-surjective function π_T. Since it is surjective so some output values can never be reached so

The cipher-only attack proceeds as follows:-

1) Collect a large number of plaintext that have been encrypted with same key.
2) Observe cipher values
3) As it is surjective so some values are never present, look for those impossible value. Analysing those values can give information about the key bits used in last round of SPN.

Let's formalize the attack mathematically

Let's denote non-surjective s-box used as

$$\pi_T : \{0,1\}^n \rightarrow \{0,1\}^n$$

Let C is the set of all observed ciphertext that have been encrypted using same key.
We define set of all impossible values π_T as

$$I = \{ y \in \{0,1\}^N \forall\ c \in C, c \neq y \}$$

Since π_T is not surjective I is not empty.

2021511192
Archit Verma

Let
$k \in \{0,1\}^N$ be the round key used in last round SPN.

$c = \pi T(x \oplus k)$ x = input into last round.

for any $y \in I$ we know that
$\forall x \in \{0,1\}^N$, $\pi T(x \oplus k) \neq y$

So we can draw a constraint on key k for $y \in I$.

$k \notin \{ x \mid \pi T(x) = y \}$.
Toying this for different keys for all $y \in I$ we can reduce our key space and hence can find our key.

2-021911 92
Archit Verma

DOMS | Page No.
Date 1 1

Question:- 10:

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

Let us take two inputs (x_1, y_1) and (x_2, y_2) hash function.

$h(x_1, y_1) = h_1$ — ①

$h(x_2, y_2) = h_2$ — ②

Now we are give definition of hash function. Using that we had:-

$h_1 = h(x_1, y_1) = (ax_1 + by_1) \bmod n$

$h_2 = h(x_2, y_2) = (ax_2 + by_2) \bmod n$.

We need to prove if we know hash value corresponding to two input then we can determine the hash value without need to calculate hash of these two.

There can be one way if we for this if we can represent that as combined linear combination of these two. Let check our hash function for a linear function.

Let do for (kx_1, ky_1)

$h(kx_1, ky_1) = (akx_1, aky_1) \bmod n$

$= k(ax_1, by_1) \bmod n$

$= kh_1 \bmod n$.

So in simple multiplication we can easily find it.

Let check for a linear combination.

2021511152

Archit Varma

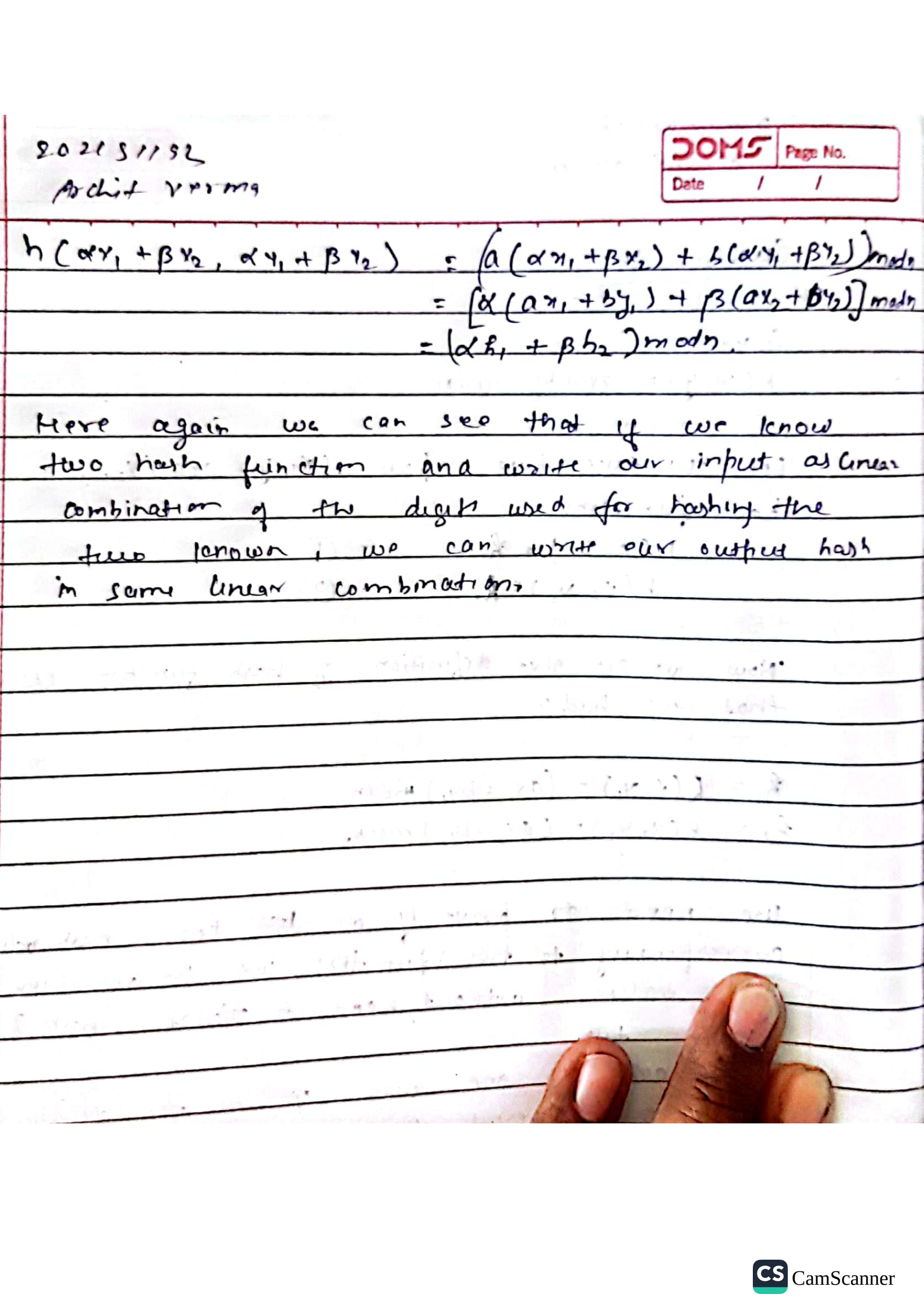
DOMS | Page No. | Date / /

$h(\alpha x_1 + \beta x_2, \alpha y_1 + \beta y_2) = [a(\alpha x_1 + \beta x_2) + b(\alpha y_1 + \beta y_2)] \bmod n$

$= [\alpha(ax_1 + by_1) + \beta(ax_2 + by_2)] \bmod n$

$= (\alpha h_1 + \beta h_2) \bmod n.$

Here again we can see that if we know two hash function and write our input as linear combination of the digit used for hashing the two known, we can write our output hash in some linear combination.



2021511192
Archit Verma

Question: 11

p :- a prime number
$(a,b) \in Z_p$
$f_{(a,b)} : Z_p \to Z_p$.
$f_{(a,b)} = (ax+b) \bmod p$.

Now given
$f_{(a,b)}(x) = y$
& $f_{(a,b)}(x') = y'$ where $y' \neq x$
we need to find if we can determine (a,b) or not

$f_{(a,b)}(x) = y \Rightarrow (ax+b) \bmod p = y$. — ①
$f_{(a,b)}(x') = y' \Rightarrow (ax'+b) \bmod p = y'$. — ②.

or $ax+b \equiv y \bmod p$ — ①
$ax'+b \equiv y' \bmod p$. — ②

from ① & ②.

$a(x'-x) \equiv (y'-y) \bmod p$. — ③

we know x', x, y', y and p so we can easily find our a from here.

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

now once a is found we can use eq^n ① or ② to find b as.

$b \equiv (y - ax) \bmod p$.

So it is possible to find, a & $b \in Z_p$ given x, x', y & y'.